THE 3-SPARSITY OF $X^n - 1$ OVER FINITE FIELDS, II

KAIMIN CHENG

Abstract. Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. For a positive integer n, the polynomial $X^n - 1 \in \mathbb{F}_q[X]$ is termed *3-sparse* over $\mathbb{F}_q$ if all its irreducible factors in $\mathbb{F}_q[X]$ are either binomials or trinomials. In 2021, Oliveira and Reis characterized all positive integers n for which $X^n - 1$ is 3-sparse over $\mathbb{F}_q$ when $q = 2$ and $q = 4$. Recently, the author provided a complete characterization for odd q. This paper extends the investigation to finite fields of even characteristic, fully determining all n such that $X^n - 1$ is 3-sparse over $\mathbb{F}_q$ for even q. This work resolves two open problems posed by Oliveira and Reis for even characteristic case.

1. Introduction

Let q be a prime power and $\mathbb{F}_q$ the finite field of q elements, with $\mathbb{F}_q^*$ its multiplicative group. The factorization of polynomials over $\mathbb{F}_q$ is a fundamental problem in finite field theory, with significant applications in coding theory [**?**] and cryptography [**?**]. For a positive integer n, the polynomial $X^n - 1 \in \mathbb{F}_q[X]$ is of particular interest, as its irreducible factors correspond to cyclic codes of length n over $\mathbb{F}_q$ [**?**]. Thus, determining the irreducible factorization of $X^n - 1$ is of critical importance.

The factorization of $X^n - 1$ has been a challenging problem studied extensively over decades. Notable contributions include [**?**, **?**, **?**, **?**], with more general results in [**?**, **?**]. A significant result by [**?**] provides an explicit factorization of $X^n - 1$ over $\mathbb{F}_q$ when each prime factor of n divides $q^2 - 1$. An intriguing property arises when all irreducible factors of $X^n - 1$ are either binomials or trinomials, leading to the definition of *3-sparse* polynomials. Such a type of polynomials has important applications, for instance, for an efficient hardware implementation of feedback shift registers (see [1]). This prompts the question of identifying all positive integers n for which $X^n - 1$ is 3-sparse over $\mathbb{F}_q$. In 2021, Oliveira and Reis [**?**] characterized such n for $q = 2$ and $q = 4$, posing the following problems:

Problem 1.1. *For any prime power q, determine all positive integers n such that $X^n - 1$ is 3-sparse over $\mathbb{F}_q$.*

Problem 1.2. *For any prime power q, prove or disprove that there are only finitely many primes p such that $X^p - 1$ is 3-sparse over $\mathbb{F}_q$.*

Recently, the author [**?**] resolved Problems **??** and **??** for odd q by showing that for any positive integer n not divisible by $\mathrm{Char}(\mathbb{F}_q)$, the binomial $X^n - 1$ is 3-sparse over $\mathbb{F}_q$ if and only if $\mathrm{rad}(n)$ divides $q^2 - 1$, where $\mathrm{rad}(n)$ is the product of distinct prime divisors of n and $\mathrm{Char}(\mathbb{F}_q)$ is the characteristic of $\mathbb{F}_q$. This paper focuses on the case of even characteristic, completing the characterization of 3-sparsity for $X^n - 1$ over $\mathbb{F}_q$.

Date: July 16, 2025.

2020 *Mathematics Subject Classification.* Primary 11T06.

Key words and phrases. Finite fields, cyclotomic polynomials, 3-sparsity, irreducible factorization.

For coprime positive integers a and m, let $\mathrm{ord}_m(a)$ denote the multiplicative order of a modulo m. The main result is stated as follows:

Theorem 1.3. *Let $q = 2^e$ with e a positive integer. For an odd positive integer n, the polynomial $X^n - 1$ is 3-sparse over $\mathbb{F}_q$ if and only if one of the following holds:*
(a) $rad(n)$ divides $q^2 - 1$.
(b) $n = 7^k n_1$ for some positive integers k and n_1 with $rad(n_1) \mid (q-1)$ when $e \equiv \pm 1 \pmod 6$.
(c) $n = 3 \cdot 7^k n_2$ for some positive integers k and n_2 with $3 \nmid n_2$ and $rad(n_1) \mid (q-1)$ when $e \equiv \pm 2 \pmod 6$.

