

# Some subgroups of a finite field and their applications for obtaining explicit factors

Manjit Singh

Email: manjitsingh.math@gmail.com

Department of Mathematics, Deenbandhu Chhotu Ram University of  
Science and Technology, Murthal-131039, India

## Abstract

Let  $\mathcal{S}_q$  denote the group of all square elements in the multiplicative group  $\mathbb{F}_q^*$  of a finite field  $\mathbb{F}_q$  of odd characteristic containing  $q$  elements. Let  $\mathcal{O}_q$  be the set of all odd order elements of  $\mathbb{F}_q^*$ . Then  $\mathcal{O}_q$  turns up as a subgroup of  $\mathcal{S}_q$ . In this paper, we show that  $\mathcal{O}_q = \langle 4 \rangle$  if  $q = 2t + 1$  and,  $\mathcal{O}_q = \langle t \rangle$  if  $q = 4t + 1$ , where  $q$  and  $t$  are odd primes. This paper also gives a direct method for obtaining the coefficients of irreducible factors of  $x^{2^n t} - 1$  in  $\mathbb{F}_q[x]$  using the information of generator elements of  $\mathcal{S}_q$  and  $\mathcal{O}_q$ , when  $q$  and  $t$  are odd primes such that  $q = 2t + 1$  or  $q = 4t + 1$ .

**Keywords:** Cyclotomic polynomials, Irreducible polynomials, Finite fields.

**Mathematics Subject Classification (2010):** 11T05, 11T55, 12E10.

## 1 Introduction

Factoring polynomials over finite fields plays an important role in algebraic coding theory for the error-free transmission of information and cryptology for the secure transmission of information. Please note that the availability of explicit factors of  $x^m - 1$  over finite fields, especially irreducible polynomials over finite fields is useful for analyzing the structure and inner-relationship of codewords of a code and other areas of electrical engineering where linear feedback shift registers (LFSR) are used (see [1, 7, 9]). For example, factoring of  $x^m - 1$  into irreducible factors over finite fields is essentially useful to describe the theory of cyclic codes of length  $m$  over finite fields.

Blake, Gao and Mullin [2] explicitly determined all the irreducible factors of  $x^{2^n} \pm 1$  over  $\mathbb{F}_p$ , where  $p$  is a prime with  $p \equiv 3 \pmod{4}$ . Chen, Li and Tuerhong [4] gave the explicit factorization of  $x^{2^m p^n} - 1$  over  $\mathbb{F}_q$ , where  $p$  is an odd prime with  $q \equiv 1 \pmod{p}$ . In [3], Brochero Martínez, Giraldo Vergara and de Oliveira generalized the results in [4] by giving the explicit factorization of  $x^m - 1$  over  $\mathbb{F}_q$ , where every prime factor of  $m$  divides  $q - 1$ . Meyn [10] obtained the irreducible factors of cyclotomic polynomials  $\Phi_{2^k}(x)$  over  $\mathbb{F}_q$  when  $q \equiv 3 \pmod{4}$ . Fitzgerald and Yucas [6] obtained the explicit factorization of  $\Phi_{2^k 3}(x)$  when  $q \equiv \pm 1 \pmod{3}$ . In [16], Wang and Wang obtained the explicit factorization of  $\Phi_{2^k 5}(x)$  for  $q \equiv \pm 2 \pmod{5}$ . When

$q$  and  $r$  are distinct odd primes, Stein [13] computed the factors of  $\Phi_r(x)$  from the traces of the roots of  $\Phi_r(x)$  over prime field  $\mathbb{F}_q$ . Assuming that the explicit factors of  $\Phi_r(x)$  are known, Tuxanidy and Wang [14] obtained the irreducible factors of  $\Phi_{2^{n_r}}(x)$  over  $\mathbb{F}_q$ , where  $r > 1$  is an arbitrary odd integer.

In this paper, the explicit factorization of  $\Phi_{2^{n_d}}(x)$  over  $\mathbb{F}_q$  is revisited for every odd prime divisor  $d$  of  $q - 1$ . Using this factorization, when  $q$  and  $t$  are primes with  $q = 2lt + 1$  for  $l = 1, 2$ , the explicit factors of  $\Phi_{2^{n_t}}(x)$  over  $\mathbb{F}_q$  are determined. This factorization provides the complete information regarding the coefficients of irreducible factors of  $x^{2^{n_t}} - 1$  over  $\mathbb{F}_q$ .

The paper is organized as follows: The necessary notations and some known results to be used throughout the paper are provided in Section 2. In Section 3, assuming  $d$  is an odd divisor of  $q - 1$ , the explicit factorization of  $x^{2^{n_d}} - 1$  over  $\mathbb{F}_q$  is reformulated in two different cases when  $q \equiv 1 \pmod{4}$  in Theorem 3.2 and, when  $q \equiv 3 \pmod{4}$  in Theorem 3.6. In end of Section 3, the explicit factorization of cyclotomic polynomial  $\Phi_{2^{n_d}}(x)$  over  $\mathbb{F}_q$  is obtained for every odd prime  $d$  with  $d|(q - 1)$ . In Section 4, we record few results concerning the square elements in the multiplicative group  $\mathbb{F}_q^*$  which appears to be new. Using these results, the coefficients of irreducible factors of  $x^{2^{n_t}} - 1$  over  $\mathbb{F}_q$  are obtained effortlessly when  $q$  and  $t$  are primes with  $q = 2lt + 1$  for  $l = 1$  or  $2$ . In Section 5, in order to illustrate our results obtained in Section 4, we find the factorization of  $x^{2^{173 \cdot 2^n}} - 1 \in \mathbb{F}_{347}[x]$ ,  $x^{704} - 1 \in \mathbb{F}_{23}[x]$ ,  $x^{2^{37 \cdot 2^n}} - 1 \in \mathbb{F}_{149}[x]$  and  $x^{2^{13 \cdot 2^n}} - 1 \in \mathbb{F}_{53}[x]$ . As a consequence to our factorization, we obtain infinite families of binomials and trinomials over finite fields.

## 2 The cyclotomic factorization of $x^{2^{n_d}} - 1$ over finite fields

It is well-known that for any integer  $n \geq 1$ , the *cyclotomic decomposition* of  $x^n - 1$  is given by

$$x^n - 1 = \prod_{k|n} \Phi_k(x); \quad \Phi_k(x) = \prod_{\substack{\gcd(i,k)=1 \\ 0 \leq i \leq k-1}} (x - \xi^i),$$

where  $\xi$  is a primitive  $k$ th root of unity in some extension field of  $\mathbb{F}_q$  and  $\Phi_k(x)$  is the  $k$ th cyclotomic polynomial. The degree of  $\Phi_k(x)$  is  $\phi(k)$ , where  $\phi(k)$  is the Euler Totient function. Let  $e$  be the least positive integer such that  $q^e \equiv 1 \pmod{n}$ . Then, in  $\mathbb{F}_q[x]$ ,  $\Phi_n(x)$  splits into the product of  $\phi(n)/e$  monic irreducible polynomials of degree  $e$ . In particular,  $\Phi_n(x)$  is irreducible over  $\mathbb{F}_q$  if and only if  $e = \phi(n)$ . Note that  $\Phi_n(x)$  is irreducible over  $\mathbb{F}_q$ , then  $\Phi_m(x)$  is also irreducible over  $\mathbb{F}_q$  for every  $m|n$  (see [9, 11]).

