

**ON FACTORIZATION OF SOME PERMUTATION POLYNOMIALS  
OVER FINITE FIELDS**

by  
**TEKGÜL KALAYCI**

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


Sabancı University

January 2019

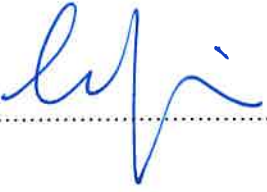
ON FACTORIZATION OF SOME PERMUTATION POLYNOMIALS OVER  
FINITE FIELDS

APPROVED BY

Prof. Dr. Alev Topuzođlu  
(Thesis Supervisor)



Prof. Dr. Cem Güneri



Prof. Dr. Erkay Savaş



Prof. Dr. Ayşe Berkman



Assoc. Prof. Dr. Wilfried Meidl



DATE OF APPROVAL: 20/12/2018

©Tekgöl Kalaycı 2019

All Rights Reserved

ON FACTORIZATION OF SOME PERMUTATION POLYNOMIALS OVER  
FINITE FIELDS

Tekgöl Kalaycı

Mathematics, PhD Thesis, January 2019

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: finite fields, permutation polynomials, factorization of polynomials,  
irreducible polynomials

**Abstract**

Factorization of polynomials over finite fields is a classical problem, going back to the 19th century. However, factorization of an important class, namely, of permutation polynomials was not studied previously. In this thesis we present results on factorization of permutation polynomials of  $\mathbb{F}_q$ ,  $q \geq 2$ .

In order to tackle this problem, we consider permutation polynomials  $F_n(x) \in \mathbb{F}_q[x]$ ,  $n \geq 0$ , which are defined recursively as compositions of monomials of degree  $d$  with  $\gcd(d, q - 1) = 1$ , and linear polynomials. Extensions of  $\mathbb{F}_q$  defined by using the recursive structure of  $F_n(x)$  satisfy particular properties that enable us to employ techniques from Galois theory. In consequence, we obtain a variety of results on degrees and number of irreducible factors of the polynomials  $F_n(x)$ .

# SONLU CİSİMLER ÜZERİNDEKİ BAZI PERMÜTASYON POLİNOMLARININ ÇARPANLARA AYRILMASI ÜZERİNE

Tekgöl Kalaycı

Matematik, Doktora Tezi, Ocak 2019

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Anahtar Kelimeler: sonlu cisimler, permütasyon polinomları, polinomların çarpanlara ayrılması, indirgenemez polinomlar

## Özet

Sonlu cisimler üzerindeki polinomların çarpanlara ayrılması, 19. yüzyıla kadar uzanan klasik bir problemdir. Buna rağmen, önemli bir sınıfın; permütasyon polinomlarının çarpanlara ayrılması daha önce çalışılmamıştı. Bu tezde  $\mathbb{F}_q$ ,  $q \geq 2$  sonlu cisimleri üzerindeki permütasyon polinomlarının çarpanları hakkında elde ettiğimiz sonuçlar sunulmaktadır.

Bu problemi çözebilmek için, özyineli biçimde tanımlanan  $F_n \in \mathbb{F}_q[x]$ ,  $n \geq 0$ , permütasyon polinomlarını ele aldık ki, bu polinomlar, dereceleri  $d_1, \dots, d_n$  olan ve  $\text{ebob}(d_i, q-1) = 1$ ,  $1 \leq i \leq n$  şartını sağlayan bir terimliler ve doğrusal polinomların bileşkesiyle oluşmaktadır. Bu permütasyon polinomlarının özyineli yapısını kullanarak tanımladığımız  $\mathbb{F}_q$  cisminin genişlemelerinin sahip olduğu bazı özellikler Galois teorisinden teknikleri kullanmamızı mümkün kılmıştır. Bu sayede  $F_n(x)$  polinomlarının indirgenemez çarpanlarının dereceleri ve sayısı hakkında pek çok sonuç elde edebildik.

*To my family*

## Acknowledgements

First of all, I would like to express my sincere and deepest gratitude to my thesis advisor Prof. Alev Topuzođlu for her motivation, guidance, encouragement and extensive knowledge. Her contributions to my academic experience and my personality have been enormous. I would like to extend my sincere thanks to Prof. Henning Stichtenoth for his guidance, patience and important contributions to my study. I also have learned a lot from his lectures. I am really honored and consider myself more than lucky to work with both Prof. Alev Topuzođlu and Prof. Henning Stichtenoth.

I would like to thank my jury members Prof. Ayşe Berkman, Prof. Cem Güneri, Assoc. Prof. Wilfried Meidl and Prof. ErKay Savař for reviewing my Ph.D. thesis and their valuable comments. I would also like to thank Dr. Giorgos Kapetanakis for his useful remarks on this work.

I would like to thank each member of the Mathematics Program of Sabancı University for providing a warm atmosphere, which always made me feel at home. I would especially like to thank my dear friends Gülizar Günay Mert, Nurdan Kuru, Tuđba Yesin, Melike Efe and Halime Ömriuzun Seyrek for their invaluable friendship and continuous support.

My most special thanks go to Neslihan Girgin, who has been more than a friend, a sister to me for the last twelve years. Her continual understanding and encouragement helped me immensely to complete this work.

Last but not least, I am deeply grateful to my family, who continuously supported me throughout my life under any circumstances. I feel their endless love, patience, and understanding in every second of my life.

## Table of Contents

<b>Abstract</b>	<b>iv</b>
<b>Özet</b>	<b>v</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Factorization of polynomials over finite fields . . . . .	1
1.2 Permutation polynomials . . . . .	5
1.3 Overview . . . . .	8
1.4 Preliminaries . . . . .	9
<b>2 Factorization of a class of permutation polynomials</b>	<b>13</b>
2.1 Degrees of irreducible factors of $F_n(x)$ . . . . .	13
2.2 The relation between the sets $\Delta_n^{(D)}$ and $\Delta_n^{(A,D)}$ . . . . .	15
2.3 Elimination of some degrees . . . . .	25
2.4 More on the set $\Delta_n^{(A,D)}$ . . . . .	31
<b>3 Consecutive permutation polynomial sequences</b>	<b>46</b>
3.1 Consecutive polynomial sequences . . . . .	46
3.2 Consecutive permutation polynomial sequences . . . . .	48
<b>Bibliography</b>	<b>60</b>



## CHAPTER 1

### Introduction

## 1.1 Factorization of polynomials over finite fields

Throughout this thesis  $\mathbb{F}_q$  denotes a finite field of characteristic  $p$ , hence  $q = p^r$ ,  $r \geq 1$ . Factorization of polynomials over  $\mathbb{F}_q$  is a classical problem. In coding theory, cryptography or number theory, there are plenty of problems solutions of which depend in one way or another on the factorization of  $f(x) \in \mathbb{F}_q[x]$ . For instance, in coding theory, a linear code  $\mathcal{C}$  of length  $n$  is cyclic if and only if its generator polynomial divides  $x^n - 1$ , i.e., cyclic codes are determined by factors of  $x^n - 1$ .

Efficient algorithms for factorization are obtained, due to the algebraic structure of  $\mathbb{F}_q[x]$ . First factorization algorithms are due to Berlekamp [11], [12]. Some well-known improvements of Berlekamp's algorithms can be found in Cantor and Zassenhaus [17], Kaltofen and Shoup [52], von zur Gathen and Shoup [50].

It is difficult to find criteria for the irreducibility of arbitrary polynomials, however there are well-known criteria for polynomials of particular types, for instance those of small weight. The following theorem, which is proven by Serret [81] for finite prime fields, characterizes irreducible binomials over  $\mathbb{F}_q$ .

**Theorem 1.1.1** [53] *Let  $2 \leq n$  be an integer,  $a \in \mathbb{F}_q^*$ ,  $t$  be the order of  $a$  in the group  $\mathbb{F}_q^*$ . Then the binomial  $x^n - a$  is irreducible if and only if the following are satisfied.*

- (i) *Each prime factor of  $n$  divides  $t$ , but does not divide  $(q - 1)/t$ ,*
- (ii) *if  $n \equiv 0 \pmod{4}$ , then  $q \equiv 1 \pmod{4}$ .*

Serret [81] also gave the explicit factorization of particular binomials  $x^n - a \in \mathbb{F}_q[x]$ . Dickson [31] considered the factorization of  $x^n - a \in \mathbb{F}_q[x]$  with  $n = q - 1$ , see also Agou [3]. Beard and West [10] and McEliece [65] tabulate factorizations of the binomials  $x^n - 1$ . More recent results on the explicit factorization of  $x^n - 1$  can be found in Blake, Gao and Mullin [14], Chen, Tuerhong [22], Martinez, Vergara, Oliveria [62] and Wu, Yue and Fan [92]. As an example, we state the following result.

**Theorem 1.1.2** [62] *Let  $n$  be a positive integer satisfying*

(i)  $q \not\equiv 3 \pmod{4}$  or  $8 \nmid n$ ,

(ii)  $\text{rad}(n) \mid (q - 1)$ , where  $\text{rad}(n)$  denotes the product of prime divisors of  $n$ ,

and set  $m = \frac{n}{\gcd(n, q-1)}$  and  $l = \frac{q-1}{\gcd(q-1, n)}$ . Then

$$x^n - 1 = \prod_{t \mid m} \prod_{\substack{1 \leq u \leq \gcd(n, q-1) \\ \gcd(u, t)=1}} (x^t - \xi^{ul})$$

is the factorization of  $x^n - 1$  into irreducible factors of  $\mathbb{F}_q[x]$ , where  $\langle \xi \rangle = \mathbb{F}_q^*$ .

The number of irreducible factors of a given binomial is also studied. Rédei [74] gives a short proof for the following formula of Schwarz [79], see also Agou [2], Butler [16], Schwarz [78].

**Theorem 1.1.3** [79] *Let  $x^n - a \in \mathbb{F}_q[x]$ ,  $a \in \mathbb{F}_q^*$ ,  $1 \leq s \leq n$ ,  $d_s = \gcd(n, p^s - 1)$  and*

$$\gamma_s = \begin{cases} d_s & \text{if } p \mid a^{\frac{p^s-1}{d_s}} - 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then the number of irreducible factors of  $x^n - a$  of degree  $m$  is

$$\frac{1}{m} \sum_{s \mid m} \mu\left(\frac{m}{s}\right) \gamma_s,$$

where the sum runs over all  $s \mid m$ , and  $\mu$  denotes the Möbius function.

Recently, Heyman and Shparlinski [43], considered various counting questions for irreducible binomials of the form  $x^n - a \in \mathbb{F}_q[x]$ . For instance, the following theorem gives an upper bound for the number of such irreducible binomials for a fixed  $q$  averaged over  $n \leq N$ .

**Theorem 1.1.4** [43] *Let  $I_n(q)$  be the number of monic irreducible binomials of the form  $x^n - a \in \mathbb{F}_q[x]$ . For any fixed positive  $B, \epsilon$ , a sufficiently large  $q$  and real  $N$  with*

$$N \geq (\log(q-1))^{(1+\epsilon)B \log_3(q)/\log_4(q)},$$

*one has*

$$\sum_{n \leq N} I_n(q) \leq \frac{(q-1)N}{(\log N)^B}.$$

Irreducibility criterion for the trinomial  $x^p - x - a \in \mathbb{F}_q[x]$  was first given by Pellet [70]. Irreducibility of  $x^p - x - a \in F_p[x]$  was already studied by Serret [80], [81]. A decomposition of  $x^q - x - a \in \mathbb{F}_q[x]$ , where  $a$  is an element of a subfield of  $\mathbb{F}_q$ , in terms of trinomials in  $\mathbb{F}_q$  was given by Dickson [32].

The factorizations of various compositions of the form  $f(g(x))$  are also considered. Varshamov [86], [87] gave a criterion for the irreducibility of the composition  $f(x^p - x - b)$ , where  $f \in \mathbb{F}_q[x]$  is irreducible and  $b \in \mathbb{F}_q$ . Factorizations of  $f(x^{p^r} - ax)$ ,  $f(x^{p^{2r}} - ax^{p^r} - bx)$  and many others for an irreducible polynomial  $f \in \mathbb{F}_q[x]$  are studied, see for instance, Agou [3], [4], Long [55], Long and Vaughan [57], [58], and Ore [68]. Factorization of polynomials of the form  $f(x^n)$ , with  $f \in \mathbb{F}_q[x]$  irreducible, is considered in Agou [2], Butler [16], Pellet [70]. Recently, Martinez and Reis [61] proved the following.

**Theorem 1.1.5** [61] *Let  $f(x)$  be an irreducible polynomial of degree  $m$ . If  $g(x)$  is any monic irreducible factor of  $f(x^n)$  and  $a \in \mathbb{F}_q^*$  has order  $n$ , then*

$$f(x^n) = \prod_{i=0}^{n-1} [a^{-mi} g(a^i x)]$$

*is the factorization of  $f(x^n)$  into irreducible factors.*

Factors of polynomials  $f(L(x))$ , where  $f$  is irreducible and  $L$  is a linearized polynomial, are studied by Agou [4], Long [55], [56], Long and Vaughan [57], [58]. Analogous problems for the multivariate case are considered in Carlitz and Long [20], and Long [59].

Williams [89] gave a factorization of Dickson polynomials. More recent results in this direction are obtained, for instance, by Chou [23], Fitzgerald and Yucas [38], [39], [40]. In [39], Fitzgerald and Yucas show that irreducible factors of Dickson polynomials can be obtained from particular cyclotomic polynomials, see Tosun [84] for

a generalization. There are also numerous results on explicit factorization of cyclotomic polynomials, for example, see Meyn [64], Tuxanidy and Wang [85], Wang and Wang [88], Wu et al. [91]. In the following theorem of Tuxanidy and Wang [85],  $Q_n$  denotes the  $n$ -th cyclotomic polynomial over  $\mathbb{F}_q$ , for  $n \in \mathbb{Z}^+$ .

**Theorem 1.1.6** [85] *Let  $m, n \in \mathbb{N}$ ,  $\gcd(m, n) = \gcd(\phi(m), s) = 1$ , where  $\phi$  denotes the Euler's totient function and  $s$  denotes the multiplicative order of  $q$  modulo  $n$ . If  $Q_n = \prod_{j=1}^{\phi(n)/s} g_j$  is the factorization of  $Q_n(x)$  over  $\mathbb{F}_q$ , then*

$$Q_{mn}(x) = \prod_{j=1}^{\phi(n)/s} \left( \prod_{k \mid m} G_{j,k} (x^k)^{\mu(m/k)} \right)$$

*is the factorization of  $Q_{mn}$  over  $\mathbb{F}_q$ , where  $G_{j,k}$  is the minimal polynomial of  $\lambda_{n,j}^k$  with  $g(\lambda_{n,j}) = 0$ .*

The problems concerning factorization pattern of a given polynomial also have received a lot of attention. Cohen [26], [27] considers the distribution of various factorization patterns among polynomials of the form  $f(x) + ag(x)$ , when  $f, g \in \mathbb{F}_q[x]$  are given and  $a \in \mathbb{F}_q$ . In Cohen [28], the distribution of factorization patterns in residue classes modulo a given polynomial or in sets of polynomials of fixed degree with preassigned coefficients are studied. An asymptotic formula for the number of polynomials of fixed degree  $d$  over  $\mathbb{F}_q$  having exactly  $s$  irreducible factors of degree  $e$  is given by Williams [90]. Car [18] and Cohen [25] obtain asymptotic formulas for the number of monic polynomials over  $\mathbb{F}_q$  of fixed degree with a certain factorization pattern. Gogia and Luthar [41] considered the same problem for the case where the degree is bounded by a positive integer. Gómez-Pérez, Ostafe and Shparlinski [34] give a lower bound for the largest degree of an irreducible factor, and an estimate on the number of irreducible factors of iterates of a polynomial  $f(x) \in \mathbb{F}_q[x]$ . Reis [76] studies polynomials of the form  $f(g^{(n)}(x))$ , where  $f, g$  are of degree at least 1 and  $g^{(n)}(x)$  denotes the  $n$ -th iterate of the polynomial  $g(x)$ . He obtains some improvements of the results in [34]. Recently in Reis [75], degree distribution of  $f(L(x))$  is given, where  $f$  is irreducible and  $L$  is linearized.

As a problem related to factorization, there has been an active interest in finding roots of polynomials over finite fields. Berlekamp [12] suggested a method to find roots

of polynomials when  $q$  is large. A root finding algorithm based on the consideration of affine multiples was developed by Berlakamp, Rumsey and Solomon [13]. Rabin [73] suggested a different method for the same problem; see also Cantor and Zassenhaus [17]. In Mann [60], the roots of  $f$  are given in terms of roots of unity over  $\mathbb{F}_q$  and polynomials in the coefficients of  $f$ , where  $f$  is irreducible and of degree not divisible by  $p$ . If  $f$  has roots in  $\mathbb{F}_q$ , Prešić [71] gave an expression of these roots depending on a primitive element of  $\mathbb{F}_q$ . Feit and Rees [37] obtained conditions for a polynomial over  $\mathbb{F}_q$  to split in  $\mathbb{F}_q$ , Šatunovskii and many others studied the same problem for the case of prime cardinality.

Further information about the algorithms and results concerning factorization of polynomials over  $\mathbb{F}_q$  can be found in Lidl and Niederreiter [53, Chapter 4], Mullen and Panario [66, Chapter 11], Shparlinski [82, Chapter 1] and references therein.

## 1.2 Permutation polynomials

A polynomial  $f \in \mathbb{F}_q[x]$  is called a *permutation polynomial* if it induces a bijection from  $\mathbb{F}_q$  to  $\mathbb{F}_q$ . Permutation polynomials have been of great interest over the last decades, due to their applications in coding theory, cryptography and combinatorics.

Permutation polynomials of finite fields of  $\mathbb{F}_p$  were first studied by Hermite [42]. The consideration of permutation polynomials of  $\mathbb{F}_q$  is due to Dickson [33]. It was first noted by Hermite [42] that any function  $\psi$  from  $\mathbb{F}_p$  into  $\mathbb{F}_p$  can be represented by a polynomial. Dickson [33] observed that the same holds for  $\mathbb{F}_q$ , and if the representing polynomial  $f$  satisfies  $\deg f < q$ , then  $f$  is the unique such polynomial. Carlitz [19], Dickson [33] and Zsigmondy [93] pointed out that  $f$  can be obtained from an interpolation formula as follows.

**Theorem 1.2.1 (Lagrange Interpolation Formula)** *For  $n \geq 0$ , let  $a_0, \dots, a_n$  be  $n + 1$  distinct elements of  $\mathbb{F}_q$ , and let  $b_0, \dots, b_n$  be  $n + 1$  arbitrary elements of  $\mathbb{F}_q$ . Then there exists a unique  $f \in \mathbb{F}_q[x]$ ,  $\deg f(x) \leq n$  such that  $f(a_i) = b_i$ , for  $i = 0, \dots, n$ . This polynomial is given by*

$$f(x) = \sum_{i=0}^n b_i \prod_{\substack{k=0 \\ k \neq i}}^n (a_i - a_k)^{-1} (x - a_k).$$

If  $\psi : \mathbb{F}_q \mapsto \mathbb{F}_q$  is already given as a polynomial function, say  $\psi : c \mapsto g(c)$  with  $g \in \mathbb{F}_q[x]$ , then  $f$  can be obtained from  $g$  by reduction modulo  $x^q - x$ , due to the following result.

**Lemma 1.2.2** *Let  $f, g \in \mathbb{F}_q[x]$ . The equality  $f(c) = g(c)$  holds for all  $c \in \mathbb{F}_q$  if and only if  $f(x) \equiv g(x) \pmod{x^q - x}$ .*

A criterion for  $f(x) \in \mathbb{F}_p[x]$  to be a permutation polynomial of  $\mathbb{F}_p$  was given by Hermite [42]. This result is generalized to polynomials in  $\mathbb{F}_q[x]$  by Dickson [33].

**Theorem 1.2.3 (Hermite's Criterion)** *A polynomial  $f \in \mathbb{F}_q[x]$  is a permutation polynomial of  $\mathbb{F}_q$  if and only if the following conditions are satisfied.*

- (i)  $f$  has exactly one root in  $\mathbb{F}_q$ ,
- (ii) for each integer  $t$  with  $1 \leq t \leq q-2$  and  $p \nmid t$ , the reduction of  $f(x)^t \pmod{x^q - x}$  has degree  $\leq q-2$ .

Some well-known examples of permutation polynomials are given in the following lemma.

**Lemma 1.2.4** (i) *Every linear polynomial over  $\mathbb{F}_q$  is a permutation polynomial of  $\mathbb{F}_q$ .*

(ii) *The monomial  $x^d$  is a permutation polynomial of  $\mathbb{F}_q$  if and only if  $\gcd(d, q-1) = 1$ .*

(iii) *The  $p$ -polynomial*

$$L(x) = \sum_{i=0}^m a_i x^{p^i} \in \mathbb{F}_q[x]$$

*is a permutation polynomial of  $\mathbb{F}_q$  if and only if  $L(x)$  only has the root 0 in  $\mathbb{F}_q$ .*

(iv) *The Dickson polynomial*

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

*where  $a \in \mathbb{F}_q^*$ , is a permutation polynomial of  $\mathbb{F}_q$  if and only if  $\gcd(k, q^2 - 1) = 1$ .*

The following variation of Hermite's criterion in terms of combinatorial identities is obtained in 2006 by Masuda, Panario and Wang [63].

**Theorem 1.2.5** [63] Let  $f(x) = a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0 \in \mathbb{F}_q[x]$ ,  $\deg(f) = m < q - 1$ , and  $S_N = \{(A_1, A_2, \dots, A_m) \in \mathbb{Z}^m : A_1 + A_2 + \dots + A_m = N, A_1 + 2 \cdot A_2 + \dots + m \cdot A_m \equiv 0 \pmod{q-1}, A_i \geq 0 \text{ for all } i, 1 \leq i \leq m, \text{ and } A_i = 0 \text{ whenever } a_i = 0\}$ . Then the following statements are equivalent.

(i)  $f(x)$  is a permutation polynomial of  $\mathbb{F}_q$ .

(ii)

$$\sum_{A_1, \dots, A_m \in S_N} \frac{N!}{A_1! \cdot A_2! \cdot \dots \cdot A_m!} a_1^{A_1} \cdot a_2^{A_2} \cdot \dots \cdot a_m^{A_m} = \begin{cases} 0, & \text{if } N = 1, 2, \dots, (q-2), \\ 1, & \text{if } N = q-1. \end{cases}$$

Permutation polynomials of various forms are studied by Akbary and Wang [5], Charpin and Kyureghyan [21], Hou [44], [46], [45] and many other researchers, see Hou [47] for a detailed survey.

For  $q \geq 2$ , permutation polynomials over  $\mathbb{F}_q$  form a group under composition and subsequent reduction modulo  $x^q - x$ , which is isomorphic to  $S_q$ . The following theorem of Carlitz [19] gives a set of generators for this group.

**Theorem 1.2.6** [19] If  $q > 2$  is a prime power, then every permutation of  $\mathbb{F}_q$  is the composition of permutations induced by  $x^{q-2}$  and by linear polynomials over  $\mathbb{F}_q$ .

Therefore, by this theorem of Carlitz, if  $F(x)$  is a permutation polynomial over  $\mathbb{F}_q$ , then there exists an integer  $n \geq 0$  and  $A = (a, a_0, \dots, a_n) \in \mathbb{F}_q^{n+2}$ , where  $a_0, a_{n+1} \in \mathbb{F}_q$ ,  $a, a_1, \dots, a_n \in \mathbb{F}_q^*$ , satisfying

$$F(x) = F^{(A)}(x) = (\dots ((ax + a_0)^{q-2} + a_1)^{q-2} + \dots + a_{n-1})^{q-2} + a_n, \quad (1.1)$$

see Çeşmelioglu, Meidl, Topuzoglu [30]. The representation in (1.1) is not unique and  $n$  is not necessarily minimal. In Aksoy et al. [6], the Carlitz rank of  $F$  is defined to be the smallest integer  $n \geq 0$  satisfying  $F(x) = F^{(A)}(x)$  for some  $A \in \mathbb{F}_q^{n+2}$ . Various problems concerning Carlitz rank and its applications are studied, see, for instance Aksoy et al. [6], Anbar et al. [7], [8], Gómez-Pérez, Ostafe, Topuzoglu [35], Işik, Topuzoglu, Winterhof, [48], Işik, Winterhof [49], Pausinger, Topuzoglu [69] and Topuzoglu [83].

The cycle structure of various types of permutation polynomials is studied; see Ahmad [1] for monomials, Lidl and Mullen [54] for Dickson permutation polynomials, and Çeşmelioglu, Meidl, Topuzoğlu [30] for polynomials of the form (1.1).

We refer to Lidl, Niederreiter [53, Chapter 7], Mullen, Panario [66, Chapter 8], and Shparlinski [82, Chapter 8] for a large variety of further results about permutation polynomials, and their applications.

### 1.3 Overview

Although factorization of polynomials over  $\mathbb{F}_q$  is a classical problem, factorization of permutation polynomials has not been studied so far. In this thesis, we are concerned with factorization of a class of recursively defined permutation polynomials, as defined below.

Let  $n \geq 1$ ,  $a \in \mathbb{F}_q^*$ ,  $a_0, a_1, \dots, a_n \in \mathbb{F}_q$ ,  $d_1, \dots, d_n$  be integers satisfying

$$d_i \geq 2 \text{ and } \gcd(d_i, q - 1) = 1 \text{ for } 1 \leq i \leq n, \quad (1.2)$$

and  $d = \text{lcm}(d_1, \dots, d_n)$ , the least common multiple of  $d_1, \dots, d_n$ . We set

$$F_0(x) := ax + a_0 \text{ and } F_i(x) := F_{i-1}(x)^{d_i} + a_i \quad (1.3)$$

for  $1 \leq i \leq n$ . By Lemma 1.2.4,  $F_i(x)$  are permutation polynomials for  $0 \leq j \leq n$ . Moreover, by Theorem 1.2.6, it is known that every permutation of  $\mathbb{F}_q$  can be represented as polynomials of the form (1.3). The definition of the polynomials  $F_n$  enables us to use techniques from Galois Theory.