Theorem **??** completely describes the 3-sparsity of $X^n - 1$ over finite fields of even characteristic, addressing Problem **??** for even q. As a direct result of Theorem **??**, we settle Problem **??**:

Corollary 1.4. *For any even prime power q, the polynomial $X^p - 1$ is 3-sparse over $\mathbb{F}_q$ for only finitely many primes p.*

The paper is organized as follows. Section 2 presents preliminary lemmas necessary for the proof of the main result. Section 3 provides the proof of Theorem **??**.

2. Preliminary Lemmas

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. For a positive integer d, the d-th cyclotomic polynomial over $\mathbb{F}_q$ is defined as:

$$\Phi_d(X) = \prod_{\substack{i=1 \\ \gcd(i,d)=1}}^{d} (X - \xi^i),$$

where ξ is a primitive d-th root of unity. If d is prime, then:

$$\Phi_d(X) = X^{d-1} + X^{d-2} + \cdots + X + 1.$$

For integers $a \geq 1$ and $b \geq 2$ with $\gcd(a,b) = 1$, let $\mathrm{ord}_b(a)$ denote the multiplicative order of a modulo b. The following lemmas are foundational:

Lemma 2.1. [**?**, Exercise 2.57] *Let r be a prime and m, n, M be positive integers with $r \nmid M$. Then:*

$$\Phi_{mr^n}(X) = \Phi_{mr}(X^{r^{n-1}}), \;\; \Phi_{Mr}(X) = \frac{\Phi_M(X^r)}{\Phi_M(X)}.$$

Lemma 2.2. [**?**, Theorem 2.47] *For a positive integer n,*

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Moreover, $\Phi_d(X)$ factors into $\frac{\phi(d)}{ord_d(q)}$ distinct irreducible monic polynomials in $\mathbb{F}_q[X]$ of degree $ord_d(q)$, where ϕ is the Euler totient function.

Lemma 2.3. [**?**, Theorem 3.46] *Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n. Then f factors into d irreducible polynomials over $\mathbb{F}_{q^k}$ of degree $\frac{n}{d}$, where $d = \gcd(n,k)$.*

Lemma 2.4. [**?**, Lemma 2.4] *Let $m_1, m_2 \geq 2$ be integers with $\gcd(m_1, m_2) = 1$. For any positive integer a with $\gcd(m_1, a) = 1$ and $\gcd(m_2, a) = 1$,*

$$ord_{m_1 m_2}(a) = lcm(ord_{m_1}(a), ord_{m_2}(a)).$$

Employing mathematical induction, as established in Lemma 2.5 of [**?**], we deduce the result, with the proof omitted for brevity:

Lemma 2.5. *Let q be an even prime power, k_1 the p-adic valuation of $q-1$, and k_2 the p-adic valuation of $q+1$. For any nonnegative integer k,*

$$ord_{p^k}(q) = \begin{cases} 1, & \text{if } p \mid (q-1) \text{ and } 1 \leq k \leq k_1, \\ p^{k-k_1}, & \text{if } p \mid (q-1) \text{ and } k > k_1, \\ 2, & \text{if } p \mid (q+1) \text{ and } 1 \leq k \leq k_2, \\ 2p^{k-k_2}, & \text{if } p \mid (q+1) \text{ and } k > k_2. \end{cases}$$

If $7 \nmid (q^2-1)$, then:

$$ord_{7^k}(q) = 3 \cdot 7^{k-1}.$$

Lemma 2.6. [**?**, Theorem 3.39] *Let $f(X)$ be a monic irreducible polynomial in $\mathbb{F}_q[X]$ of degree m, with root $\alpha \in \mathbb{F}_{q^m}$. For a positive integer t, let $G_t(X)$ be the characteristic polynomial of $\alpha^t \in \mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then:*

$$G_t(X^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(w_j X),$$

where $w_1, \ldots, w_t$ are the t-th roots of unity over $\mathbb{F}_q$, counted with multiplicity.