**Lemma 2.1** (see Theorem 10.7 in [15] and Theorem 3.75 in [9]). *Let  $l \geq 2$  be an integer and  $a \in \mathbb{F}_q^*$  such that the order of  $a$  is  $k \geq 2$ . Then the binomial  $x^l - a \in \mathbb{F}_q[x]$  is irreducible over  $\mathbb{F}_q$  if and only if the following conditions are satisfied:*

- (i) *Every prime factor of  $l$  divides  $k$ , but not  $(q-1)/k$ ;*
- (ii) *If  $4|l$ , then  $4|(q-1)$ .*

**Lemma 2.2** (Theorem 10.15 in [15]). *Let  $f(x)$  be any irreducible polynomial over  $\mathbb{F}_q$  of degree  $l \geq 1$ . Suppose that  $f(0) \neq 0$  and  $f(x)$  is of order  $e$  which is equal to the order of any root of  $f(x)$ . Let  $k$  be a positive integer, then the polynomial  $f(x^k)$  is irreducible over  $\mathbb{F}_q$  if and only if the following three conditions are satisfied:*

- (i) *Every prime divisor of  $k$  divides  $e$ ;*
- (ii)  *$\gcd(k, \frac{q^l-1}{e}) = 1$ ;*
- (iii) *If  $4|k$ , then  $4|(q^l-1)$ .*

**Lemma 2.3.** *Suppose that  $t$  is an odd prime such that  $\gcd(2t, q) = 1$ . Then in  $\mathbb{F}_q[x]$  the following properties of cyclotomic polynomials hold:*

- (i)  $\Phi_{2^{kt}}(x) = \frac{\Phi_{2^k}(x^t)}{\Phi_{2^k}(x)},$
- (ii)  $\Phi_{2^{k+r}}(x) = \Phi_{2^k}(x^{2^r})$  for integers  $k \geq 1$  and  $r \geq 0$ .
- (iii)  $\Phi_{2^{nt}}(x) = \frac{\Phi_{2^k}(x^{2^{n-k}t})}{\Phi_{2^k}(x^{2^{n-k}})}$  for all integer  $n \geq k \geq 1$ .

*Proof.* First and second part are given in [9, Exercise 2.57]. The third part is an immediate consequence of the parts (i) and (ii).  $\square$

Hereafter, let  $\mathbb{F}_q$  be a finite field with  $q = 2^s t + 1$  for some integers  $s \geq 1$  and  $t$  is odd. Let  $\alpha_{2^k}$  be a primitive  $2^k$ th root of unity of  $\mathbb{F}_q^*$ , where  $0 \leq k \leq s$ . Then, for any integer  $n \geq 1$ , we present, without proof, the well known factorization of  $x^{2^n} - 1$  over  $\mathbb{F}_q$  in the following lemma.

**Lemma 2.4.** *For any integer  $n \geq 1$ , the cyclotomic factorization of  $x^{2^n} - 1$  over  $\mathbb{F}_q$  is given by:*

$$x^{2^n} - 1 = \begin{cases} (x-1) \prod_{k=1}^n \Phi_{2^k}(x) & \text{for } 1 \leq n \leq s \\ (x-1) \prod_{k=1}^s \Phi_{2^k}(x) \prod_{r=1}^{n-s} \Phi_{2^s}(x^{2^r}) & \text{for } n > s \geq 1 \end{cases}$$

where factors  $\Phi_{2^k}(x)$  for  $1 \leq k \leq s$  and  $\Phi_{2^s}(x^{2^r})$  for  $1 \leq r \leq n-s$  can be factors as:

$$\Phi_{2^k}(x) = \prod_{1 \leq i \leq 2^{k-1}} (x - \alpha_{2^k}^{2i-1}) \text{ and } \Phi_{2^s}(x^{2^r}) = \prod_{1 \leq i \leq 2^{s-1}} (x^{2^r} - \alpha_{2^s}^{2i-1}).$$

The above lemma immediately gives the following:

**Lemma 2.5.** *For any integer  $n \geq 1$  and odd integer  $d$ , the factorization of  $x^{2^n d} - 1$  into decomposable cyclotomic polynomials over  $\mathbb{F}_q$  is*

$$x^{2^n d} - 1 = \begin{cases} (x^d - 1) \prod_{k=1}^n \Phi_{2^k}(x^d) & \text{for } 1 \leq n \leq s \\ (x^d - 1) \prod_{k=1}^s \Phi_{2^k}(x) \prod_{r=1}^{n-s} \Phi_{2^s}(x^{2^r d}) & \text{for } n > s \geq 1 \end{cases}$$

where factors  $\Phi_{2^k}(x^d)$  for  $1 \leq k \leq s$  and  $\Phi_{2^s}(x^{2^r d})$  for  $0 \leq r \leq n - s$  can be factors as:

$$\Phi_{2^k}(x^d) = \prod_{1 \leq i \leq 2^{k-1}} (x^d - \alpha_{2^k}^{2i-1}) \text{ and } \Phi_{2^s}(x^{2^r d}) = \prod_{1 \leq i \leq 2^{s-1}} (x^{2^r d} - \alpha_{2^s}^{2i-1}).$$

**Lemma 2.6.** *For any integer  $m$  relatively prime with  $q$ , let  $b$  be a primitive  $m$ th root of unity in some extension field of  $\mathbb{F}_q$ . Then*

$$x^m - 1 = \prod_{j=0}^{m-1} (x - b^j).$$

Further, if  $c \in \mathbb{F}_q^*$  such that  $c = a^m$  for some  $a \in \mathbb{F}_q^*$ , then

$$x^m - c = \prod_{j=0}^{m-1} (x - ab^j).$$

### 3 Factorization of $x^{2^n d} - 1$ over $\mathbb{F}_q$ , when $q \equiv 1 \pmod{2d}$

In this section, we reformulate the factorization of  $x^{2^n d} - 1$  into irreducible factors over  $\mathbb{F}_q$  recursively when  $d$  is an odd divisor of  $q - 1$ . In view of Lemma 2.1, each factor of  $\Phi_{2^k}(x^d)$  and  $\Phi_{2^s}(x^{2^r d})$  is reducible over  $\mathbb{F}_q$ . Thus, in order to determine the complete factorization of  $x^{2^n d} - 1$  over  $\mathbb{F}_q$ , one needs to split the decomposable cyclotomic polynomials  $\Phi_{2^k}(x^d)$  for  $1 \leq k \leq s$  and  $\Phi_{2^s}(x^{2^r d})$  for  $1 \leq r \leq n - s$  into irreducible factors over  $\mathbb{F}_q$ .

