International Journal of Pure and Applied Mathematics
Volume 97 No. 1 2014, 67-77
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v97i1.7

EXPLICIT FACTORIZATION OF $x^{2^a p^b r^c} - 1$ OVER A FINITE FIELD

Fen Li[1] §, Xiwang Cao[2]
[1,2]College of Science
Nanjing University of Aeronautics and Astronautics
Jiangsu, 210016, P.R. CHINA

Abstract: Let $\mathbb{F}_q$ be a finite field of odd order q. In this paper, the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ is given in a very explicit form, where a, b, c are positive integers and p, r are odd prime divisors of $q-1$. It is shown that all the irreducible factors of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ are either binomials or trinomials. In general, denote by $v_p(m)$ the degree of prime p in the standard decomposition of the positive integer m. Suppose that every prime factor of m divides $q-1$, one has (1) if $v_p(m) \leq v_p(q-1)$ holds true for every prime number $p|q-1$, then every irreducible factor of $x^m - 1$ in $\mathbb{F}_q$ is a binomial; (2) if $q \equiv 3 (\mathrm{mod}\ 4)$, then every irreducible factor of $x^m - 1$ is either a binomial or a trinomial.

AMS Subject Classification: 11T06
Key Words: irreducible factorization, binomial, trinomial

1. Introduction

Let $\mathbb{F}$ be a finite field ,if

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}, \tag{1}$$

where $f_i(x) \in \mathbb{F}[x]$ is irreducible over $\mathbb{F}$, we call Eq.(1) *the explicit factorization* of $f(x)$ over $\mathbb{F}$. Factoring polynomials over finite fields is very important for the study of the algebraic structure of finite fields, and is also

Received: June 26, 2014

§Correspondence author

usefull for information security and coding theory. So that research on the explicit factorization of polynomials over finite fields is a classical topic of mathematics(e.g.see[2],[3],[4],[7],[9],[10]). Although the decomposition of polynomials over finite fields have some algorithms, such as the famous Berlekamp algorithm, see [6], Chapter 4, etc., but these algorithms are only effective for a small field. Only in a few situations can we give the explicit factorization of some polynomials. For example, Fitzgerald and Yucas in [4] characterized the irreducible factors of Dickson polynomials over finite fields. Meyn in [7] generalized the main results in [2] and obtained the explicit factorization of $x^{2^m}+1$ over $\mathbb{F}_q$ by proposing a shorter approach, where q is a prime power with $q \equiv 3(\mathrm{mod}\ 4)$. In [10], B.Chen et al. obtained the explicit factorization of $x^{2^m p^n}-1$, where m, n are positive integers and $p|q-1$. and the irreducible factors of $x^{2^m p^n}-1$ over $\mathbb{F}_q$ are either binomials or trinomials. Irreducible binomials and trinomials over a finite field are extensively used in some fast algorithms implementations. See [1], [5],[8] for instance, that is why irreducible binomials and trinomials play a very important role in the study of polynomials.

This paper is based on [10], and generally obtain the irreducible factorization of $x^{2^a p^b r^c}-1$ over $\mathbb{F}_q$, where a,b,c are positive integers and p, r are odd prime factors of $q-1$. Let $\mathbb{F}_q$ be a finite field of odd order q, the explicit factorization of $x^{2^a p^b r^c}-1$ is given in a very explicit form. And we just need to distinguish the cases when $s \geq 2$ and $s = 1$, where s is the degree of 2 in the standard decomposition of $q-1$. One difference is that for $s \geq 2$, x^2+1 is reducible, and x^2+1 is irreducible over $\mathbb{F}_q$ when $s = 1$. If $s \geq 2$ the irreducible factors of $x^{2^a p^b r^c}-1$ over $\mathbb{F}_q$ are all binomials; otherwise the irreducible factors of $x^{2^a p^b r^c}-1$ over $\mathbb{F}_q$ are either binomials or trinomials. In general, denote by $v_p(m)$ the degree of prime p in the standard decomposition of the positive integer m. Suppose that every prime factor of m divides $q-1$, one has (1) if $v_p(m) \leq v_p(q-1)$ holds true for every prime number $p|q-1$, then every irreducible factor of x^m-1 in $\mathbb{F}_q$ is a binomial; (2) if $q \equiv 3(\mathrm{mod}\ 4)$, then every irreducible factor of x^m-1 is either a binomial or a trinomial. And this means that the method in [10] is still reasonable no matter there are how many prime factors of m, note that we should also suppose that all the prime factors of m divide $q-1$.