Lemma 2.7. [**?**, Lemma 2] *Let m and n be positive integers, and $a \in \mathbb{F}_q^*$ of order M in $\mathbb{F}_q^*$. Then $X^m - a$ divides $X^n - 1$ if and only if $mM \mid n$.*

Lemma 2.8. *Let q be an even prime power such that $7 \nmid (q^2-1)$, and let $\Phi_{7^k}(X) \in \mathbb{F}_q[X]$ be the 7^k-th cyclotomic polynomial for a positive integer k. Then $\Phi_{7^k}(X)$ has the irreducible factorization over $\mathbb{F}_q$:*

$$\Phi_{7^k}(X) = (X^{3\cdot 7^{k-1}} + X^{7^{k-1}} + 1)(X^{3\cdot 7^{k-1}} + X^{2\cdot 7^{k-1}} + 1).$$

Proof. Let $q = 2^e$ for a positive integer e. Since $\Phi_{7^k}(X) \in \mathbb{F}_2[X]$, we first consider its factorization over $\mathbb{F}_2$. The cyclotomic polynomial $\Phi_7(X)$ factors as:

$$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1).$$

Since $7 \nmid (q^2-1)$, we have $\gcd(e,3) = 1$. By Lemma **??**, this factorization holds over $\mathbb{F}_q$. By Lemma **??**,

$$\Phi_{7^k}(X) = \Phi_7(X^{7^{k-1}}) = (X^{3\cdot 7^{k-1}} + X^{7^{k-1}} + 1)(X^{3\cdot 7^{k-1}} + X^{2\cdot 7^{k-1}} + 1).$$

By Lemmas **??** and **??**, $\Phi_{7^k}(X)$ splits into irreducible polynomials over $\mathbb{F}_q$ of degree $3 \cdot 7^{k-1}$. Thus, the above is the irreducible factorization, as required. □

3. Proof of Theorem ??

In this section, we present the proof of Theorem **??**.

Proof of Theorem **??**. Let $q = 2^e$ for some positive integer e. We establish the theorem by proving both necessity and sufficiency.

Necessity. The case $n = 1$ is trivial. For $n \geq 2$, assume $X^n - 1$ is 3-sparse over $\mathbb{F}_q$, meaning its irreducible factors are binomials or trinomials. Let p be a prime divisor of n. We show that if $e \equiv 0 \pmod 3$, then $p \mid (q^2-1)$, and if $e \not\equiv 0 \pmod 3$, then $p \mid (q^2-1)$ or $p = 7$. Since $q^2 - 1$ is divisible by 3, we assume $p > 3$ henceforth.

Suppose $p \nmid (q^2-1)$. We aim to derive a contradiction if $e \equiv 0 \pmod 3$, and show $p = 7$ if $e \not\equiv 0 \pmod 3$. Since $X^p - 1$ divides $X^n - 1$, it is 3-sparse. By Lemma **??**, the cyclotomic polynomial $\Phi_p(X)$ divides $X^p - 1$, so its irreducible factors are binomials or trinomials. First, $\Phi_p(X)$ has no binomial factors. Suppose $\Phi_p(X)$ has a factor $X^m - a$, where $1 \le m \le p-1$ and $a \in \mathbb{F}_q^*$. By Lemma **??**, $mM \mid p$, where M is the order of a in $\mathbb{F}_q^*$. Since $M \mid (q-1)$ and $p \nmid (q^2-1)$, we have $M = m = 1$, implying $X - 1 \mid \Phi_p(X)$, a contradiction. Thus, $\Phi_p(X)$ factors as:

$$\Phi_p(X) = \prod_{i=1}^{(p-1)/t} (X^t + a_i X^{k_i} + b_i), \tag{3.1}$$

where $a_i, b_i \in \mathbb{F}_q^*$, $1 \le k_i < t$, and $t = \mathrm{ord}_p(q)$. Each factor is an irreducible trinomial. Since $\Phi_p(X) = X^{p-1} + \cdots + X + 1$, comparing the coefficient of X in (**??**) implies $\Phi_p(X)$ has an irreducible factor $X^t + aX + b$, with $a, b \in \mathbb{F}_q^*$. Let ξ be a root of $X^t + aX + b$, a primitive p-th root of unity in $\mathbb{F}_{q^t}$. Since $p > 3$, ξ^3 is also a primitive p-th root of unity. Let $g_3(X)$ be the minimal polynomial of ξ^3 over $\mathbb{F}_q$, of degree t. It is an irreducible factor of $\Phi_p(X)$, hence an irreducible trinomial over $\mathbb{F}_q$.

