


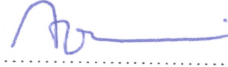
CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS  
VIA POLYNOMIAL COMPOSITION

APPROVED BY

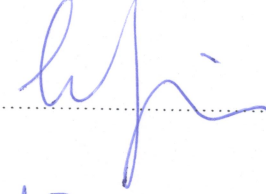
Prof. Dr. Henning Stichtenoth  
(Thesis Supervisor)



Prof. Dr. Alev Topuzoğlu



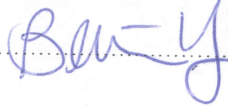
Assoc. Prof. Dr. Cem Güneri



Assist. Prof. Dr. Alp Bassa



Assoc. Prof. Dr. Berrin Yanıkoğlu



DATE OF APPROVAL: May 30, 2012

CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE  
FIELDS VIA POLYNOMIAL COMPOSITION

by  
FUNDA ÖZDEMİR

Submitted to the Graduate School of Engineering and Natural Sciences  
in partial fulfillment of  
the requirements for the degree of  
Master of Science  
Sabancı University  
Spring 2012

CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS  
VIA POLYNOMIAL COMPOSITION

APPROVED BY

Prof. Dr. Henning Stichtenoth .....  
(Thesis Supervisor)

Prof. Dr. Alev Topuzoğlu .....

Assoc. Prof. Dr. Cem Güneri .....

Assist. Prof. Dr. Alp Bassa .....

Assoc. Prof. Dr. Berrin Yanıkoğlu .....

DATE OF APPROVAL: May 30, 2012

©Funda Özdemir 2012

All Rights Reserved

CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS  
VIA POLYNOMIAL COMPOSITION

Funda Özdemir

Mathematics, Master Thesis, 2012

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Finite fields, irreducible polynomials, polynomial composition methods,  
linearized polynomials, primitive polynomials, composed product.

**Abstract**

The construction of irreducible polynomials over finite fields is currently a strong subject of interest with important applications including coding theory and cryptography. One of the most popular methods of construction of irreducible polynomials is the method of composition of polynomials where irreducible polynomials of relatively higher degrees are generated from irreducible polynomials of relatively lower degrees. In this thesis, we give some polynomial composition methods and several applications of them.

# SONLU CİSİMLER ÜZERİNDE POLİNOM BİLEŞİMİ METODU İLE İNDİRGENEMEZ POLİNOM İNŞASI

Funda Özdemir

Matematik, Yüksek Lisans Tezi, 2012

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Sonlu cisimler, indirgenemez polinomlar, polinom bileşimi yöntemleri, doğrusallaştırılmış polinomlar, ilkel polinomlar, bileşke çarpım.

## Özet

Sonlu cisimler üzerinde indirgenemez polinomların inşası, kodlama teorisi ve kriptografideki önemli uygulamaları da dahil olmak üzere son zamanlarda güçlü bir ilgi odağı oluşturmaktadır. İndirgenemez polinomların inşasında en popüler yöntemlerden biri olan polinom bileşimi metodunda, düşük dereceli indirgenemez polinomlardan yüksek dereceli indirgenemez polinomlar elde edilir. Bu tezde, bir takım polinom bileşimi yöntemleri ile bunların uygulamalarına yer verilmiştir.

*to my parents and my husband*

## Acknowledgements

First of all, I would like to express my appreciation to my supervisor Prof. Dr. Henning Stichtenoth for his patience, understanding, and guidance throughout my thesis. It has been an honor to work with him.

I also thank Prof. Dr. Alev Topuzođlu who has supported me during my thesis with her knowledge and guidance.

Special thanks also to all my graduate friends in the Mathematics Program for their helps and friendships.

Finally, the most special thanks goes to my family who have motivated and supported me unconditionally throughout my whole life, and my husband for his endless love and support.



## Table of Contents

Abstract	iv
Özet	v
Acknowledgements	vii
Introduction	ix
1 First Composition Method	1
2 Irreducibility of Polynomials of the Form $g(x)^n P(f(x)/g(x))$	7
3 Recursive Constructions	12
4 Composed Product of Polynomials	16
Bibliography	20

## Introduction

Let  $\mathbb{F}_q$  be the finite field of order  $q = p^s$  and of characteristic  $p$ , where  $p$  is a prime and  $s$  is a positive integer,  $\mathbb{F}_q^*$  be its multiplicative group which is cyclic. A generator of the cyclic group  $\mathbb{F}_q^*$  is called a primitive element of  $\mathbb{F}_q$  and its minimal polynomial over  $\mathbb{F}_p$  is called a primitive polynomial.

Throughout this thesis, we assume, unless otherwise specified, that the considered polynomials are monic, i.e. with leading coefficient 1. Let  $f(x)$  be an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$  and let  $\beta$  be a root of  $f(x)$ . The field  $\mathbb{F}_q(\beta) = \mathbb{F}_{q^n}$  is a degree  $n$  extension of  $\mathbb{F}_q$  and can be viewed as a vector space of dimension  $n$  over  $\mathbb{F}_q$ . Moreover, the conjugates of  $\beta$  with respect to  $\mathbb{F}_q$ , namely  $\beta, \beta^q, \dots, \beta^{q^{n-1}}$ , are all the roots of  $f(x)$ .

The subject of irreducible polynomials over finite fields along with several construction methods has been of considerable interest in recent years. Such polynomials, which have both theoretical and practical importance, are used to perform arithmetic in finite fields and are found in many applications, including coding theory and cryptography. One of the most popular methods of construction is the method of composition of polynomials where irreducible polynomials of relatively higher degree are produced from given irreducible polynomials of relatively lower degrees. There is a detailed literature on the problem of irreducibility of polynomial composition by several authors including Cohen, Kyureghyan-Kyureghyan, Varshamov who have approached this problem from different aspects. In this thesis, we intend to give a survey of works about polynomial composition methods.

- In Chapter 1, we present the approach of Kyureghyan-Kyureghyan [5] to the construction of irreducible polynomials over  $\mathbb{F}_q$ . Theorem 1.4 is used to obtain explicit families of irreducible polynomials of degrees  $n(q^n - 1)$  and  $n(q^n + 1)$  over  $\mathbb{F}_q$ , where  $n$  is a natural number. At the end of this chapter, the result of Cohen [3] which is one of the most applicable results in this area is proved using Theorem 1.4.
- In Chapter 2, by using the result of Cohen [3] in the previous chapter and some auxiliary results, the irreducibility of compositions of irreducible polynomials in the form  $P(f/g) := (g(x))^n P(f(x)/g(x))$  is studied for some specified relatively prime polynomials  $f$  and  $g$ , and any degree  $n$  polynomial  $P$ .
- In Chapter 3, we present how to construct recursively irreducible polynomials, using the irreducibility criteria developed in Chapter 2.
- In the final chapter, we introduce first the notion of composed product by Brawley and Carlitz [2] and state an important theorem, again due to Brawley and Carlitz [2], which says how to construct irreducible polynomials of degree  $mn$  from irreducible polynomials of degrees  $m$  and  $n$  with  $\gcd(m, n) = 1$  through the use of composed product. Moreover, we restate a result of Varshamov in [10] and a result in [5] more directly, and we prove them by using a consequence of the theorem of Brawley and Carlitz.

## First Composition Method

We say that the degree of an element  $\alpha$  over  $\mathbb{F}_q$  is equal to  $k$  and write  $\deg_q(\alpha) = k$  if  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$  or equivalently  $\alpha \in \mathbb{F}_{q^k}$  and  $\alpha \notin \mathbb{F}_{q^\nu}$  for any proper divisor  $\nu$  of  $k$ . Similarly, we say that the degree of a subset  $A = \{\alpha_1, \alpha_2, \dots, \alpha_r\} \subset \mathbb{F}_{q^k}$  over  $\mathbb{F}_q$  is equal to  $k$  and write  $\deg_q(\alpha_1, \alpha_2, \dots, \alpha_r) = k$ , if for any proper divisor  $\nu$  of  $k$  there exists at least one element  $\alpha_u \in A$  such that  $\alpha_u \notin \mathbb{F}_{q^\nu}$ .

We begin with the following well known results which can be found in [6].

**Proposition 1.1** ([6], Theorem 3.46). *Let  $f(x)$  be a monic irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$  and let  $k \in \mathbb{N}$ . Then  $f(x)$  factors into  $d$  irreducible polynomials in  $\mathbb{F}_{q^k}[x]$  of the same degree  $n/d$ , where  $d = \gcd(n, k)$ .*

**Proposition 1.2** ([6], Corollary 3.47). *An irreducible polynomial over  $\mathbb{F}_q$  of degree  $n$  remains irreducible over  $\mathbb{F}_{q^k}$  if and only if  $k$  and  $n$  are relatively prime.*

Given  $0 \leq \nu \leq k - 1$  and  $g(x) = \sum_{i=0}^m b_i x^i \in \mathbb{F}_{q^k}[x]$ , we use the notation

$$g^{(\nu)}(x) = \sum_{i=0}^m b_i^{q^\nu} x^i,$$

where  $g(x) = g^{(0)}(x)$ .