2. Preliminaries

Throughout this paper $\mathbb{F}_q$ denotes a finite field of odd order q. We denote all the non-zero elements of $\mathbb{F}_q$ by $\mathbb{F}_q^*$, i.e. the multiplicative group of $\mathbb{F}_q$. For

$\beta \in \mathbb{F}_q^*$, we denote $\mathrm{ord}(\beta)$ the order of β, then $\mathrm{ord}(\beta)$ is a divisor of $q-1$, and β is aslo called a primitive $\mathrm{ord}(\beta)$-th root of unity. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, i.e. $\mathbb{F}_q^* = \langle \xi \rangle$, where ξ is a primitive $(q-1)$-th root of unity. For any integer k, it is known that $\mathrm{ord}(\beta^k) = \frac{q-1}{\gcd(k,q-1)}$, where $\gcd(k, q-1)$ is the greatest common divisor of k and $q-1$. We also denote $v_p(m)$ the degree of p in the standard decomposition of positive integer m.

There is a criterion irreducible non-linear binomials over $\mathbb{F}_q$, which was given by Serret in 1866 (e.g. see [6], Theorem 3.75).

Lemma 1. *Assume that $k \geq 2$, $k \in N^*$. For any $\gamma \in \mathbb{F}_q^*$ with $\mathrm{ord}(\gamma) = e$, the binomial $x^k - \gamma$ is irreducible over $\mathbb{F}_q$ if and only if both the following two conditions are satisfied:*
(1) Every prime divisor of k divides e, but does not divide $\frac{q-1}{e}$;
(2) If $4|k$, then $4|(q-1)$.

By [[2],Corollary 4], we can obtain the irreducible factorization of $x^{2^m} - 1$ over a prime $\mathbb{F}_p$ where $p \equiv 3 (\mathrm{mod}\ 4)$. And one can check that when q is a power of a prime and $q \equiv 3 (\mathrm{mod}\ 4)$, we can also get the the irreducible factorization of $x^{2^m} - 1$ over $\mathbb{F}_q$ in the same way as in [2]. We denote $l = v_2(q+1)$, then we have the result as follows.

Lemma 2. *[2] Assume that $q \equiv 3 (\mathrm{mod}\ 4)$. Set $H_1 = \{0\}$; recursively define:*

$$H_i = \{\pm(\frac{h+1}{2})^{\frac{q+1}{4}} | h \in H_{i-1})\},$$

for $i = 2, 3, \ldots, l-1$; and set

$$H_l = \{\pm(\frac{h-1}{2})^{\frac{q+1}{4}} | h \in H_{l-1})\}.$$

Then the irreducible factorization of $x^{2^m} - 1$ over $\mathbb{F}_q$ is given as follows:
If $1 \leq m \leq l$, then

$$x^{2^m} - 1 = (x+1)(x-1) \cdot \prod_{i=1}^{m-1} \prod_{h \in H_i} (x^2 - 2hx + 1);$$

If $m \geq (l+1)$, then

$$x^{2^m} - 1 \quad = \quad (x+1)(x-1) \cdot \prod_{\substack{h \in H_i \\ 1 \leq i \leq (l-1)}} (x^2 - 2hx + 1)$$

$$\cdot \prod_{\substack{h \in H_l \\ 0 \le k \le (m-l-1)}} (x^{2^{k+1}} - 2hx^{2^k} - 1).$$

Finally, we recall a celebrated result which gives a criterion on the irreducibility for composition of polynomials (e.g. see [6],Theorem 3.35).