We present our results on the degrees of the irreducible factors of  $F_n(x)$  in Chapter 2, where we assume  $a = 1$  in (1.3), since the value of  $a$  does not effect the degree of an irreducible factor of  $F_n(x)$ . We also assume that

$$\gcd(d_i, q) = 1 \text{ for } 1 \leq i \leq n \quad (1.4)$$

because if  $d_i = p^k \cdot e_i$  for some  $1 \leq i \leq n$ , then it is possible to write  $F_n(x) = H_n(x)^{p^k}$ , where  $H_n(x)$  is of the form (1.3).

The first two results in Section 2.1 together, yield the set of possible degrees of the irreducible factors of  $F_n(x)$ . Naturally, degrees of the irreducible factors of  $F_n(x)$



depend on the coefficients  $a_i$  in (1.3), for  $1 \leq i \leq n$ . Consequently, we introduce the following notation.

Let  $A = (a_0, a_1, \dots, a_n) \in \mathbb{F}_q^{n+1}$ ,  $D = (d_1, \dots, d_n) \in \mathbb{Z}_+^n$  such that  $d_1, \dots, d_n$  satisfy (1.3) and (1.4). We put  $F_i^{(A,D)} := F_i(x)$ , for  $0 \leq i \leq n$ .

We define the set  $\Delta_n^{(D)}$  to be the set of possible degrees of the irreducible factors of  $F_n^{(A,D)}(x)$ , for an arbitrary  $A \in \mathbb{F}_q^{n+1}$ . Similarly,  $\Delta_n^{(A,D)}$  denotes the set of the degrees of the actual irreducible factors of  $F_n^{(A,D)}(x)$ . In Section 2.2, we investigate the relation between the sets  $\Delta_n^{(D)}$  and  $\Delta_n^{(A,D)}$ . More precisely, we first observe that for fixed  $q$  and  $D$ , there may not exist any  $A \in \mathbb{F}_q^{n+1}$  such that  $\Delta_n^{(A,D)} = \Delta_n^{(D)}$ . Afterwards, we give a necessary condition on  $D$  and  $q$ , for the existence of  $A \in \mathbb{F}_q^{n+1}$ , satisfying  $\Delta_n^{(A,D)} = \Delta_n^{(D)}$ . It is also shown that this condition is not sufficient.

When  $\Delta_n^{(A,D)} \subsetneq \Delta_n^{(D)}$  for some  $q$  and  $D$  and for all  $A \in \mathbb{F}_q^{n+1}$  we may try to eliminate some elements of  $\Delta_n^{(D)}$ , which are not in  $\Delta_n^{(A,D)}$  for any  $A$ . In Section 2.3, we give some results in this direction, i.e., on the elimination of certain elements of  $\Delta_n^{(D)}$ , under some conditions. Furthermore, using the procedure of proofs of these results, we obtain an algorithm to eliminate a subset of  $\Delta_n^{(D)}$ , when  $D$  and  $q$  are fixed. Section 2.4 consists of some existence results, i.e., we show that some  $m \in \Delta_n^{(D)}$  are necessarily in  $\Delta_n^{(A,D)}$ .

In Chapter 3, we define consecutive permutation polynomial sequences  $\{F_n^{(A,D)}\}_{n \geq 0}$  associated to the sequences  $A = \{a_n\}_{n \geq 0}$  and  $D = \{d_n\}_{n \geq 1}$ , where  $a_n \in \mathbb{F}_q^*$  and  $d_n \in \mathbb{Z}^+$  satisfy (1.2) and (1.4), in such a way that the  $n$ -th term of the sequence equals  $F_n^{(A,D)}(x)$ , where  $F_n^{(A,D)}(x)$  is defined as in Chapter 2. This definition is motivated by the definition of consecutive polynomial sequences given by Gómez-Pérez, Ostafe and Sha in [36]. The authors of [36] studied various questions concerning factorization of consecutive polynomial sequences, including the largest degree of irreducible factors and the number of irreducible factors. We consider similar problems for consecutive permutation polynomial sequences in Chapter 3.

## 1.4 Preliminaries

Here, we list well - known results from the theory of finite fields that we use in the next chapter.

Let  $d$  be a positive integer such that  $\gcd(p, d) = 1$ , and  $\zeta$  be a primitive  $d$ -th root

of unity over  $\mathbb{F}_q$ . Then the polynomial

$$Q_d(x) = \prod_{\substack{s=1 \\ \gcd(d,s)=1}}^d (x - \zeta^s) \quad (1.5)$$

is called the  $d$ -th cyclotomic polynomial over  $\mathbb{F}_q$ .

**Lemma 1.4.1** (i) Suppose  $\gcd(p, n) = 1$ . Then  $x^n - 1 = \prod_{d | n} Q_d(x)$ ,

(ii) If  $\gcd(p, d) = 1$ , then  $Q_d$  factors into  $\phi(d)/m$  distinct monic irreducible factors over  $\mathbb{F}_q$  of the same degree  $m$ , where  $m = \text{ord}_d(q)$ .

As we mentioned in Section 1.1, the factorization of  $x^n - 1$  has received a lot of attention. By Lemma 1.4.1, it is linked with the factorization of cyclotomic polynomials. Further research on explicit factorization of  $x^n - 1$  and cyclotomic polynomials can be found in [22], [40], [62], [64], [85], [88], [91].

In the next chapter, we need some classical results from Galois Theory, in particular, we use the following.

**Lemma 1.4.2** (Kummer extensions) Let  $L \supseteq M$  be finite extensions of  $K = \mathbb{F}_q$ . Suppose that  $L = M(\alpha)$  with  $\alpha^d \in M$  for some  $d$  which is relatively prime to  $q$ . Assume moreover that  $M$  contains all  $d$ -th roots of unity. Then  $L/M$  is called a Kummer extension and  $[L : M] \mid d$ .

**Lemma 1.4.3** Let  $L_1, L_2$  be finite extensions of  $K$  and let  $L = L_1 L_2$  be the compositum of  $L_1$  and  $L_2$ . Then  $[L : L_1] = [L_2 : (L_1 \cap L_2)]$  and  $[L : L_1] \mid [L_2 : K]$ .

We also use the theory of characters in the next chapter. We first recall definitions.

**Definition 1.4.1** Let  $G$  be a multiplicatively written finite abelian group of order  $|G|$  with the identity element  $1_G$ . A character  $\chi$  of  $G$  is a homomorphism from  $G$  into the multiplicative group  $U$  of complex numbers of absolute value 1. That is, a mapping  $\chi : G \rightarrow U$  is called a character of  $G$  if it satisfies

$$\chi(g_1 g_2) = \chi(g_1) \chi(g_2) \quad \text{for all } g_1, g_2 \in G \quad (1.6)$$

Let  $\chi$  be a character of  $G$ . Since  $\chi$  is a group homomorphism, we have  $\chi(1_G) = 1$ . Furthermore,

$$(\chi(g))^{|G|} = \chi(g^{|G|}) = \chi(1_G) = 1$$

for every  $g \in G$ , so that the values of  $\chi$  are  $|G|$ -th roots of unity. Note that

$$\chi(g)\chi(g^{-1}) = \chi(gg^{-1}) = \chi(1_G) = 1$$

and hence  $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$  for every  $g \in G$ , where the bar denotes complex conjugation.

If  $\chi : G \rightarrow U$  is a map such that  $\chi(g) = 1$  for all  $g \in G$ , then  $\chi$  is called the *trivial character* of  $G$ . We denote trivial character of  $G$  by  $\chi_0$ .

If  $\chi$  is a character of  $G$ , there exists a character which is called the *conjugate character* associated to  $\chi$  and denoted by  $\bar{\chi}$  and it is defined by  $\bar{\chi}(g) = \overline{\chi(g)}$  for all  $g \in G$ .

Given finitely many characters  $\chi_1, \dots, \chi_n$  of  $G$ , one can define the product character  $\chi_1 \cdots \chi_n$  by setting  $\chi_1 \cdots \chi_n(g) = \chi_1(g) \cdots \chi_n(g)$  for all  $g \in G$ . If  $\chi_1 = \dots = \chi_n = \chi$ , we denote the product character by  $\chi^n$ . Let us denote the set of characters by  $\widehat{G}$ . Obviously,  $\widehat{G}$  forms an abelian group under this multiplication of characters. As the values of characters of  $\widehat{G}$  are  $|G|$ -th roots of unity, we know that  $\widehat{G}$  is finite.

The following well-known results can be found, for instance, in [53].

**Theorem 1.4.4** *If  $\chi$  is a nontrivial character of the finite abelian group  $G$ , then*

$$(i) \sum_{g \in G} \chi(g) = 0,$$

$$(ii) \text{ If } g \in G \text{ with } g \neq 1_G, \text{ then } \sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

**Theorem 1.4.5** *The number of characters of a finite abelian group is equal to  $|G|$ .*

**Corollary 1.4.6 (Orthogonality Relations)** *Let  $\chi$  and  $\psi$  be characters of  $G$ . Then*

$$(i) \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\psi(g)} = \begin{cases} 0 & \text{for } \chi \neq \psi, \\ 1 & \text{for } \chi = \psi. \end{cases}$$

$$(ii) \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g) \overline{\chi(h)} = \begin{cases} 0 & \text{for } g \neq h, \\ 1 & \text{for } g = h. \end{cases}$$

Consider the characters of  $\mathbb{F}_q$ . Since  $\mathbb{F}_q$  contains two finite abelian groups mainly, the additive group and the multiplicative group, we have to consider their characters separately. Therefore, a character of the additive group of  $\mathbb{F}_q$  is called *additive character* and a character of the multiplicative group of  $\mathbb{F}_q$  is called *multiplicative character*.

**Theorem 1.4.7** [53] Let  $g$  be a fixed primitive element of  $\mathbb{F}_q$ . For each  $j = 0, 1, \dots, (q-2)$ , the function  $\psi_j$  with

$$\psi_j(g^k) = e^{2\pi ijk/(q-1)} \quad \text{for } k = 0, 1, \dots, (q-2)$$

defines a multiplicative character of  $\mathbb{F}_q$ , and every multiplicative character of  $\mathbb{F}_q$  is obtained in this way.

**Corollary 1.4.8** [53] The group of multiplicative characters of  $\mathbb{F}_q$  is cyclic of order  $q-1$ .

Multiplicative characters of  $\mathbb{F}_q$  can be extended to be defined at 0 as follows.

$$\chi(0) = \begin{cases} 1, & \text{for } \chi = \chi_0, \\ 0, & \text{for } \chi \neq \chi_0. \end{cases} \quad (1.7)$$

**Theorem 1.4.9** [53] Let  $\chi$  be a multiplicative character of  $\mathbb{F}_q$  of order  $s > 1$  and let  $G(x) \in \mathbb{F}_q[x]$  be a monic polynomial of positive degree that is not an  $s$ -th power of a polynomial. Let  $r$  be the number of distinct roots of  $G(x)$  in its splitting field over  $\mathbb{F}_q$ . Then for every  $a \in \mathbb{F}_q$  we have,

$$\left| \sum_{c \in \mathbb{F}_q} \chi(aG(c)) \right| \leq (r-1)q^{1/2}.$$

For the next two results, we refer to Cohen [29].

**Lemma 1.4.10** Let  $u, t, n$  be positive integers such that  $u \mid t$ ,  $t \mid n$  and  $l = n/t$ . Then

$$\sum_{u \mid t} \frac{|\mu(u)|}{\phi(u)} \sum_{\substack{v \mid l \\ \gcd(u, l/v)=1}} \phi(u \cdot v) = l \cdot W(t),$$

where  $W(t)$  denotes the number of square-free divisors of  $t$ .

**Lemma 1.4.11** Let  $k \geq 1$ ,  $t \mid q^k - 1$  and  $l = \frac{q^k - 1}{t}$ . The characteristic function  $\omega(x)$  of elements  $x \in \mathbb{F}_{q^k}^*$  of order  $t$  is

$$\omega(x) = \frac{\phi(t)}{q^k - 1} \sum_{u \mid t} \frac{\mu(u)}{\phi(u)} \sum_{\substack{v \mid l \\ \gcd(u, l/v)=1}} \sum_{\text{ord}(\chi)=u \cdot v} \chi(x).$$

Here,  $\mu$  denotes the Möbius function,  $\phi$  denotes the Euler's totient function, and the inner sum runs through the multiplicative characters of  $\mathbb{F}_{q^k}^*$  of order  $u \cdot v$ .

## CHAPTER 2

### Factorization of a class of permutation polynomials

Chapter 2 contains our main results on the degrees of the irreducible factors of a large class of permutation polynomials. Some of the results in this chapter are from [51], obtained jointly with H. Stichtenoth.

## 2.1 Degrees of irreducible factors of $F_n(x)$

We start by stating one of our main results.

**Theorem 2.1.1** [51] *If  $Q(x) \in \mathbb{F}_q[x]$  is an irreducible factor of  $F_n(x)$ , then*

$$\deg Q(x) \text{ divides } d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q).$$

**Proof:** Let  $Q(x) \in \mathbb{F}_q[x]$  be an irreducible factor of  $F_n(x)$ . We may assume  $\deg Q(x) > 1$ . Now let  $\lambda \in \bar{K}$  be a root of  $Q(x)$ , then  $\deg Q(x) = [K(\lambda) : K]$ . Let  $L = K(\zeta)$ , where  $\zeta \in \bar{K}$  is a primitive  $d$ -th root of unity, and set  $M = L \cap K(\lambda)$ . This gives

$$\deg Q(x) = [K(\lambda) : M] \cdot [M : K].$$

By Lemma 1.4.1 (ii),  $[L : K] = [K(\zeta) : K] = \text{ord}_d(q)$ . Since  $M \subseteq L$ , we obtain

$$[M : K] \mid \text{ord}_d(q).$$

Since  $[K(\lambda) : M] = [L(\lambda) : L]$  by Lemma 1.4.3, it suffices to show that

$$[L(\lambda) : L] \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1}. \tag{2.1}$$

To this end, we set  $\lambda_i = F_i(\lambda)$ , for  $i = 0, \dots, n$ . Since  $Q(\lambda) = 0$  and  $Q(x) \mid F_n(x)$ , we have  $\lambda_n = F_n(\lambda) = 0$ . Moreover, using (1.3) we get

$$\lambda_n = F_n(\lambda) = F_{n-1}(\lambda)^{d_n} + a_n = \lambda_{n-1}^{d_n} + a_n,$$

$$\lambda_{n-1} = F_{n-1}(\lambda) = F_{n-2}(\lambda)^{d_{n-1}} + a_{n-1} = \lambda_{n-2}^{d_{n-1}} + a_{n-1}.$$

Continuing in this way, we obtain

$$\begin{aligned} \lambda_{n-1}^{d_n} &= \lambda_n - a_n = -a_n, \\ \lambda_{n-2}^{d_{n-1}} &= \lambda_{n-1} - a_{n-1}, \\ &\vdots \\ \lambda_1^{d_2} &= \lambda_2 - a_2, \\ \lambda_0^{d_1} &= \lambda_1 - a_1. \end{aligned} \tag{2.2}$$

Now, consider the field extensions  $K_i = K(\lambda_{n-i})$  and  $L_i = L(\lambda_{n-i})$ , for  $0 \leq i \leq n$ . As  $\deg Q(x) > 1$ , there exists an index  $1 \leq j \leq n$  such that

$$K = K_0 = \dots = K_{n-j} \subsetneq K_{n-j+1} \subseteq \dots \subseteq K_n = K(\lambda). \tag{2.3}$$

We have  $K_{n-j+1} = K(\lambda_{j-1})$  and

$$\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K = \mathbb{F}_q,$$

by equation (2.2). Since  $d_j$  is relatively prime to  $q - 1$  and  $K \subsetneq K_{n-j+1}$ , there exists  $b \in \mathbb{F}_q^*$  such that  $\lambda_j - a_j = b^{d_j}$ . If we let  $\mu = \lambda_{j-1}/b$ , then we obtain

$$K \subsetneq K_{n-j+1} = K(\lambda_{j-1}) = K(\mu), \quad \mu^{d_j} = 1. \tag{2.4}$$

By assumption,  $d_j$  divides  $d$ , which gives  $\mu \in K(\zeta) = L$  and consequently  $\lambda_{j-1} \in L$ . Hence we see that

$$L = L_0 \subseteq L_1 \subseteq \dots \subseteq L_n.$$

For each  $i, 1 \leq i \leq n - 1$ , the extension  $L_{n-i+1}/L_{n-i}$  is defined by the equation

$$\lambda_{i-1}^{d_i} = \lambda_i - a_i \in L_{n-i}.$$

As  $d_i$  divides  $d$ ,  $L$  contains all  $d_i$ -th roots of unity for  $1 \leq i \leq n$ . Therefore,  $L_{n-i+1}/L_{n-i}$  is a Kummer extension. Hence by Lemma 1.4.2,  $[L_{n-i+1} : L_{n-i}] = [L(\lambda_{i-1}) : L(\lambda_i)]$  divides  $d_i$  for  $i = 1, \dots, n - 1$ . This proves (2.1) and finishes the proof.  $\square$

The following result shows that each divisor of  $d_1 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q)$  does not necessarily occur as the degree of some irreducible factor of  $F_n(x)$ .

**Theorem 2.1.2** [51] *If  $Q(x) \in \mathbb{F}_q[x]$  is an irreducible factor of  $F_n(x)$  satisfying  $\deg Q(x) > 1$ , then there exists some  $j \in \{1, 2, \dots, n\}$  and a prime number  $\ell \mid d_j$  such that  $\text{ord}_\ell(q)$  divides the degree of  $Q(x)$ .*

**Proof:** Let  $j$  be the index satisfying  $K = K_{n-j} \subsetneq K_{n-j+1} \subseteq \dots \subseteq K_n$ . By (2.4),  $K \subsetneq K_{n-j+1} = K(\lambda_{j-1}) = K(\mu)$ , where  $\mu^{d_j} = 1$ . Let  $e$  be the order of  $\mu$  in the cyclic group of  $d_j$ -th roots of unity over  $\mathbb{F}_q$ . Then

$$[K(\lambda_{j-1}) : K] = [K(\mu) : K] = \text{ord}_e(q).$$

for some divisor  $e$  of  $d_j$ . Let  $\ell$  be a prime divisor of  $e$ . Since  $\text{ord}_\ell(q) \mid \text{ord}_e(q)$  and  $\text{ord}_e(q) \mid \deg Q(x)$ , we get  $\text{ord}_\ell(q) \mid \deg Q(x)$ .  $\square$

**Example 2.1.1** *Let  $q = 11$ ,  $n = 2$ ,  $d_1 = 9$ ,  $d_2 = 9$ .  $a_0 = 4$ ,  $a_1 = 5$ ,  $a_2 = 1$ .  $9 = 3^2$ ,  $\text{ord}_3(11) = 2$ . Using Theorem 2.1.1 and Theorem 2.1.2, we conclude that possible degrees of the irreducible factors of the corresponding  $F_2(x)$  are*

$$1, 2, 6, 18, 54. \tag{2.5}$$

Using the computer algebra system MAGMA [15], we can explicitly factorize  $F_2(x)$ , and see that the degrees of the irreducible factors are as in (2.5). On the other hand, if we take  $a_0 = 6$ ,  $a_1 = 2$ ,  $a_2 = 10$  over the same field with the same  $d_i$ ,  $i = 1, 2$ , the explicit factorization of the corresponding  $F_2(x)$  shows that the degrees of the irreducible factors are 1, 2, 6, 18.

Example 2.1.1 shows that the degrees of the irreducible factors depend on the coefficients of  $F_n(x)$ . To emphasize this dependence, we recall the following notation. Let  $A = (a_0, a_1, \dots, a_n) \in \mathbb{F}_q^{n+1}$ ,  $D = (d_1, \dots, d_n) \in \mathbb{Z}_+^n$  such that  $d_j$  satisfy (1.3) and (1.4), for all  $1 \leq j \leq n$ ,  $F_i^{(A,D)} = F_i(x)$ ,  $0 \leq i \leq n$ . Then

$$\begin{aligned} \Delta_n^{(A,D)} &= \{\deg Q(x) : Q(x) \text{ is an irreducible factor of } F_n^{(A,D)}(x)\} \\ \Delta_n^{(D)} &= \{m \leq d_1 \cdot d_2 \cdot \dots \cdot d_n : m \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q) \\ &\quad \text{and } \text{ord}_\ell(q) \mid m \text{ for some prime } \ell \mid d\} \cup \{1\}. \end{aligned} \tag{2.6}$$

## 2.2 The relation between the sets $\Delta_n^{(D)}$ and $\Delta_n^{(A,D)}$

In terms of the notation given by (2.6), Theorem 2.1.1 and Theorem 2.1.2 tell us that  $\Delta_n^{(A,D)} \subseteq \Delta_n^{(D)}$ , for each  $A \in \mathbb{F}_q^{n+1}$ . Example 2.1.1 shows that, there exists  $A \in \mathbb{F}_{11}^3$

satisfying  $\Delta_2^{(D)} = \Delta_2^{(A,D)}$ , where  $D = (9, 9)$ . The following example shows that this is not always the case for an arbitrary  $D$ .

**Example 2.2.1** *Let  $q = 101$ ,  $D = (39, 39)$ , then  $\text{ord}_3(101) = 2$ ,  $\text{ord}_{13}(101) = \text{ord}_{39}(101) = 6$ . Therefore,*

$$\Delta_2^{(D)} = \{1, 2, 6, 18, 26, 78, 234\}$$

*Using MAGMA one can see that as  $A$  runs through  $\mathbb{F}_q^3$ ,  $\Delta_2^{(A,D)}$  is one of the following sets.*

$$\begin{aligned} &\{1\}, \{1, 2, 6\}, \{1, 6, 78\}, \{1, 2, 6, 78\}, \{1, 2, 6, 234\}, \\ &\{1, 2, 6, 78, 234\}, \{1, 2, 6, 18, 234\}, \{1, 2, 6, 18, 78, 234\}. \end{aligned}$$

*That is,  $26 \in \Delta_2^{(D)}$  but  $26 \notin \Delta_2^{(A,D)}$  for any  $A \in \mathbb{F}_q^3$ .*

In fact, Example 2.2.1 is a special case of the following result.

**Theorem 2.2.1** [51] *Suppose that  $n \geq 2$ ,  $d = \text{lcm}(d_1, d_2, \dots, d_n) = p_1 \cdot p_2$  for distinct prime numbers  $p_1, p_2$  and*

$$\text{ord}_{p_1}(q) < \text{ord}_{p_2}(q).$$

*Then  $p_2 \cdot \text{ord}_{p_1}(q) \notin \Delta_n^{(A,D)}$  for any choice of  $A \in \mathbb{F}_q^{n+1}$ .*

In order to prove this result, we need the following lemma.

**Lemma 2.2.2** *Let  $d = p_1 \cdot p_2$ , for distinct prime numbers  $p_1$  and  $p_2$  and  $m = \text{ord}_{p_1}(q) < \text{ord}_{p_2}(q)$ . Then the following hold.*

- (i)  $\gcd(p_2, \text{ord}_{p_1}(q)) = 1$ .
- (ii)  $\gcd(p_2, \text{ord}_d(q)) = 1$ .
- (iii)  $\gcd(p_2, q^m - 1) = 1$ .

**Proof:**

- (i) Suppose the contrary, i.e.,  $p_2 \mid \text{ord}_{p_1}(q)$ . This implies  $\text{ord}_{p_2}(q) < \text{ord}_{p_1}(q)$  since  $\text{ord}_{p_2}(q) < p_2$ , which contradicts the assumption that  $\text{ord}_{p_1}(q) < \text{ord}_{p_2}(q)$ .
- (ii) By a direct consequence of the Chinese Remainder Theorem, we have  $\text{ord}_d(q) = \text{lcm}(\text{ord}_{p_1}(q), \text{ord}_{p_2}(q))$ . Since  $\text{ord}_{p_2}(q) \mid p_2 - 1$  by Lagrange's Theorem, we have  $\gcd(p_2, \text{ord}_{p_2}(q)) = 1$ . Since we also have  $\gcd(p_2, \text{ord}_{p_1}(q)) = 1$  by part (i), the result follows.



(iii) Suppose the contrary, i.e.,  $p_2 \mid q^m - 1$ . This means that

$$\text{ord}_{p_2}(q) \mid \text{ord}_{p_1}(q),$$

again, contradicts the assumption that  $\text{ord}_{p_1}(q) < \text{ord}_{p_2}(q)$ .

□

**Proof of Theorem 2.2.1 :** If  $p_2 \cdot \text{ord}_{p_1}(q) \notin \Delta_n^{(D)}$ , then there is nothing to show. Now, assume that  $p_2 \cdot \text{ord}_{p_1}(q) \in \Delta_n^{(D)}$ . Note that if  $p_2 \mid d_1$ , then  $p_2 \cdot \text{ord}_{p_1}(q) \in \Delta_n^{(D)}$ , for all  $n \geq 2$ . Suppose that there exists  $A \in \mathbb{F}_q^{n+1}$  satisfying  $p_2 \cdot \text{ord}_{p_1}(q) \in \Delta_n^{(A,D)}$ , i.e., there exists an irreducible factor  $Q(x) \in \mathbb{F}_q[x]$  of  $F_n^{(A,D)}(x) = F_n(x)$  such that  $\deg Q(x) = p_2 \cdot \text{ord}_{p_1}(q)$ . As in the proof of Theorem 2.1.1, let  $\lambda \in \bar{K}$  be a root of  $Q(x)$ ,  $\lambda_i = F_i(\lambda)$ ,  $K_i = K(\lambda_{n-i})$ ,  $0 \leq i \leq n$ . Since  $\deg Q(x) > 1$ , we know that

$$K = K_{n-j-1} \subsetneq K_{n-j}, \quad \text{for some index } 0 \leq j \leq n-1.$$

By Theorem 2.1.2, we have

$$[K_{n-j} : K_{n-j-1}] = \text{ord}_{e_{j+1}}(q) \quad \text{for some } e_{j+1} \mid d_{j+1}. \quad (2.7)$$

Since  $[K_{n-j} : K]$  divides  $[K_n : K]$ , we conclude that

$$\text{ord}_{e_{j+1}}(q) \mid p_2 \cdot \text{ord}_{p_1}(q) \quad \text{for some } e_{j+1} \mid d_{j+1}. \quad (2.8)$$

Now, we will show that  $e_{j+1}$  is necessarily  $p_1$ .