**Lemma 1.3.** *Let  $f(x)$  be a monic irreducible polynomial of degree  $dk$  over  $\mathbb{F}_q$ . Then there is a monic irreducible divisor  $g(x)$  of degree  $k$  of  $f(x)$  in  $\mathbb{F}_{q^d}[x]$ . Moreover, every irreducible factor of  $f(x)$  in  $\mathbb{F}_{q^d}[x]$  is given by  $g^{(\nu)}(x)$  for some  $0 \leq \nu \leq d - 1$ . In particular, the factorization of  $f(x)$  in  $\mathbb{F}_{q^d}[x]$  is*

$$f(x) = \prod_{\nu=0}^{d-1} g^{(\nu)}(x)$$

*Proof.* By Proposition 1.1,  $f(x)$  factors into  $d$  monic irreducible polynomials in  $\mathbb{F}_{q^d}[x]$  of the same degree  $k$ . Let  $\alpha \in \mathbb{F}_{q^{dk}}$  be a root of  $f(x)$ . Then all the roots of  $f(x)$  are the conjugates of  $\alpha$  with respect to  $\mathbb{F}_q$ , namely  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{dk-1}}$ . Let  $g(x)$  be a monic irreducible divisor of  $f(x)$  of degree  $k$  in  $\mathbb{F}_{q^d}[x]$  assuming  $\alpha$  as a root. Then all the roots of  $g(x)$  are the conjugates of  $\alpha$  with respect to  $\mathbb{F}_{q^d}$ , which are  $\alpha, \alpha^{q^d}, \alpha^{q^{2d}}, \dots, \alpha^{q^{(k-1)d}}$ .

Hence we can write the factorization of  $g(x)$  and  $g^{(\nu)}(x)$ , for  $0 \leq \nu \leq d-1$ , over  $\mathbb{F}_{q^{dk}}$  as

$$\begin{aligned} g(x) &= (x - \alpha)(x - \alpha^{q^d})(x - \alpha^{q^{2d}}) \cdots (x - \alpha^{q^{dk-d}}) \\ g^{(1)}(x) &= (x - \alpha^q)(x - \alpha^{q^{d+1}})(x - \alpha^{q^{2d+1}}) \cdots (x - \alpha^{q^{dk-d+1}}) \\ g^{(2)}(x) &= (x - \alpha^{q^2})(x - \alpha^{q^{d+2}})(x - \alpha^{q^{2d+2}}) \cdots (x - \alpha^{q^{dk-d+2}}) \\ &\vdots \\ g^{(d-1)}(x) &= (x - \alpha^{q^{d-1}})(x - \alpha^{q^{2d-1}})(x - \alpha^{q^{3d-1}}) \cdots (x - \alpha^{q^{dk-1}}) \end{aligned}$$

Both polynomials  $f(x)$  and  $\prod_{\nu=0}^{d-1} g^{(\nu)}(x)$  of the same degree  $dk$  have the same  $dk$  distinct roots in  $\mathbb{F}_{q^{dk}}$ . Therefore they are equal.  $\square$

The converse of Lemma 1.3 does not hold in general: Given an irreducible polynomial of degree  $k$  over  $\mathbb{F}_{q^d}$ , the product  $\prod_{\nu=0}^{d-1} g^{(\nu)}(x)$  is a polynomial over  $\mathbb{F}_q$ , but it is not necessarily irreducible over  $\mathbb{F}_q$ . To ensure the converse statement,  $g(x)$  must be described precisely as stated in the following theorem.

**Theorem 1.4** ([5], Lemma 1). *A monic polynomial  $f(x) \in \mathbb{F}_q[x]$  of degree  $n = dk$  is irreducible over  $\mathbb{F}_q$  if and only if there is a monic irreducible polynomial  $g(x) = \sum_{i=0}^k g_i x^i$  over  $\mathbb{F}_{q^d}$  of degree  $k$  such that  $\mathbb{F}_q(g_0, \dots, g_k) = \mathbb{F}_{q^d}$  and  $f(x) = \prod_{\nu=0}^{d-1} g^{(\nu)}(x)$  in  $\mathbb{F}_{q^d}[x]$ .*

*Proof.* Suppose  $f(x)$  is irreducible over  $\mathbb{F}_q$ . Then by Lemma 1.3 there is an irreducible polynomial  $g(x) = \sum_{i=0}^k g_i x^i$  of degree  $k$  over  $\mathbb{F}_{q^d}$  such that

$$f(x) = \prod_{\nu=0}^{d-1} g^{(\nu)}(x) \tag{1.1}$$

over  $\mathbb{F}_{q^d}$ . Next we show that the set of coefficients of  $g(x)$  generates  $\mathbb{F}_{q^d}$ . Suppose, on the contrary, that  $\mathbb{F}_q(g_0, \dots, g_k) = \mathbb{F}_{q^s}$ , for some proper divisor  $s$  of  $d$  with  $d = rs$ . Then, because of  $\mathbb{F}_{q^s}[x] \subset \mathbb{F}_{q^d}[x]$ , the polynomial  $g(x)$  is also irreducible over  $\mathbb{F}_{q^s}$  and by Lemma 1.3

$$f(x) = \prod_{\omega=0}^{s-1} h^{(\omega)}(x) \tag{1.2}$$

over  $\mathbb{F}_{q^s}$  and  $h^{(\omega)}(x) = \sum_{j=0}^{rk} h_j^{q^\omega} x^j$ ,  $0 \leq \omega \leq s-1$ , are distinct irreducible polynomials of degree  $rk$  over  $\mathbb{F}_{q^s}$ . Then, by combining the equations (1.1) and (1.2), we get

$$f(x) = \prod_{\omega=0}^{s-1} h^{(\omega)}(x) = \prod_{\nu=0}^{d-1} g^{(\nu)}(x)$$

in  $\mathbb{F}_{q^s}[x]$ , which contradicts to the uniqueness of the decomposition into irreducible factors in  $\mathbb{F}_{q^s}[x]$ .

For the proof of the converse, let  $g(x) = \sum_{i=0}^k g_i x^i$  be an irreducible polynomial of degree  $k$  over  $\mathbb{F}_{q^d}$  with  $\mathbb{F}_q(g_0, \dots, g_k) = \mathbb{F}_{q^d}$  and let  $\alpha \in \mathbb{F}_{q^{dk}}$  be a zero of  $g(x)$ . Further, let  $f(x)$  be the minimal polynomial of  $\alpha$  over  $\mathbb{F}_q$  of degree  $n$ . We want to prove that  $n = dk$ . Let  $l = \gcd(n, k)$ . Then  $f$  has exactly  $l$  irreducible factors in  $\mathbb{F}_{q^d}[x]$ , by Proposition 1.1. Since  $g$  divides  $f$  over  $\mathbb{F}_{q^d}$ , we get

$$f(x) = \prod_{\nu=0}^{l-1} g^{(\nu)}(x).$$

However,  $f$  factors into  $l$  irreducible polynomials also over  $\mathbb{F}_{q^l} \subseteq \mathbb{F}_{q^d}$ . The condition  $\mathbb{F}_q(g_0, \dots, g_k) = \mathbb{F}_{q^d}$  forces  $l = d$  which means  $d$  divides  $n$ . Hence we have shown that  $\mathbb{F}_{q^d}$  is a subfield of  $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ , implying that  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}(\alpha)$ , i.e.  $\mathbb{F}_{q^n} = \mathbb{F}_{q^{dk}}$  and consequently  $n = dk$ .  $\square$

Now we obtain explicit families of irreducible polynomials of degree  $n(q^n - 1)$  from a given primitive polynomial of degree  $n$  over  $\mathbb{F}_q$ , using Theorem 1.4 and the following theorem.

**Theorem 1.5** ([1] Chapter 5, Theorem 24 (Dickson's theorem)). *Let  $q = p^s$ ,  $m$  be a divisor of  $s$  and  $p^m \neq 2$ . Suppose  $\beta, \theta \in \mathbb{F}_q$  and  $\theta$  is a primitive element of  $\mathbb{F}_q$ . Then the polynomial*

$$f(x) = x^{p^m} - \theta x + \beta$$

*is the product of a linear polynomial and an irreducible polynomial of degree  $p^m - 1$  over  $\mathbb{F}_q$ .*

**Theorem 1.6** ([5], Theorem 7). *Let  $q^n > 2$ ,  $\beta, \gamma \in \mathbb{F}_q$ ,  $\beta \neq -\gamma$  and  $f(x)$  be a primitive polynomial of degree  $n$  over  $\mathbb{F}_q$ . Set  $h(x) = f((\beta + \gamma)x + 1)$  and  $h^*(x) = x^n h(\frac{1}{x})$ . Then the polynomial*

$$F(x) = (x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right) \left(h^*(x - \gamma)\right)^{-1}$$

*is an irreducible polynomial of degree  $n(q^n - 1)$  over  $\mathbb{F}_q$ .*

*Proof.* Let  $\alpha$  be a root of  $f(x)$ . Then

$$f(x) = \prod_{\nu=0}^{n-1} \left(x - \alpha^{q^\nu}\right) \tag{1.3}$$

holds in  $\mathbb{F}_{q^n}[x]$ . Substituting  $(x - \gamma)^{-1}(x^{q^n} + \beta)$  for  $x$  in (1.3), and multiplying both sides of the equation by  $(x - \gamma)^n$ , we get

$$\begin{aligned} (x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right) &= \prod_{\nu=0}^{n-1} \left(x^{q^n} - \alpha^{q^\nu} x + \beta + \gamma \alpha^{q^\nu}\right) \\ &= \prod_{\nu=0}^{n-1} \left(x^{q^n} - \alpha x + \beta + \gamma \alpha\right)^{(\nu)} \end{aligned}$$