By Lemma **??**, the characteristic polynomial $G_3(X)$ of ξ^3 satisfies:

$$G_3(X^3) = X^{3t} + c_{2t+1}X^{2t+1} + c_{2t}X^{2t} + c_{t+2}X^{t+2} + c_{t+1}X^{t+1} + c_t X^t + a^3X^3 + b^3,$$

where:

$$c_{2t+1} = a(w^{2t+1} + w^{t+2} + 1), \quad c_{2t} = b(w^{2t} + w^t + 1), \quad c_{t+2} = a^2(w^{2t+1} + w^{t+2} + 1),$$
$$c_{t+1} = abw(w^{2t} + w^{2t-1} + w^{t+1} + w^{t-1} + w + 1), \quad c_t = b^2(w^{2t} + w^t + 1),$$

and w is a primitive cubic root of unity. We compute:

$$(c_{2t+1}, c_{2t}, c_{t+2}, c_{t+1}, c_t) = \begin{cases} (0, b, 0, 0, b^2), & \text{if } t \equiv 0 \pmod 3, \\ (a, 0, a^2, 0, 0), & \text{if } t \equiv 1 \pmod 3, \\ (0, 0, 0, ab, 0), & \text{if } t \equiv 2 \pmod 3. \end{cases}$$

Thus:

$$G_3(X) = \begin{cases} X^t + bX^{2t/3} + b^2X^{t/3} + a^3X + b^3, & \text{if } t \equiv 0 \pmod 3, \\ X^t + aX^{(2t+1)/3} + a^2X^{(t+2)/3} + a^3X + b^3, & \text{if } t \equiv 1 \pmod 3, \\ X^t + abX^{(t+1)/3} + a^3X + b^3, & \text{if } t \equiv 2 \pmod 3. \end{cases} \tag{3.2}$$

Since $g_3(X)$ divides $G_3(X)$ and both have degree t, we have $g_3(X) = G_3(X)$. As $p \nmid (q^2-1)$, $t \ge 3$. Since $g_3(X)$ is a trinomial, it follows that $t = 3$ and:

$$g_3(X) = X^3 + bX^2 + b^3.$$

We consider two cases:

Case 1: $e \equiv 0 \pmod 3$**.** Observe:

$$g_3(X) = b^3\left((X/b)^3 + (X/b)^2 + 1\right) = b^3 g(X/b), \tag{3.3}$$

where $g(X) = X^3 + X^2 + 1$. Since $g_3(X)$ is irreducible over $\mathbb{F}_q$, so is $g(X)$. However, $g(X)$ is irreducible over $\mathbb{F}_2$, and since $3 \mid e$, Lemma **??** implies $g(X)$ factors into three linear polynomials over $\mathbb{F}_q$, a contradiction.

Case 2: $e \not\equiv 0 \pmod 3$**.** We claim $p = 7$. Since $7 \nmid (q^2-1)$, Lemma **??** gives the irreducible factorization of $\Phi_7(X)$ over $\mathbb{F}_q$:

$$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1).$$

Let γ be a root of $g(X) = X^3 + X^2 + 1$, a primitive 7-th root of unity. From (**??**), $g_3(X) = b^3 g(X/b)$, and ξ^3 is a root of $g_3(X)$. Thus, $\theta := \xi^3/b$ is a conjugate of γ over $\mathbb{F}_q$, hence a primitive 7-th root of unity. Since $\xi^3, \theta, b \in \mathbb{F}_{q^3}^*$, and $|b|$ divides $q-1$ while $|\theta| = 7$, with $7 \nmid (q-1)$, we have $\gcd(|b|, |\theta|) = 1$. Thus:

$$p = |\xi^3| = |b\theta| = |b| \cdot |\theta| = 7|b|,$$

implying $p = 7$, as required.

For $e \not\equiv 0 \pmod 3$, we prove:

- If $e \equiv \pm 2 \pmod 6$, then $X^{63} - 1$ is not 3-sparse over $\mathbb{F}_q$.
- For a prime p with $p \mid (q+1)$, $X^{7p} - 1$ is not 3-sparse over $\mathbb{F}_q$.