**Theorem 3.1.** *Let  $d$  be an odd integer such that  $q \equiv 1 \pmod{2^k d}$ , where  $1 \leq k \leq s$ . Let  $\gamma$  be a primitive  $d$ th root of unity in  $\mathbb{F}_q^*$ . Then, for any integer  $r \geq 0$ , the complete factorization of  $\Phi_{2^k}(x^{2^r d})$  is*

$$\Phi_{2^k}(x^{2^r d}) = \Phi_{2^k}(x^{2^r}) \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 1 \leq j \leq d-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j),$$

where

$$\Phi_{2^k}(x^{2^r}) = \Phi_{2^{k+r}}(x) = \begin{cases} \prod_{i=1}^{2^{k+r-1}} (x - \alpha_{2^{k+r}}^{2i-1}) & \text{if } k+r \leq s \\ \prod_{i=1}^{2^{s-1}} (x - \alpha_{2^{k+r-s}}^{2i-1}) & \text{if } k+r > s. \end{cases}$$

*Proof.* For any integer  $r \geq 0$  and  $1 \leq k \leq s$ , observe that

$$\Phi_{2^k}(x^{2^r d}) = \prod_{1 \leq i \leq 2^{k-1}} (x^{2^r d} - \alpha_{2^k}^{2i-1}) = \prod_{1 \leq i \leq 2^{k-1}} ((x^{2^r})^d - \alpha_{2^k}^{d(2i-1)}).$$

Let  $\gamma$  be a primitive  $d$ th root of unity in  $\mathbb{F}_q^*$ . Then, by Lemma 2.6

$$\begin{aligned} \Phi_{2^k}(x^{2^r d}) &= \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 0 \leq j \leq d-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j) \\ &= \Phi_{2^k}(x^{2^r}) \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 1 \leq j \leq d-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j). \end{aligned}$$

This completes the proof.  $\square$

**Theorem 3.2.** *Let  $d$  be any odd integer and  $q \equiv 1 \pmod{2d}$ . Then, for any integer  $n \geq 1$ , the factorization of  $x^{2^n d} - 1$  over  $\mathbb{F}_q$  is given as:*

$$x^{2^n d} - 1 = \begin{cases} \prod_{j=0}^{d-1} \left( (x - \gamma^j) \prod_{\substack{i=1 \\ 1 \leq k \leq n}}^{2^{k-1}} (x - \alpha_{2^k}^{2i-1} \gamma^j) \right) & \text{if } n \leq s \\ \prod_{j=0}^{d-1} \left( (x - \gamma^j) \prod_{\substack{i=1 \\ 1 \leq k \leq s}}^{2^{k-1}} (x - \alpha_{2^k}^{2i-1} \gamma^j) \prod_{\substack{i=1 \\ 1 \leq r \leq n-s}}^{2^{s-1}} (x^{2^r} - \alpha_{2^s}^{2i-1} \gamma^j) \right) & \text{if } n > s \end{cases}$$

Further, if  $n > s \geq 2$ , the factorization  $x^{2^n d} - 1$  over  $\mathbb{F}_q$  has  $2^{s-1}(n-s+2)d$  irreducible factors, however if  $q \equiv 3 \pmod{4}$ , all nonlinear factors in the factorization are reducible over  $\mathbb{F}_q$  except binomials  $x^2 + \gamma^j$  for all  $0 \leq j \leq d-1$ .

*Proof.* In Theorem 3.1, on substituting  $r = 0$  and  $k = s$  in the polynomial  $\Phi_{2^k}(x^{2^r d})$ , we obtain  $\Phi_{2^k}(x^d) = \Phi_{2^k}(x) \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 1 \leq j \leq d-1}} (x - \alpha_{2^k}^{2i-1} \gamma^j)$  and  $\Phi_{2^s}(x^{2^r d}) = \Phi_{2^s}(x^{2^r}) \prod_{\substack{1 \leq i \leq 2^{s-1} \\ 1 \leq j \leq d-1}} (x^{2^r} - \alpha_{2^s}^{2i-1} \gamma^j)$  respectively. The result now follows from Lemma 2.5. Further, when  $n > s \geq 2$ , the irreducibility of

its nonlinear factors can be proved by Lemma 2.1. For  $q \equiv 3 \pmod{4}$  i.e.  $s = 1$ , the factorization of  $x^{2^nd} - 1$  over  $\mathbb{F}_q$  reduces to

$$x^{2^nd} - 1 = \prod_{j=0}^{d-1} \left( (x - \gamma^j)(x + b^j) \prod_{1 \leq r \leq n-1} (x^{2^r} + \gamma^j) \right).$$

By Lemma 2.1, factors  $x^{2^r} + \gamma^j$  are reducible over  $\mathbb{F}_q$  for every  $r \geq 2$ .  $\square$

Consider the case  $q \equiv 3 \pmod{4}$ . Let  $Q = q^2 = 2^u v + 1$ ,  $u \geq 3$  and  $2 \nmid v$ . Let  $\beta_{2^k}$  be a primitive  $2^k$ th root of unity in  $\mathbb{F}_Q^*$ . Note that  $\beta_{2^k} := \alpha_{2^k}$  when  $\beta_{2^k} \in \mathbb{F}_q$ .

(i) A quadratic character  $\chi$  on  $\langle \beta_{2^u} \rangle \subseteq \mathbb{F}_Q^*$  is defined as

$$\chi(\beta_{2^k}) = \beta_{2^k}^{q+1} = \begin{cases} 1 & \text{if } 0 \leq k < u \\ -1 & \text{if } k = u \end{cases}$$

(ii) A trace is a mapping  $\mathbb{T} : \mathbb{F}_Q \rightarrow \mathbb{F}_q$  defined as  $\mathbb{T}(x) = x + x^q$  for all  $x \in \mathbb{F}_Q$ . Further, for any positive integer  $r \geq 1$ , we define the  $r$ th trace  $\mathbb{T}_r : \mathbb{F}_Q \rightarrow \mathbb{F}_q$  such that  $\mathbb{T}_r(x) = \mathbb{T}(x^r)$ .