If  $e_{j+1} = p_2$ , then from (2.8), we get

$$\text{ord}_{p_2}(q) \mid p_2 \cdot \text{ord}_{p_1}(q).$$

Since  $\gcd(p_2, \text{ord}_{p_2}(q)) = 1$ , we get  $\text{ord}_{p_2}(q) \mid \text{ord}_{p_1}(q)$ , which contradicts the assumption that  $\text{ord}_{p_1}(q) < \text{ord}_{p_2}(q)$ .

Similarly, assuming  $e_{j+1} = d$ , from (2.8), we get

$$\text{ord}_d(q) \mid p_2 \cdot \text{ord}_{p_1}(q).$$

Since  $\gcd(p_2, \text{ord}_d(q)) = 1$  by Lemma 2.2.2 (ii), we get  $\text{ord}_d(q) \mid \text{ord}_{p_1}(q)$ . But this is not the case, since  $\text{ord}_d(q) = \text{lcm}(\text{ord}_{p_1}(q), \text{ord}_{p_2}(q))$  and  $\text{ord}_{p_1}(q) < \text{ord}_{p_2}(q)$ . Therefore,  $e_{j+1} = p_1$ , and hence by (2.7),  $K_{n-j}$  contains all primitive  $p_1$ -th roots of unity. We know  $K_{n-j+1} = K(\lambda_{j-1})$ , and

$$\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K_{n-j}. \quad (2.9)$$

by equation (2.2). Now, we will show that  $[K_{n-j+1} : K_{n-j}] = 1$  for the cases  $d_j = p_1, p_2, d$ .

**Case 1 :** Assume  $d_j = p_1$ . Since  $K_{n-j}$  contains all  $p_1$ -th roots of unity, together with (2.9), we conclude that  $K_{n-j+1}/K_{n-j}$  is a Kummer extension. Therefore,  $[K_{n-j+1} : K_{n-j}]$  is 1 or  $p_1$ . If the latter holds, then we get

$$p_1 \cdot \text{ord}_{p_1}(q) \mid p_2 \cdot \text{ord}_{p_1}(q),$$

which is a contradiction. Hence,  $[K_{n-j+1} : K_{n-j}] = 1$ .

**Case 2 :** Assume  $d_j = p_2$ . By equation (2.9),  $\lambda_{j-1}$  is a root of the polynomial  $x^{d_j} - \lambda_j + a_j \in K_{n-j}[x]$ . Lemma 2.2.2 (iii) implies that there exists  $\mu \in K_{n-j}$  satisfying  $\mu^{d_j} = \lambda_j - a_j$ , which shows that the polynomial  $x^{d_j} - \lambda_j + a_j$  is reducible over  $K_{n-j}$ . That is,  $[K_{n-j+1} : K_{n-j}] < p_2$ . If  $[K_{n-j+1} : K_{n-j}] = k > 1$ , then we get

$$k \cdot \text{ord}_{p_1}(q) \mid p_2 \cdot \text{ord}_{p_1}(q),$$

which is a contradiction since  $1 < k < p_2$ . Hence,  $[K_{n-j+1} : K_{n-j}] = 1$ .

**Case 3 :** Assume  $d_j = d$ . Consider the element  $\delta = \lambda_{j-1}^{p_2}$  and note that  $K_{n-j} \subseteq K_{n-j}(\delta) \subseteq K_{n-j+1}$ . Equation (2.9) implies

$$\delta^{p_1} = \lambda_j - a_j \in K_{n-j} \tag{2.10}$$

Since  $K_{n-j}$  contains all primitive  $p_1$ -th roots of unity, together with (2.10), we conclude that  $K_{n-j}(\delta)/K_{n-j}$  is a Kummer extension. Therefore  $[K_{n-j}(\delta) : K_{n-j}]$  is 1 or  $p_1$ . If the latter holds, we obtain a contradiction in a similar way to the proof of Case 1. Therefore,  $K_{n-j}(\delta) = K_{n-j}$ . Now,  $\lambda_{j-1}$  is a root of the polynomial  $x^{p_2} - \delta \in K_{n-j}[x]$ . Using Lemma 2.2.2 (iii), one can show that the polynomial  $x^{p_2} - \delta$  is reducible as in the proof of Case 2. That is,  $[K_{n-j+1} : K_{n-j}] < p_2$ , and hence  $[K_{n-j+1} : K_{n-j}] > 1$  gives a contradiction. Therefore

$$\deg Q(x) = [K_n : K] = \text{ord}_{p_1}(q),$$

when  $n = 2$ , which is impossible.

If  $n > 2$ , one can similarly consider these three cases where  $m$  is replaced by  $[K_{n-j+i} : K]$  and  $d_i$  is replaced by  $d_{j-i+1}$ , for each  $2 \leq i \leq j$  and conclude that

$$K_{n-j} = K_{n-j+1} = \dots = K_n.$$

Therefore,

$$\deg Q(x) = [K_n : K] = \text{ord}_{p_1}(q),$$

again, a contradiction. Hence there is no  $A \in \mathbb{F}_q^{n+1}$  with  $p_2 \cdot \text{ord}_{p_1}(q) \in \Delta_n^{(A,D)}$ .  $\square$

We generalize the idea of this proof for the case of an arbitrary integer  $d$ , and give a necessary condition on  $q$  and  $d$ , for the existence of  $A \in \mathbb{F}_q^{n+1}$  satisfying  $\Delta_n^{(A,D)} = \Delta_n^{(D)}$  for  $n \geq 2$ . We need the following lemmas.

**Lemma 2.2.3** *Let  $u \in \mathbb{Z}$  satisfying  $\gcd(\ell, u) = 1$  for a prime number  $\ell$ . Then*

- (i) *If  $\gcd(u - 1, \ell) = \ell$ , then  $u \in \mathbb{Z}_{\ell^k}^*$  for any  $k \in \mathbb{Z}^+$ . Moreover, if  $k \geq 2$  then  $\text{ord}_{\ell^k}(u) \mid \ell^{k-1}$ .*
- (ii) *If  $\gcd(u - 1, \ell) = 1$ , then  $u \in \mathbb{Z}_{\ell^k}^*$  for any  $k \in \mathbb{Z}^+$ . Moreover, if  $k \geq 2$ ,  $m_1 = \text{ord}_{\ell}(u)$ ,  $m_2 = \text{ord}_{\ell^k}(u^{m_1})$ , then  $\text{ord}_{\ell^k}(u) = m_1 \cdot m_2$ .*

**Proof:**

- (i) Since  $\phi(\ell) \mid \phi(\ell^k)$ , where  $\phi$  is the Euler's totient function, there is a ring homomorphism  $\psi : \mathbb{Z}_{\ell^k}^* \rightarrow \mathbb{Z}_{\ell}^*$ . If  $u \equiv 1 \pmod{\ell}$ , then clearly  $u \in \mathbb{Z}_{\ell^k}^*$  for any  $k \in \mathbb{Z}^+$  and  $u \in \text{Ker}(\psi)$ , where  $\text{Ker}(\psi)$  denotes the kernel of the ring homomorphism  $\psi$ . We will show that  $\text{Ker}(\psi)$  has  $\ell^{k-1}$  elements, that is  $|\text{Ker}(\psi)| = \ell^{k-1}$ . If  $k = 1$ , then it is clear. If  $k \geq 2$ , then

$$\begin{aligned} |\text{Ker}(\psi)| &= |\{u : u = \ell \cdot v + 1, 0 < \ell \cdot v + 1 < \ell^k\}| \\ &= |\{u : u = \ell \cdot v + 1, 0 \leq v < \frac{\ell^k - 1}{\ell}\}| \\ &= |\{u : u = \ell \cdot v + 1, 0 \leq v < \frac{\ell^k}{\ell} - \frac{1}{\ell}\}| \\ &= |\{u : u = \ell \cdot v + 1, 0 \leq v < \frac{\ell^k}{\ell}\}| = \ell^{k-1}. \end{aligned}$$

By Lagrange's Theorem, the order of any subgroup of  $\text{Ker}(\psi)$  divides the order of  $\text{Ker}(\psi)$ . Thus,  $\text{ord}_{\ell^k}(u) \mid \ell^{k-1}$ .

- (ii) Since  $u^{\text{ord}_{\ell^k}(u)} \equiv 1 \pmod{\ell^k}$ ,  $u^{\text{ord}_{\ell^k}(u)} \equiv 1 \pmod{\ell}$ . Thus  $m_1 \mid \text{ord}_{\ell^k}(u)$ . Since  $m_2 = \frac{\text{ord}_{\ell^k}(u)}{\gcd(m_1, \text{ord}_{\ell^k}(u))}$  and  $m_1 \mid \text{ord}_{\ell^k}(u)$ , we get  $\text{ord}_{\ell^k}(u) = m_1 \cdot m_2$ . Note that  $m_2 \mid \ell^{k-1}$  by part (i).

$\square$

**Lemma 2.2.4** *Let  $d \in \mathbb{Z}^+$ ,  $d_{\mathcal{P}} = \{\ell : \ell \mid d, \ell \text{ is a prime}\}$ . Put  $O = \{\text{ord}_{\ell}(q) : \ell \in d_{\mathcal{P}}\}$ . Suppose that  $r_{\ell}$  denotes the integer satisfying  $\ell^{r_{\ell}} \parallel d$  for any  $\ell \in d_{\mathcal{P}}$ . If  $|O| \geq 2$ , let  $m$  be the smallest element in  $O$ , with  $m = \text{ord}_{\ell_1}(q)$ ,  $\ell_1 \in d_{\mathcal{P}}$ , and  $\ell_2$  be the largest element in  $d_{\mathcal{P}}$ , satisfying  $m < \text{ord}_{\ell_2}(q)$ . Then*

(i)  $\gcd(\ell_2, m) = 1$ .

(ii) If  $e \mid d$  and  $m \nmid \text{ord}_e(q)$ , then  $\gcd(e, q^m - 1) = 1$ .

(iii) If  $e \mid d$  and  $\text{ord}_e(q) = m$ , then  $\gcd(\ell_2, e) = 1$ .

(iv) If  $\ell \in d_{\mathcal{P}}$ ,  $\ell \neq \ell_2$  and  $\text{ord}_{\ell}(q) > m$ , then  $\gcd(\ell_2, \text{ord}_{\ell^{r_{\ell}}}(q)) = 1$ .

(v)  $\text{ord}_{\ell_2^{r_{\ell_2}}}(q^m) = m_1 \cdot m_2$ , where  $m_1 > 1$ ,  $\gcd(\ell_2, m_1) = 1$  and  $m_2 \mid \ell_2^{r_{\ell_2}-1}$ .

**Proof:**

(i) Suppose that  $\ell_2 \mid m$ . Then we get  $\text{ord}_{\ell_2}(q) < \ell_2 \leq m$ , which contradicts the assumption that  $\text{ord}_{\ell_2}(q) > m$ .

(ii) Suppose that  $\gcd(e, q^m - 1) > 1$ . Then there exists a prime divisor  $\ell$  of  $e$  such that  $\ell \mid q^m - 1$ . The latter implies  $\text{ord}_{\ell}(q) \mid m$  and hence, we obtain that  $\text{ord}_{\ell}(q) = m$ , as  $m$  is the smallest element of  $O$ . But then  $\text{ord}_{\ell}(q) \mid \text{ord}_e(q)$ , which contradicts the assumption.

(iii) Suppose that  $\ell_2 \mid e$ . Then, we have  $\text{ord}_{\ell_2}(q) \mid \text{ord}_e(q)$ , which implies  $\text{ord}_{\ell_2}(q) \leq m$ , contradicting the assumption that  $\text{ord}_{\ell_2}(q) > m$ .

(iv) Suppose that  $r_{\ell} = 1$  and  $\ell_2 \mid \text{ord}_{\ell}(q)$ . Then we get

$$\text{ord}_{\ell_2}(q) < \ell_2 \leq \text{ord}_{\ell}(q) < \ell.$$

But this gives a contradiction to the assumption on  $\ell_2$ , being the largest prime divisor of  $d$  satisfying  $\text{ord}_{\ell}(q) > m$ . Hence,  $\gcd(\ell_2, \text{ord}_{\ell}(q)) = 1$ . Now, let  $r_{\ell} \geq 2$ . Since

$$\text{ord}_{\ell^{r_{\ell}}}(q) = m_2 \cdot \text{ord}_{\ell}(q)$$

for some  $m_2 \mid \ell^{r_{\ell}-1}$  by Lemma 2.2.3 (ii), we get  $\gcd(\ell_2, \text{ord}_{\ell^{r_{\ell}}}(q)) = 1$ .

(v) Suppose that  $r_{\ell_2} = 1$ . We have  $1 < m_1$  since

$$m_1 = \text{ord}_{\ell_2}(q^m) = \frac{\text{ord}_{\ell_2}(q)}{\gcd(\text{ord}_{\ell_2}(q), m)}$$

and  $\text{ord}_{\ell_2}(q) > m$ . We also have  $\gcd(\ell_2, m_1) = 1$ , since  $m_1 \mid \ell_2 - 1$ . If  $r_{\ell_2} \geq 2$ , then again by Lemma 2.2.3 (ii), we have  $\text{ord}_{\ell_2}^{r_{\ell_2}}(q^m) = m_1 \cdot m_2$ , where  $m_2 \mid \ell_2^{r_{\ell_2}-1}$ .

□

**Theorem 2.2.5** *Let  $n \geq 2$ ,  $D = (d_1, d_2, \dots, d_n)$ ,  $d = \text{lcm}(d_1, d_2, \dots, d_n)$ ,  $d_{\mathcal{P}} = \{\ell : \ell \mid d, \ell \text{ is a prime}\}$ , and*

$$O = \{\text{ord}_{\ell}(q) : \ell \in d_{\mathcal{P}}\}. \quad (2.11)$$

*If  $\Delta_n^{(D)} = \Delta_n^{(A,D)}$  for some  $A \in \mathbb{F}_q^{n+1}$ , then either*

(i)  $|O| = 1$ , or

(ii)  $|O| \geq 2$ , and  $\ell_2 \nmid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q)$ , where  $\ell_2$  is the largest element in  $d_{\mathcal{P}}$  with  $\text{ord}_{\ell_2}(q) > m$ , and  $m$  is the smallest element in  $O$ .

**Proof:** We use the notation of Lemma 2.2.4 above and prove the contrapositive of this statement.

Suppose that the set  $O$  has at least two elements,  $m = \text{ord}_{\ell_1}(q)$  is the smallest element of  $O$  and  $\ell_2$  is the largest prime divisor of  $d$  satisfying  $\text{ord}_{\ell_2}(q) > m$ . Suppose also  $\ell_2 \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q)$ . This implies that  $\ell_2 \cdot m \in \Delta_n^{(D)}$ . We now show that  $\ell_2 \cdot m \notin \Delta_n^{(A,D)}$ , for any choice of  $A \in \mathbb{F}_q^{n+1}$ . Suppose the contrary, i.e., there exists  $A \in \mathbb{F}_q^{n+1}$  such that  $\ell_2 \cdot m \in \Delta_n^{(A,D)}$ , and an irreducible factor  $Q(x) \in \mathbb{F}_q[x]$  of  $F_n^{(A,D)}(x) = F_n(x)$  satisfying  $\deg Q(x) = \ell_2 \cdot m$ . As in the previous proofs, take a root  $\lambda \in \bar{K}$  of  $Q(x)$  and set  $\lambda_i := F_i(\lambda)$ ,  $K_i = K(\lambda_{n-i})$ , for  $0 \leq i \leq n$ . As  $\deg Q(x) > 1$ , let  $0 \leq j \leq n$  be the index satisfying

$$K = K_0 = K_{n-j-1} \subsetneq K_{n-j} \subseteq \dots \subseteq K_n = K(\lambda).$$

As  $K_{n-j} = K(\lambda_j)$  and  $\lambda_j^{d_{j+1}} = \lambda_{j+1} - a_{j+1} \in K(\lambda_{j+1}) = K_{n-j-1} = K$  by (2.2), we have  $[K_{n-j} : K] = \text{ord}_{e_{j+1}}(q)$  for some  $e_{j+1} \mid d_{j+1}$  by Theorem 2.1.2. Therefore,

$$\text{ord}_{e_{j+1}}(q) \mid \ell_2 \cdot m. \quad (2.12)$$

First, we assume  $\gcd(\ell_2, \text{ord}_{e_{j+1}}(q)) = \ell_2$ . By Lemma 2.1.1 (i), (iii), (iv) and Lemma 2.2.3 (ii), we deduce that  $\ell_2^r \mid \text{ord}_{e_{j+1}}(q)$  for some  $2 \leq r \leq r_{\ell_2}$ . Together with (2.12), we get

$$\text{ord}_{\ell_2^r}(q) \mid \ell_2 \cdot m', \quad (2.13)$$

for some  $m' \mid m$ . By using Lemma 2.2.3 (ii), we obtain that  $\text{ord}_{\ell_2}(q) \mid m'$ , which contradicts the assumption that  $\text{ord}_{\ell_2}(q) > m$ . Therefore  $\gcd(\ell_2, \text{ord}_{e_{j+1}}(q)) = 1$ . Then, Equation (2.12) implies  $\text{ord}_{e_{j+1}}(q) \mid m$ , which means

$$\text{ord}_{e_{j+1}}(q) = m, \quad (2.14)$$

as  $m$  is the smallest element of  $O$ . Now, we will show that

$$[K(\lambda_{j-1}) : K(\lambda_j)] = [K_{n-j+1} : K_{n-j}] = 1,$$

by examining three different cases for  $d_j$ , since  $\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K(\lambda_j) = K_{n-j}$  by (2.2).

**Case 1 :** Assume  $m \nmid \text{ord}_{d_j}(q)$ . By Lemma 2.2.4 (ii), we have  $\gcd(d_j, q^m - 1) = 1$ , hence we know the existence of  $\mu \in K_{n-j}$  satisfying

$$\mu^{d_j} = \lambda_{j-1}^{d_j} = \lambda_j - a_j \in K_{n-j}. \quad (2.15)$$

Equation (2.15) tells us that  $\lambda_{j-1}$  is a root of the polynomial  $x^{d_j} - \lambda_j + a_j \in K_{n-j}[x]$  and we may write

$$x^{d_j} - \lambda_j + a_j = x^{d_j} - \mu^{d_j} = \left(\frac{x}{\mu}\right)^{d_j} - 1. \quad (2.16)$$

By Lemma 1.4.1,  $[K_{n-j+1} : K_{n-j}] = 1$  or  $\text{ord}_{e_j}(q^m)$  for some  $e_j \mid d_j$ . If  $\ell_2^r \mid e_j$  for some  $1 \leq r \leq r_{\ell_2}$ , then by Lemma 2.2.4 (v) we have

$$m_1 \cdot m_2 \mid [K_{n-j+1} : K_j],$$

where  $\gcd(\ell_2, m_1) = 1$ ,  $m_1 > 1$ ,  $m_2 \mid \ell_2^{r_{\ell_2}-1}$ . Therefore, we get

$$m_1 \cdot m_2 \cdot m \mid p_2 \cdot m,$$

where  $m_1 > 1$  and  $\gcd(\ell_2, m_1) = 1$ , a contradiction.

If  $\ell_2 \nmid e_j$ , then by Lemma 2.2.4 (iv), we obtain a contradiction in a similar way.

**Case 2 :** Assume  $m \mid \text{ord}_{d_j}(q)$  and  $\text{ord}_{e_j}(q) > m$  for all  $e_j \mid d_j$ .

We have  $\gcd(d_j, q^m - 1) = 1$ , because otherwise, there exists a divisor  $e_j$  of  $d_j$  such that

$e_j \mid q^m - 1$ . As  $m$  is the smallest element of  $O$ , we get  $\text{ord}_{e_j}(q) = m$ , which contradicts the assumption. Therefore, as in the proof of Case 1, we get  $[K_{n-j+1} : K_{n-j}] = 1$ .

**Case 3 :** Assume  $m \mid \text{ord}_{d_j}(q)$  and  $\text{ord}_{e_j}(q) = m$  for some  $e_j \mid d_j$ .

If  $\text{ord}_{d_j}(q) = m$ , then  $K_{n-j+1}/K_{n-j}$  is a Kummer extension, which implies  $[K_{n-j+1} : K_{n-j}] \mid d_j$ . Since  $\gcd(\ell_2, d_j) = 1$  by Lemma 2.2.4 (iii), we get  $[K_{n-j+1} : K_{n-j}] = 1$ .

If  $m$  is a proper divisor of  $\text{ord}_{d_j}(q)$ , let  $e_j \mid d_j$  satisfying  $\text{ord}_{e_j}(q) = m$ . As  $\text{ord}_{d_j}(q) \neq m$  by assumption, there exists  $s_j > 1$  such that  $d_j = e_j \cdot s_j$ . Now, consider the element  $\delta = \lambda_{j-1}^{s_j}$  and notice that  $K_{n-j} \subseteq K_{n-j}(\delta) \subseteq K_{n-j+1}$ . By (2.2), we know that

$$\delta^{e_j} = (\lambda_{j-1}^{s_j})^{e_j} = \lambda_j - a_j \in K_{n-j} \quad (2.17)$$

Equation (2.14) tells us  $K_{n-j}$  contains all  $e_j$ -th roots of unity, as  $\text{ord}_{e_j}(q) = m$ . Together with equation (2.17) we have  $K_{n-j}(\delta)/K_{n-j}$  is a Kummer extension. Hence  $[K_{n-j}(\delta) : K_{n-j}] \mid e_j$ . By Lemma 2.2.4 (iii), we know that  $\gcd(\ell_2, e_j) = 1$ . Hence  $K_{n-j}(\delta) = K_{n-j}$ . If  $\text{ord}_{s_j}(q) = m$ , then  $K_{n-j+1}/K_{n-j}(\delta)$  is a Kummer extension. Similarly, we obtain  $K_{n-j+1} = K_{n-j}(\delta) = K_{n-j}$  by Lemma 2.2.4 (iii).

If  $\text{ord}_{s_j}(q) > m$ , there are two subcases.

If  $\gcd(s_j, q^m - 1) = 1$ , then, as in the proof of Case 1, there exists an element  $\mu \in K_{n-j}$  such that

$$\mu^{s_j} = \delta \in K_{n-j}. \quad (2.18)$$

Since  $\delta = \lambda_{j-1}^{s_j}$ ,  $\lambda_{j-1}$  is a root of the polynomial  $x^{s_j} - \delta \in K_{n-j+1}[x]$ . Together with equation (2.18), we obtain that  $\lambda_{j-1}$  is a root of the polynomial

$$x^{s_j} - \delta = x^{s_j} - \mu^{s_j} = \left(\frac{x}{\mu}\right)^{s_j} - 1 \in K_{n-j}[x]. \quad (2.19)$$

Therefore,  $[K_{n-j+1} : K_{n-j}] = 1$  or  $\text{ord}_{s'_j}(q^m) > 1$  for some  $s'_j \mid s_j$ . The latter gives a contradiction by Lemma 2.2.4 (iv) and (v).

If  $\gcd(s_j, q^m - 1) > 1$ , then similarly one can show that  $K_{n-j+1}$  contains a field extension, which contains  $K_{n-j}(\delta) = K_{n-j}$  and has degree relatively prime to  $\ell_2$  over  $K_{n-j}$ , since  $\text{ord}_{s_j}(q)$  and  $m$  are not equal. Continuing in this way, we conclude that  $K_{n-j} = K_{n-j+1}$ , as  $d_j$  has finitely many divisors.

If  $n = 2$ , we get  $[K_2 : K] = \deg Q(x) = m$ , a contradiction.

If  $n > 2$ , one can similarly consider these three cases, where  $m$  is replaced by  $[K_{n-j+i} : K]$  and  $d_i$  is replaced by  $d_{j-i+1}$ , for each  $2 \leq i \leq j$ , and obtain that

$$K_{n-j} = K_{n-j+1} = \dots = K_n,$$

and hence  $[K_n : K] = \deg Q(x) = m$ , again, a contradiction. Therefore, there is no  $A \in \mathbb{F}_q^{n+1}$  with  $\Delta_n^{(A,D)} = \Delta_n^{(D)}$ .  $\square$

**Remark 2.2.1** Note that if  $n = 1$ , then  $\Delta_1^{(D)} = \{\text{ord}_e(q) : e \mid d_1\} \cup \{1\}$ . Let  $A = (a_0, a_1) \in \mathbb{F}_q^2$ . Then

$$F_1^{(A,D)}(x) = F_1(x) = (x + a_0)^{d_1} + a_1.$$

If  $a_1 \neq 0$ , then there exists  $b \in \mathbb{F}_q^*$  satisfying  $b^{d_1} = -a_1$  since  $x^{d_1}$  is a permutation polynomial by Lemma 1.2.4 (i), and hence

$$F_1(x) = (x + a_0)^{d_1} + a_1 = \left( \frac{x + a_0}{b} \right)^{d_1} - 1.$$

By Lemma 1.4.1, we have  $\Delta_1^{(A,D)} = \Delta_1^{(D)}$ .

**Remark 2.2.2** Note that the conditions on  $m$  and  $\ell_2$  are necessary. If  $m$  is not the smallest element of  $O$ , then it is possible that  $m = \text{ord}_d(q)$  and if this is the case, it is possible that  $\text{ord}_{e_{j+1}}(q) = \text{ord}_d(q)$  in (2.12). That is,  $K_{n-j}$  contains all  $d$ -th roots of unity. Therefore, it is possible that

$$[K_n : K] = [K_{n-j+1} : K] = \ell_2 \cdot m = \ell_2 \cdot \text{ord}_d(q),$$

since  $K_{n-j+1}/K_{n-j}$  is a Kummer extension. If  $\ell_2$  is not the largest prime factor of  $d$  satisfying  $\text{ord}_{\ell_2}(q) > m$ , then it is possible that  $\ell_2 \mid \text{ord}_\ell(q^m)$  for some prime divisor  $\ell_2 \neq \ell$  of  $d$ . Hence, it is possible that  $[K_n : K] = \ell_2 \cdot m$  as above.

The necessary condition given by Theorem 2.2.5 is not sufficient, as the following example indicates.