For the first, let $q = 2^e$ with $e \equiv \pm 2 \pmod 6$, so $e = 2t$ with $\gcd(t, 3) = 1$. With the assistance of a computer, the irreducible factors of $\Phi_{63}(X)$ over $\mathbb{F}_4$ are given by:

$$X^3 + X^2 + X + w, X^3 + X^2 + X + w + 1, X^3 + X^2 + wX + w + 1,$$
$$X^3 + X^2 + (w+1)X + w, X^3 + wX^2 + X + w + 1, X^3 + wX^2 + wX + w,$$
$$X^3 + wX^2 + (w+1)X + w, X^3 + wX^2 + (w+1)X + w + 1, X^3 + (w+1)X^2 + X + w,$$
$$X^3 + (w+1)X^2 + wX + w, X^3 + (w+1)X^2 + wX + w + 1, X^3 + (w+1)X^2 + (w+1)X + w + 1,$$

where w is a primitive element of $\mathbb{F}_4$. Since $\mathbb{F}_q$ is an extension of $\mathbb{F}_4$ of degree t, Lemma **??** implies these factors remain irreducible over $\mathbb{F}_q$. Thus, $X^{63} - 1$ is not 3-sparse, as all factors are quadrinomials.

For the second, let $p \mid (q+1)$. We show $\Phi_{7p}(X)$ has an irreducible factor over $\mathbb{F}_q$ that is neither a binomial nor a trinomial. If $p = 3$, the irreducible factorization of $\Phi_{21}(X)$ over $\mathbb{F}_2$ is:

$$\Phi_{21}(X) = (X^6 + X^4 + X^2 + X + 1)(X^6 + X^5 + X^4 + X^2 + 1). \tag{3.4}$$

Since $e \not\equiv 0 \pmod 3$, $\gcd(6, e) = 1$, and by Lemma **??**, (**??**) holds over $\mathbb{F}_q$, so $X^{21} - 1$ is not 3-sparse. For $p > 3$ with $p \mid (q+1)$, $p \neq 7$. Suppose all irreducible factors of $\Phi_{7p}(X)$ are binomials or trinomials. By Lemmas **??** and **??**, all factors have degree 6. From Lemma **??**,

$$\Phi_7(X^p) = \Phi_{7p}(X)\Phi_7(X).$$

This implies that $\Phi_{7p}(X)$ has the term X. Then $\Phi_{7p}(X)$ must have an irreducible factor $X^6 + aX + b$ for some $a, b \in \mathbb{F}_q^*$. Let ξ be a root of $X^6 + aX + b$. Then, from (**??**), the minimal polynomial of ξ^3 over $\mathbb{F}_q$ is:

$$g_3(X) = X^6 + bX^4 + b^2X^2 + a^3X + b^3,$$

an irreducible factor of $\Phi_{7p}(X)$, which is neither a binomial nor a trinomial. Thus, $X^{7p} - 1$ is not 3-sparse over $\mathbb{F}_q$.

This completes the proof of necessity.

Sufficiency. For $n = 1$, $X - 1$ is 3-sparse. For $n \geq 2$ satisfying condition (a), (b), or (c), we show that $\Phi_d(X)$ factors into binomials or trinomials for all divisors $d \geq 2$ of n.

Case 1: n satisfies Condition (a). For a divisor $d \geq 2$ of n, write $d = p_1^{f_1} \cdots p_k^{f_k}$ for some primes $p_1, \ldots, p_k$ with each $p_i \mid (q^2 - 1)$, and for some positive integers $f_1, \ldots, f_k$. Let v_i be the p_i-adic valuation of $q^2 - 1$. We consider:

Subcase 1-1: $f_i \leq v_i$ for all i. By Lemmas **??** and **??**,

$$\mathrm{ord}_d(q) = \mathrm{lcm}(\mathrm{ord}_{p_1^{f_1}}(q), \ldots, \mathrm{ord}_{p_k^{f_k}}(q)) = 1 \text{ or } 2.$$

By Lemma **??**, $\Phi_d(X)$ factors into irreducible polynomials over $\mathbb{F}_q$ of degree 1 or 2, which are binomials or trinomials.