**Lemma 3.3** (Lemma 2.6 in [12]). *For any fixed  $3 \leq k \leq u$ . The cyclotomic polynomial  $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$  over  $\mathbb{F}_q$  can be splits into irreducible factors as*

$$\Phi_{2^k}(x) = \prod_{1 \leq i \leq 2^{k-3}} (x^2 \pm \mathbb{T}(\beta_k^{2^{i-1}})x + \chi(\beta_k)).$$

**Lemma 3.4** (Theorem 3.3 in [12]). *If  $q \equiv 3 \pmod{4}$  and  $3 \leq k \leq u$ . Then there are  $2^{k-2}$  distinct traces  $\mathbb{T}(\beta_k^{2^{i-1}})$  such that the first  $2^{k-3}$  traces are given by the linear recursive sequence  $\mathbb{T}_{2i-1}(\beta_{2^k}) = \mathbb{T}(\beta_{2^k})\mathbb{T}(\beta_{2^{k-1}}^{i-1}) - \chi(\beta_{2^k})\mathbb{T}(\beta_{2^k}^{2^{i-3}})$  and the rest of  $2^{k-3}$  are  $-\mathbb{T}(\beta_{2^k}^{2^{i-1}})$ . The initial terms of the sequence are  $\mathbb{T}(\beta_4) = 0$  and for  $3 \leq k \leq u$ ,  $\mathbb{T}(\beta_{2^k}) = (\mathbb{T}(\beta_{2^{k-1}}) + 2\chi(\beta_{2^k}))^{(t+1)/2}$ .*

The following result is a useful tool for proving our next theorem. The empty product assumed to be 1.

**Theorem 3.5.** *Assume that  $q \equiv 3 \pmod{4}$  and  $q \equiv 1 \pmod{d}$ . Then  $\Phi_4(x^d) = x^{2d} + 1 = \prod_{0 \leq j \leq d-1} (x^2 + \gamma^j)$  and for  $3 \leq k \leq u$ , the irreducible factorization of decomposable cyclotomic polynomial  $\Phi_{2^k}(x^d)$  over  $\mathbb{F}_q$  is given by:*

$$\Phi_{2^k}(x^d) = \Phi_{2^k}(x) \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 1 \leq j \leq d-1}} (x^2 \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2^{i-1}})x + \chi(\beta_{2^k})\gamma^{2j}).$$

Further, for any integer  $r \geq 1$  and  $3 \leq k \leq u$ , the factorization of decomposable cyclotomic polynomial  $\Phi_{2^k}(x^{2^r d})$  over  $\mathbb{F}_q$  is given by:

$$\Phi_{2^k}(x^{2^r d}) = \Phi_{2^k}(x^{2^r}) \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 1 \leq j \leq d-1}} (x^{2^{r+1}} \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2^{i-1}}) x^{2^r} + \chi(\beta_{2^k}) \gamma^{2j}).$$

Furthermore, the decomposable polynomial  $\Phi_{2^u}(x^{2^r d})$  is a product of  $2^{u-2}$  irreducible trinomials over  $\mathbb{F}_q$ , while the decomposable polynomial  $\Phi_{2^k}(x^{2^r d})$ , where  $2 \leq k \leq u-1$ , is a product of  $2^{k-2}$  reducible trinomials over  $\mathbb{F}_q$ .

*Proof.* Since  $q$  is odd prime power, so  $q^2 \equiv 1 \pmod{4}$ , i.e.,  $Q \equiv 1 \pmod{4}$ . Replacing  $q$  by  $Q$  and  $\alpha_{2^k}$  by  $\beta_{2^k}$  in the result of Theorem 3.1, we obtain the factorization of  $\Phi_{2^k}(x^d)$  over  $\mathbb{F}_Q$  such as

$$\Phi_{2^k}(x^d) = \Phi_{2^k}(x) \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 1 \leq j \leq d-1}} (x - \beta_{2^k}^{2^{i-1}} \gamma^j)$$

where integer  $1 \leq k \leq u$ . Clearly,  $\Phi_2(x^d) = x^d + 1 = (x+1) \prod_{1 \leq j \leq d-1} (x + \gamma^j)$  and  $\Phi_4(x^d) = x^{2d} + 1 = \prod_{0 \leq j \leq d-1} (x^2 + \gamma^j) = (x^2 + 1) \prod_{1 \leq j \leq d-1} (x^2 + \gamma^j)$ . Further, for  $3 \leq k \leq u$ , we can write

$$\begin{aligned} \Phi_{2^k}(x^d) &= \Phi_{2^{k-2}}(x^{4d}) \\ &= \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 0 \leq j \leq d-1}} (x^4 - \beta_{2^{k-2}}^{2^{i-1}} \gamma^j) \\ &= \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 0 \leq j \leq d-1}} (x - \beta_{2^k}^{2^{i-1}} \gamma^j)(x + \beta_{2^k}^{2^{i-1}} \gamma^j)(x^2 + \beta_{2^{k-1}}^{2^{i-1}} \gamma^j). \end{aligned}$$

For any fixed  $0 \leq j \leq d-1$ , using the permutation  $i \mapsto 2^{k-3} - i + 1$  on the set of integers  $1 \leq i \leq 2^{k-3}$ , we obtain

$$\prod_{i=1}^{2^{k-3}} (x^2 + \beta_{2^{k-1}}^{2^{i-1}} \gamma^j) = \prod_{i=1}^{2^{k-3}} (x^2 - \beta_{2^{k-1}}^{-2^{i+1}} \gamma^j).$$

Since  $\beta_{2^k}^{2^{q(2i-1)}} = \beta_{2^{k-1}}^{-2^{i+1}}$ , so that  $x^2 - \beta_{2^{k-1}}^{-2^{i+1}} \gamma^{2j} = (x - \beta_{2^k}^{q(2i-1)} \gamma^j)(x + \beta_{2^k}^{q(2i-1)} \gamma^j)$ . Therefore

$$\prod_{i=1}^{2^{k-3}} (x^2 - \beta_{2^{k-1}}^{-2^{i+1}} \gamma^j) = \prod_{i=1}^{2^{k-3}} (x - \beta_{2^k}^{q(2i-1)} \gamma^j)(x + \beta_{2^k}^{q(2i-1)} \gamma^j).$$