Lemma 3. *Let m be a positive integer, and $f(x) \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ with $\deg f = n > 0$. Suppose that $f(0) \neq 0$ and $f(x)$ is of period e which is equal to the order of any root of $f(x)$. Then $f(x^m)$ is irreducible over $\mathbb{F}_q$ if and only if the following three conditions are satisfied:*
(1) Each prime divisors of m divides e;
(2) $\gcd(m, \frac{q^n-1}{e}) = 1$;
(3) If $4|m$, then $4|(q^n - 1)$.

3. Main Results

Let $\mathbb{F}_q$ be a finite field of odd order q and we also assume that p, r are odd prime factors of $q-1$. Write $q-1 = 2^s p^t r^u d$, where s, t, u are positive integers and $\gcd(2pr, d) = 1$. We first give the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ when $s \ge 2, b \le t, c \le u$.

Theorem 1. *When $s \ge 2, b \le t, c \le u$, the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ is given as follow:*
(i) If $a \le s$, then

$$x^{2^a p^b r^c} - 1 = \prod_{i=0}^{2^a p^b r^c - 1} (x - \alpha_1^i),$$

where $\alpha_1 = \xi^{2^{s-a} p^{t-b} r^{u-c} d}$ is a primitive $2^a p^b r^c$-th root of unity;
(ii) If $a >$ s, then

$$x^{2^a p^b r^c} - 1 = \prod_{k=0}^{2^s p^b r^c - 1} (x - \beta_1^k) \cdot \prod_{i=0}^{a-s-1} \prod_{j=1, 2 \nmid j}^{2^s p^b r^c} (x^{2^{a-s-i}} - \beta_1^j),$$

where $\beta_1 = \xi^{p^{t-b} r^{u-c} d}$ is a primitive $2^s p^b r^c$-th root of unity.

Proof. If $b \le t$, $c \le u$ and $a \le s$, there exists a primitive $2^a p^b r^c$-th root of unity $\alpha_1 = \xi^{2^{s-a}p^{t-b}r^{u-c}d}$ over $\mathbb{F}_q$, so the result follows trivially.

If $b \le t$, $c \le u$ and $a >$ s, then there exists a primitive $2^s p^b r^c$-th root of unity $\beta_1 = \xi^{p^{t-b}r^{u-c}d}$ over $\mathbb{F}_q$. For each $0 \le k \le 2^s p^b r^c - 1$, we have $(\beta_1^k)^{2^a p^b r^c} = 1$, hence $x - \beta_1^k$ is an irreducible factor in $\mathbb{F}_q[x]$. For every $0 \le k \le 2^s p^b r^c - 1$ and $1 \le j \le 2^s p^b r^c$ with $2 \dagger j$, we can see that:

$$\operatorname{ord}(\beta_1^j) = \frac{\operatorname{ord}(\beta_1)}{\gcd(\operatorname{ord}(\beta_1), j)} = \frac{2^s p^b r^c}{\gcd(2^s p^b r^c, j)} = \frac{2^s p^b r^c}{\gcd(p^b r^c, j)},$$
$$\frac{q-1}{\operatorname{ord}(\beta_1^j)} = \frac{2^s p^t r^u d}{\operatorname{ord}(\beta_1^j)} = d p^{t-b} r^{u-c} \gcd(p^b r^c, j).$$

so $2 | \operatorname{ord}(\beta_1^j)$ and $2 \dagger \frac{q-1}{\operatorname{ord}(\beta_1^j)}$, we know that $x^{2^{a-s-i}} - \beta_1^j$ is irreducible by Lemma 1. Let λ be a root of $x^{2^{a-s-i}} - \beta_1^j$ in some extension field of $\mathbb{F}_q$, hence $\lambda^{2^{a-s-i}} = \beta_1^j$. Then $\lambda^{2^a p^b r^c} = (\lambda^{2^{a-s-i}})^{2^{(s+i)} p^b r^c} = 1$, so $x^{2^{a-s-i}} - \beta_1^j$ is an irreducible divisor of $x^{2^a p^b r^c} - 1$. Because $x - \beta_1^k$ and $2^{a-s-i} - \beta_1^j$ are irreducible and distinct from each other, then