Since  $q^n > 2$  and  $\alpha^{q^\nu}$  is a primitive element in  $\mathbb{F}_{q^n}$ , by Theorem 1.5 each of the polynomials  $g^{(\nu)}(x) := (x^{q^n} - \alpha^{q^\nu}x + \beta + \gamma\alpha^{q^\nu})$  is product of a linear polynomial and an irreducible polynomial of degree  $q^n - 1$  over  $\mathbb{F}_{q^n}$ . Also if  $\theta$  is a root of  $g(x)$  in  $\mathbb{F}_{q^n}$ , then  $\theta^{q^\nu} \in \mathbb{F}_{q^n}$  is a root of  $g^{(\nu)}(x)$ , where  $\theta^{q^\nu} = (\beta + \gamma\alpha^{q^\nu})(\alpha^{q^\nu} - 1)^{-1}$ . Thus the linear factor of  $g^{(\nu)}$  is  $x - \theta^{q^\nu}$  and the irreducible factor of  $g^{(\nu)}$  is

$$Q^{(\nu)}(x) = \frac{x^{q^n} - \alpha^{q^\nu}x + \beta + \gamma\alpha^{q^\nu}}{x - \theta^{q^\nu}} = \frac{x^{q^n} - \theta^{q^{n+\nu}} - \alpha^{q^\nu}(x - \theta^{q^\nu})}{x - \theta^{q^\nu}}$$

over  $\mathbb{F}_{q^n}$ . Note that the constant term of  $Q^{(\nu)}(x)$  is  $1 - \alpha^{q^\nu}$ , and in particular the degree of the set of its coefficients is  $n$  over  $\mathbb{F}_q$ . Therefore, by Theorem 1.4 the polynomial  $\prod_{\nu=0}^{n-1} Q^{(\nu)}(x)$  is irreducible over  $\mathbb{F}_q$ . To complete the proof observe that  $(\beta + \gamma)^{-1}(\alpha - 1)$  is a root of  $h(x) = f((\beta + \gamma)x + 1)$  and so  $\theta = (\beta + \gamma)(\alpha - 1)^{-1} + \gamma$  is a root of  $(h^*(x - \gamma))$ . Then in  $\mathbb{F}_{q^n}[x]$  it holds

$$\prod_{\nu=0}^{n-1} (x - \theta^{q^\nu}) = h^*(x - \gamma)$$

which yields

$$F(x) = \frac{(x - \gamma)^n f\left((x - \gamma)^{-1}(x^{q^n} + \beta)\right)}{\prod_{\nu=0}^{n-1} (x - \theta^{q^\nu})} = \prod_{\nu=0}^{n-1} Q^{(\nu)}(x)$$

Finally, the irreducibility of  $F(x)$  over  $\mathbb{F}_q$  follows from Theorem 1.4.  $\square$

Further we use the following result by Sidelnikov [9] that enables explicit constructions of irreducible polynomials of degree  $n(q^n + 1)$ .

**Theorem 1.7.** *Let  $\omega \in \mathbb{F}_q$  and  $x_0 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$  such that  $x_0^{q+1} = 1$ . Then the polynomial*

$$f(x) = x^{q+1} - \omega x^q - (x_0 + x_0^q - \omega)x + 1 \in \mathbb{F}_q[x]$$

*is irreducible if and only if  $\frac{\omega - x_0^q}{\omega - x_0}$  is a generating element of the multiplicative subgroup  $S := \{y \in \mathbb{F}_{q^2} | y^{q+1} = 1\}$  of  $\mathbb{F}_{q^2}$ .*

**Theorem 1.8** ([5], Theorem 9). *Let  $f(x)$  be an irreducible polynomial of degree  $2n$  over  $\mathbb{F}_q$  of order  $e(q^n + 1)$ . Further let  $\psi(x) \in \mathbb{F}_q[x]$  be the minimal polynomial of  $\beta^{q^n} + \beta + 1$ , where  $\beta = \alpha^e$  for a root  $\alpha \in \mathbb{F}_{q^{2n}}$  of  $f(x)$ . Then the polynomial*

$$x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1$$

*is irreducible over  $\mathbb{F}_{q^n}$ . Moreover,  $\psi(x)$  and  $F(x) = x^n \psi\left(\frac{x^{q^n+1} + x^{q^n} + 1}{x}\right)$  are irreducible polynomials over  $\mathbb{F}_q$  of degrees  $n$  and  $n(q^n + 1)$ , respectively.*

*Proof.* Since  $\text{ord}(f(x)) = e(q^n + 1)$  and  $f(x)$  is irreducible, we have that  $\alpha^{e(q^n+1)} = \beta^{q^n+1} = 1$ . Thus  $\text{ord}_q(\beta) = q^n + 1$  which does not divide  $q^k - 1$  for  $k \leq n$  but  $q^{2n} - 1$ . Hence  $\deg_q(\beta) = 2n$ . Because  $\beta \in \mathbb{F}_{q^{2n}}$ ,  $(\beta^{q^n} + \beta + 1)^{q^n} = \beta^{q^n} + \beta + 1$  which means  $\lambda := \beta^{q^n} + \beta + 1 \in \mathbb{F}_{q^n}$ . Next we show that  $\deg_q \lambda = n$ . Indeed, suppose that  $\lambda \in \mathbb{F}_{q^d}$  for some divisor  $d$  of  $n$ . We have

$$\beta\lambda = \beta^{q^n+1} + \beta^2 + \beta = 1 + \beta^2 + \beta,$$

and consequently,  $\beta^2 + (1 - \lambda)\beta + 1 = 0$ . Therefore  $\beta$  is a root of the quadratic polynomial  $x^2 - (1 - \lambda)x + 1$  over  $\mathbb{F}_{q^d}$ , implying that  $[\mathbb{F}_{q^{2n}} : \mathbb{F}_{q^d}] \leq 2$  and thus  $d = n$ . Since  $\psi(x)$  is the minimal polynomial of  $\lambda$ ,  $\deg(\psi(x)) = n$ .

Next we show that the conditions of Theorem 1.7 are fulfilled also. Indeed, since  $\beta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$  such that  $\beta^{q^n+1} = 1$ , choose  $x_0 = \beta$  and  $\omega = -1$ . It remains to note that  $\frac{\omega - x_0^{q^n}}{\omega - x_0} = \frac{-1 - \beta^{q^n}}{-1 - \beta} = \beta^{q^n}$  generates S. Therefore, by Theorem 1.7,  $x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1$  is irreducible over  $\mathbb{F}_{q^n}$ .

To complete the proof, we show that  $F(x)$  is irreducible of degree  $n(q^n + 1)$  over  $\mathbb{F}_q$ . Since  $\psi(x)$  is the minimal polynomial of  $\beta^{q^n} + \beta + 1$  over  $\mathbb{F}_q$ ,

$$\psi(x) = \prod_{\nu=0}^{n-1} (x - (\beta^{q^n} + \beta + 1)^{q^\nu}). \quad (1.4)$$

Substituting  $\frac{x^{q^n+1} + x^{q^n} + 1}{x}$  for  $x$  in (1.4), and multiplying both sides of the equation by  $x^n$ , we obtain

$$\begin{aligned} F(x) = x^n \psi\left(\frac{x^{q^n+1} + x^{q^n} + 1}{x}\right) &= \prod_{\nu=0}^{n-1} (x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)^{q^\nu} x + 1) \\ &= \prod_{\nu=0}^{n-1} (x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1)^{(q^\nu)}. \end{aligned}$$

By Theorem 1.4,  $F(x)$  is irreducible over  $\mathbb{F}_q$  since  $x^{q^n+1} + x^{q^n} - (\beta^{q^n} + \beta + 1)x + 1$  is irreducible over  $\mathbb{F}_{q^n}$  and  $\deg_q(\beta^{q^n} + \beta + 1) = n$ .  $\square$

The following result by S. Cohen [3] was employed by several authors to give iterative constructions of irreducible polynomials over finite fields and Theorem 1.4 yields a proof for this result.

**Theorem 1.9** ([3], Lemma 1). *Let  $f(x), g(x) \in \mathbb{F}_q[x]$  be relatively prime polynomials and let  $P(x) \in \mathbb{F}_q[x]$  be an irreducible polynomial of degree  $n$ . Then the composition*

$$F(x) = g(x)^n P(f(x)/g(x))$$

*is irreducible over  $\mathbb{F}_q$  if and only if  $f(x) - \lambda g(x)$  is irreducible over  $\mathbb{F}_{q^n}$  for some root  $\lambda \in \mathbb{F}_{q^n}$  of  $P(x)$ .*

*Proof.* Let  $\lambda \in \mathbb{F}_{q^n}$  be a root of  $P(x)$ . Since all the roots of  $P(x)$  are the conjugates of  $\lambda$ , the polynomial  $P(x)$  is the product  $\prod_{\nu=0}^{n-1} (x - \lambda^{q^\nu})$  and thus

$$F(x) = g(x)^n P(f(x)/g(x)) = \prod_{\nu=0}^{n-1} (f(x) - \lambda^{q^\nu} g(x)) = \prod_{\nu=0}^{n-1} (f(x) - \lambda g(x))^{(\nu)}$$

is irreducible over  $\mathbb{F}_q$  if and only if  $f(x) - \lambda g(x)$  is irreducible over  $\mathbb{F}_{q^n}$ , by Theorem 1.4. □



## Irreducibility of Polynomials of the Form $g(x)^n P(f(x)/g(x))$

Let  $f(x), g(x) \in \mathbb{F}_q[x]$  and let  $P(x) = \sum_{i=0}^n c_i x^i \in \mathbb{F}_q[x]$  of degree  $n$ . Then the following composition

$$P(f/g) := g(x)^n P(f(x)/g(x)) = \sum_{i=0}^n c_i f(x)^i g(x)^{n-i}$$

is again a polynomial in  $\mathbb{F}_q[x]$ . Theorem 1.9 establishes the conditions under which the composition polynomial  $P(f/g)$  is irreducible over  $\mathbb{F}_q[x]$ .

**Definition 2.1.** For  $\alpha \in \mathbb{F}_{q^n}$  the *trace* of  $\alpha$ , denoted by  $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ , is defined by

$$Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-2}} + \alpha^{q^{n-1}}.$$

For convenience, we denote  $Tr_{\mathbb{F}_{q^n}/\mathbb{F}_q} = Tr_{q^n/q}$ .