**Example 2.2.2** Let  $q = 29$ ,  $n = 2$ ,  $D = (15, 5)$ , then  $d = 15 = 3 \cdot 5$ . We have  $\text{ord}_3(29) = \text{ord}_5(29) = \text{ord}_{15}(29) = 2$ . Thus by Theorem 2.1.1 and Theorem 2.1.2,  $\Delta_2^{(D)} = \{1, 2, 6, 10, 30\}$ . Calculations show that, if  $A \in \mathbb{F}_q^3$ , then  $\Delta_2^{(A,D)}$  is one of the following:

$$\{1\}, \{1, 2\}, \{1, 2, 6\}, \{1, 6\}, \{1, 2, 10\}, \{1, 2, 30\}.$$

That is, there is no  $A \in \mathbb{F}_q^3$  such that  $\Delta_2^{(A,D)} = \Delta_2^{(D)}$ .

**Remark 2.2.3** Note that for fixed  $q$ , one can always find  $d_1 = d_2 = \dots d_n = \ell$ , where  $\ell$  is a prime number satisfying (1.2) and (1.4), so that the condition given by Theorem



2.2.5 (i) is satisfied. On the other hand, if  $D$  is fixed, consider  $d = \text{lcm}(d_1, d_2, \dots, d_n) = \ell_1^{r_{\ell_1}} \cdot \ell_2^{r_{\ell_2}} \cdot \dots \cdot \ell_k^{r_{\ell_k}}$  for distinct primes  $\ell_i$ ,  $1 \leq i \leq k$ . Since (1.2) and (1.4) implies that  $d$  is odd, we have  $1 \not\equiv -1 \pmod{\ell_i^{r_{\ell_i}}}$ , for all  $1 \leq i \leq k$ . Consider the system of congruences

$$\begin{aligned} x &\equiv -1 \pmod{\ell_1^{r_{\ell_1}}}, \\ x &\equiv -1 \pmod{\ell_2^{r_{\ell_2}}}, \\ &\vdots \\ x &\equiv -1 \pmod{\ell_k^{r_{\ell_k}}}. \end{aligned}$$

By the Chinese Remainder Theorem, there exists a unique solution  $s \equiv -1 \pmod{d}$ . Dirichlet's Prime Number Theorem tells us that there are infinitely many prime numbers  $q$  satisfying  $q \equiv -1 \pmod{d}$ . Note that since  $\text{ord}_{\ell_i^{r_{\ell_i}}}(q) = 2$  and  $1 \neq \text{ord}_{\ell_i}(q) \mid \text{ord}_{\ell_i^{r_{\ell_i}}}(q)$ , we have  $\text{ord}_{\ell_i}(q) = 2$  for all  $1 \leq i \leq k$ . That is, for fixed  $D$ , there are infinitely many prime numbers  $q$  such that condition (i) of Theorem 2.2.5 is satisfied.

## 2.3 Elimination of some degrees

In the proof of Theorem 2.2.5, we actually eliminated  $\ell_2 \cdot m$  from the set  $\Delta_n^{(D)}$ , as one can see from the following corollary of the proof of Theorem 2.2.5. We use the notation of Lemma 2.1.1 and Theorem 2.2.5.

**Corollary 2.3.1** *Let  $n \geq 2$ . Suppose that*

- (i)  $|O| \geq 2$ , and
- (ii)  $\ell_2 \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q)$ .

*Then  $\ell_2 \cdot m \in \Delta_n^{(D)}$ , but  $\ell_2 \cdot m \notin \Delta_n^{(A,D)}$ , for any choice of  $A \in \mathbb{F}_q^{n+1}$ .*

We use a similar technique to prove that it is possible to eliminate other elements of  $\Delta_n^{(D)}$ , under certain conditions.

**Theorem 2.3.2** *Let  $n \geq 2$  and suppose the following hold.*

- (i)  $\text{gcd}(d, \text{ord}_d(q)) = 1$ , and
- (ii) *there exists  $k \mid \text{ord}_d(q)$ , where  $1 < k < \text{ord}_d(q)$  such that  $\text{ord}_e(q) \neq k$  for all  $e \mid d$ .*

Then  $r \cdot k \in \Delta_n^{(D)}$  but  $r \cdot k \notin \Delta_n^{(A,D)}$ , for all  $r \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1}$  and for any choice of  $A \in \mathbb{F}_q^{n+1}$ .

**Proof:** Clearly,  $r \cdot k \in \Delta_n^{(D)}$ . We now show that there is no  $A \in \mathbb{F}_q^{n+1}$  such that  $r \cdot k \in \Delta_n^{(A,D)}$ . Suppose the contrary, i.e., there exists  $A \in \mathbb{F}_q^{n+1}$  such that  $r \cdot k \in \Delta_n^{(A,D)}$ . Then,  $F_n^{(A,D)}(x) = F_n(x)$  has an irreducible factor  $Q(x) \in \mathbb{F}_q[x]$ , where  $\deg Q(x) = r \cdot k$ . Using the notation of Theorem 2.2.5, we let  $0 \leq j$  to be the index satisfying

$$K = K_{n-j-1} \subsetneq K_{n-j} \subseteq \dots \subseteq K_n,$$

as  $\deg Q(x) > 1$ . By Theorem 2.1.2,  $[K_{n-j} : K] = m = \text{ord}_{e_{j+1}}(q)$  for some  $e_{j+1} \mid d_{j+1}$  and hence  $m \mid r \cdot k$ . Since  $\gcd(d, \text{ord}_d(q)) = 1$ , we have  $\text{ord}_{e_{j+1}}(q) \mid k$ . Note that  $m = \text{ord}_{e_{j+1}}(q) \neq k$  by assumption. Therefore,  $j = 0$  gives  $[K_n : K] = m < k$ , a contradiction. Thus  $1 \leq j$  and we consider  $[K_{n-j+1} : K]$ . As we know,  $K_{n-j+1} = K(\lambda_{j-1})$  and  $\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K_{n-j}$ .

**Case 1 :** Assume  $\text{ord}_{d_j}(q) \nmid m$ . We have two subcases.

If  $\gcd(d_j, q^m - 1) = 1$ , then there exists  $\mu \in K_{n-j}$  satisfying  $\mu^{d_j} = \lambda_j - a_j$ . Therefore,  $\lambda_{j-1}$  is a root of the polynomial

$$x^{d_j} - \lambda_j + a_j = x^{d_j} - \mu^{d_j} = \left(\frac{x}{\mu}\right)^{d_j} - 1 \in K_{n-j}[x].$$

Thus,  $[K_{n-j+1} : K_{n-j}]$  equals 1 or  $\text{ord}_{e_j}(q^m) > 1$  for some  $e_j \mid d_j$ . Note that  $\gcd(e_j, e_{j+1}) = 1$ , since  $\gcd(d_j, q^m - 1) = 1$ . Now, we will show that  $[K_{n-j+1} : K] = m \cdot \text{ord}_{e_j}(q^m) \neq k$ . Suppose that

$$k = m \cdot \text{ord}_{e_j}(q^m) = \frac{m \cdot \text{ord}_{e_j}(q)}{\gcd(m, \text{ord}_{e_j}(q))} = \text{lcm}(m, \text{ord}_{e_j}(q)).$$

Since  $\gcd(e_j, e_{j+1}) = 1$ , we have  $e_j \cdot e_{j+1} \mid d$  and

$$\text{ord}_{e_j \cdot e_{j+1}}(q) = \text{lcm}(\text{ord}_{e_j}(q), \text{ord}_{e_{j+1}}(q)) = \text{lcm}(m, \text{ord}_{e_j}(q)) = k,$$

which contradicts our assumption. Therefore,  $[K_{n-j+1} : K]$  is a proper divisor of  $r \cdot k$ . Now, assume  $\gcd(d_j, q^m - 1) = f_j > 1$ . As  $f_j \neq d_j$  by assumption, there exists  $s_j > 1$  such that  $d_j = f_j \cdot s_j$ . Consider the element  $\delta = \lambda_{j-1}^{d_j/f_j} = \lambda_{j-1}^{s_j}$  and notice that  $K_{n-j} \subseteq K_{n-j}(\delta) \subseteq K_{n-j+1}$ . We know that

$$\delta^{f_j} = (\lambda_{j-1}^{s_j})^{f_j} = \lambda_j - a_j \in K_{n-j} \tag{2.20}$$

Since  $f_j \mid q^m - 1$ ,  $K_{n-j}$  contains all  $f_j$ -th roots of unity. Together with (2.20),  $K_{n-j}(\delta)/K_{n-j}$  is a Kummer extension. That is,

$$[K_{n-j}(\delta) : K_{n-j}] = f'_j \text{ for some } f'_j \mid f_j. \quad (2.21)$$

We have  $\gcd(f'_j, k) = 1$  by assumption. Hence  $[K_{n-j}(\delta) : K_{n-j}] = f'_j$  is relatively prime to  $k$ .

Now,  $\lambda_{j-1}$  is a root of the polynomial  $x^{s_j} - \delta \in K_{n-j}(\delta)[x]$ .

If  $\gcd(s_j, q^{f'_j \cdot m} - 1) = 1$ , then as in the proof of the first subcase, there exists  $\mu \in K_{n-j}(\delta)$  such that  $\mu^{s_j} = \delta$  and hence

$$x^{s_j} - \delta = x^{s_j} - \mu^{s_j} = \left(\frac{x}{\mu}\right)^{s_j} - 1.$$

Therefore,  $[K_{n-j+1} : K_{n-j}(\delta)]$  equals 1 or  $\text{ord}_{s'_j}(q^{f'_j \cdot m})$  for some  $s'_j \mid s_j$ . In a similar way to the proof of the first subcase, consider

$$[K_{n-j+1} : K] = f'_j \cdot \text{ord}_{s'_j}(q^{f'_j \cdot m}) \cdot m. \quad (2.22)$$

Since  $\gcd(f'_j, \text{ord}_{s'_j}(q)) = 1$  by assumption, we have

$$\text{ord}_{s'_j}(q^{f'_j \cdot m}) \cdot m = \frac{m \cdot \text{ord}_{s'_j}(q)}{\gcd(m \cdot f'_j, \text{ord}_{s'_j}(q))} = \frac{m \cdot \text{ord}_{f'_j}(q)}{\gcd(m, \text{ord}_{s'_j}(q))} = \text{lcm}(m, \text{ord}_{s'_j}(q)). \quad (2.23)$$

Similar to the proof of the first subcase, we have  $\gcd(e_{j+1}, s'_j) = 1$  and hence  $e_{j+1} \cdot s'_j \mid d$  and  $\text{ord}_{s'_j \cdot e_{j+1}}(q) = \text{lcm}(m, \text{ord}_{s'_j}(q))$ . Therefore,  $[K_{n-j+1} : K] = f'_j \cdot \text{ord}_{s'_j}(q^{f'_j \cdot m}) \cdot m$  must be a proper divisor of  $r \cdot k$ .

If  $\gcd(s_j, q^{f'_j \cdot m} - 1) > 1$ , then similarly one can show that  $K_{n-j+1}$  contains a field extension, which contains  $K_{n-j}(\delta)$  and has degree relatively prime to  $k$  over  $K_{n-j}(\delta)$ . Continuing in this way, we obtain  $[K_{n-j+1} : K]$  as a proper divisor of  $r \cdot k$ , since  $d_j$  has finitely many divisors.

**Case 2 :** Assume  $\text{ord}_{d_j}(q) \mid m$ . Then  $K_{n-j+1}/K_{n-j}$  is a Kummer extension. Therefore,  $[K_{n-j+1} : K_{n-j}] \mid d_j$ . By assumption,  $[K_{n-j+1} : K_{n-j}]$  is relatively prime to  $k$  and hence  $[K_{n-j+1} : K]$  is a proper divisor of  $r \cdot k$ .

If  $n = 2$ , we get  $[K_2 : K] = \deg Q(x) < r \cdot k$ , a contradiction.

If  $n > 2$ , then one can similarly consider these two cases, where  $m$  is replaced by  $[K_{n-j+i} : K]$  and  $d_i$  is replaced by  $d_{j-i+1}$ , for each  $2 \leq i \leq j$ . One obtains that  $[K_n : K] = \deg Q(x) < r \cdot k$ , again, a contradiction. Therefore, there does not exist  $A \in \mathbb{F}_q^{n+1}$  such that  $r \cdot k \in \Delta_n^{(A,D)}$ .  $\square$

**Theorem 2.3.3** *Let  $n \geq 2$  and suppose the following hold.*

(i)  $r \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1}$ ,  $1 < r$  and

(ii) there exists a prime divisor  $\ell$  of  $r$  such that  $\gcd(\ell, \text{ord}_d(q)) = 1$ , and

(iii)  $\text{ord}_\ell(q) \nmid r \cdot k$ , where  $k \mid \text{ord}_d(q)$ ,  $1 < k$ .

Then  $r \cdot k \in \Delta_n^{(D)}$  but  $r \cdot k \notin \Delta_n^{(A,D)}$ , for any choice of  $A \in \mathbb{F}_q^{n+1}$ .

**Proof:** Clearly,  $r \cdot k \in \Delta_n^{(D)}$ . We now show that there is no  $A \in \mathbb{F}_q^{n+1}$  with  $r \cdot k \in \Delta_n^{(A,D)}$ . Now, suppose the contrary, i.e., there exists  $A \in \mathbb{F}_q^{n+1}$  such that  $r \cdot k \in \Delta_n^{(A,D)}$ . Then,  $F_n^{(A,D)}(x) = F_n(x)$  has an irreducible factor  $Q(x) \in \mathbb{F}_q[x]$ , where  $\deg Q(x) = r \cdot k$ . As in the proof of Theorem 2.3.2, let  $0 \leq j$  be the index satisfying

$$K = K_{n-j-1} \subsetneq K_{n-j} \subseteq \dots \subseteq K_n.$$

Then, in a similar way to the proof of Theorem 2.3.2, we get  $m \mid r \cdot k$ , where  $m = [K_{n-j} : K] = \text{ord}_{e_{j+1}}(q)$  for some  $e_{j+1} \mid d_{j+1}$ . Note that  $m = \text{ord}_{e_{j+1}}(q) \neq r \cdot k$ , since  $\gcd(\ell, \text{ord}_d(q)) = 1$ . Therefore,  $j = 0$  gives  $[K_n : K] = m < r \cdot k$ , a contradiction. Thus  $1 \leq j$  and we consider  $[K_{n-j+1} : K]$ .

Now, we will show that  $[K_{n-j+1} : K_{n-j}]$  is relatively prime to  $\ell$ . As we know,  $K_{n-j+1} = K(\lambda_{j-1})$  and  $\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K_{n-j}$ .

**Case 1 :** Assume  $\text{ord}_{d_j}(q) \nmid m$ . We have two subcases.

If  $\gcd(d_j, q^m - 1) = 1$ , then we get  $[K_{n-j+1} : K_{n-j}]$  equals 1 or  $\text{ord}_{e_j}(q^m) > 1$  for some  $e_j \mid d_j$ , as in the first case of the proof of Theorem 2.3.2. By assumption,  $\gcd(\ell, \text{ord}_{e_j}(q)) = \gcd(\ell, \text{ord}_{e_j}(q^m)) = 1$ . Hence  $[K_{n-j+1} : K_{n-j}]$  is relatively prime to  $\ell$ .

Assume  $\gcd(d_j, q^m - 1) = f_j > 1$ . As  $\text{ord}_{d_j}(q) \neq m$  are not equal by assumption, there exists  $s_j > 1$  such that  $d_j = f_j \cdot s_j$ . Consider the element  $\delta = \lambda_{j-1}^{d_j/f_j} = \lambda_{j-1}^{s_j}$ . Then we have  $K_{n-j} \subseteq K_{n-j}(\delta) \subseteq K_{n-j+1}$  and  $K_{n-j}(\delta)/K_{n-j}$  is a Kummer extension. That is,  $[K_{n-j}(\delta) : K_{n-j}] = f'_j$  for some  $f'_j \mid f_j$ . We have  $\gcd(\ell, f'_j) = 1$ , since  $\text{ord}_\ell(q) \nmid r \cdot k$  by assumption.

Now,  $\lambda_{j-1}$  is a root of the polynomial  $x^{s_j} - \delta \in K_{n-j}(\delta)[x]$ .

If  $\gcd(s_j, q^{f'_j \cdot m} - 1) = 1$ , then as in the proof of the first subcase, there exists  $\mu \in K_{n-j}(\delta)$  such that  $\mu^{s_j} = \delta$  and hence  $[K_{n-j+1} : K_{n-j}(\delta)]$  equals 1 or  $\text{ord}_{s'_j}(q^{f'_j \cdot m})$  for some  $s'_j \mid s_j$ .

By assumption,  $\gcd(\ell, \text{ord}_{s_j}(q^{f_j^m})) = 1$ . That is,  $[K_{n-j+1} : K_{n-j}(\delta)]$  is relatively prime to  $\ell$ .

If  $\gcd(s_j, q^{f_j^m} - 1) > 1$ , then similarly one can show that  $K_{n-j+1}$  contains a field extension, which contains  $K_{n-j}(\delta)$  and has degree relatively prime to  $\ell$  over  $K_{n-j}(\delta)$ .

Continuing in this way, we conclude that  $[K_{n-j+1} : K_{n-j}]$  is relatively prime to  $\ell$ , since  $d_j$  has finitely many divisors.

**Case 2 :** Assume  $\text{ord}_{d_j}(q) \mid m$ . Then  $K_{n-j+1}/K_{n-j}$  is a Kummer extension. Therefore,  $[K_{n-j+1} : K_{n-j}] \mid d_j$ . By assumption,  $[K_{n-j+1} : K_{n-j}]$  is relatively prime to  $\ell$ . If  $n = 2$ , we get  $[K_2 : K] = \deg Q(x)$  is relatively prime to  $\ell$ , a contradiction.

If  $n > 2$ , then one can similarly consider these two cases, where  $m$  is replaced by  $[K_{n-j+i} : K]$  and  $d_i$  is replaced by  $d_{j-i+1}$ , for each  $2 \leq i \leq j$ . One obtains that  $[K_n : K] = \deg Q(x)$  is relatively prime to  $\ell$ , again, a contradiction. Therefore, there is no  $A \in \mathbb{F}_q^{n+1}$  such that  $r \cdot k \in \Delta_n^{(A,D)}$ .  $\square$

**Example 2.3.1** Let  $q = 97$ ,  $n = 2$ ,  $D = (95, 95)$ . Then  $d = 19 \cdot 5$ ,  $\text{ord}_5(97) = 4$ ,  $\text{ord}_{19}(97) = 18$ ,  $\text{ord}_{95}(97) = 36$ , hence

$$\Delta_2^{(D)} = \{1, 4, 12, 18, 20, 36, 60, 76, 90, 180, 228, 342, 380, 684, 1140, 1710, 3420\}.$$

In order to see whether it is possible to eliminate some elements of the set  $\Delta_2^{(D)}$ , we factorize its elements.

$$\begin{array}{llll} 4 = 2 \cdot 2 = \text{ord}_5(q) & 12 = 2^2 \cdot 3 & 18 = 3^2 \cdot 2 = \text{ord}_{19}(q) & 20 = 2^2 \cdot 5 \\ 36 = 2^2 \cdot 3^2 = \text{ord}_{95}(q) & 60 = 2^2 \cdot 5 \cdot 3 & 76 = 19 \cdot 4 & 90 = 3^2 \cdot 5 \cdot 2 \\ 180 = 3^2 \cdot 2^2 \cdot 5 & 228 = 2^2 \cdot 19 \cdot 3 & 342 = 3^2 \cdot 2 \cdot 19 & 380 = 2^2 \cdot 19 \cdot 5 \\ 684 = 3^2 \cdot 2^2 \cdot 19 & 1140 = 2^2 \cdot 19 \cdot 5 \cdot 3 & 1710 = 3^2 \cdot 19 \cdot 5 \cdot 2 & 3420 = 3^2 \cdot 19 \cdot 5 \cdot 2 \end{array}$$

Theorem 2.3.2 implies that

- (i) 12 with  $k = 12$ ,  $r = 1$ ,
- (ii) 60 with  $k = 12$ ,  $r = 5$ ,
- (iii) 228 with  $k = 12$ ,  $r = 19$ ,
- (iv) 1140 with  $k = 12$ ,  $r = 95$ ,

are not in  $\Delta_2^{(A,D)}$  for any choice of  $A \in \mathbb{F}_q^3$ . Theorem 2.3.3 implies that

(i) 76 with  $k = 4$ ,  $r = 19$ ,

(ii) 90 with  $k = 18$ ,  $r = 5$ ,

(iii) 380 with  $k = 4$ ,  $r = 95$ ,

(iv) 1710 with  $k = 18$ ,  $r = 95$ ,

are not in  $\Delta_2^{(A,D)}$  for any choice of  $A \in \mathbb{F}_q^3$ . Therefore, we obtain the set

$$\bar{\Delta}_2^{(D)} = \{1, 4, 18, 20, 36, 180, 342, 684, 3420\}.$$

Calculations by MAGMA show that  $\Delta_2^{(A,D)}$  is one of the following, as  $A$  runs through  $\mathbb{F}_q^3$ .

$$\begin{aligned} & \{1\}, \{1, 4, 18, 36\}, \{1, 4, 18, 36, 342, 684\}, \{1, 4, 18, 20, 36, 180, 684\}, \\ & \{1, 20, 180, 342, 684, 3420\}, \{1, 4, 18, 36, 180, 342, 684\}, \{1, 4, 18, 20, 36, 180, 3420\}, \\ & \{1, 4, 18, 36, 342, 684, 3420\}, \{1, 4, 18, 20, 36, 180, 684, 3420\}, \{1, 4, 18, 20, 36, 180, 342, 684\}, \\ & \{1, 4, 18, 36, 180, 342, 684, 3420\}, \{1, 4, 18, 20, 36, 180, 342, 684, 3420\}. \end{aligned}$$

Therefore, for every  $m \in \bar{\Delta}_2^{(D)}$ , there exists  $A \in \mathbb{F}_{97}^3$  with  $m \in \Delta_2^{(A,D)}$ .

**Remark 2.3.1** Let  $r \cdot k$  be an arbitrary element of  $\Delta_n^{(D)}$ . Using the notation in the proofs of Theorem 2.3.2 and Theorem 2.3.3, we need to assume the following, in order to eliminate  $r \cdot k$  from the set  $\Delta_n^{(D)}$ .

(i)  $\text{ord}_e(q) \neq r \cdot k$  for all  $e \mid d$ .

(ii) If  $f \mid d$  such that  $\text{ord}_f(q) \mid m_1$ , for some  $m_1 \mid r \cdot k$ , then  $\text{gcd}(f, r \cdot k) = 1$ , so that  $f'_j \cdot m_1$ , where  $f'_j$  is given by (2.21), is not equal to  $r \cdot k$ .

(iii) If  $m_1 \mid r \cdot k$ ,  $\text{ord}_f(q) \mid m_1$  for some  $f \mid d$  and  $\text{ord}_s(q^{f \cdot m_1}) \mid r \cdot k$  for some  $s \mid d$ , then  $\text{gcd}(f, \text{ord}_s(q)) = 1$ , so that  $\text{gcd}(f'_j, \text{ord}_{s'_j}(q)) = 1$ , in (2.22), and hence we obtain (2.23).

**Remark 2.3.2** Observe that there are three different cases in the proofs of Theorem 2.3.2 and Theorem 2.3.3. But, there may exist  $D$  such that some of these cases do not

occur. Suppose we know  $D$  explicitly and orders of  $q$  modulo  $d_i$  for all  $1 \leq i \leq n$ . Then it may be possible to eliminate further elements of the set  $\Delta_n^{(D)}$  of the form  $r \cdot k$ , where  $r \mid d_1 \cdot d_2 \cdot \dots \cdot d_{n-1}$  and  $k \mid \text{ord}_d(q)$ , although conditions of these theorems or conditions given by Remark 2.3.1 are not satisfied. We have the following consequence of the proofs of Theorem 2.3.2 and Theorem 2.3.3.

**Algorithm 2.3.1** Let  $m \in \Delta_n^{(D)}$  and  $E = \{d_j : \text{ord}_{e_j}(q) \mid m \text{ for some } e_j \mid d_j, 1 \leq j \leq n\}$ . For each  $d_j \in E$ , let  $M_j = \{m_j : m_j = \text{ord}_{e_j}(q) \mid m \text{ for some } e_j \mid d_j\}$ . If  $1 < j$ , then consider  $\text{gcd}(d_{j-i}, q^{m_{j-i+1}}) = h_{j-i}$ , for  $1 \leq i \leq j-1$ ,

(i) If  $h_{j-i} = 1$ , set  $m_{j-i} = t \cdot m_{j-i+1}$  for some fixed  $t$ , where  $t \in \{t : t = \text{ord}_e(q^{m_{j-i+1}}) \text{ for some } e \mid d_{j-i}\} \cup \{1\}$

(ii) If  $h_{j-i} = d_{j-i}$ , then set  $m_{j-i} = e \cdot m_{j-i+1}$  for some fixed  $e \mid d_{j-i}$ .

(iii) If  $1 < h_{j-i} < d_{j-i}$ , let  $f_0 = h_{j-i}$ ,  $u_0 = s_0 \cdot m_{j-i+1}$ , for some fixed  $s_0 \mid f_0$ ,  $l_0 = d_{j-i}$ . Let  $0 < k$ ,  $l_{k+1} = \frac{l_k}{f_k}$ , where  $f_k = \text{gcd}(l_k, q^{u_{k-1}} - 1)$  with  $u_k = s_k \cdot u_{k-1}$ , for some fixed  $s_k \mid f_k$ .

If  $f_k = 1$  for some  $1 < k$ , then set  $m_{j-i+i} = u_{k-1} \cdot t$ , for some  $t \in \{t : t = \text{ord}_e(q^{u_{k-1}}) \text{ for some } e \mid l_k\} \cup \{1\}$ .

If  $f_k = l_k$  for some  $1 < k$ , then set  $m_{j-i} = u_k$ .

If  $m_1 \neq m$ , for all possible values for  $m_1$ , then  $m \notin \Delta_n^{(A,D)}$ , for any choice of  $A \in \mathbb{F}_q^{n+1}$ .

**Proof:** We follow the steps of the proofs of Theorem 2.3.2 and Theorem 2.3.3. Note that in part (iii),  $f_k$  equals 1 or  $l_k$ , for some  $1 < k$  since  $d_{j-i}$  has finitely many divisors for all  $1 \leq i \leq j-1$ . □

## 2.4 More on the set $\Delta_n^{(A,D)}$

Our next result shows that there is some symmetry among the degrees of the irreducible factors of  $F_n(x)$ .