Subcase 1-2: $f_i > v_i$ for some i. Suppose there are u indices $1 \le i_1 < \cdots < i_u \le k$ such that $f_{i_j} > v_{i_j}$ for $1 \le j \le u$. Write $d = p_{i_1}^{f_{i_1}} \cdots p_{i_u}^{f_{i_u}} D$ and $d_0 = p_{i_1}^{v_{i_1}} \cdots p_{i_u}^{v_{i_u}} D$. By Lemma **??**,

$$\Phi_{d_0 p_{i_1}^{f_{i_1}-v_{i_1}}}(X) = \Phi_{d_0}(X^{p_{i_1}^{f_{i_1}-v_{i_1}}}) = \prod_i (X^{t_0 p_{i_1}^{f_{i_1}-v_{i_1}}} + a_i X^{k_i p_{i_1}^{f_{i_1}-v_{i_1}}} + b_i), \tag{3.5}$$

where $\prod_i (X^{t_0} + a_i X^{k_i} + b_i)$ is the irreducible factorization of $\Phi_{d_0}(X)$ over $\mathbb{F}_q$, with $t_0 = \mathrm{ord}_{d_0}(q)$ from Subcase 1-1. By Lemmas **??** and **??**,

$$\mathrm{ord}_{d_0 p_{i_1}^{f_{i_1}-v_{i_1}}}(q) = p_{i_1}^{f_{i_1}-v_{i_1}} t_0.$$

Thus, (**??**) is the irreducible factorization of $\Phi_{d_0 p_{i_1}^{f_{i_1}-v_{i_1}}}(X)$. Iterating this process, the irreducible factorization of $\Phi_d(X)$ over $\mathbb{F}_q$ is:

$$\Phi_d(X) = \prod_i (X^{t_0 p_{i_1}^{f_{i_1}-v_{i_1}} \cdots p_{i_u}^{f_{i_u}-v_{i_u}}} + a_i X^{k_i p_{i_1}^{f_{i_1}-v_{i_1}} \cdots p_{i_u}^{f_{i_u}-v_{i_u}}} + b_i).$$

Thus, $\Phi_d(X)$ factors into irreducible binomials or trinomials over $\mathbb{F}_q$.

Case 2: n satisfies Condition (b). Let $e \equiv \pm 1 \pmod 6$, so $7 \nmid (q^2-1)$ and $3 \nmid (q-1)$. For a divisor $d \ge 2$ of n, if $7 \nmid d$, the result follows from Case 1. If $7 \mid d$, consider:

Subcase 2-1: $d = 7^h$ for some positive integer h. By Lemma **??**, $\Phi_d(X)$ factors into trinomials.

Subcase 2-2: $d = 7^h p_1^{f_1} \cdots p_s^{f_s}$ for primes $p_1, \dots, p_s$ with $p_i \mid (q-1)$ and positive integers $h, f_1, \dots, f_s$. First, assume $f_i \le v_i$, where v_i is the p_i-adic valuation of $q-1$. Let $d_1 = 7 p_1^{f_1} \cdots p_s^{f_s}$. By Lemmas **??** and **??**,

$$\mathrm{ord}_{p_1^{f_1} \cdots p_s^{f_s}}(q) = 1, \quad \mathrm{ord}_{d_1}(q) = 3.$$

By Lemma **??**, $\Phi_{d_1}(X)$ factors into irreducible polynomials of degree 3, and $\Phi_{p_1^{f_1} \cdots p_s^{f_s}}(X)$ factors into linear polynomials. Assume their irreducible factorizations are:

$$\Phi_{p_1^{f_1} \cdots p_s^{f_s}}(X) = \prod_{\alpha \in R} (X + \alpha), \quad \Phi_{d_1}(X) = \prod_{a,b,c} (X^3 + aX^2 + bX + c),$$

where R is the set of primitive $(p_1^{f_1} \cdots p_s^{f_s})$-th roots of unity. By Lemma **??**,

$$\prod_{\alpha \in R} (X^7 + \alpha) = \prod_{a,b,c} (X^3 + aX^2 + bX + c) \cdot \prod_{\alpha \in R} (X + \alpha).$$