**Definition 2.2.** A *trinomial* is a polynomial with three nonzero terms, one of them being the constant term.

**Definition 2.3.** A polynomial of the form

$$l(x) = \sum_{i=0}^n a_i x^{q^i}$$

with coefficients in  $\mathbb{F}_q$  is called a *linearized polynomial* over  $\mathbb{F}_q$ .

**Definition 2.4.** A polynomial of the form  $l(x) - b \in \mathbb{F}_q[x]$ , where  $l(x)$  is a linearized polynomial over  $\mathbb{F}_q$  and  $b \in \mathbb{F}_q$ , is called an *affine polynomial* over  $\mathbb{F}_q$ .

**Proposition 2.5** ([7], Lemma 3.4). *Suppose that the linearized polynomial  $l(x)$  has no nonzero root in  $\mathbb{F}_q$ . Then for any  $b \in \mathbb{F}_q$ , the affine polynomial  $l(x) - b$  has a linear factor  $x - A$ ,  $A \in \mathbb{F}_q$ .*

**Proposition 2.6** ([7], Theorem 3.5). *With the notation of Proposition ??, the trinomial  $x^p - x - \alpha$  is irreducible in  $\mathbb{F}_q[x]$  if and only if  $Tr_{q/p}(\alpha) \neq 0$ .*

**Proposition 2.7** ([7], Corollary 3.6). *For  $a, b \in \mathbb{F}_q^*$ , the trinomial  $x^p - ax - b$  is irreducible over  $\mathbb{F}_q$  if and only if  $a = A^{p-1}$  for some  $A \in \mathbb{F}_q^*$  and  $Tr_{q/p}(b/A^p) \neq 0$ .*

Now we consider some special cases of  $P(f/g)$ :

(a)  $f(x) = x^2 + 1$  and  $g(x) = x$ . Then  $P(f/g) = x^n P(x + x^{-1})$ . We distinguish the cases:  $q$  even and  $q$  odd.

Recall that if  $h(x)$  is a polynomial of degree  $k$  then its *reciprocal* is the polynomial  $h^*(x) = x^k h(1/x)$ , and if  $h(x) = h^*(x)$  then  $h(x)$  is said to be self-reciprocal.

**Theorem 2.8.** *Let  $q = 2^m$  and let  $P(x) = \sum_{i=0}^n c_i x^i \in \mathbb{F}_q[x]$  be irreducible over  $\mathbb{F}_q$  of degree  $n$  and with  $c_0 \neq 0$ . Then  $x^n P(x + x^{-1})$  is a self-reciprocal polynomial of degree  $2n$  over  $\mathbb{F}_q$ , and*

(i)  $x^n P(x + x^{-1})$  is irreducible over  $\mathbb{F}_q$  if and only if  $\text{Tr}_{q/2}(c_1/c_0) \neq 0$ .

(ii)  $x^n P^*(x + x^{-1})$  is irreducible over  $\mathbb{F}_q$  if and only if  $\text{Tr}_{q/2}(c_{n-1}/c_n) \neq 0$ .

*Proof.* Let  $R(x) = x^n P(x + x^{-1})$ . Clearly,  $R(x)$  is of degree  $2n$  and

$$x^{2n} R(1/x) = x^{2n} x^{-n} P(x + x^{-1}) = R(x)$$

Thus  $R(x)$  is self-reciprocal.

Now we prove (i); the proof of (ii) is similar. By Theorem 1.9,  $R(x)$  is irreducible over  $\mathbb{F}_q$  if and only if  $x^2 + 1 - \alpha x$  is irreducible over  $\mathbb{F}_{q^n}$  for some root  $\alpha \in \mathbb{F}_{q^n}$  of  $P(x)$ . By Proposition 2.7, the last condition is equivalent to  $\text{Tr}_{q^n/2}(\alpha^{-2}) \neq 0$ . Since

$$\begin{aligned} \text{Tr}_{q^n/2}(\alpha^{-2}) &= (\text{Tr}_{q^n/2}(\alpha^{-1}))^2 = (\text{Tr}_{q/2}(\text{Tr}_{q^n/2}(\alpha^{-1})))^2 \\ &= (\text{Tr}_{q/2}(-c_1/c_0))^2 \\ &= (\text{Tr}_{q/2}(c_1/c_0))^2, \end{aligned}$$

it is also equivalent to  $(\text{Tr}_{q/2}(c_1/c_0)) \neq 0$ . □

Part (i) of Theorem 2.8 was obtained by Meyn ([8], Theorem 6), and part (ii) is stated as Theorem 3.10(ii) in [7].

**Theorem 2.9** ([8], Theorem 8). *Let  $q$  be a power of an odd prime and  $P(x)$  be an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$ . Then  $x^n P(x + x^{-1})$  is irreducible over  $\mathbb{F}_q$  if and only if  $P(2)P(-2) \notin \mathbb{F}_q^{*2}$ .*

*Proof.* By Theorem 1.9,  $x^n P(x + x^{-1})$  is irreducible over  $\mathbb{F}_q$  if and only if  $x^2 - \alpha x + 1$  is irreducible over  $\mathbb{F}_{q^n}$ , where  $\alpha$  is a root of  $P(x)$ . This is equivalent to the condition  $\alpha^2 - 4 \notin \mathbb{F}_{q^n}^{*2}$ , which is true if and only if

$$\begin{aligned} -1 &= (\alpha^2 - 4)^{(q^n-1)/2} \\ &= \{[(2 - \alpha)(-2 - \alpha)]^{(q^n-1)/(q-1)}\}^{(q-1)/2} \\ &= \left\{ \prod_{i=0}^{n-1} [(2 - \alpha)(-2 - \alpha)]^{q^i} \right\}^{(q-1)/2} \\ &= \left\{ \prod_{i=0}^{n-1} (2 - \alpha^{q^i})(-2 - \alpha^{q^i}) \right\}^{(q-1)/2} \\ &= \{P(2)P(-2)\}^{(q-1)/2} \end{aligned}$$

that is,  $P(2)P(-2) \notin \mathbb{F}_q^{*2}$ . □

**Corollary 2.10** ([7], Corollary 3.12). *Let  $q$  be an odd prime power and  $P(x)$  be an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$ . Then  $2^n x^n P((x+x^{-1})/2)$  is irreducible over  $\mathbb{F}_q$  if and only if  $P(1)P(-1) \notin \mathbb{F}_q^{*2}$ .*

*Proof.* Let  $P_0(x) = 2^n P(x/2)$  and apply Theorem 2.9 to  $P_0(x)$ . □

(b)  $f(x) = x^p - x - b$  and  $g(x) = 1$ . Then  $P(f/g) = P(x^p - x - b)$ .

**Theorem 2.11** ([7], Theorem 3.13). *Let  $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$  be an irreducible polynomial over  $\mathbb{F}_q$  of characteristic  $p$  and let  $b \in \mathbb{F}_q$ . Then the polynomial  $P(f/g) = P(x^p - x - b)$  is irreducible over  $\mathbb{F}_q$  if and only if  $\text{Tr}_{q/p}(nb - a_{n-1}) \neq 0$ .*

*Proof.* Let  $\alpha$  be a root of  $P(x)$  in  $\mathbb{F}_{q^n}$ . By Theorem 1.9,  $P(x^p - x - b)$  is irreducible over  $\mathbb{F}_q$  if and only if  $x^p - x - b - \alpha$  is irreducible over  $\mathbb{F}_{q^n}$ . By Proposition 2.6 this is equivalent to the condition

$$\begin{aligned} \text{Tr}_{q^n/p}(b + \alpha) &= \text{Tr}_{q/p}(\text{Tr}_{q^n/q}(b + \alpha)) \\ &= \text{Tr}_{q/p}(nb - a_{n-1}) \neq 0. \end{aligned}$$

□

(c)  $f(x) = l(x)$  is a linearized polynomial and  $g(x) = 1$ . The irreducibility of these types of polynomials was established by Agou in a series of papers in 1977, 1978, 1980. First we consider the simple case  $l(x) = x^p - ax$ , where  $a \in \mathbb{F}_q^*$ . Then  $P(f/g) = P(x^p - ax)$ .

**Theorem 2.12** ([7], Theorem 3.14). *Let  $P(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$  be an irreducible polynomial over  $\mathbb{F}_q$  of characteristic  $p$  and let  $\alpha$  be a root of  $P(x)$ . Then for any  $a \in \mathbb{F}_q^*$ ,  $P(x^p - ax)$  is irreducible over  $\mathbb{F}_q$  if and only if*

$$a^{n_1(q-1)/(p-1)} = 1 \quad \text{and} \quad \text{Tr}_{q^n/p}(\alpha/A^p) \neq 0,$$

where  $n_1 = \gcd(n, p-1)$  and  $A \in \mathbb{F}_{q^n}^*$  such that  $A^{p-1} = a$ . In particular, if  $A \in \mathbb{F}_q^*$  then  $P(x^p - A^{p-1}x)$  is irreducible over  $\mathbb{F}_q$  if and only if  $\text{Tr}_{q/p}(c_{n-1}/A^p) \neq 0$ .