**Theorem 2.4.1** [51] Let  $Q(x)$  be an irreducible factor of  $F_n^{(A,D)}(x) = F_n(x)$  for some fixed  $A \in \mathbb{F}_q^{n+1}$ , satisfying  $\deg Q(x) = s > 1$ . Suppose  $e \mid d_1$ ,  $1 < e$  and  $m = \text{ord}_e(q)$ .

Then there exists an irreducible factor  $R(x)$  of  $F_n(x)$  satisfying

$$\deg R(x) = \frac{\text{lcm}(m, s)}{f},$$

for some integer  $f \mid \gcd(m, s)$ .

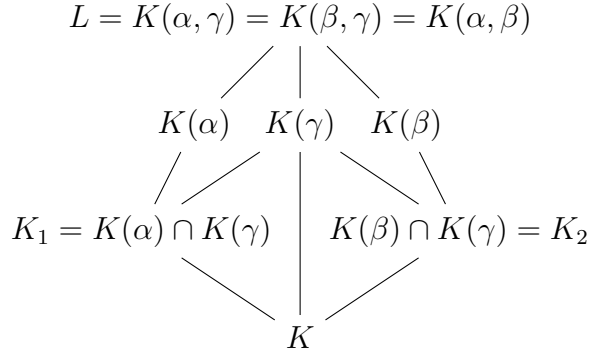
In order to prove Theorem 2.4.1, we need the following lemma.

**Lemma 2.4.2** *Let  $\alpha, \beta, \gamma$  be non-zero elements of  $\bar{K} = \bar{\mathbb{F}}_q$  satisfying  $K(\alpha, \beta, \gamma) = K(\alpha, \gamma) = K(\beta, \gamma) = K(\alpha, \beta)$ . Let  $[K(\alpha) : K] = s$ ,  $[K(\beta) : K] = m$ . Then*

$$[K(\gamma) : K] = \frac{\text{lcm}(m, s)}{f},$$

for some  $f \mid \gcd(m, s)$ .

**Proof:** Set  $L := K(\alpha, \beta, \gamma)$ ,  $K_1 := K(\alpha) \cap K(\gamma)$ ,  $K_2 := K(\beta) \cap K(\gamma)$ ,  $g := \gcd(m, s)$ . Consider the following diagram.



Using Lemma 1.4.2 (ii) on the left hand side of the diagram, we get

$$[L : K(\gamma)] = [K(\alpha) : K_1] = \frac{s}{g} = \frac{\text{lcm}(m, s)}{m} \quad (2.24)$$

If we use Lemma 1.4.2 (ii) on the right hand side of the diagram, we get

$$[L : K(\beta)] = [K(\gamma) : K_2] = \frac{\text{lcm}(m, s)}{s} = \frac{m}{g}. \quad (2.25)$$

If  $[K_1 : K] = u$  and  $[K_2 : K] = v$  for some  $u \mid s$ ,  $v \mid m$ , then combining (2.24) and (2.25), we obtain

$$[K(\gamma) : K] = \frac{s \cdot u}{g} = \frac{m \cdot v}{g}. \quad (2.26)$$

Since  $\gcd(s/g, m/g) = 1$ , Equation (2.26) implies

$$u = k \cdot \frac{m}{g}, \quad v = k \cdot \frac{s}{g}, \quad (2.27)$$



for some  $k \in \mathbb{Z}$ , which yields  $[K(\gamma) : K] = \frac{k \cdot m \cdot s}{g^2}$ . Now we will show that  $k \mid g$ . Using (2.27) we get

$$k = \frac{g \cdot u}{m} = \frac{g \cdot v}{s}. \quad (2.28)$$

Since  $u \mid s$  and  $v \mid m$ , there exist integers  $k_1$  and  $k_2$  such that  $s = k_1 \cdot u$  and  $m = k_2 \cdot v$ . Substituting these into Equation (2.28), we obtain

$$k = \frac{g}{k_2} = \frac{g}{k_1},$$

which shows that  $k \mid g$ . By all above we get

$$[K(\gamma) : K] = \frac{m \cdot s}{g \cdot f} = \frac{\text{lcm}(m, s)}{f},$$

for some  $f \mid g$ . □

**Proof of Theorem 2.4.1 :** Let  $\lambda \in \bar{K}$  be a root of  $F_n^{(A,D)}(x) = F_n(x)$ . Suppose that  $[K(\lambda) : K] = s$ ,  $1 < s$ . We firstly show that the following holds.

$$(x + a_0)^{d_1} - (\lambda + a_0)^{d_1} \mid F_n(x) \quad (2.29)$$

To show this, we make a change of variable  $y = (x + a_0)^{d_1}$ . Then

$$F_n(x) = S(y) = (\dots (y + a_1)^{d_2} + \dots + a_{n-1})^{d_n} + a_n.$$

Since  $F_n(\lambda) = 0$ ,  $S((\lambda + a_0)^{d_1}) = 0$ , thus  $y - (\lambda + a_0)^{d_1} \mid S(y)$ . Hence we obtain (2.29). By this divisibility relation, we conclude that  $F(\theta) = 0$ , where  $\theta = \zeta(\lambda + a_0) - a_0$ , and  $\zeta$  is a  $d_1$ -th root of unity. Since we assumed that  $1 < s$ ,  $\lambda + a_0 \neq 0$  and hence we get  $K(\zeta, \lambda) = K(\zeta, \theta) = K(\lambda, \theta)$ . If we let  $\alpha = \lambda + a_0$ ,  $\beta = \zeta$ ,  $\gamma = \theta$  in Lemma 2.4.2, we conclude that  $F_n(x)$  has an irreducible factor  $R(x) \in \mathbb{F}_q[x]$  satisfying

$$\deg R(x) = \frac{\text{lcm}(m, s)}{f},$$

where  $m = \text{ord}_{d_1}(q)$  and  $f$  is some divisor of  $\text{gcd}(m, s)$ .

**Corollary 2.4.3** [51] *Let  $A \in \mathbb{F}_q^{n+1}$  such that  $F_n^{(A,D)}(-a_0) = F_n(-a_0) \neq 0$ . Then  $\text{ord}_e(q) \in \Delta_n^{(A,D)}$  for every  $e \mid d_1$ ,  $1 < e$ .*

**Proof:** As  $F_n(x)$  is a permutation polynomial, it has a unique root in  $\mathbb{F}_q$ , say  $\lambda$ . By assumption  $\lambda \neq -a_0$  and hence  $\lambda + a_0 \neq 0$ . Therefore, as in the proof of Theorem 2.4.1, if we take  $\zeta$  as a  $d_1$ -th root of unity,  $\theta = \zeta(\lambda + a_0) - a_0$ , then we conclude that  $\text{ord}_e(q) \in \Delta_n^{(A,D)}$  for all  $e \mid d_1$ ,  $1 < e$ . □

**Example 2.4.1** Let  $n = 2$ ,  $q = 59$ ,  $D = (357, 357)$  and hence  $d = 17 \cdot 7 \cdot 3$ .  $\text{ord}_3(q) = 2$ ,  $\text{ord}_7(q) = 6$ ,  $\text{ord}_{17}(q) = 8$ . Using Theorem 2.1.1 and Theorem 2.1.2, we see that

$$\Delta_2^{(D)} = \{1, 2, 4, 6, 8, 12, 14, 18, 24, 28, 34, 36, 42, 56, 68, 72, 84, 102, 126, 136, 168, 204, \\ 238, 252, 306, 408, 476, 504, 612, 714, 952, 1224, 1428, 2142, 2856, 4284, 8568\}$$

In order to see whether it is possible to eliminate some of the elements of  $\Delta_2^{(D)}$ , we factorize its elements.

$2 = 2$	$4 = 2 \cdot 2$	$6 = 3 \cdot 2 = \text{ord}_{21}(q)$
$8 = 2^3 = \text{ord}_{51}(q)$	$12 = 2^2 \cdot 3$	$14 = 7 \cdot 2$
$18 = 3^2 \cdot 2$	$24 = \text{ord}_{357}(q) = \text{ord}_{119}(q) = 2^3 \cdot 3$	$28 = 2^2 \cdot 7$
$34 = 17 \cdot 2$	$36 = 2^2 \cdot 3^2$	$42 = 7 \cdot 3 \cdot 2$
$56 = 2^3 \cdot 7$	$68 = 2^2 \cdot 17$	$72 = 2^3 \cdot 3^2$
$84 = 2^2 \cdot 7 \cdot 3$	$102 = 17 \cdot 3 \cdot 2$	$126 = 3^2 \cdot 7 \cdot 2$
$136 = 2^3 \cdot 17$	$168 = 2^3 \cdot 7 \cdot 3$	$204 = 2^2 \cdot 17 \cdot 3$
$238 = 17 \cdot 7 \cdot 2$	$252 = 3^2 \cdot 2^2 \cdot 7$	$306 = 3^2 \cdot 17 \cdot 2$
$408 = 2^3 \cdot 17 \cdot 3$	$476 = 2^2 \cdot 17 \cdot 7$	$504 = 2^3 \cdot 3^2 \cdot 7$
$612 = 3^2 \cdot 3^2 \cdot 17$	$714 = 17 \cdot 7 \cdot 3 \cdot 2$	$952 = 2^3 \cdot 17 \cdot 7$
$1224 = 2^3 \cdot 3^2 \cdot 17$	$1428 = 2^2 \cdot 17 \cdot 7 \cdot 3$	$2142 = 3^2 \cdot 17 \cdot 7 \cdot 2$
$2856 = 2^3 \cdot 17 \cdot 7 \cdot 3$	$4284 = 3^2 \cdot 2^2 \cdot 17 \cdot 7$	$8568 = 2^3 \cdot 3^2 \cdot 17 \cdot 7$

Theorem 2.3.3 implies that

$14$  with  $r = 7$ ,  $k = 2$ ,

$28$  with  $r = 7$ ,  $k = 4$ ,

$34$  with  $r = 17$ ,  $k = 2$ ,

$56$  with  $r = 7$ ,  $k = 8$ ,

$68$  with  $r = 17$ ,  $k = 4$ ,

$84$  with  $r = 7$ ,  $k = 12$ , or  $r = 21$ ,  $k = 4$ ,

102 with  $r = 17, k = 6$ , or  $r = 51, k = 2$ ,

204 with  $r = 17, k = 12$ , or  $r = 51, k = 4$ ,

238 with  $r = 119, k = 2$ ,

306 with  $r = 51, k = 6$ ,

476 with  $r = 119, k = 4$ ,

612 with  $r = 51, k = 12$ ,

714 with  $r = 119, k = 6$ , or  $r = 357, k = 2$ ,

952 with  $r = 119, k = 8$ ,

1428 with  $r = 119, k = 12$ , or  $r = 357, k = 4$ ,

2856 with  $r = 357, k = 8$ ,

4824 with  $r = 357, k = 12$ ,

are not in  $\Delta_2^{(A,D)}$  for any choice of  $A \in \mathbb{F}_q^3$ . In addition, since we know  $D$  explicitly and all of the orders of  $q$  modulo  $d_i$ , for  $1 \leq i \leq n$ , by Algorithm 2.3.1, we eliminate 4, 12, 36, 252 from the set  $\Delta_2^{(D)}$ . Therefore, our set of possible degrees,  $\Delta_2^{(D)}$ , is reduced to the following set:

$$\bar{\Delta}_2^{(D)} = \{1, 2, 6, 8, 18, 24, 42, 72, 126, 136, 168, 408, 504, 1224, 2856, 8568\}$$

Calculations by MAGMA show that for each  $m \in \bar{\Delta}_2^{(D)}$ , there exists  $A \in \mathbb{F}_q^3$  such that  $m \in \Delta_2^{(A,D)}$ . Now let us show how one uses Theorem 2.4.1 to see which elements of the set lie together in  $\Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$ . Using the notation of Theorem 2.4.1, we have  $m = 24$ .

(i) If  $s = 2$ , we have

$$\frac{\text{lcm}(m, s)}{f} = \frac{\text{lcm}(2, 24)}{f}, \quad f \mid \text{gcd}(2, 24)$$

Hence, if 2 is in  $\Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$ , then 12 or 24 is also in  $\Delta_2^{(A,D)}$ . Since we know that 12 cannot be in  $\Delta_2^{(A,D)}$ , we get  $24 \in \Delta_2^{(A,D)}$ . Hence, using

Theorem 2.4.1, we find a new element of  $\Delta_2^{(A,D)}$  without referring to explicit factorization of  $F_2^{(A,D)}(x)$ .

- (ii) If we take  $s = 6$ , similarly we obtain 4, 8, 12 or 24 is in  $\Delta_2^{(A,D)}$ . Only 8 and 24 is in the reduced form  $\bar{\Delta}_2^{(D)}$ . Calculations show that if  $6 \in \Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$ , then  $24 \in \Delta_2^{(A,D)}$ , but  $8 \notin \Delta_2^{(A,D)}$ . Hence, not every integer, which is obtained by using Theorem 2.4.1 lies in  $\Delta_2^{(A,D)}$ , even though it is an element of the reduced form  $\bar{\Delta}_2^{(D)}$ .
- (iii) If we take  $s = 8$ , then we obtain 6, 12, 24. Only 6 and 24 are in the reduced form  $\bar{\Delta}_2^{(D)}$ . Calculations show that if  $8 \in \Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$ ,  $6, 24 \in \Delta_2^{(A,D)}$ . This shows that every integer obtained by Theorem 2.4.1, which lie in  $\bar{\Delta}_2^{(D)}$ , may also be an element of  $\Delta_2^{(A,D)}$ .
- (iv) If we take  $s = 24$ , then we obtain 1, 2, 3, 4, 6, 8, 12, 24. Only 1, 2, 6, 8 in the reduced form  $\bar{\Delta}_2^{(D)}$ . Calculations show that if  $24 \in \Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$ , then  $6 \in \Delta_2^{(A,D)}$ . Note that if  $6 \in \Delta_2^{(A,D)}$ , then  $24 \in \Delta_2^{(A,D)}$  by (ii). The same is true for 8 by (iii). On the other hand, the converse does not hold, i.e., 8 is an integer which is obtained by using Theorem 2.4.1 and lies in the reduced form  $\bar{\Delta}_2^{(D)}$ , however  $8 \notin \Delta_2^{(A,D)}$  for any  $A$  satisfying  $24 \in \Delta_2^{(A,D)}$ .
- (v) If we take  $s = 42$ , then we obtain 28, 56, 168. Only 168 is in the reduced form of  $\Delta_2^{(D)}$ . Hence, using Theorem 2.4.1, we find a new element of  $\Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$  without referring to the explicit factorization of  $F_2^{(A,D)}(x)$ .
- (vi) If we take  $s = 168$ , then we obtain 7, 14, 21, 28, 56, 84, 168. Only 168 lies in the reduced form of  $\Delta_2^{(D)}$ . Hence there may be integers in the set  $\Delta_2^{(A,D)}$  for some fixed  $A \in \mathbb{F}_q^3$  such that, Theorem 2.4.1, does not yield a new element of  $\Delta_2^{(A,D)}$ .

Although Theorem 2.4.1 gives some degrees, which occur together in the explicit factorization, we can not obtain the whole set  $\Delta_n^{(A,D)}$ , by using a few known elements

of  $\Delta_n^{(A,D)}$ , as we see in Example 2.4.1.

Therefore, for an integer  $m$  in the reduced form  $\bar{\Delta}_2^{(D)}$ , one of the main problems is to find  $A \in \mathbb{F}_q^{n+1}$ , such that  $m \in \Delta_n^{(A,D)}$ , for  $n \geq 2$ . Note that Corollary 2.4.3 guarantees the existence of  $A \in \mathbb{F}_q^{n+1}$  such that  $m = \text{ord}_e(q) \in \Delta_n^{(A,D)}$ , for every divisor  $e \mid d_1$ ,  $1 < e$ . In order to see this, fix some  $B = (b_0, b_1, \dots, b_n) \in \mathbb{F}_q^{n+1}$ . If  $F_n^{(B,D)}(-b_0) = 0$ , then consider  $A = (a_0, a_1, \dots, a_n) \in \mathbb{F}_q^{n+1}$ , where  $a_i = b_i$  for  $0 \leq i \leq n-1$ ,  $a_n = b_n + 1$ . In this case

$$F_n^{(A,D)}(-a_0) = F_n^{(B,D)}(-b_0) + 1 \neq 0.$$

Hence by Corollary 2.4.3,  $\text{ord}_e(q) \in \Delta_n^{(A,D)}$ , for every  $e \mid d_1$ ,  $1 < e$ .

Now, let  $n = 2$ ,  $m \in \Delta_2^{(D)}$ . Now, we will find some conditions on  $q$  and  $D$ , which imply the existence of  $A \in \mathbb{F}_q^3$  satisfying  $m \in \Delta_2^{(A,D)}$ . I would like to express my gratitude to Giorgos Kapetanakis for his valuable comments on this part.

If  $m = \text{ord}_e(q)$  for some  $e \mid d_1 \cdot d_2$ ,  $1 < e$  and  $A = (0, 0, a_2)$ , where  $a_2 \in \mathbb{F}_q^*$ , then clearly  $m \in \Delta_2^{(A,D)}$ . For the remaining elements  $m$  of  $\Delta_2^{(D)}$ , we now observe that, in order to show the existence of  $A \in \mathbb{F}_q^3$  satisfying  $m \in \Delta_2^{(D)}$ , one can assume without loss of generality that  $A = (0, 1, a_2)$ , with  $a_2 \in \mathbb{F}_q^*$ .

**Lemma 2.4.4** *If  $A = (a_0, a_1, a_2) \in \mathbb{F}_q^3$ , where  $a_1 \neq 0$ , then there exists  $B = (0, 1, b_2) \in \mathbb{F}_q^3$  and  $c \in \mathbb{F}_q^*$  such that*

$$F_2^{(A,D)}(x) = c^{d_1 \cdot d_2} \cdot F_2^{(B,D)}\left(\frac{x + a_0}{c}\right). \quad (2.30)$$

**Proof:** Let  $c$  be the unique element of  $\mathbb{F}_q^*$  satisfying  $c^{d_1} = a_1$ . Let  $b_2$  be the unique element of  $\mathbb{F}_q$  such that  $b_2 \cdot c^{d_1 \cdot d_2} = a_2$ . Then

$$F_2^{(B,D)}\left(\frac{x + a_0}{c}\right) = c^{-(d_1 \cdot d_2)}((x + a_0)^{d_1} + c^{d_1})^{d_2} + b_2 \cdot c^{d_1 \cdot d_2}.$$

That is,

$$\begin{aligned} F_2^{(B,D)}\left(\frac{x + a_0}{c}\right) &= c^{-(d_1 \cdot d_2)}((x + a_0)^{d_1} + a_1)^{d_2} + a_2 \\ &= c^{-(d_1 \cdot d_2)} F_2^{(A,D)}(x), \end{aligned}$$

hence the result follows. □

**Remark 2.4.1** *If  $A \in \mathbb{F}_q^3$  and  $a_1 = 0$ , then  $F_2^{(A,D)}(x) = (x + a_0)^{d_1 \cdot d_2} + a_2$ , and hence  $\Delta_2^{(A,D)} = \{1\} \cup \{\text{ord}_e(q) : e \mid d_1 \cdot d_2\}$ , when  $a_2 \neq 0$ , and  $\Delta_2^{(A,D)} = \{1\}$ , when  $a_2 = 0$ .*

If  $A \in \mathbb{F}_q^3$ , where  $a_1 \neq 0$ , then by Lemma 2.4.4, there exists  $B = (0, 1, b_2) \in \mathbb{F}_q^3$  such that Equation (2.30) is satisfied. That is, if

$$F_2^{(B,D)}(x) = R_1(x) \cdot R_2(x) \cdot \dots \cdot R_m(x),$$

where  $R_1, \dots, R_m$  are irreducible over  $\mathbb{F}_q$ , then

$$F_2^{(A,D)}(x) = c^{d_1 \cdot d_2} \cdot R_1\left(\frac{x + a_0}{c}\right) \cdot R_2\left(\frac{x + a_0}{c}\right) \cdot \dots \cdot R_m\left(\frac{x + a_0}{c}\right),$$

where  $c$  is the unique element of  $\mathbb{F}_q^*$  satisfying  $c^{d_1} = a_1$ . That is, we may assume without loss of generality that  $A = (0, 1, a_2)$ .

We consider the set

$$\{r \cdot k : r \mid d_1, k \mid \text{ord}_d(q), r \cdot k \in \Delta_2^{(D)}\}. \quad (2.31)$$

By Theorem 2.3.2 and Algorithm 2.3.1, we know that if  $\gcd(d, \text{ord}_d(q)) = 1$  and

- (i)  $k \neq \text{ord}_e(q)$  for all  $e \mid d$  or,
- (ii)  $\text{ord}_r(q) \nmid k$ , when  $1 < r$ ,

then  $r \cdot k \notin \Delta_2^{(A,D)}$ , for any choice of  $A \in \mathbb{F}_q^3$ . Therefore, we assume  $k = \text{ord}_e(q)$  for some  $e \mid d$  and if  $1 < r$ , then  $\text{ord}_r(q) \mid k = \text{ord}_e(q)$ . In order to see whether there exists  $A \in \mathbb{F}_q^3$  satisfying  $r \cdot k \in \Delta_2^{(A,D)}$ , we assume  $A = (0, 1, a_2) \in \mathbb{F}_q^3$ , with  $a_2 \neq 0$ . The following lemma characterizes the roots of  $F_2(x)$ .

**Lemma 2.4.5** *Let  $A = (0, 1, a_2) \in \mathbb{F}_q^3$  with  $a_2 \neq 0$ . Then the set of zeros of  $F_2^{(A,D)}(x) = F_2(x)$  is equal to the following set:*

$$C = \{\lambda \in \bar{\mathbb{F}}_q : \lambda^{d_1} - (\alpha - 1) = 0 \text{ where } \alpha^{d_2} + a_2 = 0\}. \quad (2.32)$$

**Proof:** If  $\lambda \in C$ , then  $F_2(\lambda) = (\lambda^{d_1} + 1)^{d_2} + a_2 = \alpha^{d_2} + a_2 = 0$ . This shows that every element of the set  $C$  is a root of  $F_2(x)$ . Now, suppose  $a_2 \neq -1$ . Since  $\gcd(d_1, q) = 1$  and  $\alpha \neq 1$ , the polynomial  $x^{d_1} - (\alpha - 1)$  has  $d_1$  distinct zeros in  $\bar{\mathbb{F}}_q$ , for each zero  $\alpha$  of the polynomial  $x^{d_2} + a_2$ . Since  $\gcd(d_2, q) = 1$  and  $a_2 \neq 0$ , there are  $d_2$  distinct zeros of the polynomial  $x^{d_2} + a_2$  in  $\bar{\mathbb{F}}_q$ . Therefore, the set  $C$  has  $d_1 \cdot d_2$  elements. Now, we will show that  $\gcd(F_2, F_2') = 1$ , so that  $F_2(x)$  is separable. The formal derivative of  $F_2(x)$  is

$$F_2'(x) = d_1 \cdot d_2 \cdot (x^{d_1} + 1)^{d_2-1} \cdot x^{d_1-1}. \quad (2.33)$$

Since

$$F_2(x) = (x^{d_1} + 1)^{d_2} + a_2, \quad a_2 \neq 0, \quad (2.34)$$

we have  $\gcd(F_2(x), F_2'(x)) > 1$  if and only if 0 is a root of  $F_2(x)$ . As  $a_2 \neq -1$ , we have  $F_2(0) \neq 0$ . Therefore,  $F_2(x)$  is a separable polynomial over  $\mathbb{F}_q$  of degree  $d_1 \cdot d_2$ , hence it has  $d_1 \cdot d_2$  distinct roots. Therefore, the set of zeros of  $F_2(x)$  is equal to  $C$ .

If  $a_2 = -1$ , then clearly,  $C$  has  $d_1 \cdot (d_2 - 1) + 1$  distinct elements, and  $F_2(0) = F_2(-a_0) = 0$ . By (2.29), we see that 0 is a root of  $F_2(x)$  with multiplicity at least  $d_1$ . Therefore, by (2.33) and (2.34), 0 is the only root which has multiplicity greater than 1, and the multiplicity is  $d_1$ . Hence,  $F_2(x)$  has  $d_1 \cdot (d_2 - 1) + 1$  distinct roots and the set of zeros of  $F_2(x)$  is equal to  $C$ .  $\square$

Lemma 2.4.5 yields that in order to show the existence of  $A \in \mathbb{F}_q^3$  satisfying  $r \cdot k \in \Delta_2^{(A,D)}$ , where  $r \cdot k$  is given by (2.31), we have to show the existence of  $\alpha - 1 = \xi$  satisfying the following conditions.

(i)  $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = k$ ,

(ii)  $(1 + \xi)^e \in \mathbb{F}_q^*$  for some  $e \mid d_2$ ,

(iii) There exists  $\lambda \in \overline{\mathbb{F}}_q$  such that  $\lambda^{d_1} = \xi$  and  $[\mathbb{F}_{q^k}(\lambda) : \mathbb{F}_{q^k}] = r$ .

Note that when  $(1 + \xi)^e = 1$ , for some  $e \mid d_2$ , then it is possible that  $\xi = 0$ , therefore we also assume that  $(1 + \xi)^e \neq 1$  for all  $e \mid d_2$ . In the following lemma,  $N_{q^k/q}(\eta)$  denotes the norm of  $\eta \in \mathbb{F}_{q^k}$  over  $\mathbb{F}_q$ , and if  $\eta \in \mathbb{F}_{q^k}^*$ ,  $\text{ord}(\eta)$  denotes the order of  $\eta$  in the cyclic group  $\mathbb{F}_{q^k}^*$ .