$$\prod_{k=0}^{2^s p^b r^c - 1} (x - \beta_1^k) \cdot \prod_{i=0}^{a-s-1} \prod_{j=1, 2 \dagger j}^{2^s p^b r^c} (x^{2^{a-s-i}} - \beta_1^j) \text{ divides } x^{2^a p^b r^c} - 1,$$

It is clear that the degree of the polynomial on the left side above is equal to

$$2^s p^b r^c + (2^s p^b r^c - 2^{s-1} p^b r^c) \sum_{i=1}^{a-s} 2^i = x^{2^a p^b r^c}.$$

This completes the proof of the theorem. □

Next we give the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ under the conditions $s \ge 2, a > s, b \le t$ and $c > u$.

Theorem 2. *When $s \ge 2, a > s, b \le t, c > u$, the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ is given by:*

$$x^{2^a p^b r^c} - 1 = \prod_{k_1=0}^{2^s p^b r^u - 1} (x - \beta_2^{k_1}) \cdot \prod_{k_2=0}^{a-s-1} \prod_{e=1, 2 \dagger e}^{2^s p^b r^u} (x^{2^{a-s-k_2}} - \beta_2^e)$$
$$\cdot \prod_{k_3=0}^{c-u-1} \prod_{v=1, p \dagger v}^{2^s p^b r^u} (x^{r^{c-u-k_3}} - \beta_2^v) \cdot \prod_{i=1}^{a-s} \prod_{j=1}^{c-u} \prod_{\substack{w=1, 2 \dagger w \\ r \dagger w}}^{2^s p^b r^u} (x^{2^i p^j} - \beta_2^w).$$

where $\beta_2 = \xi^{p^{t-b}d}$ is a primitive $2^s p^b r^u$-th root of unity.

Proof. When $a > s, b \le t, c > u$, $\beta_2 = \xi^{p^{t-b}d}$ is a primitive $2^s p^b r^u$-th root of unity. It is easy to check that all the factors on the right side of formula above are irreducible divisors of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$. And the degree of the polynomial on the right side of the equation is

$$\begin{aligned}
&2^s p^b r^u + (2^s p^b r^u - 2^{s-1} p^b r^u) \sum_{i=1}^{a-s} 2^i + (2^s p^b r^u - 2^s p^b r^{u-1}) \sum_{i=1}^{c-u} r^i \\
&+(2^s p^b r^u - 2^{s-1} p^b r^u - 2^s p^b r^{u-1} + 2^{s-1} p^b r^{u-1}) \sum_{i=1}^{a-s} 2^i \sum_{i=1}^{c-u} r^i \\
&= x^{2^a p^b r^c}.
\end{aligned}$$

□

For the three inequalities $a > s$, $b > t$ and $c > u$, we have the conditions as follows:
(1) $a \le s, b \le t, c \le u$;
(2) $a > s, b \le t, c \le u$;
(3) $a > s, b \le t, c > u$;
(4) $a > s, b > t, c > u$.

For the four conditions above, we have discuss the irreducible factorization of $x^{2^a p^b r^c} - 1$ under condition (1)(2)(3), and now we are now ready to formulate the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ where $a > s, b > t, c > u$.