Further,  $\beta_{2^k}^{2^{i-1}} \gamma^j$  and  $-\beta_{2^k}^{2^{i-1}} \gamma^j$  are non-conjugate elements in  $\mathbb{F}_Q \setminus \mathbb{F}_q$  for any  $1 \leq i \leq 2^{k-3}$ . Therefore the minimal polynomial of  $\pm \beta_{2^k}^{2^{i-1}} \gamma^j$

is  $x^2 \pm \mathbb{T}(\beta_{2^k}^{2i-1}\gamma^j)x + (\beta_{2^k}^{2i-1}\gamma^j)^{q+1}$ . Note that  $\mathbb{T}(\beta_{2^k}^{2i-1}\gamma^j) = \gamma^j\mathbb{T}(\beta_{2^k}^{2i-1})$  and  $(\beta_{2^k}^{2i-1}\gamma^j)^{q+1} = \gamma^{2j}\chi(\beta_{2^k}^{2i-1}) = \gamma^{2j}\chi(\beta_{2^k})$  for every  $1 \leq i \leq 2^{k-3}$  and  $3 \leq k \leq u$ . Thus we obtain  $\Phi_{2^k}(x^d)$  over  $\mathbb{F}_q$  is

$$\Phi_{2^k}(x^d) = \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 0 \leq j \leq d-1}} (x^2 \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2i-1})x + \gamma^{2j}\chi(\beta_{2^k})).$$

Further, for any integer  $r \geq 1$ , using the transformation  $x \rightarrow x^{2^r}$ , we have

$$\begin{aligned} \Phi_{2^k}(x^{2^r d}) &= \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 0 \leq j \leq d-1}} (x^{2^{r+1}} \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2i-1})x^{2^r} + \chi(\beta_{2^k})\gamma^{2j}) \\ &= \Phi_{2^k}(x^{2^r}) \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 1 \leq j \leq d-1}} (x^{2^{r+1}} \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2i-1})x^{2^r} + \chi(\beta_{2^k})\gamma^{2j}). \end{aligned}$$

Then by Lemma 2.2, every trinomial  $x^{2^{r+1}} \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2i-1})x^{2^r} + \chi(\beta_{2^k})\gamma^{2j}$  is reducible for  $3 \leq k \leq u-1$  and irreducible over  $\mathbb{F}_q$  for  $k = u$ .  $\square$

In the following theorem, we determine the factorization of  $x^{2^nd} - 1$  over  $\mathbb{F}_q$ , when  $q \equiv 3 \pmod{4}$  and  $q \equiv 1 \pmod{d}$ .

**Theorem 3.6.** *If  $q \equiv 3 \pmod{4}$  and  $d \mid (q-1)$ , then  $x^{2^nd} - 1$  can be written as a product of  $d(2^{u-2}(n-u+2)+1)$  irreducible factors over  $\mathbb{F}_q$  as:*

$$\begin{aligned} x^{2^nd} - 1 &= (x^{2^n} - 1) \prod_{1 \leq j \leq d-1} (x \pm \gamma^j) \prod_{\substack{2 \leq k \leq u-1 \\ 1 \leq i \leq 2^{k-2} \\ 1 \leq j \leq d-1}} (x^2 - \gamma^j \mathbb{T}(\beta_{2^k}^{2i-1})x + \gamma^{2j}) \\ &\quad \prod_{\substack{0 \leq r \leq n-u \\ 1 \leq i \leq 2^{u-3} \\ 1 \leq j \leq d-1}} (x^{2^{r+1}} \pm \gamma^j \mathbb{T}(\beta_{2^u}^{2i-1})x^{2^r} - \gamma^{2j}). \end{aligned}$$

*Proof.* By substituting  $s = 1$  in Lemma 2.5, the factorization of  $x^{2^nd} - 1$  over  $\mathbb{F}_q$  reduces to

$$x^{2^nd} - 1 = (x^d - 1) \Phi_2(x^d) \prod_{1 \leq r \leq n-1} \Phi_2(x^{2^r d}).$$

At this point, we recall  $u = \max\{r \in \mathbb{Z} : 2^r \mid (Q-1)\}$ . Then we write

$$\begin{aligned} x^{2^nd} - 1 &= (x^{2^d} - 1) \prod_{k=2}^{u-1} \Phi_{2^k}(x^d) \prod_{r=u}^n \Phi_{2^r}(x^d) \\ &= \prod_{j=0}^{d-1} \left( (x \pm \gamma^j)(x^2 + \gamma^j) \prod_{k=3}^{u-1} \Phi_{2^k}(x^d) \prod_{r=0}^{n-u} \Phi_{2^r}(x^{2^r d}) \right). \end{aligned}$$

The result now follows from Theorem 3.5.  $\square$



In the following corollary, the factorization of  $\Phi_{2^n d}(x)$  over  $\mathbb{F}_q$  is to be deduced for every prime odd divisor  $d$  of  $q - 1$ .

**Corollary 3.1.** *Let  $q$  be an odd prime power and  $d$  be an odd prime such that  $d \mid (q - 1)$ .*

- (i) *If  $q \equiv 1 \pmod{4}$  and  $2 \leq k \leq s$ . Then, for any integer  $n \geq k$ , the factorization of  $\Phi_{2^n d}(x)$  over  $\mathbb{F}_q$  into  $2^{k-1}(d-1)$  factors is given by:*

$$\Phi_{2^n d}(x) = \prod_{\substack{1 \leq i \leq 2^{k-1} \\ 1 \leq j \leq d-1}} (x^{2^{n-k}} - \alpha_{2^k}^{2^{i-1}} \gamma^j).$$

*All these factors of  $\Phi_{2^n d}(x)$  are irreducible over  $\mathbb{F}_q$  when  $k = s$ .*

- (ii) *If  $q \equiv 3 \pmod{4}$  and  $3 \leq k \leq u$ . Then, for any  $n \geq k$ , the factorization of  $\Phi_{2^n d}(x)$  into  $2^{k-2}(d-1)$  factors over  $\mathbb{F}_q$  is given by:*

$$\Phi_{2^n d}(x) = \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 1 \leq j \leq d-1}} (x^{2^{n-k+1}} \pm \gamma^j \mathbb{T}(\beta_{2^k}^{2^{i-1}}) x^{2^{n-k}} + \chi(\beta_{2^k}) \gamma^{2^j}).$$

*All these factors of  $\Phi_{2^n d}(x)$  are irreducible over  $\mathbb{F}_q$  when  $k = u$ .*

*Proof.* For any integer  $n \geq k \geq 1$ , by Lemma 2.3 (iii), the cyclotomic polynomial  $\Phi_{2^n d}(x)$  over  $\mathbb{F}_q$  is

$$\Phi_{2^n d}(x) = \frac{\Phi_{2^k}(x^{2^{n-k}d})}{\Phi_{2^k}(x^{2^{n-k}})} \text{ for integer } n \geq k \geq 1.$$

The remaining part of proof now follows from Theorem 3.1 and Theorem 3.5. The irreducibility follows from Lemma 2.1 for binomials and Lemma 2.2 for trinomials factors of  $\Phi_{2^n d}(x)$  over  $\mathbb{F}_q$ .  $\square$

## 4 Main results

In this section, we introduce a direct method to obtain the coefficients of irreducible factors of  $\Phi_{2^n t}(x)$  and hence of  $x^{2^n t} - 1$  over  $\mathbb{F}_q$  when  $q$  and  $t$  are odd primes such that either  $q = 2t + 1$  or  $q = 4t + 1$ . First, we define  $\mathcal{S}_q = \{a^2 : a \in \mathbb{F}_q^*\}$  and  $\mathcal{O}_q = \{a \in \mathbb{F}_q^* : O_q(a) \text{ is odd}\}$ , where  $O_q(a)$  denotes the order of  $a \in \mathbb{F}_q^*$ . Note that  $\mathcal{S}_3 = \mathcal{O}_3 = \{1\}$ ,  $\mathcal{S}_5 = \mathcal{O}_5 = \{1, 4\}$ ,  $\mathcal{S}_7 = \mathcal{O}_7 = \{1, 2, 4\}$ .