By uniqueness of factorization, for any $\beta \in R$, there exist unique $\alpha \in R$ and $a_i, b_i, c_i \in \mathbb{F}_q$ $(i = 1, 2)$ such that:

$$X^7 + \beta = (X^3 + a_1 X^2 + b_1 X + c_1)(X^3 + a_2 X^2 + b_2 X + c_2)(X + \alpha). \tag{3.6}$$

Comparing coefficients in (**??**) yields:

$$\begin{cases} a_1 + a_2 + \alpha = 0, \\ (a_1 + a_2)\alpha + b_1 + b_2 + a_1 a_2 = 0, \\ (b_1 + b_2)\alpha + a_1 a_2 \alpha + a_1 b_2 + b_1 a_2 + c_1 c_2 = 0, \\ (c_1 + c_2 + a_1 b_2 + b_1 a_2)\alpha + a_1 c_2 + c_1 a_2 + b_1 b_2 = 0, \\ (a_1 c_2 + c_1 a_2)\alpha + b_1 b_2 \alpha + b_1 c_2 + b_2 c_1 = 0, \\ (b_1 c_2 + b_2 c_1)\alpha + c_1 c_2 = 0, \end{cases}$$

implying $\beta = \alpha^7$. Thus:

$$X^7 - \beta = X^7 - \alpha^7 = \alpha^7 (X/\alpha - 1)\Phi_7(X/\alpha).$$

By Lemma **??**,

$$X^7 - \beta = (X + \alpha)(X^3 + \alpha^2 X + \alpha^3)(X^3 + \alpha X^2 + \alpha^3).$$

Thus, $\Phi_{d_1}(X)$ has the irreducible factorization over $\mathbb{F}_q$:

$$\Phi_{d_1}(X) = \prod_{\alpha \in R} (X^3 + \alpha^2 X + \alpha^3)(X^3 + \alpha X^2 + \alpha^3).$$

By Lemma **??**,

$$\Phi_d(X) = \Phi_{d_1}(X^{7^{h-1}}) = \prod_{\alpha \in R} (X^{3\cdot 7^{h-1}} + \alpha^2 X^{7^{h-1}} + \alpha^3)(X^{3\cdot 7^{h-1}} + \alpha X^{2\cdot 7^{h-1}} + \alpha^3). \tag{3.7}$$

By Lemmas **??** and **??**, $\mathrm{ord}_d(q) = 3 \cdot 7^{h-1}$. By Lemma **??**, $\Phi_d(X)$ factors into irreducible polynomials of degree $3 \cdot 7^{h-1}$, so (**??**) is the irreducible factorization of $\Phi_d(X)$ over $\mathbb{F}_q$.

If $f_i > v_i$ for some i, suppose there are u indices $1 \le i_1 < \cdots < i_u \le s$ such that $f_{i_j} > v_{i_j}$. Write $d = 7^h p_{i_1}^{f_{i_1}} \cdots p_{i_u}^{f_{i_u}} D$ and $d_2 = 7^h p_{i_1}^{v_{i_1}} \cdots p_{i_u}^{v_{i_u}} D$. From (**??**),

$$\Phi_{d_2}(X) = \prod_{\alpha \in R_1} (X^{3\cdot 7^{h-1}} + \alpha^2 X^{7^{h-1}} + \alpha^3)(X^{3\cdot 7^{h-1}} + \alpha X^{2\cdot 7^{h-1}} + \alpha^3), \tag{3.8}$$

where R_1 is the set of primitive $(p_{i_1}^{v_{i_1}} \cdots p_{i_u}^{v_{i_u}} D)$-th roots of unity. Since:

$$\Phi_d(X) = \Phi_{d_2 p_{i_1}^{f_{i_1}-v_{i_1}} \cdots p_{i_u}^{f_{i_u}-v_{i_u}}}(X) = \Phi_{d_2}(X^{p_{i_1}^{f_{i_1}-v_{i_1}} \cdots p_{i_u}^{f_{i_u}-v_{i_u}}}),$$

the factorization of $\Phi_d(X)$ follows from (**??**). Note that each $p_i \neq 3$. It follows from Lemmas **??** and **??** that $\mathrm{ord}_d(q) = 3 \cdot 7^{h-1} p_{i_1}^{f_{i_1}-v_{i_1}} \cdots p_{i_u}^{f_{i_u}-v_{i_u}}$, which, by Lemma **??**, is the degree of each irreducible factors. So, the factorization of $\Phi_d(X)$ is the irreducible factorization over $\mathbb{F}_q$.