**Lemma 2.4.6** *Let  $k \geq 2$ ,  $q > 2$ , and  $t \mid q^k - 1$ ,  $2 < t$ ,  $e \mid q^k - 1$ . Then the following statements are equivalent.*

(i) *There exists  $\xi \in \mathbb{F}_{q^k}^*$  such that  $\text{ord}(\xi) = t$  and  $(1 + \xi)^e \in \mathbb{F}_q^* \setminus \{1\}$ .*

(ii) *There exists  $\eta \in \mathbb{F}_{q^k}^*$ , such that  $N_{q^k/q}(\eta) \neq 1$  and  $\text{ord}(\eta^s - 1) = t$ , where  $s = \frac{q^k - 1}{e \cdot (q - 1)}$ .*

**Proof:** Suppose that there exists an element  $\xi \in \mathbb{F}_{q^k}^*$ ,  $\text{ord}(\xi) = t$ , where  $t > 2$  and  $(1 + \xi)^e \in \mathbb{F}_q^* \setminus \{1\}$ . Then there exists an element,  $\eta \in \mathbb{F}_{q^k}$  such that  $N_{q^k/q}(\eta) = (1 + \xi)^e \neq 0, 1$ , since  $N_{q^k/q}$  is onto. Hence  $\eta \in \mathbb{F}_{q^k}^*$ . Conversely, suppose that there

exists  $\eta \in \mathbb{F}_{q^k}^*$  such that  $N_{q^k/q}(\eta) \neq 1$  and  $\text{ord}(\eta^s - 1) = t > 2$ , where  $s = \frac{q^k-1}{e \cdot (q-1)}$ . Let  $\eta^s - 1 = \xi$ . Substituting  $s$ , we get  $\eta^{\frac{q^k-1}{e \cdot (q-1)}} = \xi + 1$ . Therefore, we get

$$N_{q^k/q}(\eta) = \eta^{\frac{q^k-1}{q-1}} = (1 + \xi)^e \in \mathbb{F}_q^* \setminus \{1\},$$

by assumption and hence the result follows.  $\square$

**Remark 2.4.2** We note that the characteristic function for elements  $x \in \mathbb{F}_{q^k}^*$  with  $N_{q^k/q}(x) = \beta$ , where  $\beta \in \mathbb{F}_q^*$  is given by

$$\Omega_\beta(x) = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \bar{\chi}(\beta) \tilde{\chi}(x), \quad (2.35)$$

where the sum runs through the multiplicative characters of  $\mathbb{F}_q$ ,  $\bar{\chi}$  stands for the inverse of  $\chi$  and  $\tilde{\chi}$  for the lift of  $\chi$  to a multiplicative character of  $\mathbb{F}_{q^k}$ , that is, for  $x \in \mathbb{F}_{q^k}$ ,  $\tilde{\chi}(x) = \chi(N_{q^k/q}(x))$ . This follows immediately by Corollary 1.4.6 (ii) implying that

$$\Omega_\beta(x) = \begin{cases} 1, & \text{if } N_{q^k/q}(x) = \beta, \\ 0, & \text{otherwise.} \end{cases} \quad (2.36)$$

**Lemma 2.4.7** Let  $2 \leq k$ ,  $2 < q$ ,  $t \mid q^k - 1$ ,  $2 < t$ ,  $e \mid q^k - 1$ ,  $l = \frac{q^k-1}{t}$ . If

$$e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}},$$

then there exists an element  $\xi \in \mathbb{F}_{q^k}^*$ , where  $\text{ord}(\xi) = t$  and  $(1 + \xi)^e \in \mathbb{F}_q^* \setminus \{1\}$ .

**Proof:** Lemma 2.4.6 implies that to find an element  $\xi \in \mathbb{F}_{q^k}^*$  with the desired properties, it suffices to find some  $\eta \in \mathbb{F}_{q^k}^*$ , with  $N_{q^k/q}(\eta) = \beta \in \mathbb{F}_q^* \setminus \{1\}$  and  $\text{ord}(\eta^s - 1) = t$ , where  $s = \frac{q^k-1}{e \cdot (q-1)}$ . We note that such  $\beta$  exists since  $q > 2$ . Now, let  $l = \frac{q^k-1}{t}$ . The characteristic function for elements of  $\mathbb{F}_{q^k}^*$ , of order  $t$  is

$$\omega(x) = \frac{\phi(t)}{q^k - 1} \sum_{u \mid t} \frac{\mu(u)}{\phi(u)} \sum_{\substack{v \mid l \\ \gcd(u, l/v)=1}} \sum_{\text{ord}(\chi)=u \cdot v} \chi(x),$$

see Lemma 1.4.11. By Remark 2.4.2, the characteristic function for elements  $x \in \mathbb{F}_{q^k}^*$  with  $N_{q^k/q}(x) = \beta$ , where  $\beta \in \mathbb{F}_q^*$  is given by (2.35).

Fix some  $\beta \in \mathbb{F}_q^* \setminus \{1\}$ . Let  $N_t$  be the number of elements of  $\eta \in \mathbb{F}_{q^k}^*$ , such that  $\text{ord}(\eta^s - 1) = t$  and  $N_{q^k/q}(\eta) = \beta$ . From the above, it follows that

$$N_t = \sum_{\substack{x \in \mathbb{F}_{q^k}^* \\ x, x^s - 1 \neq 0}} \omega(x^s - 1) \Omega_\beta(x).$$



Note that  $x = 0$  implies that  $x^s - 1 = -1$ , which has order  $2 \neq t$ . Also, if  $x^s - 1 = 0$ , we get that  $N_{q^k/q}(x) = 1 \neq \beta$ , i.e.,  $\Omega_\beta(x) = 0$ . Hence

$$N_t = \sum_{x \in \mathbb{F}_{q^k}} \omega(x^s - 1) \Omega_\beta(x).$$

The latter implies

$$\begin{aligned} N_t &= \frac{\phi(t)}{(q^k - 1) \cdot (q - 1)} \sum_{x \in \mathbb{F}_{q^k}} \sum_{u \mid t} \frac{\mu(u)}{\phi(u)} \sum_{\substack{v \mid l \\ \gcd(u, l/v)=1}} \sum_{\text{ord}(\chi_1)=u \cdot v} \sum_{\chi_2 \in \widehat{\mathbb{F}_q^*}} \chi_1(x^s - 1) \bar{\chi}_2(\beta) \tilde{\chi}_2(x) \\ &= \frac{\phi(t)}{(q^k - 1) \cdot (q - 1)} \sum_{u \mid t} \frac{\mu(u)}{\phi(u)} \sum_{\substack{v \mid l \\ \gcd(u, l/v)=1}} \sum_{\text{ord}(\chi_1)=u \cdot v} \sum_{\chi_2 \in \widehat{\mathbb{F}_q^*}} \bar{\chi}_2(\beta) \sum_{x \in \mathbb{F}_{q^k}} \chi_1(x^s - 1) \tilde{\chi}_2(x). \end{aligned} \quad (2.37)$$

Now consider

$$\left| \sum_{x \in \mathbb{F}_{q^k}} \chi_1(x^s - 1) \tilde{\chi}_2(x) \right| \quad (2.38)$$

and suppose that  $\chi_1$  is non-trivial. As the group of multiplicative characters of  $\mathbb{F}_q$  is cyclic by Theorem 1.4.8, let  $\chi_g$  be a generator of this group. Then there exists  $u_1$  and  $u_2$  such that  $\chi_1 = \chi_g^{u_1}$  and  $\tilde{\chi}_2 = \chi_g^{u_2}$ . Then (2.38) becomes

$$\left| \sum_{x \in \mathbb{F}_{q^k}} \chi_g^{u_1}(x^s - 1) \chi_g^{u_2}(x) \right| \quad (2.39)$$

Since  $\chi_g^{u_1}(x^s - 1) = \chi_g((x^s - 1)^{u_1})$  and  $\chi_g^{u_2}(x) = \chi_g(x^{u_2})$ , substituting into (2.39), we get

$$\left| \sum_{x \in \mathbb{F}_{q^k}} \chi_g((x^s - 1)^{u_1}) \chi_g(x^{u_2}) \right| = \left| \sum_{x \in \mathbb{F}_{q^k}} \chi_g((x^s - 1)^{u_1} x^{u_2}) \right| \leq s \cdot q^{k/2}, \quad (2.40)$$

where the last inequality follows from Theorem 1.4.9. When  $\chi_1$  is trivial, Theorem 1.4.4 and Equation (1.7) give

$$\sum_{x \in \mathbb{F}_{q^k}} \tilde{\chi}_2(x) = \begin{cases} q^k, & \text{if } \chi_2 \text{ is trivial,} \\ 0, & \text{otherwise.} \end{cases}$$

By standard properties of characters, we have that  $|\bar{\chi}_2(\beta)| = 1$  for every  $\chi_2$  and  $\beta \neq 0$ . In addition, there are exactly  $\phi(u \cdot v)$  multiplicative characters of order  $u \cdot v$ . Now,

we separate the term that corresponds to trivial  $\chi_1$  in (2.37), plug in the bound from (2.40), use Lemma 1.4.10, to obtain

$$\left| \frac{N_t \cdot (q^k - 1) \cdot (q - 1)}{\phi(t)} - q^k \right| \leq s \cdot l \cdot W(t) \cdot (q - 1) \cdot q^{k/2}.$$

The latter implies that  $N_t \neq 0$ , if

$$q^{k/2} > s \cdot l \cdot W(t) \cdot (q - 1).$$

Substituting  $s = \frac{q^k - 1}{e \cdot (q - 1)}$ , we get

$$e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}}. \quad (2.41)$$

□

We refer to Schwarz [79] for the proof of the following lemma.

**Lemma 2.4.8** [79] *Let  $r \geq 2$ ,  $a \in \mathbb{F}_q^*$ ,  $s = \gcd(r, q - 1)$ . Then there exists  $b \in \mathbb{F}_q^*$  satisfying  $b^r = a$  if and only if  $a^{\frac{q-1}{s}} = 1$ .*

**Theorem 2.4.9** *Let  $2 < q$ ,  $D = (d_1, d_2)$ ,  $k = \text{ord}_e(q)$  for some  $e \mid d_2$ ,  $\gcd(d_1, q^k - 1) = u$ , and  $l = u \cdot f$  for some  $f \mid q^k - 1$  with  $2 \neq t = \frac{q^k - 1}{l} \in \mathbb{Z}$ . If*

(i)  $\text{ord}_t(q) = k$ , and

(ii)  $e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}}$ ,

then there exists  $A \in \mathbb{F}_q^3$  such that  $\{k\} \cup \{k \cdot \text{ord}_r(q^k) : r \mid d_1, 1 < r\} \subseteq \Delta_2^{(A,D)}$ .

**Proof:** Since  $2 \neq t$ , by Lemma 2.4.7, there exists an element  $\xi \in \mathbb{F}_{q^k}^*$  of order  $t$  satisfying  $(1 + \xi)^e \in \mathbb{F}_q^* \setminus \{1\}$ , by (i) and (ii). Let  $(1 + \xi)^e = b \in \mathbb{F}_q^* \setminus \{1\}$ ,  $A = (0, 1, a_2)$ , where  $-b^{d_2/e} = a_2 \in \mathbb{F}_q^* \setminus \{1\}$ , and consider  $F_2^{(A,D)}(x)$ . By Lemma 2.4.5, the set of zeros of  $F_2^{(A,D)}(x)$  is equal to  $C$ , where  $C$  is given by (2.32). Note that we have  $x^e - b \mid x^{d_2} + a_2$ , so, there exists a root  $\lambda \in \bar{\mathbb{F}}_q$  of  $F_2^{(A,D)}(x)$  such that  $\lambda$  is also a root of  $x^{d_1} - \xi$ . Note that  $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = k$ , since  $\xi$  has order  $t$ , and  $\text{ord}_t(q) = k$  by assumption (i). Since  $t = \frac{q^k - 1}{l}$ , by Lemma 2.4.8, there exists  $\gamma \in \mathbb{F}_{q^k}$  such that  $\gamma^{d_1} = \xi$ . Then we get

$$x^{d_1} - \gamma^{d_1} = \left( \frac{x}{\gamma} \right)^{d_1} - 1 = \prod_{r \mid d_1} Q_r \left( \frac{x}{\gamma} \right),$$

where  $Q_r$  denotes the  $r$ -th cyclotomic polynomial over  $\mathbb{F}_{q^k}$ . □

**Theorem 2.4.10** *Let  $2 < q$ ,  $D = (d_1, d_2)$ ,  $1 < r$ ,  $d_1 = r \cdot s$ ,  $h = \gcd(e, s)$ ,  $\text{ord}_r(q) \mid k$ , where  $k = \text{ord}_e(q)$  for some  $e \mid d_2$  and  $f$  is a divisor of  $q^k - 1$ , satisfying  $\gcd(r, f) = 1$ ,  $l = \frac{f \cdot s}{h}$ ,  $2 \neq t = \frac{q^k - 1}{l}$ . If*

$$(i) \text{ord}_t(q) = k \text{ and}$$

$$(ii) e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}},$$

*then there exists  $A \in \mathbb{F}_q^3$  such that  $r \cdot k \in \Delta_2^{(A, D)}$ .*

**Proof:** As in the proof of Theorem 2.4.9, there exists  $\xi \in \mathbb{F}_{q^k}$  with the same properties. Now, consider  $F_2^{(A, D)}(x)$ , where  $A = (0, 1, a_2)$ ,  $a_2 = (1 + \xi)^{d_2}$ , and  $x^{d_1} - \xi$ . By Lemma 2.4.8, there exists  $\gamma \in \mathbb{F}_{q^k}$  such that  $\gamma^l = \gamma^{\frac{f \cdot s}{h}} = \xi$ . Since

$$x^{d_1} - \xi = (x^r)^s - (\gamma^{\frac{f}{h}})^s,$$

we get  $x^r - \gamma^{\frac{f}{h}} \mid x^{d_1} - \xi$ . Note that

$$\text{ord}(\gamma^{\frac{f}{h}}) = \text{ord}(\gamma^{\frac{f \cdot s}{h}}) \cdot \gcd(\text{ord}(\gamma^{\frac{f}{h}}), s) = t \cdot s' \quad \text{for some } s' \mid s.$$

Hence the conditions of Theorem 1.1.1 are satisfied. That is, the polynomial  $x^r - \gamma^{\frac{f}{h}}$  is irreducible over  $\mathbb{F}_{q^k}$ . So, there exists a root of  $\lambda$  of  $F_2(x)$ , such that  $[\mathbb{F}_q(\lambda) : \mathbb{F}_q] = r \cdot k$ .  $\square$

**Corollary 2.4.11** *Let  $q > 2$ . Suppose that the following hold.*

$$(i) \text{ord}_r(q) = k \text{ for all } r \mid d_1,$$

$$(ii) k \mid k_e, \text{ where } k_e = \text{ord}_e(q), \text{ for all } e \mid d_2,$$

$$(iii) \text{there exists } e \mid d_2 \text{ such that } k = \text{ord}_e(q) = k_e,$$

$$(iv) \text{the conditions of Theorem 2.4.9 and Theorem 2.4.10 are satisfied for all } e \mid d_2.$$

*Then there exists  $A \in \mathbb{F}_q^3$  such that  $\Delta_2^{(A, D)} = \Delta_2^{(D)}$ .*

**Proof:** Assumptions (ii) and (iv) imply that there exists  $A = (0, 1, a_2) \in \mathbb{F}_q^3$ , where  $a_2 \neq 0, 1$ , such that  $\{k_e\} \cup \{k_e \cdot \text{ord}_r(q^{k_e}) : r \mid d_1\} \subseteq \Delta_2^{(A, D)}$  for all  $e \mid d_2$ , by Theorem 2.4.9. Similarly, assumptions (ii) and (iv) imply that  $r \cdot k_e \in \Delta_n^{(A, D)}$  for each  $r \mid d_1$  and  $k_e = \text{ord}_e(q)$  for all  $e \mid d_2$ . Note that by assumption (iii), there exists  $e \mid d_2$  such that  $k_e = \text{ord}_e(q) = k$ , and hence  $k = k_e$  and  $r \cdot k_e = r \cdot k$  are in  $\Delta_n^{(A, D)}$ . By (i), we conclude that  $\Delta_2^{(A, D)} = \Delta_2^{(D)}$ .  $\square$

**Example 2.4.2** Let  $q = 3$ ,  $n = 2$ ,  $D = (11, 121)$ . Then  $\text{ord}_{11}(3) = \text{ord}_{121}(3) = 5$ . Using notations of Theorem 2.4.10, we have  $k = 5$ ,  $r = 11$ ,  $s = h = 11$ . We let  $f = 1$  and obtain  $t = 3^5 - 1$ . We observe that

$$121 > W(3^5 - 1) \cdot \frac{3^5 - 1}{3^{5/2}},$$

and hence by Theorem 2.4.10, there exists  $A \in \mathbb{F}_q^3$  such that  $11 \cdot 5 = 55 \in \Delta_2^{(A,D)}$ . Note that conditions (i), (ii), (iii) of Corollary 2.4.11 are satisfied. Then  $\Delta_2^{(A,D)} = \Delta_2^{(D)}$ , since we need not to check whether conditions of Theorem 2.4.9 are satisfied, as  $\text{ord}_{11}(3) = \text{ord}_{121}(3)$ . By MAGMA, one can see that if  $A = (1, 2, 2)$ , then  $\Delta_2^{(A,D)} = \{1, 5, 55\}$ .

We end this chapter with the following remark.

Let  $D = (d_1, \dots, d_n)$ ,  $A \in \mathbb{F}_q^{n+1}$ . Consider the permutation  $\sigma$  of  $\mathbb{F}_q$  induced by  $F_n^{(A,D)}(x)$ . If  $d_1 \cdot d_2 \cdot \dots \cdot d_n \leq q - 2$ , then  $F_n^{(A,D)}(x)$  is the unique polynomial which represents  $\sigma$  by Theorem 1.2.1. In general one would expect  $F_n^{(A,D)}$  to be a polynomial with large weight when  $q$  is large. However, we can express the same polynomial in the form (1.3) with only  $n + 1$  coefficients  $a_0, a_1, \dots, a_n$ . The two examples below exhibit the cycle structure of such polynomials in the case  $n = 2$ .

**Example 2.4.3** Consider the following permutation

$$\sigma = (0 \ 1 \ 7 \ 9 \ 5 \ 2 \ 3 \ 4 \ 6 \ 10 \ 8)$$

of  $\mathbb{F}_{11}$ . By Theorem 1.2.1, there exists a unique polynomial  $F(x)$  of degree less than 11, satisfying  $F(c) = \sigma(c)$  for all  $c \in \mathbb{F}_{11}$ . We have

$$F(x) = x^9 + 4x^8 + x^7 + 7x^6 + 6x^5 + x^4 + 7x^3 + x + 1,$$

with weight 9. However,

$$F_2(x) = ((x + 9)^3 + 10)^3 + 4 = F_2^{(A,D)}(x),$$

where  $A = (9, 10, 4) \in \mathbb{F}_{11}^3$  and  $D = (3, 3)$ . Therefore, degrees of the irreducible factors of  $F(x) = F_2(x)$  lie in  $\Delta_2^{(D)} = \{1, 2, 6\}$ , since  $\text{ord}_3(11) = 2$ . Note that

$$F(x) = F_2^{(A,D)}(x) = (x + 3)(x^2 + 2x + 6)(x^6 + 10x^5 + 5x^4 + 9x^3 + 7x^2 + 10x + 8),$$

so that  $\Delta_2^{(A,D)} = \Delta_2^{(D)}$ .

**Example 2.4.4** Consider the following permutation

$$\sigma = (0\ 4\ 3\ 8\ 7\ 6\ 9)$$

of  $\mathbb{F}_{11}$ . By Theorem 1.2.1, there exists a unique polynomial  $F(x)$  of degree less than 11, satisfying  $F(c) = \sigma(c)$  for all  $c \in \mathbb{F}_{11}$ . We have

$$F(x) = x^9 + x^8 + 9x^7 + 8x^6 + 6x^5 + 7x^4 + 2x^3 + 2x^2 + 5x + 4,$$

with weight 10. However,

$$F_2(x) = ((x + 5)^3 + 8)^3 + 3 = F_2^{(A,D)}(x),$$

where  $A = (5, 8, 3) \in \mathbb{F}_{11}^3$ , and  $D = (3, 3)$ . Therefore, degrees of the irreducible factors of  $F(x) = F_2(x)$  lie in  $\Delta_2^{(D)} = \{1, 2, 6\}$ , since  $\text{ord}_3(11) = 2$ . Note that

$$F(x) = F_2^{(A,D)}(x) = (x + 2)(x^2 + 2x + 5)(x^6 + 8x^5 + x^4 + 10x^3 + 9x^2 + 3x + 7),$$

so that  $\Delta_2^{(A,D)} = \Delta_2^{(D)}$ .

## CHAPTER 3

### Consecutive permutation polynomial sequences

In this chapter we first consider the so-called consecutive polynomial sequences, recursively defined by Gómez-Pérez, Ostafe, Sha in [36].

Similarly we recursively define a sequence of permutation polynomials. Consider a sequence  $A = \{a_n\}_{n \geq 0}$  of elements of  $\mathbb{F}_q^*$  and a sequence  $D = \{d_n\}_{n \geq 1}$  of elements of  $\mathbb{Z}^+$  satisfying (1.2) and (1.4). The sequence  $F = F^{(A,D)} = \{F_n^{(A,D)}\}_{n \geq 0}$  is called a *consecutive permutation polynomial sequence* in  $\mathbb{F}_q[x]$ , associated to the sequences  $A$  and  $D$ , if

$$F_n(x) = F_n^{(A,D)}(x) = (\dots (a_0x + a_1)^{d_1} + a_2)^{d_2} + \dots + a_n)^{d_n} + a_{n+1}. \quad (3.1)$$

The authors of [36] studied various questions on irreducible factors of terms of consecutive polynomial sequences. Our aim is to study analogous questions for consecutive permutation polynomial sequences. Our methods are completely different from that of [36].

### 3.1 Consecutive polynomial sequences

In van der Poorten [72] it is observed that the numbers

$$19, 197, 1979, 19793, 197933, 1979339, 19793393, 197933933, 1979339339$$

are all prime numbers. After this observation, van der Poorten came up with the following question: Is there such an infinite chain of prime numbers in some base  $b$ ? This question is related to the existence of the largest truncatable prime in a given base

b. We recall that a prime number is called a *truncatable prime* if it gives a sequence of prime numbers when the digits are removed always from the left or always from the right. Observe that the above integer 1979339339 is not a truncatable prime. Angell and Godwin [9], give heuristic arguments for the length of the largest truncatable prime in base  $b$  and compute the largest truncatable primes in base  $b$ , where  $3 \leq b \leq 15$ .

Mullen and Shparlinski [67] asked an analogous question about polynomials over finite fields. They consider polynomials of the form  $f_n \in \mathbb{F}_q[x]$  satisfying  $\deg f_n = n$ ,

$$f_n = a_n x^n + f_{n-1}, \quad n \geq 1, \quad (3.2)$$

and denote by  $L(q)$ , the largest  $L$  such that  $f_1, f_2, \dots, f_L$  are irreducible. Mullen and Shparlinski [67] posed the problems of finding upper and lower bounds for  $L(q)$ , in terms of  $q$ . Chow and Cohen [24] give a lower bound for  $L(q)$ .

**Theorem 3.1.1** [24] (i) If  $q \neq 3$ , then  $L(q) > \frac{\log q}{2 \log \log q}$ .  
(ii)  $L(3) = 3$ .

In [36], the following definition is given, motivated by the question of Mullen and Shparlinski [67] above. Consider a sequence  $a = \{a_n\}_{n \geq 0}$  of elements of  $\mathbb{F}_q^*$ . The sequence  $f = \{f_n\}_{n \geq 1}$  is called a *consecutive polynomial sequence* in  $\mathbb{F}_q[x]$ , associated to the sequence  $a$ , if  $f_n(x) = a_n x^n + \dots + a_1 x + a_0$ ,  $n \geq 1$ . If all polynomials  $f_n$ ,  $n \geq 1$  are irreducible, then  $f$  is called a *consecutive irreducible polynomial sequence* and  $a$  is called a *consecutive irreducible sequence*.

Consider a consecutive permutation polynomial sequence  $f$ . In [36], the authors introduce the following notation;

- (i)  $\mathcal{D}(f_n)$  : the largest degree of the irreducible factors of  $f_n$ ;
- (ii)  $\omega(f_n)$ : the number of distinct monic irreducible factors of  $f_n$ ;
- (iii)  $I_N$  : the number of consecutive irreducible polynomial sequences of  $N$  elements.

They considered the problems of finding upper and lower bounds for  $\mathcal{D}(f_n)$ ,  $\omega(f_n)$ ,  $I_N$  and  $L(q)$ .

**Theorem 3.1.2** [36] *Let  $f$  be an infinite consecutive polynomial sequence. For any integers  $n \geq 2q - 1$  and  $s$  satisfying  $0 < s \leq \frac{\log((n+1)/2)}{\log q}$ , one has*

$$\max\{\mathcal{D}(f_n), \mathcal{D}(f_{n+s})\} > \frac{\log((n+1)/2) + \log \log q - \log \log((n+1)/2)}{\log q}. \quad (3.3)$$

Moreover, if  $p \nmid (n+1)$  or  $p \nmid s$ , then

$$\max\{\mathcal{D}(f_n), \mathcal{D}(f_{n+s})\} > \frac{\log((n+1)/2)}{\log q}. \quad (3.4)$$

As a corollary of this result, an asymptotic bound for  $\mathcal{D}(f_n)$  is obtained in [36]. We recall that for functions  $g(n)$  and  $h(n)$ , the assertion  $h(n) \gg g(n)$  is equivalent to  $|g(n)| \leq c \cdot h(n)$  for all  $n$ , where  $0 < c$  is a constant.

**Corollary 3.1.3** [36] *If  $f$  is an infinite consecutive polynomial sequence, then for almost all integers  $n \geq 1$ ,*

$$\mathcal{D}(f_n) \gg \frac{\log n}{\log q}.$$

**Theorem 3.1.4** [36] *There exists a consecutive polynomial sequence  $f$  over  $\mathbb{F}_q$  of  $N$  elements, if*

$$N \geq \lfloor \sqrt{2(q-1)} + 3/2 \rfloor$$

*such that all the terms in the sequence are pairwise relatively prime.*

## 3.2 Consecutive permutation polynomial sequences

In this section, we consider problems of the previous section for consecutive permutation polynomial sequences. Let  $F$  be a consecutive permutation polynomial sequence. As in the previous section, we use the following notation:

- (i)  $\mathcal{D}(F_n)$ : the largest degree of the irreducible factors of  $F_n$ ;
- (ii)  $\omega(F_n)$ : the number of distinct monic irreducible factors of  $F_n$ .