**Theorem 4.1.** *For any odd prime power  $q$ ,  $\mathcal{S}_q$  and  $\mathcal{O}_q$  are subgroups of  $\mathbb{F}_q^*$  such that  $\mathcal{O}_q \subseteq \mathcal{S}_q$ . Further, if  $q = 2^s t + 1$  for some integer  $s \geq 1$  and  $t$  is an odd integer. Then, the subgroup  $\mathcal{O}_q$  has  $t$  distinct element and the set  $\mathcal{S}_q \setminus \mathcal{O}_q$  contains  $(2^{s-1} - 1)t$  elements of  $\mathcal{S}_q$ . Further,  $\mathcal{O}_q = \mathcal{S}_q$  if and only if  $q \equiv 3 \pmod{4}$ .*

*Proof.* Let  $q = 2^s t + 1$  with integer  $s \geq 1$  and  $t$  is odd. Since  $\mathcal{S}_q$  contains  $(q-1)/2$  distinct elements of  $\mathbb{F}_q^*$ , so the order of  $\mathcal{S}_q$ , i.e.,  $|\mathcal{S}_q| = 2^{s-1}t$ . Now let  $a \in \mathcal{O}_q$  with  $|a| = l$ , then  $l$  is odd. By the converse of Lagrange's theorem,  $l|(q-1)$ . Since  $l$  is odd, so  $l|t$  and hence  $a \in \mathcal{S}_q$ . It follows that  $\mathcal{O}_q \subseteq \mathcal{S}_q$  and  $|\mathcal{O}_q| = \max\{l : |a| = l \text{ and } a \in \mathcal{O}_q\} = t$ . In view of the above, it is trivial to note the number of elements in  $\mathcal{S}_q \setminus \mathcal{O}_q$  is  $(2^{s-1} - 1)t$ . Further, if  $q \equiv 3 \pmod{4}$ , then  $s = 1$  and hence  $\mathcal{O}_q = \mathcal{S}_q$ .  $\square$

**Theorem 4.2.** *Let  $q$  and  $t$  be odd primes such that  $q = 2t + 1$ . Then  $\mathcal{S}_q = \mathcal{O}_q = \langle 4 \rangle$ .*

*Proof.* By Theorem 4.1,  $\mathcal{S}_q = \mathcal{O}_q$ . Since  $4 \in \mathcal{S}_q$ , so  $4 \in \mathcal{O}_q$ . Note that  $\mathcal{O}_q$  is cyclic group of prime order  $t$ , so any element of  $\mathcal{O}_q$ , except 1, works as a generator. It follows that  $\mathcal{O}_q = \langle 4 \rangle$ .  $\square$

**Lemma 4.3** (see Corollary 7.10 in [8]). *If  $p$  is an odd prime then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

**Theorem 4.4.** *Let  $q$  and  $t$  be odd primes such that  $q = 4t + 1$ . Then  $t, \sqrt{t} \in \mathcal{S}_q$ . Further*

- (i)  $\mathcal{O}_q = \langle t \rangle$ .
- (ii)  $\mathcal{S}_q = \langle 4 \rangle$  and  $\mathcal{O}_q = \langle 16 \rangle$  for  $q > 13$ .

*Proof.* Let  $q = 2t + 1$ , where  $q$  and  $t$  be primes. Since  $4, -1 \in \mathcal{S}_q$  and  $4t = -1 \in \mathbb{F}_q^*$ , so that  $t \in \mathcal{S}_q$  and hence  $\sqrt{t} \in \mathbb{F}_q^*$ . From Lemma 4.3, it follows that  $2 \notin \mathcal{S}_q$  as  $q \equiv 5 \pmod{8}$ . Since  $2\sqrt{t} = \sqrt{-1}$  or  $2\sqrt{t} = -\sqrt{-1}$  with 2 and  $\pm\sqrt{-1}$  do not belong to  $\mathcal{S}_q$ , so that  $\sqrt{t} \in \mathcal{S}_q$  because the product of a square and non-square element always a non-square element in  $\mathbb{F}_q^*$ .

- (i) In this item, we shall show that  $t$  is an element of  $\mathcal{O}_q$  of the order  $t$ , that is  $O_q(t) = t$ . Since  $t \in \mathcal{S}_q$ , so  $O_q(t) = t$  or  $2t$ . On contrary assume that,  $O_q(t) = 2t$ . This yields that  $t^t \equiv -1 \pmod{q}$ . Using the fact  $4t \equiv -1 \pmod{q}$  and the arithmetic in  $\mathbb{F}_q$ , we have  $t^{(t-1)/2} \pm 2 \equiv 0 \pmod{q}$ . This implies  $2 \in \mathcal{S}_q$  or  $-2 \in \mathcal{S}_q$ , a contradiction.
- (ii) Recall  $2 \notin \mathcal{S}_q$ . Therefore the order of 2 is  $4t$ . Using exponent rule, it follows that  $O_q(4) = O_q(2^2) = \frac{4t}{\gcd(2, 4t)} = 2t$  and  $O_q(4^2) = \frac{2t}{\gcd(2, 2t)} = t$ . This completes the proof.

$\square$

**Remark 4.1.** Since  $t \in \mathcal{O}_q = \langle 16 \rangle$ , so  $t = 16^i$  for some unique integer  $1 \leq i \leq t-1$ . Thus  $\sqrt{t} = 4^i$  and hence  $\sqrt{t} \in \mathcal{S}_q$ . For example taking  $q = 53$ , then  $t = 13 = 16^6$  and  $\sqrt{t} = 16^3 = 15 \in \mathcal{O}_{53}$ .