Thus, each irreducible factor of $\Phi_d(X)$ is a trinomial.

Case 3: n satisfies Condition (c). Let $e \equiv \pm 2 \pmod 6$, so $7 \nmid (q^2 - 1)$ and $3 \mid (q-1)$. For a divisor $d \ge 2$ of n, if $7 \nmid d$, the result follows from Case 1. If $7 \mid d$ but $3 \nmid d$, the result follows from Case 2. If $21 \mid d$, then we can write $d = 7^h p_1 p_2^{f_2} \cdots p_s^{f_s}$ for some primes $p_2, \ldots, p_s > 3$ with each $p_i \mid (q-1)$, $p_1 = 3$ and positive integers $h, f_2, \ldots, f_s$. Following the proof of Case 2, we have that all irreducible factors of $\Phi_d(X)$ are trinomials.

This completes the proof of sufficiency, and thus Theorem **??**. □

Conflict of Interest

The author declares that there is no conflict of interest.

Acknowledgment

This work was conducted during the author's academic visit to RICAM, Austrian Academy of Sciences. The author sincerely thanks Professor Arne Winterhof at RICAM for his thorough review of the manuscript and for offering invaluable suggestions.

This research was partially supported by the China Scholarship Council Fund (Grant No. 202301010002) and the Scientific Research Innovation Team Project of China West Normal University (Grant No. KCXTD2024-7).

References

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

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

[3] F. R. Beyl, Cyclic subgroups of the prime residue group, Amer. Math. Monthly **84** (1977), 46-48.

[4] I. F. Blake, S. Gao, R. C. Mullin, Explicit factorization of $x^{2^k}+1$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$, Appl. Algebra Eng. Commun. Comput. **4** (1993), 89-94.

[5] F. E. Brochero-Martinez, L. Reis, L. Silva-Jesus, Factorization of composed polynomials and applications, Discret. Math. **342** (2019), 111603.

[6] F. E. Brochero-Martinez, C.R. Giraldo Vergara, L. de Oliveira, Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$, Des. Codes Cryptogr. **77** (2015), 277-286.

[7] K. Cheng, The 3-sparsity of $X^n - 1$ over finite fields, arXiv:2507.06655v2, 2025.

[8] B. Chen, L. Li, R. Tuerhong, Explicit factorization of $x^{2^m p^n} - 1$ over a finite field, Finite Fields Appl. **24** (2013), 95-104.

[9] A. M. Graner, Closed formulas for the factorization of $X^n - 1$, the n-th cyclotomic polynomial, $X^n - a$ and $f(X^n)$ over a finite field for arbitrary positive integers n, arXiv:2306.11183, 2023.

[10] B. Hanson, D. Panario, D. Thomson, Swan-like results for binomials and trinomials over finite fields of odd characteristic, Des. Codes Cryptogr. **61** (2011), 273-283.

[11] H. W. Lenstra Jr., On the Chor-Rivest knapsack cryptosystem, J. Cryptol. **3** (1991), 149-155.

[12] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, 1997.

[13] H. Meyn, Factorization of the cyclotomic polynomials $x^{2^n}+1$ over finite fields, Finite Fields Appl. **2** (1996), 439-442.

[14] D. Oliveira, L. Reis, On polynomials $x^n - 1$ over binary fields whose irreducible factors are binomials and trinomials, Finite Fields Appl. **73** (2021), 101837.

[15] J. H. Van Lint, *Introduction to Coding Theory*, 3rd ed., Graduate Texts in Mathematics, vol. 86, Springer, New York, 1998.

[16] J. von zur Gathen, Irreducible trinomials over finite fields, in *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, 2001 Jul 1, pp. 332-336.

[17] L. Wang, Q. Wang, On explicit factors of cyclotomic polynomials over finite fields, Des. Codes Cryptogr. **63** (2012), 87-104.

School of Mathematics and Information, China West Normal University, Nanchong, 637002, P. R. China

Email address: `ckm20@126.com`