*Proof.* By Theorem 1.9,  $P(x^p - ax)$  is irreducible over  $\mathbb{F}_q$  if and only if  $x^p - ax - \alpha$  is irreducible over  $\mathbb{F}_{q^n}$ . By Proposition 2.7, this is equivalent to  $a = A^{p-1}$  for some  $A \in \mathbb{F}_{q^n}^*$  and  $\text{Tr}_{q^n/p}(\alpha/A^p) \neq 0$ . Clearly,  $a = A^{p-1}$  for some  $A \in \mathbb{F}_{q^n}^*$  if and only if

$$a^{(q^n-1)/(p-1)} = 1 \tag{2.1}$$

Since  $a \in \mathbb{F}_q^*$ ,  $a^{q-1} = 1$ . Thus (2.1) holds if and only if  $a^h = 1$ , where

$$h = \gcd\left(\frac{q^n - 1}{p - 1}, q - 1\right) = \frac{q - 1}{p - 1} \gcd\left(\frac{q^n - 1}{q - 1}, p - 1\right)$$

But  $(q^n - 1)/(q - 1) = q^{n-1} + q^{n-2} + \dots + 1 \equiv n \pmod{p-1}$ . Hence  $h = n_1(q-1)/(p-1)$ .

Moreover, if  $A \in \mathbb{F}_q^*$  then  $a^{n_1(q-1)/(p-1)} = A^{n_1(q-1)} = 1$  holds automatically and

$$\begin{aligned} \text{Tr}_{q^n/p}(\alpha/A^p) &= \text{Tr}_{q/p}(\text{Tr}_{q^n/q}(\alpha/A^p)) \\ &= \text{Tr}_{q/p}(\text{Tr}_{q^n/q}(\alpha)/A^p) \\ &= -\text{Tr}_{q/p}(c_{n-1}/A^p) \end{aligned}$$

Therefore, the last assertion also holds.  $\square$

Now we turn to the general case, i.e.  $l(x)$  is any linearized polynomial. To determine when  $P(l(x))$  is irreducible for any linearized polynomial  $l(x)$ , we need some preliminary results in [7].

**Lemma 2.13.** *Given a linearized polynomial  $l(x)$  over  $\mathbb{F}_q$ , there exists another linearized polynomial  $g(x)$  over  $\mathbb{F}_q$  and an element  $r$  in  $\mathbb{F}_q$  such that*

$$l(x) = g(x^p - x) + rx.$$

*Proof.* Let  $l(x) = a_\nu x^{p^\nu} + a_{\nu-1} x^{p^{\nu-1}} + \dots + a_0 x$ . We use induction on  $\nu$  to prove the lemma. The case  $\nu = 0$  is trivial. Suppose  $\nu \geq 1$  and put

$$\bar{l}(x) = l(x) - a_\nu (x^p - x)^{p^{\nu-1}} = (a_{\nu-1} + a_\nu) x^{p^{\nu-1}} + a_{\nu-2} x^{p^{\nu-2}} + \dots,$$

another linearized polynomial but of degree (at most)  $p^{\nu-1}$ . By induction, there is a linearized polynomial  $\bar{g}(x)$  such that  $\bar{l}(x) = \bar{g}(x^p - x) + rx$ . Then  $l(x) = \bar{g}(x^p - x) + a_\nu (x^p - x)^{p^{\nu-1}} + rx$ . Put  $g(x^p - x) = \bar{g}(x^p - x) + a_\nu (x^p - x)^{p^{\nu-1}}$  where  $g$  is the required linearized polynomial for the conclusion.  $\square$

**Lemma 2.14.** *Suppose the linearized polynomial  $l(x)$  over  $\mathbb{F}_q$  has a non-zero root  $A$  in  $\mathbb{F}_q$ . Then there exists a linearized polynomial  $g(x)$  such that  $l(x) = g(x^p - A^{p-1}x)$ .*

*Proof.*  $l(Ax)$  is a linearized polynomial over  $\mathbb{F}_q$  with 1 as a root. By Lemma 2.13, there exists another linearized polynomial  $\tilde{g}(x)$  and  $r \in \mathbb{F}_q$  such that  $l(Ax) = \tilde{g}(x^p - x) + rx$ . In fact,  $r = 0$  because the substitution  $x = 1$  yields  $0 = \tilde{g}(0) + r = r$ . Thus  $l(Ax) = \tilde{g}(x^p - x)$ , which yields that  $l(x) = \tilde{g}(\frac{x^p - A^{p-1}x}{A^p}) = g(x^p - A^{p-1}x)$  for some linearized polynomial  $g(x) = \tilde{g}(\frac{x}{A^p})$ .  $\square$

**Lemma 2.15.** *Suppose  $l(x)$  is a linearized polynomial over  $\mathbb{F}_q$  of degree  $p^\nu$  with  $\nu \geq 2$ . Then for any  $b$  in  $\mathbb{F}_q$ ,  $l(x) - b$  is irreducible over  $\mathbb{F}_q$  if and only if (i)  $p = \nu = 2$ , and (ii)  $l(x)$  has the form*

$$l(x) = x(x + A)(x^2 + Ax + B) \tag{2.2}$$

where  $A, B \in \mathbb{F}_q$  such that the quadratics  $x^2 + Ax + B$  and  $x^2 + Bx + b$  are both irreducible over  $\mathbb{F}_q$ .

*Proof.* By Proposition 2.5 we may assume that  $l(x)$  has a nonzero root  $A$  in  $\mathbb{F}_q$ . Using Lemma 2.14, we write  $l(x) = g(x^p - A^{p-1}x)$  and put  $\bar{g}(x) = g(x) - b$  for some linearized polynomial  $g(x)$  over  $\mathbb{F}_q$ . Then  $l(x) - b = \bar{g}(x^p - A^{p-1}x)$ . Next, we apply the last assertion of Theorem 2.12 with  $P(x) = \bar{g}(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1x - b$  and  $n = \deg(\bar{g}(x)) = p^{\nu-1}$ . Since  $\bar{g}$  is an affine polynomial, the coefficient  $b_{n-1}$  of  $x^{n-1}$  in  $\bar{g}$  is zero unless  $p^{\nu-1} - 1 = p^{\nu-2}$  which occurs only if  $p = \nu = 2$ . Hence,  $\text{Tr}_{q/p}(b_{n-1}/A^p) = 0$  and  $l(x) - b$  is reducible except when  $p = \nu = 2$ . Now suppose that  $p = \nu = 2$ , and  $g(x) = x^2 + Bx$ , where  $B \in \mathbb{F}_q$ . Hence  $\bar{g}(x) = x^2 + Bx + b$  and

$$l(x) = g(x^2 - Ax) = x(x + A)(x^2 + Ax + B)$$

By Theorem 2.12 again,  $l(x) - b = \bar{g}(x^2 - Ax)$  is irreducible over  $\mathbb{F}_q$  if and only if  $\bar{g}(x) = x^2 + Bx + b$  is irreducible over  $\mathbb{F}_q$  and  $\text{Tr}_{q/p}(B/A^2) \neq 0$ . The latter condition, by Proposition 2.7, is equivalent to  $x^2 + Ax + B$  being irreducible over  $\mathbb{F}_q$ . This completes the proof.  $\square$

**Theorem 2.16** ([7], Theorem 3.18). *Let  $P(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$  be a monic irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$ , and let  $l(x)$  be a monic linearized polynomial over  $\mathbb{F}_q$  of degree  $p^\nu$  with  $\nu \geq 2$ . Then  $P(l(x))$  is irreducible over  $\mathbb{F}_q$  if and only if (i)  $p = \nu = 2$ , (ii)  $n$  is odd, and (iii)  $l(x)$  has the form (2.2) where  $A, B \in \mathbb{F}_q$  and both  $x^2 + Ax + B$  and  $x^2 + Bx + c_{n-1}$  are irreducible over  $\mathbb{F}_q$ .*

*Proof.* By Theorem 1.9,  $P(l(x))$  is irreducible over  $\mathbb{F}_q$  if and only if  $l(x) - \alpha$  is irreducible over  $\mathbb{F}_{q^n}$ , for some  $\alpha \in \mathbb{F}_{q^n}$  such that  $P(\alpha) = 0$ . Applying Lemma 2.15 to  $l(x) - \alpha$ , we conclude that  $P(l(x))$  is irreducible over  $\mathbb{F}_q$  if and only if  $p = \nu = 2$ , and  $l(x)$  has the form (2.2) where  $A, B \in \mathbb{F}_{q^n}$  with both  $x^2 + Ax + B$  and  $x^2 + Bx + \alpha$  irreducible over  $\mathbb{F}_{q^n}$ .

Assume now that  $p = \nu = 2$ . Then  $\deg(l(x)) = 4$  and  $\deg(l(x)/x) = 3$ . If  $l(x)/x$  is irreducible over  $\mathbb{F}_q$  or a product of three linear factors over  $\mathbb{F}_q$ , then it remains so over  $\mathbb{F}_{q^n}$ . So for  $l(x)/x$  to have a quadratic irreducible factor over  $\mathbb{F}_{q^n}$ , it must be a product of a linear factor and a quadratic irreducible factor over  $\mathbb{F}_q$ , and, by Proposition 1.2,  $n$  must be odd so that the quadratic remains irreducible over  $\mathbb{F}_{q^n}$ . Now assume further that  $l(x)$  is of the form (2.2) where  $A, B \in \mathbb{F}_{q^n}$  with both  $x^2 + Ax + B$  and  $x^2 + Bx + \alpha$  irreducible over  $\mathbb{F}_{q^n}$ . Then  $A, B \in \mathbb{F}_q$ ,  $x^2 + Ax + B$  is irreducible over  $\mathbb{F}_q$ , and  $n$  is odd.