**Theorem 4.5.** Let  $q$  and  $t$  be odd primes.

(i) If  $q = 4t+1$ . Then, for any integer  $n \geq k$ , the factorization of  $\Phi_{2^{n_t}}(x)$  over  $\mathbb{F}_q$  is given by:

$$\Phi_{2^{n_t}}(x) = \prod_{1 \leq j \leq t-1} (x^{2^{n-2}} \pm \sqrt{-1} \cdot 16^j).$$

(ii) If  $q = 2t+1$  and  $3 \leq k \leq u$ . Then, for any  $n \geq k$ , the factorization of  $\Phi_{2^{n_t}}(x)$  over  $\mathbb{F}_q$  is given by:

$$\Phi_{2^{n_t}}(x) = \prod_{\substack{1 \leq i \leq 2^{k-3} \\ 1 \leq j \leq t-1}} (x^{2^{n-k+1}} \pm 4^j \mathbb{T}(\beta_{2^k}^{2i-1}) x^{2^{n-k}} + \chi(\beta_{2^k}) 16^j).$$

*Proof.* Let  $q$  and  $t$  be odd primes. The proof will follow by applying Theorem 4.2 and Theorem 4.4 in Corollary 3.1 in two different cases  $q = 4t+1$  and  $q = 2t+1$ .  $\square$

**Remark 4.2.** In particular, the factorization  $\Phi_{2^{n_5}}(x)$  is the same as in [16, Theorem 3.1& 3.2]) when  $q \equiv 1 \pmod{5}$  and the factorization  $\Phi_{2^{n_3}}(x)$  is same as in [6, Propostion 3 (see parts 1-3)] when  $q \equiv 1 \pmod{3}$ . Further, in view of [16, Corollary 3.3], the computation of the coefficients of factors of  $\Phi_{2^{n_5}}(x)$  requires to solve two nonlinear recurrence relations, while in our case, all coefficients can be obtained directly using Theorem 4.2 or Theorem 4.4.

In the following two theorems, we obtain the factorization of  $x^{2^{n_t}} - 1$  into irreducible factors over  $\mathbb{F}_q$  when either  $q = 2t+1$  or  $q = 4t+1$ . In particular, the factorization of  $x^{2^{n_t}} - 1$  into irreducible factors in  $\mathbb{F}_q[x]$  plays a very important role to describe cyclic codes of length  $2^{n_t}$  over  $\mathbb{F}_q$ .

**Theorem 4.6.** Let  $q$  and  $t$  be odd primes such that  $q = 2t+1$ , then

$$\begin{aligned} x^{2^{n_t}} - 1 &= \prod_{0 \leq j \leq t-1} (x \pm 4^j) \prod_{\substack{2 \leq k \leq u-1 \\ 1 \leq i \leq 2^{k-2} \\ 0 \leq j \leq t-1}} (x^2 - 4^j \mathbb{T}(\beta_{2^k}^{2i-1}) x + 4^{2j}) \\ &\quad \prod_{\substack{0 \leq r \leq n-u \\ 1 \leq i \leq 2^{u-3} \\ 0 \leq j \leq t-1}} (x^{2^{r+1}} \pm 4^j \mathbb{T}(\beta_{2^u}^{2i-1}) x^{2^r} - 4^{2j}). \end{aligned}$$

*Proof.* The proof follows immediately by using Theorem 3.4, Theorem 3.6 and Theorem 4.2.  $\square$

**Theorem 4.7.** *Let  $q$  and  $t$  be odd primes such that  $q = 4t + 1$ . Then the factorization of  $x^{2^{nt}} - 1$  into the product of  $2nt$  irreducible polynomials over  $\mathbb{F}_q$  is given as:*

$$x^{2^{nt}} - 1 = \prod_{j=0}^{t-1} \left( (x \pm 16^j)(x \pm \sqrt{-1} \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2^r} \pm \sqrt{-1} \cdot 16^j) \right).$$

*Proof.* The proof follows immediately from Theorem 3.2 and Theorem 4.4.  $\square$

## 5 Worked Examples

In this section, we give some examples to illustrate our results. In particular, if  $q$  and  $t$  are primes such that  $q \in \{2t + 1, 4t + 1\}$ , then all coefficients of irreducible factors can be determined directly.

**Example 5.1.** *Let  $q = 347 = 2 \cdot 173 + 1$ . Then  $s = 1$ ,  $t = 173$  and  $u = 3$ . Now  $\beta_2 = -1$ ,  $\mathbb{T}(\beta_4) = 0$  and  $\mathbb{T}(\beta_8) = \sqrt{-2} = (-2)^{87} = 107$ . By Theorem 4.2, 4 is a primitive 173th root of unity in  $\mathbb{F}_{347}^*$ . This follows that  $x^{173} - 1 = \prod_{j=0}^{172} (x - 4^j)$  and  $x^{173} + 1 = \prod_{j=0}^{172} (x + 4^j)$ . Also  $x^{346} + 1 = \prod_{j=0}^{172} (x^2 + 4^j)$ . Further, for  $n \geq 3$ , by Theorem 4.6, the factorization of  $x^{173 \cdot 2^n} - 1$  into  $173(2n - 1)$  irreducible factors over  $\mathbb{F}_{347}$  is given as:*

$$x^{173 \cdot 2^n} - 1 = \prod_{0 \leq j \leq 172} \left( (x \pm 4^j)(x^2 + 4^{2j}) \prod_{0 \leq r \leq n-3} (x^{2^{r+1}} \pm 4^j \cdot 107x^{2^r} - 4^{2j}) \right).$$

**Example 5.2.** *Let  $q = 23 = 2 \cdot 11 + 1$ . Then  $s = 1$ ,  $t = 11$  and  $u = 4$ . In  $\mathbb{F}_{23}^*$ ,  $\beta_2 = -1$ ,  $\mathbb{T}(\beta_4) = 0$ ,  $\mathbb{T}(\beta_8) = \sqrt{2} = 2^6 = -5$  and  $\mathbb{T}(\beta_{16}) = \sqrt{-5-2} = (-7)^6 = 4$ ,  $\mathbb{T}_3(\beta_{16}) = 7$ . By Theorem 4.2, 4 is a primitive 11th root of unity in  $\mathbb{F}_{11}^*$ . This follows that  $x^{11} - 1 = \prod_{j=0}^{10} (x - 4^j)$  and  $x^{11} + 1 = \prod_{j=0}^{10} (x + 4^j)$ . Also  $x^{22} + 1 = \prod_{j=0}^{10} (x^2 + 4^j)$ . Further, by Theorem 4.6, the factorization of  $x^{352} - 1$  into 143 irreducible factors over  $\mathbb{F}_{23}$  is given as:*

$$\begin{aligned} x^{352} - 1 &= \prod_{0 \leq j \leq 10} \left( (x \pm 4^j) \prod_{\substack{2 \leq k \leq 3 \\ 1 \leq i \leq 2^{k-2}}} (x^2 - 4^j \mathbb{T}(\beta_{2^k}^{2^i-1})x + 4^{2j}) \right. \\ &\quad \left. \prod_{1 \leq i \leq 2} (x^2 \pm 4^j \mathbb{T}(\beta_{16}^{2^i-1})x - 4^{2j})(x^4 \pm 4^j \mathbb{T}(\beta_{16}^{2^i-1})x^2 - 4^{2j}) \right) \\ &= (x^{44} - 1) \prod_{\substack{0 \leq j \leq 10 \\ \eta \in \{4, 7\}}} \left( (x^2 \pm 4^j \cdot 5x + 4^{2j}) \right. \\ &\quad \left. \cdot (x^2 \pm 4^j \eta x - 4^{2j})(x^4 \pm 4^j \eta x^2 - 4^{2j}) \right). \end{aligned}$$