Each term of  $F$  is a permutation polynomial and hence is reducible over  $\mathbb{F}_q$ . Therefore, it is not possible to consider questions regarding irreducibility for consecutive permutation polynomial sequences. We give lower and upper bounds for  $\mathcal{D}(F_n)$  in the following result. We first recall the definition of the set  $O$ , in (2.11).

$$O = \{\text{ord}_\ell(q) : \ell \text{ is a prime divisor of } d = \text{lcm}(d_1, d_2, \dots, d_n)\}.$$



**Theorem 3.2.1** Let  $F = F^{(A,D)}$  be a consecutive permutation polynomial sequence. Then

$$m \leq \mathcal{D}(F_n) \leq d_1 \cdot d_2 \cdot \dots \cdot d_{n-1} \cdot \text{ord}_d(q), \quad (3.5)$$

where  $1 < m$  is the smallest element of the set  $O$  given by (2.11).

**Proof:** Each term of  $F$  is a consecutive permutation polynomial sequence, hence has a unique root in  $\mathbb{F}_q$ . We have  $1 < \mathcal{D}(F_n)$ , since we have assumed  $A$  is a sequence of elements of  $\mathbb{F}_q^*$  and  $\gcd(d_i, q) = 1$  for all terms  $d_i$  of the sequence  $D$ . By Theorem 2.1.1 and Theorem 2.1.2, degrees of the irreducible factors of  $F_n$  lie in the set  $\Delta_n^{(D)}$ . The smallest element  $1 < m$  of the set  $\Delta_n^{(D)}$  is the smallest element of the set  $O$  given by (2.11). Thus,  $m$  is a lower bound for  $\mathcal{D}(F_n)$ . The upper bound for  $\mathcal{D}(F_n)$  directly follows from Theorem 2.1.1.  $\square$

**Remark 3.2.1** We recall that that if  $n = 1$ , the upper bound for  $\mathcal{D}(F_n^{(A,D)})$  is attained for every choice of  $A$  and  $D$ , by Remark 2.2.1. Suppose  $n = 2$  and  $D$  is a sequence such that the conditions of Theorem 2.4.10 are satisfied for  $r = d_1$ , and  $k = \text{ord}_{d_2}(q)$ . Then Theorem 2.4.10 implies the existence of a sequence  $A$  such that the upper bound for  $\mathcal{D}(F_n^{(A,D)})$  is attained.

**Lemma 3.2.2** Let  $F = F^{(A,D)}$  be a consecutive permutation polynomial sequence,  $s \geq 2$  and put

$$G_s(x) = (\dots ((x^{d_{n+2}} + a_{n+3})^{d_{n+3}} + a_{n+4})^{d_{n+4}} + \dots + a_{n+s})^{d_{n+s}} + a_{n+s+1}. \quad (3.6)$$

Then the following hold.

- (i)  $\gcd(F_n, F_{n+s}) = 1$  if and only if  $G_s(a_{n+2}) \neq 0$ .
- (ii)  $\gcd(F_n, F_{n+s}) > 1$  if and only if  $F_n^{d_{n+1}} \mid F_{n+s}$ .

**Proof:**

- (i) First of all, observe that

$$G_s(F_{n+1}(x)) = (\dots (F_{n+1}^{d_{n+2}} + a_{n+3})^{d_{n+3}} + \dots + a_{n+s})^{d_{n+s}} + a_{n+s+1} = F_{n+s}(x). \quad (3.7)$$

Substituting

$$F_{n+1} = F_n^{d_{n+1}} + a_{n+2} \quad (3.8)$$

into (3.7), we see that  $F_{n+s}$  is a polynomial in  $F_n$ , with constant term  $G_s(a_{n+2})$ . Therefore, for an irreducible factor  $Q(x)$  of  $F_n(x)$ , we have  $Q(x) \mid F_{n+s}(x)$  if and only if  $G_s(a_{n+2}) = 0$ . Equivalently,  $\gcd(F_n, F_{n+s}) = 1$  if and only if  $G_s(a_{n+2}) \neq 0$ .

(ii) If  $\gcd(F_n, F_{n+s}) > 1$ , then  $G_s(a_{n+2}) = 0$  by part (i). Hence, the result follows by (3.7) and (3.8).  $\square$

**Remark 3.2.2** We have  $\gcd(F_n, F_{n+1}) = 1$  for all  $n \geq 0$  by (3.8), since  $a_{n+2} \in \mathbb{F}_q^*$ .

**Theorem 3.2.3** If  $N \leq q$ , then there exists a consecutive permutation polynomial sequence  $F$  of  $N$  elements such that all the terms in the sequence are pairwise relatively prime. Moreover, the number of such sequences is

(i)  $(q-1)^{N+1}$ , for  $N = 1, 2$ .

(ii)  $(q-1)^3 \cdot \prod_{i=2}^{N-1} (q-i)$ , for  $3 \leq N \leq q$ .

**Proof:** By Remark 3.2.2, the result holds for  $N = 2$ . We will show that for fixed  $D$  and  $3 \leq N \leq q$ , there exists a sequence  $A$  such that the condition given by Lemma 3.2.2 (i) is satisfied for each  $n$  and  $s$  with  $2 \leq n+s \leq N$ , so that  $\gcd(F_n, F_{n+s}) = 1$  for all  $2 \leq n+s \leq N$ , by Lemma 3.2.2 (i).

Fix  $a_0, a_1, a_2 \in \mathbb{F}_q^*$ . Consider  $F_0 = a_0x + a_1$ ,  $F_1 = F_0^{d_1} + a_2$ . We have  $\gcd(F_0, F_1) = 1$  by Remark 3.2.2. If there exists  $a_3 \in \mathbb{F}_q^*$  satisfying

$$a_2^{d_2} + a_3 \neq 0, \tag{3.9}$$

and  $F_2 = F_1^{d_2} + a_3$ , then  $G_2 = (a_2^{d_2} + a_3) \neq 0$ . By Lemma 3.2.2, we have  $\gcd(F_0, F_2) = 1$ . Note that  $\gcd(F_1, F_2) = 1$ , by Remark 3.2.2. There are  $q-2$  different choices for the element  $a_3$  to satisfy condition (3.9), since there exists only one element  $b \in \mathbb{F}_q^*$  such that

$$a_2^{d_2} + b = 0.$$

Now, let us fix  $a_3$ . If there exists  $a_4$  satisfying

$$\begin{aligned} a_3^{d_3} + a_4 &\neq 0, \\ (a_2^{d_2} + a_3)^{d_3} + a_4 &\neq 0. \end{aligned} \tag{3.10}$$

and  $F_3 = F_2^{d_3} + a_4$ , then  $G_2(a_3) \neq 0$  and  $G_3(a_2) \neq 0$ . Again by Lemma 3.2.2, we have  $\gcd(F_1, F_3) = \gcd(F_0, F_3) = 1$ . Note that  $\gcd(F_2, F_3) = 1$  by Remark 3.2.2 again.

Since  $a_2 \in \mathbb{F}_q^*$ , the conditions in (3.10) are different and hence there are  $q - 3$  different choices for the element  $a_4$ . Now, we fix  $a_4$  and continue in this way. Then, we have only one choice for the element  $a_q$ , where  $F_{q-1} = F_{q-2}^{d_{q-1}} + a_q$  so that  $\gcd(F_h, F_j) = 1$  for all  $0 \leq h < j \leq q - 1$ . This shows the existence of a consecutive permutation polynomial sequence of  $N$  elements, where  $1 \leq N \leq q$ , such that all terms in the sequence are pairwise relatively prime. Note that as there will be  $q - 1$  different conditions for the number  $a_{q+1}$ , where  $F_q = F_{q-1}^{d_q} + a_{q+1}$ , we have  $\gcd(F_q, F_j) > 1$  for some  $0 \leq j < q - 1$ .

In order to find the number of such sequences, we follow steps of the proof above: We have  $(q - 1)^2$  different such sequences of 1 element,  $(q - 1)^3$  different such sequences of 2 elements and  $(q - 1)^3 \cdot (q - 2) \cdot (q - 3) \cdot \dots \cdot (q - N + 1)$  different such sequences of  $N$  elements, where  $3 \leq N \leq q$ .  $\square$

In [36], an irreducible polynomial  $Q(x) \in \mathbb{F}_q[x]$  is called a primitive irreducible divisor of  $f_n$ , if  $Q \mid f_n$  but  $Q \nmid f_j$  for all  $j < n$ , and the following problem is posed: Can one show that *almost all* terms of a consecutive polynomial sequence have primitive irreducible divisors? This problem has not been solved so far. In order to solve it in the case of consecutive permutation polynomial sequences, we need the following lemmas.

**Lemma 3.2.4** *Let  $F$  be a consecutive permutation polynomial sequence. Then  $F_n(x)$  is separable if and only if  $\gcd(F_j, F_n) = 1$  for all  $0 \leq j \leq n - 1$ .*

**Proof:** The formal derivative of  $F_n(x)$  is;

$$F'_n(x) = d_n \cdot F_{n-1}^{d_n-1} \cdot d_{n-1} \cdot F_{n-2}^{d_{n-1}-1} \cdot \dots \cdot d_1 \cdot F_0^{d_1-1} \cdot a_0. \quad (3.11)$$

Hence the result follows.  $\square$

**Lemma 3.2.5** *Let  $F$  be a consecutive permutation polynomial sequence.*

*If  $\gcd(F_n, F_s) > 1$  for some  $s \geq n + 2$ , then  $F_n$  divides  $F_s$  with multiplicity  $l$ , where*

(i)  $d_{n+1} \mid l$ , and

(ii) *there exist divisors  $d_{i_1}, \dots, d_{i_l}$  of  $l$ , satisfying  $n + 1 \leq i_j \leq s - 1$ ,  $i_{j+1} \neq i_j + 1$ .*

**Proof:** Let  $s \geq n + 2$ . Suppose that  $\gcd(F_n, F_s) > 1$ . Then  $F_n^{d_n+1} \mid F_s$  by Lemma 3.2.2 (ii). Let  $l$  be the multiplicity of  $F_n$  in  $F_s$ . In order to find  $l$ , we consider the formal derivative of  $F_s(x)$ . We have

$$F'_s(x) = d_s \cdot F_{s-1}^{d_s-1} \cdot d_{s-1} \cdot F_{s-2}^{d_{s-1}-1} \cdot \dots \cdot d_{n+1} \cdot F_n^{d_{n+1}-1} \cdot \dots \cdot d_1 \cdot F_0^{d_1-1} \cdot a_0. \quad (3.12)$$

Equation (3.12) shows that  $d_{n+1}$  is a proper divisor of  $l$  if and only if  $F_n \mid F_h$  and  $F_h \mid F_s$  for some  $n+2 \leq h < s$ . Therefore, (3.12) implies that  $l$  is a product of  $d_i$ 's, for some  $n+1 \leq i \leq s-1$  which are non-consecutive, since consecutive terms of the sequence are relatively prime by Remark 3.2.2.  $\square$

**Lemma 3.2.6** *Let  $F$  be a consecutive permutation polynomial sequence. Then the following hold.*

(i) *If  $\gcd(F_j, F_n) > 1$  for some  $j < n$ , then  $\gcd(F_{j+1}, F_n) = 1$ .*

(ii) *If  $\gcd(F_j, F_n) > 1$  and  $\gcd(F_h, F_n) > 1$  for some  $h < n$ ,  $h \neq j$ , then  $\gcd(F_h, F_j) > 1$ .*

**Proof:**

(i) Suppose that  $\gcd(F_j, F_n) > 1$  for some  $j < n$ . Then by Lemma 3.2.2 (i), we have

$$G_{n-j}(a_{j+2}) = (\dots((a_{j+2}^{d_{j+2}} + a_{j+3})^{d_{j+3}} + a_{j+4})^{d_{j+4}} + \dots + a_n)^{d_n} + a_{n+1} = 0.$$

Note that

$$G_{n-j-1}(a_{j+3}) = (\dots(a_{j+3}^{d_{j+3}} + a_{j+4})^{d_{j+4}} + \dots + a_n)^{d_n} + a_{n+1} \neq 0,$$

since  $G_{n-j}(a_{j+2}) = 0$  and  $a_{j+2} \neq 0$ . Therefore,  $\gcd(F_{j+1}, F_n) = 1$  by Lemma 3.2.2.

(ii) Suppose that  $\gcd(F_j, F_n) > 1$  and  $\gcd(F_h, F_n) > 1$  for some  $h < j < n$ . By Lemma 3.2.2 we have

$$G_{n-j}(a_{j+2}) = (\dots(a_{j+2}^{d_{j+2}} + a_{j+3})^{d_{j+3}} + \dots + a_n)^{d_n} + a_{n+1} = 0,$$

$$G_{n-h}(a_{h+2}) = (\dots(a_{h+2}^{d_{h+2}} + a_{h+3})^{d_{h+3}} + \dots + a_{j+1})^{d_{j+1}} + a_{j+2})^{d_{j+2}} \dots + a_n)^{d_n} + a_{n+1} = 0.$$

This implies that

$$G_{j-h}(a_{h+2}) = (\dots(a_{h+2}^{d_{h+2}} + a_{h+3})^{d_{h+3}} + \dots + a_{j+1})^{d_{j+1}} = 0,$$

equivalently  $F_h^{d_{h+1}} \mid F_j$  by Lemma 3.2.2. If  $j < h$ , then one can similarly show that  $F_j^{d_{j+1}} \mid F_h$ .

$\square$

**Theorem 3.2.7** *Let  $F$  be a consecutive permutation polynomial sequence. Then each term of  $F$  has a primitive irreducible divisor.*

**Proof:** If  $n = 1$ , then the statement follows from Remark 3.2.2. Let  $n \geq 2$  be fixed and consider  $F_n$ . If  $\gcd(F_j, F_n) = 1$ , for all  $0 \leq j < n$ , then the result follows. If  $\gcd(F_j, F_n) > 1$  for some  $0 \leq j < n - 1$ , then by Lemma 3.2.5 we have  $F_j^{d_{j+1}} \mid F_n$ . By Lemma 3.2.6 (i),  $F_j$  and  $F_{j+1}$  do not divide  $F_n$  simultaneously. Therefore, in order to show the existence of a primitive divisor of  $F_n$ , we consider the case, where

- (i)  $\gcd(F_j, F_n) > 1$  for some of the non-consecutive  $j$ 's, for  $0 \leq j < n - 1$ , and
- (ii) if there exists  $h \neq j$  such that  $F_h \mid F_n$ , then  $\gcd(F_h, F_j) = 1$ .

But (ii) does not hold by Lemma 3.2.6 (ii). We thus consider the case

$$F_{n-2}^{d_{n-1}} \mid F_n, \text{ and } F_h^{d_{h+1}} \mid F_{n-2} \quad (3.13)$$

for the maximum number of  $h$ 's, where  $0 \leq h < n - 2$ , since  $F_{n-2}$  has the highest degree among the possible divisors  $F_j$  of  $F_n$ . Consider

$$R(x) = \frac{F_n(x)}{F_{n-2}^{d_{n-1}}(x)}.$$

We have  $\deg R(x) > 1$ , since  $\deg(F_{n-2}^{d_{n-1}}) < \deg(F_n)$ , as  $d_i \geq 2$ . By (3.11) and Lemma 3.2.2 (ii),  $\gcd(F_j, R) = 1$  for all  $j < n$ . Hence, there exists an irreducible factor  $Q(x)$  of  $F_n(x)$  such that  $\gcd(Q, F_j) = 1$  for all  $0 \leq j \leq n - 1$ .

□

We now obtain an upper bound for the number of irreducible factors of  $F_n$ .

**Theorem 3.2.8** *Let  $F$  be a consecutive permutation polynomial sequence. Then*

$$2 \leq \omega(F_n) \leq \left\lfloor \frac{\prod_{i=1}^n d_i - d_1}{m} \right\rfloor + \sum_{e \mid d_1} \frac{\phi(e)}{2},$$

for  $n \geq 1$ , where  $1 < m$  is the smallest element of the set  $O$  in (2.11) and  $\phi$  denotes the Euler's totient function.

**Proof:** Let  $n \geq 1$  and consider  $F_n$ . For the minimum number of distinct irreducible factors of  $F_n$ , we consider the case where  $F_n$  has an irreducible factor of  $Q$  of degree  $r$ , where  $r$  is the maximum element of  $\Delta_n^{(D)}$ . Since  $1 < r$  and  $F_n$  has a linear factor also,

we have  $2 \leq \omega(F_n)$ . Note that the multiplicity of the linear factor can be greater than 1.

For the maximum number of distinct irreducible factors of  $F_n$ , we consider the following case. Suppose that the root  $\lambda \in \mathbb{F}_q$  of  $F_n(x)$  satisfies  $a_0\lambda + a_1 \in \mathbb{F}_q^*$ . Using a similar argument that we used to obtain (2.29), we get

$$(a_0x + a_1)^{d_1} - (a_0\lambda + a_1)^{d_1} \mid F_n(x). \quad (3.14)$$

Since  $a_0\lambda + a_1 \in \mathbb{F}_q^*$ , we have

$$\left(\frac{a_0x + a_1}{b}\right)^{d_1} - 1 \mid F_n(x), \quad (3.15)$$

where  $b$  is the unique element of  $\mathbb{F}_q^*$  satisfying  $b^{d_1} = a_0\lambda + a_1$ . By Theorem 1.4.1 (i), we have

$$\left(\frac{a_0x + a_1}{b}\right)^{d_1} - 1 = \prod_{e \mid d_1} Q_e \left(\frac{a_0x + a_1}{b}\right).$$

We also have that each term in the above product factors into  $\phi(e)/\text{ord}_e(q)$  distinct irreducible factors and  $2 \leq \text{ord}_e(q)$  by the assumption that  $\gcd(d_1, q-1) = 1$ . Therefore, the divisor in (3.15) has at most  $1 < \sum_{e \mid d_1} \frac{\phi(e)}{2}$  distinct irreducible factors. Note that if  $a_0\lambda + a_1 = 0$ , then relation (3.14) gives only one irreducible factor of  $F_n$ . Now, we continue with the quotient

$$S(x) = \frac{F_n(x)}{(a_0x + a_1)^{d_1} - (a_0\lambda + a_1)^{d_1}}.$$

If  $n = 1$ , then  $S(x) = 1$ . If  $n > 1$ , then  $F_n(x)$  has maximum number of distinct irreducible factors when  $S(x)$  factors into irreducible polynomials of the smallest possible degree. We know that  $F_n$  has a linear factor which already divides  $(a_0x + a_1)^{d_1} - (a_0\lambda + a_1)^{d_1}$ . Hence the result follows.  $\square$

**Remark 3.2.3** *If  $D$  is a fixed sequence, by Dirichlet's Prime Number Theorem, there are infinitely many prime numbers  $q$  such that the upper bound is attained for  $n = 1$ . Obviously, the same holds for the lower bound.*

The lower bound in (3.5) can be improved under special conditions.

**Corollary 3.2.9** *Let  $q$  be odd,  $n \geq 4$ ,  $D = \{d_i\}_{i \geq 1}$ ,  $k = \text{ord}_e(q)$  for some  $e \mid d_2$ .*

(i) Suppose that the conditions of Theorem 2.4.9 are satisfied. Then there exists a sequence  $A = \{a_i\}_{i \geq 0}$  such that  $\text{lcm}(k, \text{ord}_r(q)) \leq \mathcal{D}(F_n^{(A,D)})$ , for every  $r \mid d_1$ ,  $1 < r$ .

(ii) Suppose that the conditions of Theorem 2.4.10 are satisfied  $r \mid d_1$ ,  $1 < r$ . Then there exists a sequence  $A = \{a_i\}_{i \geq 0}$  such that  $r \cdot k \leq \mathcal{D}(F_n^{(A,D)})$ .

**Proof:**

(i) By Theorem 2.4.9, there exists  $B = (b_0, b_1, b_2)$ , where  $b_i \in \mathbb{F}_q^*$  for  $i = 1, 2, 3$  such that  $\{k\} \cup \{k \cdot \text{ord}_r(q^k) : r \mid d_1, 1 < r\} \subseteq \Delta_2^{(B,D)}$ . Now fix  $b_i \in \mathbb{F}_q^*$ , where  $3 \leq i \leq n+1$ ,  $i \neq 4$  and consider the polynomial

$$T_1(x) = (\dots(x^{d_4} + b_5)^{d_5} + \dots + b_n)^{d_n} + b_{n+1} \in \mathbb{F}_q[x].$$

Note that  $T_1(x)$  is a permutation polynomial of  $\mathbb{F}_q$  since  $\text{gcd}(d_i, q-1) = 1$  for all  $i \geq 1$ . Therefore,  $T_1(x)$  has a unique zero in  $\mathbb{F}_q$ , say  $b_4$ . If  $b_4 \in \mathbb{F}_q^*$ , then let  $A = \{a_i\}_{i \geq 0}$  such that  $a_i = b_i$  for  $0 \leq i \leq n+1$  and consider the consecutive permutation polynomial sequence  $\{F_i^{(A,D)}\}$  of  $\mathbb{F}_q[x]$ . Then  $T_1(x) = G_s(x)$ , with  $s = n-2$ , where  $G_s(x)$  is given by (3.6) for  $s \geq 2$ . Since  $T_1(a_4) = G_{n-2}(a_4) = 0$ , by Lemma 3.2.2, we have

$$F_2^{(A,D)}(x) \mid F_n^{(A,D)}(x).$$

Hence  $k \cdot \text{ord}_r(q^k) = \text{lcm}(k, \text{ord}_r(q)) \leq \mathcal{D}(F_n^{(A,D)})$ . If  $b_4 = 0$ , then let  $a_i \in \mathbb{F}_q^*$  such that  $a_i = b_i$  for  $0 \leq i \leq n$ ,  $i \neq 4$ , and  $a_{n+1} = b_{n+1} + 1$ . If  $b_{n+1} + 1 = 0$ , then consider  $a_{n+1} = b_{n+1} - 1 \in \mathbb{F}_q^*$ , since  $q$  is odd. Now, consider the polynomial

$$T_2(x) = (x^{d_4} + a_5)^{d_5} + \dots + a_n)^{d_n} + a_{n+1} = T_1(x) \pm 1.$$

Again, since  $\text{gcd}(d_i, q-1) = 1$  for all  $i \geq 0$ ,  $T_2(x)$  is a permutation polynomial of  $\mathbb{F}_q$ . Therefore,  $T_2(x)$  has a unique zero in  $\mathbb{F}_q$ , say  $a_4$ . Note that  $a_4 \in \mathbb{F}_q^*$  since  $T_2(0) = T_1(0) \pm 1 = \pm 1$ . Now, let  $A = \{a_i\}_{i \geq 0}$  and consider the consecutive permutation polynomial sequence  $\{F_i^{(A,D)}\}$  of  $\mathbb{F}_q[x]$ . Then  $T_2(x) = G_s(x)$ , with  $s = n-2$  again. Since  $T_2(a_4) = G_{s-2}(a_4) = 0$ , by Lemma 3.2.2,

$$F_2^{(A,D)}(x) \mid F_n^{(A,D)}(x),$$

and hence  $\text{lcm}(k, \text{ord}_r(q)) \leq \mathcal{D}(F_n^{(A,D)})$ .

(ii) By Theorem 2.4.10, there exists  $B = (b_0, b_1, b_2)$ , where  $b_i \in \mathbb{F}_q^*$  for  $i = 1, 2, 3$  such that  $r \cdot k \in \Delta_2^{(B,D)}$ . The method of proof of (i) can be used again to obtain the result. □

We have shown in Corollary 3.2.9 that the lower bound in (3.5) can be improved under some special conditions. The Corollary 3.2.12 and Corollary 3.2.13 below present improvements under different conditions. We need the following lemmas.

**Lemma 3.2.10** *Let  $F = \{F_i^{(A,D)}\}$  be a consecutive permutation polynomial sequence and  $n \geq 2$  be fixed. Consider the  $n$ -th term of a given consecutive permutation polynomial sequence  $F$  and set*

$$H_0(x) = x^{d_n} + a_{n+1} \quad H_i(x) = x^{d_{n-i}} + a_{n-i+1} - \alpha_{i-1}, \quad (3.16)$$

where  $\alpha = \alpha_0 \in \bar{\mathbb{F}}_q$  satisfies  $H_0(\alpha_0) = 0$  and  $H_i(\alpha_i) = 0$ , for  $1 \leq i \leq n$ . Then  $F_j \mid F_n$  for some  $j \leq n - 2$  if and only if  $H_{n-j-1}$  is not separable.

**Proof:** By Lemma 3.2.2,  $F_j \mid F_n$  if and only if  $G_{n-j}(a_{j+2}) = 0$ . Now, consider  $H_{n-j-1} = x^{d_{j+1}} + a_{j+2} - \alpha_{n-j-2}$ . Since  $\gcd(d_i, q) = 1$ , for all  $1 \leq i \leq n$ ,  $H_{n-j-1}$  is not separable if and only if  $a_{j+2} = \alpha_{n-j-2}$ . Since  $\alpha_{n-j-2}$  is a root of  $H_{n-j-2} = x^{d_{j+2}} + a_{j+3} - \alpha_{n-j-3}$ ,  $a_{j+2}$  is a root of  $x^{d_{j+2}} + a_{j+3} - \alpha_{n-j-3}$ . That is,  $a_{j+2}^{d_{j+2}} + a_{j+3} = \alpha_{n-j-3}$ . Continuing in this way, we get  $H_{n-j-1}$  is not separable if and only if  $G_{n-j}(a_{j+2}) = 0$ . □

In the following, we use the same notation as in Lemma 3.2.10.

**Lemma 3.2.11** *Let  $F = \{F_i^{(A,D)}\}$  be a consecutive permutation polynomial sequence. Let  $C$  be the set of roots of  $F_n(x)$  for a fixed  $n \geq 2$  and consider*

$$C_n = \{\lambda \in \bar{\mathbb{F}}_q : \lambda^{d_1} + a_2 - \alpha_{n-2} = 0, \text{ where } \alpha_i \text{ is a root of } H_i(x) = x^{d_{n-i}} + a_{n-i+1} - \alpha_{i-1}, 1 \leq i \leq n-2, \alpha_0^{d_n} \in \mathbb{F}_q^*\} \quad (3.17)$$

Then  $C = C_n$ .