Finally, by Proposition 2.7,  $x^2 + Bx + \alpha$  is irreducible over  $\mathbb{F}_{q^n}$  if and only if  $\text{Tr}_{q^n/p}(\alpha/B^2) \neq 0$ . But

$$\begin{aligned} \text{Tr}_{q^n/p}(\alpha/B^2) &= \text{Tr}_{q/p}(\text{Tr}_{q^n/q}(\alpha/B^2)) \\ &= \text{Tr}_{q/p}(\text{Tr}_{q^n/q}(\alpha)/B^2) \\ &= -\text{Tr}_{q/p}(c_{n-1}/B^2). \end{aligned}$$

By Proposition 2.7 again,  $\text{Tr}_{q/p}(c_{n-1}/B^2) \neq 0$  if and only if  $x^2 + Bx + c_{n-1}$  is irreducible over  $\mathbb{F}_q$ . This completes the proof.  $\square$

## Recursive Constructions

Based on the irreducibility criteria developed in the previous chapter, we study how to recursively construct irreducible polynomials of arbitrarily large degrees.

First we introduce the following recursive construction of Varshamov [10].

**Theorem 3.1.** *Let  $p$  be a prime and let  $f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$  be irreducible over  $\mathbb{F}_p$ . Suppose that there exists an element  $a \in \mathbb{F}_p^*$  such that  $(na + c_{n-1})f'(a) \neq 0$ . Further let  $g(x) = x^p - x + a$  and define  $f_k(x)$  for  $k = 0, 1, 2, \dots$  recursively by*

$$\begin{aligned} f_0(x) &= f(g(x)), \\ f_k(x) &= f_{k-1}^*(g(x)) \quad \text{for } k \geq 1, \end{aligned}$$

where  $f_{k-1}^*(x)$  is the reciprocal polynomial of  $f_{k-1}(x)$ . Then for all  $k \geq 0$ ,  $f_k(x)$  is irreducible over  $\mathbb{F}_p$  of degree  $np^{k+1}$ .

*Proof.* For any  $k \geq 0$ , let  $\deg f_k(x) = n_k$  and

$$f_k(x) = \sum_{i=0}^{n_k} b_{ki} x^i.$$

Denote by  $(P_k)$  the family of claims:

- $b_{k1} = f'_k(a) \neq 0$ ,
- both  $f_k(x)$  and  $f'_k(x)$  are constant on  $\mathbb{F}_p$ ,
- $f_k(x)$  is irreducible over  $\mathbb{F}_p$ ,
- $n_k = np^{k+1}$ .

We prove  $(P_k)$  by induction on  $k$ .

When  $k = 0$ , we have

$$f'_0(x) = f'(g(x))g'(x)$$

Then

$$\begin{aligned}
b_{01} &= (f'_0(x))|_{x=0} \\
&= (f'(g(x))g'(x))|_{x=0} \\
&= -f'(a) \quad (\text{since } g(0) = a, g'(0) = -1)
\end{aligned}$$

and

$$\begin{aligned}
f'_0(a) &= (f'(g(x))g'(x))|_{x=a} \\
&= -f'(a) \quad (\text{since } g(a) = a, g'(a) = -1)
\end{aligned}$$

Thus  $b_{01} = f'_0(a) = -f'(a) \neq 0$ , by assumption. Clearly  $g(x)$  is constant on  $\mathbb{F}_p$  and  $g'(x) = -1$ , hence both  $f_0(x) = f(g(x))$  and  $f'_0(x)$  are constant on  $\mathbb{F}_p$ . Since  $\deg f_0(x) = np$ ,  $n_0 = np$ . From Theorem 2.11,  $f_0(x) = f(g(x))$  is irreducible over  $\mathbb{F}_p$  if and only if  $\text{Tr}_{p/p}(na + c_{n-1}) = na + c_{n-1} \neq 0$ . By assumption  $na + c_{n-1} \neq 0$ , so  $f_0(x)$  is irreducible over  $\mathbb{F}_p$ .

Now assume that  $(P_k)$  is true for  $k \geq 0$ . We prove that  $(P_{k+1})$  is also true. Since  $f(x)$  and  $f^*(x)$  have the same degree and by induction hypothesis  $n_k = np^{k+1}$ ,  $f_{k+1}(x) = f_k^*(g(x))$  is of degree  $n_{k+1} = np^{k+2}$ . The constant term  $b_{k0} \neq 0$  since  $f_k(x)$  is irreducible, and also  $b_{k1} \neq 0$  by induction hypothesis. Thus  $b_{k0}^{-1}f_k^*(x)$  is monic and the coefficient of  $x^{n_k-1}$  is  $b_{k0}^{-1}b_{k1} \neq 0$ . Then

$$\text{Tr}_{p/p}(n_k a + b_{k0}^{-1}b_{k1}) = \text{Tr}_{p/p}(np^{k+1}a + b_{k0}^{-1}b_{k1}) = b_{k0}^{-1}b_{k1} \neq 0,$$

It follows from Theorem 2.11 that  $f_{k+1}(x) = f_k^*(g(x))$  is irreducible over  $\mathbb{F}_p$ . By definition

$$f_{k+1}(x) = f_k^*(g(x)) = \sum_{i=0}^{n_k} b_{ki}g(x)^{n_k-i}$$

Thus

$$\begin{aligned}
f'_{k+1}(x) &= \sum_{i=0}^{n_k-1} b_{ki}(n_k - i)g(x)^{n_k-i-1}g'(x) \\
&= \sum_{i=0}^{n_k-1} b_{ki}ig(x)^{n_k-i-1} \quad (\text{since } g'(x) = -1)
\end{aligned}$$

Because  $g(x)$  is constant on  $\mathbb{F}_p$ , so are  $f_{k+1}(x)$  and  $f'_{k+1}(x)$ . Moreover,

$$\begin{aligned}
b_{k+1,1} &= (f'_{k+1}(x))|_{x=0} = (f_k^{*\prime}(g(x))g'(x))|_{x=0} \\
&= -f_k^{*\prime}(a) \\
&= f'_k(a^{-1})a^{n_k-2} \\
&= f'_k(a)a^{n_k-2},
\end{aligned}$$

which is nonzero by the induction hypothesis. Similarly,

$$f'_{k+1}(a) = (f'_{k+1}(x))|_{x=a} = (f'_k(g(x))g'(x))|_{x=a} = -f'_k(a)$$

which is again non-zero as above. This completes the proof of  $(P_{k+1})$ .

By induction  $(P_k)$  holds for all  $k \geq 0$ . In particular, for all  $k \geq 0$ ,  $f_k(x)$  is irreducible over  $\mathbb{F}_p$  of degree  $np^{k+1}$ .  $\square$

The next construction is over  $\mathbb{F}_q$ , for  $q$  even, and is based on Theorem 2.8.

**Theorem 3.2** ([11], Theorem 10.26). *Let  $q = 2^m$  and let  $f(x) = \sum_{i=0}^n c_i x^i$  be irreducible over  $\mathbb{F}_q$  of degree  $n$  with  $c_0 c_n \neq 0$ . Suppose that  $\text{Tr}_{q/2}(c_1/c_0) \neq 0$  and  $\text{Tr}_{q/2}(c_{n-1}/c_n) \neq 0$ . For all  $k \geq 0$ , define polynomials recursively:*

$$\begin{aligned} f_0(x) &= f(x), \\ f_k(x) &= x^{n2^{k-1}} f_{k-1}(x + x^{-1}) \quad \text{for } k \geq 1. \end{aligned}$$

Then  $f_k(x)$  is a self-reciprocal irreducible polynomial of degree  $n2^k$  over  $\mathbb{F}_q$  for all  $k \geq 1$ .

*Proof.* It is easily seen by Theorem 2.8 and by induction on  $k$  that  $f_k(x)$  is of degree  $n2^k$  for every  $k \geq 0$  and  $f_k(x)$  is a self-reciprocal polynomial for every  $k \geq 1$ . We apply induction on  $k$  to prove that  $f_k(x)$  is irreducible for every  $k \geq 1$ . Since  $\text{Tr}_{q/2}(c_1/c_0) \neq 0$  by assumption,  $f_1(x) = x^n f_0(x + x^{-1})$  is irreducible by Theorem 2.8. Let  $k \geq 1$  and assume that  $f_k(x)$  is irreducible. Let  $n_k = n2^k$  and  $f_k(x) = \sum_{i=0}^{n_k} c_{ki} x^i$ ,  $k \geq 0$ . We have

$$\begin{aligned} f_k(x) &= x^{n_{k-1}} f_{k-1}(x + x^{-1}) \\ &= x^{n_{k-1}} \sum_{i=0}^{n_{k-1}} c_{k-1,i} (x + x^{-1})^i \\ &= x^{n_{k-1}} \sum_{i=0}^{n_{k-1}} c_{k-1,i} ((1 + x^2)/x)^i \\ &= \sum_{i=0}^{n_{k-1}} c_{k-1,i} (1 + x^2)^i x^{n_{k-1}-i} \\ &= \sum_{i=0}^{n_k} c_{ki} x^i. \end{aligned}$$

Thus

$$c_{k0} = c_{k-1, n_{k-1}} \quad \text{and} \quad c_{k1} = c_{k-1, n_{k-1}-1} \quad (3.1)$$

By Theorem 2.8,  $f_{k+1}(x) = x^{n2^k} f_k(x + x^{-1})$  is irreducible over  $\mathbb{F}_q$

$$\text{Tr}_{q/2}(c_{k1}/c_{k0}) \neq 0 \quad (3.2)$$



Since  $f_j(x)$  is self-reciprocal for  $j \geq 1$ , (3.1) implies

$$\begin{aligned} c_{k0} &= c_{k-1, n_{k-1}} = c_{k-1, 0} = \cdots = c_{10} = c_{0, n_0} = c_n \\ c_{k1} &= c_{k-1, n_{k-1}-1} = c_{k-1, 1} = \cdots = c_{11} = c_{0, n_0-1} = c_{n-1}. \end{aligned}$$

Since  $Tr_{q/2}(c_{n-1}/c_n) \neq 0$  by assumption, (3.2) is true for  $k \geq 1$ , and so  $f_{k+1}(x)$  is irreducible over  $\mathbb{F}_q$  for  $k \geq 1$ .  $\square$

The final construction is over  $\mathbb{F}_q$ , for  $q$  odd, based on Corollary 2.10 and is due to Cohen [4].