Further, using recursive approach, the factorization of  $x^{704} - 1$  into 187 irreducible factors over  $\mathbb{F}_{23}$  is given by

$$x^{704} - 1 = (x^{352} - 1) \prod_{\substack{0 \leq j \leq 10 \\ \eta \in \{4,7\}}} (x^8 \pm 4^j \eta x^4 - 4^{2j}).$$

Note that  $23^4 \equiv 1 \pmod{352}$ . By Theorem 4.5, the factorization of cyclotomic polynomial  $\Phi_{352}(x)$  into 40 (i.e.  $\phi(352)/4$ ) irreducible factors over  $\mathbb{F}_{23}$  is given by:

$$\begin{aligned} \Phi_{352}(x) &= \prod_{\substack{1 \leq i \leq 2 \\ 1 \leq j \leq 10}} (x^4 \pm 4^j \mathbb{T}(\beta_{16}^{2i-1})x^2 - 16^j) \\ &= \prod_{j=1}^{10} (x^4 \pm 4^j \cdot 4x^2 - 16^j)(x^4 \pm 4^j \cdot 7x^2 - 16^j). \end{aligned}$$

**Example 5.3.** Let  $q = 149 = 4 \cdot 37 + 1$ . Then  $s = 2$ ,  $t = 37$ . By Theorem 4.4,  $\alpha_4 = \sqrt{-1} = \sqrt{148} = 2\sqrt{37} = 2 \cdot 16^9 = -44$ . Using Theorem 4.7, the factorization of  $x^{2^n \cdot 37} - 1$  over  $\mathbb{F}_{149}$  can be written as a product of  $74n$  irreducible factors as:

$$x^{2^n \cdot 37} - 1 = \prod_{j=0}^{36} \left( (x \pm 16^j)(x \pm 44 \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2^r} \pm 44 \cdot 16^j) \right).$$

**Example 5.4.** Let  $q = 53 = 4 \cdot 13 + 1$ . Then  $s = 2$ ,  $t = 13$ . By Theorem 4.4,  $\alpha_4 = \sqrt{-1} = \sqrt{52} = 2\sqrt{13} = 2 \cdot 16^3 = 30$ . Using Theorem 4.7, the factorization of  $x^{2^n \cdot 13} - 1$  over  $\mathbb{F}_{53}$  can be written as a product of  $26n$  irreducible factors as:

$$x^{2^n \cdot 13} - 1 = \prod_{j=0}^{12} \left( (x \pm 16^j)(x \pm 30 \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2^r} \pm 30 \cdot 16^j) \right).$$

**Example 5.5.** Let  $q = 59 = 2 \cdot 29 + 1$ . Then  $t = 29$  and  $u = 3$ . Then  $\mathbb{T}(\beta_4) = 0$  and  $\mathbb{T}(\beta_8) = \sqrt{-2} = (-2)^{15} = 36$ . Then by Theorem 4.5, the factorization  $\Phi_{464}(x)$  over  $\mathbb{F}_{59}$  is given by

$$\Phi_{464}(x) = \prod_{j=1}^{28} (x^4 \pm 4^j \cdot 36x^2 - 16^j)$$

with 56 irreducible trinomials over  $\mathbb{F}_{59}$ .

## References

- [1] E. R. Berlekamp, Bit- Serial Reed-Solomon encodes. IEEE Trans. Inf. Theory. **28** 869-874 (1982).

- [2] I. F. Blake, S. Gao, R.C. Mullin, Explicit Factorization of  $x^{2^k} + 1$  over  $\mathbb{F}_p$  with  $p \equiv 3(\text{mod } 4)$ . App. Algebra Engrg. Comm. Comput. **4**, 89-94 (1993).
- [3] F. E. Brochero Martínez, C. R. Giraldo Vergara, L. B. de Oliveira, Explicit factroization of  $x^n - 1 \in \mathbb{F}_q[x]$ . Des. Codes Cryptogr. **77**, 277-286 (2015).
- [4] B. Chen, L. Li, R. Tuerhong, Explicit factorization of  $x^{2^m p^n} - 1$  over a finite field. Finite Fields Appl. **24**, 95-104 (2013).
- [5] R. W. Fitzgerald, J. L. Yucas, Factors of Dickson polynomials over finite fields. Finite Fields Appl. **11**, 724-737 (2005).
- [6] R. W. Fitzgerald, J. L. Yucas, Explicit factorization of cyclotomic and Dickson polynomials over finite fields. Arithmetic of Finite Fields. Lecture Notes in Comput. Sci. vol. 4547, pp. 1-10. Springer, Berlin (2007).
- [7] S. Golomb, G. Gong, Signal design for good correlation: For wireless communication, cryptography, and radar. Cambridge University Press. Cambridge (2005).
- [8] G. A. Jones, J. M. Jones, Elementary Number Theory. Springer-Verlag, Berlin (1998).
- [9] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1986).
- [10] H. Meyn, Factorization of cyclotomic polynomial  $x^{2^n} + 1$  over finite fields. Finite Fields Appl. **2**, 439-442 (1996).
- [11] S. Roman, Field Theory. Springer-Verlag. Graduate Texts in Mathematics, New York (1995)
- [12] M. Singh, S. Batra, Some special cyclic codes of length  $2^n$ . J. Algebra Appl. **17**(1), 170002 (1-17) (2017).
- [13] G. Stein, Using the theory of cyclotomy to factor cyclotomic polynomials over finite fields. Math. Comp. **70**(235), 1237-1251 (2001).
- [14] A. Tuxanidy, Q. Wang, Composed products and factors of cyclotomic polynomials over finite fields. Des. Codes Cryptogr. **69**, 203-231 (2013).
- [15] Z. Wan, Lectures on Finite Fields and Galois Rings. World Scientific Publishing, Singapore, (2003).
- [16] L. Wang, Q. Wang, On explicit factors of cyclotomic polynomials over finite fields. Des. Codes Cryptogr. **63**(1), 87-104 (2011).