**Proof:** Clearly, every element  $\lambda \in C_n$  is a root of  $F_n(x)$ , that is,  $\lambda \in C$ . We now show that the sets  $C$  and  $C_n$  have the same number of elements. First, suppose  $F_n$  is separable. Then the set  $C$  has  $d_1 \cdot d_2 \cdot \dots \cdot d_n$  elements. By Lemma 3.2.4,  $\gcd(F_j, F_n) = 1$  for all  $0 \leq j < n$ . Using Lemma 3.2.10, we have  $H_{n-j-1}$  is separable



for all  $0 \leq j \leq n-1$ . Therefore, the set  $C_n$  has  $d_1 \cdot d_2 \cdot \dots \cdot d_n$  elements. Now, assume  $F_n$  is not separable. By Lemma 3.2.4,  $F_j \mid F_n$  for some  $0 \leq j \leq n-2$ . Then Lemma 3.2.10 implies that  $H_{n-j-1} = x^{d_{j+1}}$ . If  $\gcd(F_h, F_n) = 1$  for all  $h < n$ ,  $h \neq j$ , then  $H_{n-h+1}$  is separable for all  $h < n$ ,  $h \neq j$ , and hence the set  $C_n$  has  $d_{j+1} \cdot (d_1 \cdot d_2 \cdot \dots \cdot d_j \cdot d_{j+2} \cdot \dots \cdot d_n - 1) + 1$  elements. Note that in this case, (3.11) shows that  $F_n$  has  $d_{j+1} \cdot (d_1 \cdot d_2 \cdot \dots \cdot d_j \cdot d_{j+2} \cdot \dots \cdot d_n - 1) + 1$  distinct roots. If  $\gcd(F_h, F_n) > 1$  for some  $h < n$ ,  $h \neq j$ , then similarly one can show that the set  $C$  and  $C_n$  have the same number of elements, and the result follows.  $\square$

**Corollary 3.2.12** *Let  $2 < q$ ,  $2 \leq n$ ,  $D = \{d_i\}_{i \geq 1}$ ,  $k = \text{ord}_e(q)$  for some  $e \mid d_n$ ,  $\gcd(d_{n-1}, q^k - 1) = u$  and  $l = u \cdot f$  for some  $f \mid q^k - 1$  with  $2 \neq t = \frac{q^k - 1}{l} \in \mathbb{Z}$ . If*

$$(i) \text{ord}_t(q) = k, \text{ and}$$

$$(ii) e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}},$$

*then there exists a sequence  $A = \{a_i\}_{i \geq 0}$  such that  $\text{lcm}(k, \text{ord}_r(q)) \leq \mathcal{D}(F_n^{(A,D)})$ , for every  $r \mid d_n, 1 < r$ .*

**Proof:** Suppose (i) and (ii) hold. Then there exists  $\xi \in \overline{\mathbb{F}}_q$  such that  $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = k$ , with  $(1 + \xi)^e = c \in \mathbb{F}_q^* \setminus \{1\}$ , by Lemma 2.4.7. Let  $a_i \in \mathbb{F}_q^*$ , for  $0 \leq i \leq n-1$ ,  $a_n = 1$ ,  $a_{n+1} = -c^{d_n/e}$ , and  $A = \{a_i\}_{i \geq 0}$ . Consider the consecutive permutation polynomial sequence  $\{F_i^{(A,D)}\}_{i \geq 0}$ , and  $H_0(x) = x^{d_n} - c^{d_n/e} = x^{d_n} + a_{n+1}$  as in (3.16). We have  $x^e - c \mid H_0(x)$  and hence  $1 + \xi \in \mathbb{F}_{q^k}$  is a root of  $H_0(x)$ . Now, let  $\alpha_0 = 1 + \xi$ ,  $H_1(x) = x^{d_{n-1}} + 1 - \alpha_0 = x^{d_{n-1}} - \xi$ . Then there exists  $\lambda \in \overline{\mathbb{F}}_q$  such that  $H_1(\lambda) = 0$  and  $[\mathbb{F}_q(\lambda) : \mathbb{F}_q] = k \cdot \text{ord}_r(q^k) = \text{lcm}(k, \text{ord}_r(q))$ , for every  $r \mid d_n, 1 < r$ , by Theorem 2.4.9. Lemma 3.2.11 implies that  $\text{lcm}(k, \text{ord}_r(q)) \leq \mathcal{D}(F_n)$ .  $\square$

**Corollary 3.2.13** *Let  $2 < q$ ,  $2 \leq n$ ,  $1 < r$ ,  $d_{n-1} = r \cdot s$ ,  $h = \gcd(e, s)$ ,  $\text{ord}_r(q) \mid k$ , where  $k = \text{ord}_e(q)$  for some  $e \mid d_n$ , and  $f$  is a divisor of  $q^k - 1$ , satisfying  $\gcd(r, f) = 1$ ,  $l = \frac{f \cdot s}{h}$ ,  $2 \neq t = \frac{q^k - 1}{l}$ . If*

$$(i) \text{ord}_t(q) = k \text{ and}$$

$$(ii) e > l \cdot W(t) \cdot \frac{q^k - 1}{q^{k/2}},$$

*then there exists a sequence  $A = \{a_i\}_{i \geq 0}$  such that  $r \cdot k \leq \mathcal{D}(F_n^{(A,D)})$ .*

**Proof:** We use the same notation as in Corollary 3.2.12. Suppose (i) and (ii) hold. Then here exists  $\lambda \in \bar{\mathbb{F}}_q$  such that  $H_1(\lambda) = 0$  and  $[\mathbb{F}_q(\lambda) : \mathbb{F}_q] = r \cdot k$ , by Theorem 2.4.10. Hence,  $r \cdot k \leq \mathcal{D}(F_n)$ , by Lemma 3.2.11.

**Remark 3.2.4** Here we show that  $\mathcal{D}(F_n)$  is not a strictly increasing function of  $n$ , when  $F$  is a consecutive permutation polynomial sequence.

Consider distinct prime numbers  $d_i$ ,  $1 \leq i \leq n$ , and integers  $2 \leq l_i$  such that

$$(i) \text{ord}_{d_i}(l_i) = m_i,$$

$$(ii) m_{i+1} \mid m_i, m_i \neq m_{i+1}, \text{ for } 1 \leq i \leq n-1.$$

Now consider the system of congruences

$$x \equiv l_1 \pmod{d_1},$$

$$x \equiv l_2 \pmod{d_2},$$

$$\vdots$$

$$x \equiv l_n \pmod{d_n}.$$

The Chinese Remainder Theorem tells us that this system has a unique solution  $l$  modulo  $d$ , where  $d = d_1 \cdot d_2 \cdot \dots \cdot d_n = \text{lcm}(d_1, \dots, d_n)$ . By Dirichlet's Prime Number Theorem, there exists a prime number  $q$  such that  $q \equiv l \pmod{d}$ . Moreover  $\text{ord}_d(q) = m_1$  since  $m_1 = \text{lcm}(m_1, \dots, m_n)$ . Now, consider a sequence  $A$  of elements of  $\mathbb{F}_q^*$ ,  $D = \{d_i\}_{i \geq 1}$ , and the consecutive permutation polynomial sequence  $F = \{F_i^{(A, D)}\}$ .

We have  $\mathcal{D}(F_1) = m_1$  and we now show that  $\mathcal{D}(F_n) \leq m_1$ . Note that

$$\Delta_n^{(D)} = \Delta_1^{(D)} \cup \{r \cdot k : r \mid d_1 \cdot \dots \cdot d_{n-1}, k \mid m_1, r \cdot k \in \Delta_n^{(D)}\}.$$

That is,  $\mathcal{D}(F_n) > m_1$  if and only if there exists an irreducible factor  $Q(x) \in \mathbb{F}_q[x]$  of  $F_n(x)$  such that  $\deg Q(x) = r \cdot k$  with  $r \mid d_1 \cdot \dots \cdot d_{n-1}, 1 < r, k \mid m_1$ . We now assume that such  $Q(x)$  exists. Using the notation of Theorem 2.3.2, there exists  $1 \leq j \leq n$  such that  $K = K_{n-j-1} \subsetneq K_{n-j} \subseteq \dots \subseteq K_n$ ,  $[K_{n-j} : K] = m_{j+1} = \text{ord}_{d_{j+1}}(q)$  since  $d_{j+1}$  is a prime. Then we consider  $[K_{n-j+1} : K]$ . We recall that  $K_{n-j+1} = K(\lambda_{j-1})$  and  $\lambda_{j-1}^{d_j} = \lambda_j - a_j \in K(\lambda_j) = K_{n-j}$ . We have  $\gcd(d_j, q^{m_{j+1}} - 1) = 1$ , as  $m_{j+1} < m_j$  and  $d_j$  is a prime, hence  $[K_{n-j+1} : K_{n-j}]$  equals 1 or  $\text{ord}_{d_j} q^{m_{j+1}} = \frac{m_j}{\gcd(m_j, m_{j+1})} = \frac{m_j}{m_{j+1}}$ , as in the proof of Theorem 2.3.2. That is,  $[K_{n-j+1} : K]$  equals  $m_{j+1}$  or  $m_j$ . If  $n = 2$ ,

then  $[K_2 : K] < r \cdot k$ , and we get a contradiction. If  $n > 2$ , one can similarly show that  $[K_n : K]$  is at most  $m_1$ , a contradiction. Hence  $\mathcal{D}(F_n) \leq m_1$ .

The following example shows that  $\mathcal{D}(F_n)$  is not a non-decreasing function of  $n$ .

**Example 3.2.1** Let  $q = 29$ ,  $D$  be a finite sequence of 3 elements with  $d_1 = 5, d_2 = 17, d_3 = 3$ .  $A$  be a finite sequence of 5 elements with  $a_0 = 1, a_1 = 9, a_2 = 1, a_3 = 2, a_4 = 6$ . Consider the associated consecutive permutation polynomial sequence of 4 elements  $\{F_n^{(A,D)}\}$ . Explicit factorization shows that  $\mathcal{D}(F_2) = 80$ , but  $\mathcal{D}(F_3) = 16$ .

# Bibliography

- [1] S. Ahmad, *Cycle structure of automorphisms of finite cyclic groups*. J. Comb. Thy., **6**, (1969), 370-374.
- [2] S. Agou, *Factorisation sur un corps fini  $\mathbb{F}_{p^n}$  des polynômes composés  $f(X^s)$  lorsque  $f(X)$  est un polynôme irréductible de  $\mathbb{F}_{p^n}[X]$* , L' Enseignement Math., IIe Ser., **22**, (1976), 305-312.
- [3] S. Agou, *Factorisation sur un corps fini  $\mathbb{F}_{p^n}$  des polynômes composés  $f(X^{p^r} - aX)$  lorsque  $f(X)$  est un polynôme irréductible de  $\mathbb{F}_{p^n}(X)$* , J. Number Theory, **9**, (1977), 229-239.
- [4] S. Agou, *Sur la factorisation des polynômes  $f(X^{p^{2r}} - aX^{p^r} - bX)$  sur un corps fini  $\mathbb{F}_{p^s}$* , J. Number Theory, **12**, (1980), 447-459.
- [5] A. Akbary, Q. Wang, *On polynomials of the form  $x^r f(x^{(q-1)}/l)$* , Int. J. Math. Math. Sci., (2007), Art. ID 23408.
- [6] E. Aksoy, A. Çesmelioglu, W. Meidl, A. Topuzoglu, *On the Carlitz rank of a permutation polynomial*, Finite Fields Appl., **15**, (2009), 428-440.
- [7] N. Anbar, A. Odzak, V. Patel, L. Quoos, A. Somoza, A. Topuzoglu, *On the Carlitz rank of permutation polynomials: recent developments*, (2018). In: Bouw I., Ozman E., Johnson-Leung J., Newton R. (eds) Women in Numbers Europe II. Association for Women in Mathematics Series, vol **11**. Springer, Cham.
- [8] N. Anbar, A. Odzak, V. Patel, L. Quoos, A. Somoza, A. Topuzoglu, *On the differences of permutation polynomials*, Finite Fields Appl., **49**, (2018), 132-142.
- [9] I.O. Angell, H.J. Godwin, *On truncatable primes*, Math. Comput. **31**, (1977), 265-267.

- [10] J. T. Beard, Jr., K. I. West, *Factorization tables for  $x^n - 1$  over  $GF(q)$* , Math. Comp., **28**, (1974), 1167-1168.
- [11] E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell System Tech. J., **46**, (1967), 1853-1859.
- [12] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp., **24**, (1970), 713-735.
- [13] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solution of algebraic equations over finite fields*, Information and Control, **10**, (1967), 553-564.
- [14] I.F. Blake, S. Gao, R.C. Mullin, *Explicit factorization of  $x^{2^k} + 1$  over  $\mathbb{F}_p$  with prime  $p \equiv 3 \pmod{4}$* , Appl. Algebra Eng. Commun. Comput., **4**, (2), (1993), 89-94.
- [15] W. Bosma, J. Cannon, C. Playoust, *The Magma Algebra System I. the user language*, J. Symbolic Computation, vol. **24**, (1997), 235-265.
- [16] M. C. R. Butler, *The irreducible factors of  $f(x^m)$  over a finite field*, J. London Math. Soc., 2nd Ser., **30**, (1955), 480-482.
- [17] D. G. Cantor, H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp., **36**, (1981), 587-592.
- [18] M. Car, *Factorisation dans  $\mathbb{F}_q[X]$* , C. R. Acad. Sci. Paris, Sér. I, Math., **294**, (1982), 147-150.
- [19] L. Carlitz, *Permutations in a finite field*, Proc. Am. Math. Soc., **4**, (1953), 538.
- [20] L. Carlitz, A. F. Long, Jr., *The factorization of  $Q(L(x_1), \dots, L(x_k))$  over a finite field where  $Q(x_1, \dots, x_k)$  is of first degree and  $L(x)$  is linear*, Acta. Arith., **32**, (1977), 407-420.
- [21] P. Charpin, G.M. Kyureghyan, *When does  $G(x)+Tr(H(x))$  permute  $\mathbb{F}_{p^n}$  ?*, Finite Fields Appl., **15**, (2009), 615-632.
- [22] B. Chen, L. Li, R. Tuerhong, *Explicit factorization of  $X^{2^m p^n} - 1$  over a finite field*, Finite Fields Appl., **24**, (2013), 95-104.

- [23] W.-S. Chou *The factorization of Dickson polynomials over finite fields* *Finite Fields Appl.*, **3**, (1997), 84-96.
- [24] W.-S. Chou, S.D. Cohen, *Polynomial distribution and sequences of irreducible polynomials over finite fields*, *J. Number Theory*, **75**, (1999), 145-159.
- [25] S. D. Cohen, *Further arithmetical functions in finite fields*, *Proc. Edinburgh Math Soc.* (2), **16**, (1969), 349-363.
- [26] S. D. Cohen, *The distribution of polynomials over finite fields*, *Acta Arith.*, **17**, (1970), 255-271.
- [27] S. D. Cohen, *The distribution of polynomials over finite fields II*, *Acta Arith.*, **20**, (1972), 53-62.
- [28] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, *J. London Math. Soc.*, 2nd Ser. **6**, (1972), 93-102.
- [29] S. D. Cohen, *The orders of related elements of a finite field*, *Ramanujan Journal*, Vol. **7**, (2003), 169-183.
- [30] A. Çeşmelioglu, W. Meidl, A. Topuzoğlu, *On the cycle structure of permutation polynomials*, *Finite Fields Appl.*, **14**, (2008), 593-614.
- [31] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, *Trans. Amer. Math. Soc.*, **12**, (1911), 75-98.
- [32] L. E. Dickson, *Higher irreducible congruences*, *Bull. Amer. Math. Soc.*, **3**, (1897), 381-389.
- [33] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, *Ann. of Math.*, **11**, (1896/97), 65-120.
- [34] D. Gómez-Pérez, A. Ostafe, I. Shparlinski, *On irreducible divisors of iterated polynomials*. *Rev. Mat. Iberoam.*, **30**, (2014), no. 4, 1123-1134.

- [35] D. Gómez-Pérez, A. Ostafe, A. Topuzoğlu, *On the Carlitz rank of permutations of  $\mathbb{F}_q$  and pseudorandom sequences*, J. Complex., **30**, (2014), 279-289.
- [36] D. Gómez-Pérez, A. Ostafe, M. Sha, *The arithmetic of consecutive polynomial sequences over finite fields*, Finite Fields Appl., **50**, (2018), 35-65.
- [37] W. Feit, E. Rees, *A criterion for a polynomial to factor completely over the integers*, Bull.London. Math. Soc., **10**, (1978), 191-192.
- [38] R. W. Fitzgerald, J. L. Yucas, *Factors of Dickson polynomials over finite fields*, Finite Fields Appl., **11**, (2005), 724-737.
- [39] R.W. Fitzgerald, J. L. Yucas, *Generalized reciprocals, factors of Dickson polynomials and generalized cyclotomic polynomials over finite fields* Finite Fields Appl., **13**, (2007), 492-515.
- [40] R. W. Fitzgerald, J. L. Yucas, *Explicit Factorizations of Cyclotomic and Dickson Polynomials over Finite Fields*, In : Arithmetic of Finite Fields. Lecture Notes in Computer Science, vol. **4547**, pp. 110. Springer, Berlin (2007).
- [41] S. K. Gogia, I. S. Luthar, *Norms from certain extensions of  $\mathbb{F}_q(T)$* , Acta Arith., **38**, (1981), 325-340.
- [42] C. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sciences, **57**, (1863), 750-757; Oevres 2, Gauthier-Villars, Paris, (1908), 200-208.
- [43] R. Heyman, I. E. Shparlinski, *Counting irreducible binomials over finite fields*, Finite Fields Appl., **38**, (2016), 1-12.
- [44] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Comb. Theory, Ser. A, **118**, (2011), 448-454.
- [45] X. Hou, *A class of permutation trinomials over finite fields*, Acta Arith., **162**, (2014), 51-64.
- [46] X. Hou, *A class of permutation binomials over finite fields*, J. Number Theory, **133**, (2013), 3549-3558.

- [47] X. Hou, *Permutation polynomials over finite fields - a survey of recent advances*, Finite Fields Appl., **32**, (2015), 82-119.
- [48] L. Işık, A. Topuzoğlu, A. Winterhof, *Complete mappings and Carlitz rank*, Des. Codes Cryptogr. **85**, (1), (2017), 121-128.
- [49] L. Işık, A. Winterhof, *Carlitz rank and index of permutation polynomials*, Finite Fields Appl., **49**, (2018), 156-165.
- [50] J. von zur Gathen and V. Shoup, *Computing Frobenius maps and factoring polynomials*, Computational Complexity, **2**, (1992), 187-224.
- [51] T. Kalaycı, H. Stichtenoth, A. Topuzoğlu, *Irreducible factors of a class of permutation polynomials*, (2019), preprint.
- [52] E. Kalfoten, V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, Math. Comp., **67**, (1998), 1179-1197.
- [53] R. Lidl, H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl., vol. **20**, Cambridge Univ. Press, Cambridge, (1997).
- [54] R. Lidl, G.L. Mullen, *Cycle structure of Dickson permutation polynomials*, Math. J. Okayama Univ., **33**, (1991), 1-11.
- [55] A. F. Long, Jr., *Factorization of irreducible polynomials over a finite field with the substitution  $x^{p^r} - x$  for  $x$* , Duke Math. J., **40**, (1973), 63-76.
- [56] A. F. Long, Jr., *Factorization of irreducible polynomials over a finite field with the substitution  $x^{q^r} - x$  for  $x$* , Acta Arith., **25**, (1973), 65-80.
- [57] A. F. Long, Jr., T. P. Vaughan, *Factorization of  $q(h(T)(x))$  over a finite field, where  $q(x)$  is irreducible and  $h(T)(x)$  is linear II*, Linear Algebra Appl., **11**, (1975), 53-72.
- [58] A. F. Long, Jr., T. P. Vaughan, *Factorization of  $q(h(T)(x))$  over a finite field, where  $q(x)$  is irreducible and  $h(T)(x)$  is linear I*, Linear Algebra Appl., **13**, (1976), 207-221.



- [59] A. F. Long, Jr., *A theorem on factorable irreducible polynomials in several variables over a finite field with the substitution  $x_i^{q^r} - x_i$  for  $x_i$* , Math. Nachr. **63**, (1974), 123-130.
- [60] H. B. Mann, *The solutions of equations by radicals*, J. Algebra, **29**, (1974), 551-574.
- [61] F. E. Brochero Martinez, L. Reis, *Factoring polynomials of the form  $f(x^n) \in \mathbb{F}_q[x]$* , Finite Fields Appl., **49**, (2018), 166-179.
- [62] F. E. Brochero Martinez, C.R. Giraldo Vergara, L. Batista de Oliveira, *Explicit factorization of  $x^n - 1 \in \mathbb{F}_q[x]$* , Des. Codes Cryptogr., **77**, (2015), 277-286.
- [63] A. M. Masuda, D. Panario, and Q. Wang, *The number of permutation binomials over  $\mathbb{F}_{4p+1}$  where  $p$  and  $4p + 1$  are primes*, Electron. J. Combin., **13**, (2006), R65.
- [64] H. Meyn, *Factorization of the cyclotomic polynomials  $x^{2n} + 1$  over finite fields*, Finite Fields Appl. **2**, (1996), 439-442.
- [65] R. J. McEliece, *Table of polynomials of period  $e$  over  $GF(p)$* , Math. Comp., **23**, (1969), C1-C6.
- [66] G. Mullen, D. Panario: *Handbook of Finite Fields*, Chapman and Hall / CRC, (2013).
- [67] G. L. Mullen, I. Shparlinski, *Open problems and conjectures in finite fields*, (1996). In: S.D. Cohen, H. Niederreiter (Eds.), Finite Fields and Applications, London Math. Soc. Lecture Note Ser., vol. **233**, Cambridge University Press, 313-332.
- [68] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc., **36**, (1934), 243-274.
- [69] F. Pausinger, A. Topuzoğlu, *On the discrepancy of two families of permuted van der Corput sequences*, Unif. Distrib. Theory, **13**, (2018), no.1, 47-64.
- [70] A. E. Pellet, *Sur les fonctions irréductibles suivant un module premier et une fonction modulaire.*, C. R. Acad. Sci. Paris. **70**, (1870), 328-330.

- [71] M .D. Prešić, *A method for solving equations in finite fields*, Mat Vesnik, **7**, (1970), 507-509.
- [72] A.J. van der Poorten, *A quote*, Math. Intell., **7**, (2), (1985), 40.
- [73] M. Rabin, *Probabilistic algorithms in finite fields*, SIAM Journal on Computing, **9**, (1980), 273-280.
- [74] L. Rédei, *A short proof of a theorem of Št. Schwarz concerning finite fields*, Časopis Pěst. Mat. Fys., **75**, (1950), 211-212.
- [75] L. Reis, *Factorization of a class of composed polynomials*, Des. Codes Cryptogr., (2018), <https://doi.org/10.1007/s10623-018-0568-0>.
- [76] L. Reis, *On the factorization of iterated polynomials*, (2018), arXiv:1810.07715.
- [77] S. O. Šatunovskii, *Conditions for the existence of  $n$  distinct roots of a congruence of  $n$ th degree for a prime modulus* (Russian), Izv. Fiz.-Mat Obšč., Kazan, (2), **12**, no.3, (1902), 33-49.
- [78] Š. Schwarz, *A contribution to the reducibility of binomial congruences* (Slovak), Časopis Pěst. Mat. Fys., **71**, (1946), 21-31.
- [79] Š. Schwarz, *On the reducibility of binomial congruences and on the bound of the least integer belonging to a given exponent mod  $p$* , Časopis Pěst. Mat. Fys., **74**, (1949), 1-16.
- [80] J. A. Serret, *Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modularie irréductible*, Mém. Acad. Sci., Inst. de France **35**, (1866), 617-688.
- [81] J.-A. Serret, *Cours d'Algèbre Supérieure. Tome I*, Les Grands Classiques Gauthier- Villars. [Gauthier-Villars Great Classics]. Éditions Jacques Gabay, Sceaux, 1992, Reprint of the fourth (1877) edition.
- [82] I. E. Shparlinski, *Finite Fields : Theory and Computation*, Kluwer, Dordrecht, 1999.

- [83] A. Topuzođlu, *Carlitz rank of permutations of finite fields: A survey*, Journal of Symbolic Computation **64**, (2014), 182-193.
- [84] C. Tosun, *Explicit factorizations of generalized Dickson polynomials of order  $2m$  via generalized cyclotomic polynomials over finite fields*, Finite Fields Appl., **38**, (2016), 40-56.
- [85] A. Tuxanidy, Q. Wang, *Composed products and factors of cyclotomic polynomials over finite fields*, Des. Codes Cryptogr., **69**, (2), (2013), 203-231.
- [86] R. R. Varshamov, *A certain linear operator in a Galois field and its applications* (Russian), Studia, Sci. Math. Hungar., **8**, (1973), 5-19.
- [87] R. R. Varshamov, *Operator substitutions in a Galois field, and their applications* (Russian), Dokl. Akad. Nauk SSSR, **211**, (1973), 768-771.
- [88] L. Wang, Q. Wang, *On explicit factors of cyclotomic polynomials over finite fields*, Des. Codes Cryptogr., **63**, (1), (2012), 87-104.
- [89] K. S. Williams, *Note on Dickson's permutation polynomials*, Duke Math. J., **38**, (1971), 659-665.
- [90] K. S. Williams, *Polynomials with irreducible factors of specified degree*, Canad Math. Bull., **12**, (1969), 221-223.
- [91] H. Wu, L. Zhu, R. Feng, S. Yang, *Explicit factorizations of cyclotomic polynomials over finite fields*, Des. Codes Cryptogr., **83**, (1), (2016), 197-217.
- [92] Y. Wu, Q. Yue, S. Fan, *Further factorizations of  $x^n - 1$  over a finite field*, Finite Fields Appl., **54**, (2018), 197-215.
- [93] K. Zsigmondy, *Über die Anzahl derjenigen ganzen ganzzahligen Functionen  $n$ ten Grades von  $x$ , welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen.*, Sitzungsber. Wien Abt II, **103**, (1894), 135-144.