**Theorem 3.3.** *Let  $q$  be odd and let  $f(x)$  be a monic irreducible polynomial of degree  $n \geq 1$  over  $\mathbb{F}_q$ , where  $n$  is even if  $q \equiv 3 \pmod{4}$ . Suppose that  $f(1)f(-1) \notin \mathbb{F}_q^{*2}$ . Define*

$$\begin{aligned} f_0(x) &= f(x) \\ f_k(x) &= (2x)^{n_{k-1}} f_{k-1}((x+x^{-1})/2) \quad \text{for } k \geq 1, \end{aligned}$$

where  $n_k$  denotes the degree of  $f_k(x)$ . Then  $f_k(x)$  is an irreducible polynomial over  $\mathbb{F}_q$  of degree  $n2^k$  for every  $k \geq 1$ .

*Proof.* It is easy to see by induction on  $k$  that  $f_k(x)$  is of degree  $n_k = n2^k$  for every  $k \geq 0$ . For  $k \geq 1$ , we have

$$\begin{aligned} f_k(1)f_k(-1) &= 2^{n_{k-1}} f_{k-1}(1)(-2)^{n_{k-1}} f_{k-1}(-1) \\ &= (-1)^{n_{k-1}} 2^{2n_{k-1}} f_{k-1}(1)f_{k-1}(-1) \\ &= \cdots \\ &= (-1)^n d_k^2 f_0(1)f_0(-1), \quad \text{for some } d_k \in \mathbb{F}_q, \\ &= c_k^2 f_0(1)f_0(-1), \quad \text{for some } d_k \in \mathbb{F}_q, \end{aligned}$$

because either  $-1$  is a square in  $\mathbb{F}_q^*$  (when  $q \equiv 1 \pmod{4}$ ) or  $n$  is even. Hence  $f_k(1)f_k(-1)$  is always a non-square in  $\mathbb{F}_q^*$ , for  $k \geq 0$ . Hence applying induction on  $k$ , we can prove, by Corollary 2.10, that  $f_k(x)$  is irreducible over  $\mathbb{F}_q$  for every  $k \geq 1$ .  $\square$

## Composed Product of Polynomials

Let  $f(x)$  and  $g(x)$  be monic polynomials in  $\mathbb{F}_q[x]$ . The *composed sum* of  $f$  and  $g$  is the polynomial defined by

$$f \oplus g = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta)) \quad (4.1)$$

while the *composed multiplication* of  $f$  and  $g$  is the polynomial defined by

$$f \odot g = \prod_{\alpha} \prod_{\beta} (x - (\alpha\beta)) \quad (4.2)$$

where the products are taken over all the roots  $\alpha$  of  $f$  and  $\beta$  of  $g$ , including multiplicities.

In 1987, Brawley and Carlitz [2] defined a more general notion of polynomial composition, denoted by  $f \diamond g$ , for which  $f \oplus g$  and  $f \odot g$  are special cases.

Let  $G$  be a nonempty subset of the algebraic closure  $\overline{\mathbb{F}_q}$  of  $\mathbb{F}_q$  with the property that  $G$  is invariant under the Frobenius automorphism  $\alpha \mapsto \sigma(\alpha) = \alpha^q$  (i.e., if  $\alpha \in G$ , then  $\sigma(\alpha) \in G$ ), and suppose there is defined on  $G$  a binary operation  $\diamond$  such that  $(G, \diamond)$  is a group and for all  $\alpha, \beta \in G$ ,

$$\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta) \quad (4.3)$$

Then for monic polynomials  $f$  and  $g$  whose coefficients are in  $\mathbb{F}_q$  and whose roots lie in  $G$ , the *composed product*, denoted by  $f \diamond g$ , is the polynomial defined by

$$f \diamond g = \prod_{\alpha} \prod_{\beta} (x - (\alpha \diamond \beta)) \quad (4.4)$$

where again the products are over all roots of  $\alpha$  of  $f$  and  $\beta$  of  $g$ . It is clear that

$$\deg f \diamond g = (\deg f)(\deg g)$$

and it is also clear that when  $G = \overline{\mathbb{F}_q}$  and  $\diamond$  is the usual addition (respectively, the usual multiplication) on  $\overline{\mathbb{F}_q}$ , then (4.4) becomes (4.1) (respectively (4.2)).

The following theorem, which is due to Brawley and Carlitz [2], indicates precisely when the composed product is irreducible.

**Theorem 4.1.** *Let  $(G, \diamond)$  be a  $\sigma$ -invariant group satisfying (4.3) and let  $f, g$  be monic polynomials in  $\mathbb{F}_q[x]$  with roots in  $G$ . If  $\deg f = m$  and  $\deg g = n$ , then the composed product  $f \diamond g$  is irreducible in  $\mathbb{F}_q[x]$  if and only if  $f$  and  $g$  are both irreducible in  $\mathbb{F}_q[x]$  and  $\gcd(m, n) = 1$ .*

*Proof.* See [7], p.56-57. □

Now we state the following easy consequences of Theorem 4.1 which are applied in the proofs of the next theorems regarding polynomial composition.

**Corollary 4.2.** *Let  $f$  and  $g$  be irreducible polynomials over  $\mathbb{F}_q$  with  $\deg f = m$  and  $\deg g = n$ , where  $\gcd(m, n) = 1$ , and suppose that  $\alpha$  and  $\beta$  are respective roots of  $f$  and  $g$ . Then*

$$\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_q(\alpha \diamond \beta)$$

*In particular,  $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_q(\alpha + \beta) = \mathbb{F}_q(\alpha\beta)$ .*

**Corollary 4.3.** *Suppose that  $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$  and  $[\mathbb{F}_q(\beta) : \mathbb{F}_q] = n$  with  $\gcd(m, n) = 1$ . Further suppose that  $F(x) \in \mathbb{F}_q[x]$  is a polynomial of degree  $mn$  such that  $F(\alpha \diamond \beta) = 0$ . Then  $F(x)$  is irreducible in  $\mathbb{F}_q[x]$ .*

Now we will apply the results above to prove the following result of Varshamov [10] which is restated as follows.

**Theorem 4.4.** *Let  $r$  be an odd prime number which does not divide  $q$ , and  $r - 1$  be the order of  $q$  modulo  $r$ . Further let  $n > 1$ ,  $\gcd(n, r - 1) = 1$  and  $f(x)$  be an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$  with  $\text{ord}(f) = t$ , and  $\psi(x) \in \mathbb{F}_q[x]$  be the minimal polynomial of  $\alpha^r$  for a zero  $\alpha$  of  $f$ . Then  $\psi(x)$  has degree  $n$  and*

$$F(x) = (f(x))^{-1}\psi(x^r)$$

*is an irreducible polynomial of degree  $(r - 1)n$  over  $\mathbb{F}_q$ . Moreover,  $\text{ord}(F(x)) = rt$ .*

*Proof.* First we prove that the degree of  $\psi$  is  $n$ . Assume that  $\psi(x) \in \mathbb{F}_q[x]$  is the minimal polynomial of  $\alpha^r$  for a zero  $\alpha$  of  $f(x)$ . In order to prove that the degree of  $\psi$  is  $n$ , we show that  $\deg_q(\alpha^r) = n$ , i.e.  $\mathbb{F}_q(\alpha^r) = \mathbb{F}_{q^n}$ , by proving that the multiplicative order of  $\alpha^r$  is equal to the one of  $\alpha$ . By assumption the order of  $f$  is  $t$  which implies being order of  $\alpha$  is also  $t$ . Thus the order of  $\alpha^r$  is  $\frac{t}{\gcd(t, r)}$  and it is enough to show that  $\gcd(t, r) = 1$ . By the assumption, we have  $r - 1 \neq 1$  is the smallest  $i$  satisfying the congruence  $q^i \equiv 1 \pmod{r}$ , and  $t$  divides  $q^n - 1$ , and further

$$\gcd(q^n - 1, q^{r-1} - 1) = q^{\gcd(n, r-1)} - 1 = q - 1.$$

Since  $r$  divides  $q^{r-1} - 1$  and  $t$  divides  $q^n - 1$ , we have  $\gcd(t, r)$  divides  $\gcd(q^n - 1, q^{r-1} - 1) = q - 1$ . Being  $r$  an odd prime implies  $\gcd(t, r) = 1$  or  $r$ , but  $r$  does not divide  $q - 1$ . Hence  $\gcd(t, r) = 1$ .

Now we consider the polynomial  $F(x) = (f(x))^{-1}\psi(x^r)$ . Let  $\beta$  be a primitive  $r$ th root of unity over  $\mathbb{F}_q$ . Then the  $r$ th cyclotomic polynomial  $h(x) = x^{r-1} + x^{r-2} + \dots + x + 1$ , which is irreducible over  $\mathbb{F}_q$  if and only if  $r$  is a prime number and the order of  $q$  modulo  $r$  is  $r - 1$ , is the minimal polynomial of  $\beta$  over  $\mathbb{F}_q$ . Now we have two irreducible polynomials  $f(x)$  and  $h(x)$  assuming  $\alpha$  and  $\beta$  as roots, respectively, and  $\gcd(n, r - 1) = 1$ . So by Corollary 4.2,  $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_q(\alpha\beta)$ , i.e.  $\deg_q(\alpha\beta) = n(r - 1)$ . We claim that  $\alpha\beta$  is a root of the polynomial  $F(x) = (f(x))^{-1}\psi(x^r)$ . First note that  $\alpha\beta$  is not a root of  $f(x)$ , otherwise  $\alpha\beta = \alpha^{q^i}$  for some  $0 \leq i \leq n - 1$  which implies  $\beta = \alpha^{q^i - 1} \in \mathbb{F}_{q^n}$  and this contradicts to the assumption that  $\gcd(n, r - 1) = 1$ . Then

$$F(\alpha\beta) = \frac{\psi((\alpha\beta)^r)}{f(\alpha\beta)} = \frac{\psi(\alpha^r \beta^r)}{f(\alpha\beta)} = \frac{\psi(\alpha^r)}{f(\alpha\beta)} = 0$$

Since the degree of  $F(x)$  is  $n(r - 1)$  and  $\deg_q(\alpha\beta) = n(r - 1)$ ,  $F(x)$  is the minimal polynomial of  $\alpha\beta$  over  $\mathbb{F}_q$ . Hence  $F(x)$  is irreducible over  $\mathbb{F}_q$ .

We complete the proof with

$$\text{ord}(F(x)) = \text{ord}_q(\alpha\beta) = \text{lcm}(\text{ord}(\alpha), \text{ord}(\beta)) = \text{lcm}(t, r) = rt.$$

□

Recall that a polynomial of the form  $L(x) = \sum_{i=0}^n a_i x^{q^i} \in \mathbb{F}_q[x]$  is called a linearized polynomial over  $\mathbb{F}_q$ . It is easy to see that a linearized polynomial represents a linear mapping on  $\mathbb{F}_q$ , where  $\mathbb{F}_q$  is considered as a vector space over  $\mathbb{F}_p$ , i.e.  $L(\beta + \gamma) = L(\beta) + L(\gamma)$  and  $L(c\beta) = cL(\beta)$  for any  $\beta, \gamma \in \mathbb{F}_q$  and  $c \in \mathbb{F}_p$ . The polynomials

$$L(x) = \sum_{i=0}^n a_i x^{q^i} \quad \text{and} \quad l(x) = \sum_{i=0}^n a_i x^i$$

are called  $q$ -associates of each other. More precisely,  $l(x)$  is the conventional  $q$ -associate of  $L(x)$ , and  $L(x)$  is the linearized  $q$ -associate of  $l(x)$ .

**Proposition 4.5** ([6], Theorem 3.63). *Let  $f(x)$  be irreducible in  $\mathbb{F}_q[x]$  and let  $F(x)$  be its linearized  $q$ -associate. Then the degree of every irreducible factor of  $x^{-1}F(x) \in \mathbb{F}_q[x]$  is equal to  $\text{ord}(f(x))$ .*

The next result, due to Ore-Gleason-Marsh [12], is an immediate consequence of Proposition 4.5.

**Theorem 4.6.** *Let  $f(x) = \sum_{u=0}^n a_u x^u \in \mathbb{F}_q[x]$  and  $F(x)$  be its linearized  $q$ -associate. Then  $f(x)$  is a primitive polynomial over  $\mathbb{F}_q$  if and only if  $x^{-1}F(x) = \sum_{u=0}^n a_u x^{q^u - 1}$  is irreducible over  $\mathbb{F}_q$ .*

Given an irreducible polynomial of degree  $n$  and a primitive polynomial of degree  $m$  over  $\mathbb{F}_q$ , the next theorem, which is stated in a bit different way in [5] as Theorem 5, yields an irreducible polynomial of degree  $n(q^m - 1)$  over  $\mathbb{F}_q$ .

**Theorem 4.7.** Let  $\gcd(n, q^m - 1) = 1$ , and  $L(x) = \sum_{\nu=0}^m b_\nu x^{q^\nu}$  such that its conventional  $q$ -associate  $l(x) \neq x - 1$  is a primitive polynomial of degree  $m$  over  $\mathbb{F}_q$ . Further, let  $f(x)$  be an irreducible polynomial of degree  $n$  over  $\mathbb{F}_q$  and  $\psi(x)$  be the minimal polynomial of  $L(\alpha)$  over  $\mathbb{F}_q$ , for a zero  $\alpha \in \mathbb{F}_{q^n}$  of  $f(x)$ . Then  $\psi(x)$  has degree  $n$  and

$$F(x) = (f(x))^{-1}\psi(L(x))$$

is an irreducible polynomial of degree  $n(q^m - 1)$  over  $\mathbb{F}_q$ .

*Proof.* First we prove that the degree of  $\psi$  is  $n$ . Assume that  $\psi(x) \in \mathbb{F}_q[x]$  is the minimal polynomial of  $L(\alpha)$  for a zero  $\alpha$  of  $f(x)$ . In order to prove that the degree of  $\psi$  is  $n$ , we show that  $\deg_q(L(\alpha)) = n$ . Assume on the contrary that for some  $k < n$ ,

$$\begin{aligned} \deg_q(L(\alpha)) = k &\quad \Rightarrow & L(\alpha)^{q^k} &= L(\alpha) \\ &\quad \Rightarrow & L(\alpha^{q^k}) &= L(\alpha) \\ &\quad \Rightarrow & L(\alpha^{q^k} - \alpha) &= 0 \\ &\quad \Rightarrow & \alpha^{q^k} - \alpha &\text{ is a root of } L(x). \end{aligned}$$

Then  $\alpha^{q^k} - \alpha$  is also a root of  $x^{-1}L(x)$  since  $\deg_q(\alpha) = n$  implies  $\alpha^{q^k} \neq \alpha$  for  $k < n$ .

Because  $l(x)$  is a primitive polynomial,  $x^{-1}L(x)$  is irreducible over  $\mathbb{F}_q$  by Proposition 4.5. Let  $\beta \in \mathbb{F}_{q^{q^m-1}}$  be a root of  $x^{-1}L(x)$ . The roots of  $x^{-1}L(x)$  are all the conjugates of  $\beta$ , namely  $\beta, \beta^q, \beta^{q^2}, \dots, \beta^{q^{q^m-2}}$ , so  $\alpha^{q^k} - \alpha = \beta^{q^j}$  for some  $0 \leq j \leq q^m - 2$ . This yields that  $\beta^{q^j} \in \mathbb{F}_q(\alpha)$ , contradicting to the assumption that  $\gcd(n, q^m - 1) = 1$ .

Next we show that  $F(x) = (f(x))^{-1}\psi(L(x))$  is an irreducible polynomial of degree  $n(q^m - 1)$ . We have two irreducible polynomials  $f(x)$  and  $x^{-1}L(x)$  with respective roots  $\alpha$  and  $\beta$ , and respective degrees  $n$  and  $q^m - 1$  with  $\gcd(n, q^m - 1) = 1$ . Then by Corollary 4.2,  $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_q(\alpha + \beta)$ , i.e.  $\deg_q(\alpha + \beta) = n(q^m - 1)$ . Now our claim is that  $\alpha + \beta$  is a root of  $F(x) = (f(x))^{-1}\psi(L(x))$ . First note that  $\alpha + \beta$  is not a root of  $f(x)$ , otherwise  $\alpha + \beta = \alpha^{q^k}$  for some  $1 \leq k \leq n - 1$  which yields  $\beta = \alpha^{q^k} - \alpha \in \mathbb{F}_{q^n}$  and this contradicts to the assumption that  $\gcd(n, q^m - 1) = 1$ . Then

$$F(\alpha + \beta) = \frac{\psi(L(\alpha + \beta))}{f(\alpha + \beta)} = \frac{\psi(L(\alpha) + L(\beta))}{f(\alpha + \beta)} = \frac{\psi(L(\alpha))}{f(\alpha + \beta)} = 0.$$

Since the degree of  $F(x)$  is  $n(q^m - 1)$  and  $\deg_q(\alpha + \beta) = n(q^m - 1)$ ,  $F(x)$  is the minimal polynomial of  $\alpha + \beta$  over  $\mathbb{F}_q$ . Hence  $F(x)$  is irreducible over  $\mathbb{F}_q$ .  $\square$

# Bibliography

- [1] Albert A.A., *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, 1956.
- [2] Brawley J.V., Carlitz L., “Irreducibles and the composed product for polynomials over a finite field”, *Discrete Math.*, **65**, 115-139 (1987).
- [3] Cohen S., “On irreducible polynomials of certain types in finite fields”, *Proc. Camb. Phil. Soc.*, **66**, 335-344 (1969).
- [4] Cohen S., “The explicit construction of irreducible polynomials over finite fields”, *Designs, Codes and Cryptography*, **2**, 169-174 (1992).
- [5] Kyuregyan M., Kyureghyan G., “Irreducible compositions of polynomials over finite fields”, *Designs, Codes and Cryptography*, **61**, 301-314 (2011).
- [6] Lidl R., Niederreiter H., *Finite Fields*, Cambridge University Press, 1987.
- [7] Menezes A., Blake I.F., Gao X., Mullin R.C., Vanstone S.A., Yaghoobian T., *Applications of Finite Fields*, Kluwer Academic Publishers, 1993.
- [8] Meyn H., “On the construction of irreducible self-reciprocal polynomials over finite fields”, *Applicable Algebra in Engineering, Communication and Computing* **1**, 43-53 (1990).
- [9] Sidelnikov V.M., “On normal bases of a finite field”, *Math. USSR Sbornik* **61**, 485-494 (1988).
- [10] Varshamov R., “A general method of synthesizing irreducible polynomials over Galois fields”, *Soviet Math. Dokl.* **29**, 334-336 (1984) .
- [11] Wan Z.-X., *Lectures on Finite Fields and Galois Rings*, World Sci. Publ. Co., New Jersey, 2003.
- [12] Zierler N., “Linear recurring sequences”, *J. Soc. Ind. Appl. Math.* **7**, 31-48 (1959).