Theorem 3. *When $a > s, b > t, c > u$, the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ is given by:*

$$\begin{aligned}
x^{2^a p^b r^c} - 1 = &\prod_{k=0}^{2^s p^t r^u - 1} (x - \beta_3^k) \cdot \prod_{i_1=0}^{a-s-1} \prod_{j_1=1, 2 \dagger j_1}^{2^s p^t r^u} (x^{2^{a-s-i_1}} - \beta_3^{j_1}) \\
&\cdot \prod_{i_2=0}^{b-t-1} \prod_{j_2=1, p \dagger j_2}^{2^s p^t r^u} (x^{p^{b-t-i_2}} - \beta_3^{j_2}) \cdot \prod_{i_3=0}^{c-u-1} \prod_{j_3=1, r \dagger j_3}^{2^s p^b r^u} (x^{r^{c-u-i_3}} - \beta_3^{j_3}) \\
&\cdot \prod_{i_4=1}^{a-s} \prod_{j_4=1}^{b-t} \prod_{\substack{d_1=1 \\ 2 \dagger d_1 \\ p \dagger d_1}}^{2^s p^t r^u} (x^{2^{i_4} p^{j_4}} - \beta_3^{d_1}) \cdot \prod_{i_5=1}^{a-s} \prod_{j_5=1}^{c-u} \prod_{\substack{d_2=1 \\ 2 \dagger d_2 \\ r \dagger d_2}}^{2^s p^t r^u} (x^{2^{i_5} r^{j_5}} - \beta_3^{d_2})
\end{aligned}$$

$$\cdot \prod_{i_6=1}^{b-t} \prod_{j_6=1}^{c-u} \prod_{\substack{d_3=1 \\ p\dagger d_3 \\ r\dagger d_3}}^{2^s p^t r^u} (x^{p^{i_6} r^{j_6}} - \beta_3^{d_3}) \cdot \prod_{i=1}^{a-s} \prod_{j=1}^{b-t} \prod_{k=1}^{c-u} \prod_{\substack{w=1 \\ 2\dagger w \\ p\dagger w,\, r\dagger w}}^{2^s p^t r^u} (x^{2^i p^j r^k} - \beta_3^w).$$

where $\beta_3 = \xi^d$ is a primitive $2^s p^t r^u$-th root of unity.

The proof of this theorem is similar to that of Theorem 1-2, so we omit the details. Recall that $q - 1 = 2^s p^t r^u d$, where s, t, u are positive integers, $\gcd(2pr, d) = 1$, and $s \geq 2$. In the rest of this section, we focus on the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ under the condition $s = 1$, i.e. $4\dagger(q-1)$. Taking arguments similar to Theorem 1, we can get the irreducible factorization of $x^{p^b r^c} - 1$ over $\mathbb{F}_q$. Here we just show the situation where $b \leq t, c > u$, and the other three situations can be get similarly.

Theorem 4. *Let p, r be odd prime divisors of $q-1$, $b \leq t, c > u$, then the irreducible factorization of $x^{p^b r^c} - 1$ over $\mathbb{F}_q$ is given by:*

$$x^{p^b r^c} - 1 = \prod_{k=0}^{p^b r^u - 1} (x - \beta^k) \cdot \prod_{i=1}^{c-u} \prod_{j=1, r\dagger j}^{p^b r^u} (x^{r^i} - \beta^j),$$

where $\beta = \xi^{2p^{t-b}d}$ is a primitive $p^b r^u$-th root of unity.

By Theorem 4, we can get:

$$x^{2^a p^b r^c} - 1 = \prod_{k=0}^{p^b r^u - 1} (x^{2^a} - \beta^k) \cdot \prod_{i=1}^{c-u} \prod_{j=1, r\dagger j}^{p^b r^u} (x^{2^a r^i} - \beta^j). \tag{2}$$

So it is necessary to know the explicit factorization of every factors on the right side of Formula(2). We first consider the irreducible factorization of $x^{2^a} - \beta^k$ for each $0 \leq k \leq p^b r^u - 1$. As mentioned before, there is $\beta = \xi^{2p^{t-b}d}$ be $p^b r^u$-th root of unity. Then $\mathrm{ord}(\xi^{2^a}) = \frac{q-1}{\gcd(q-1, 2^a)} = \frac{2p^t r^u d}{\gcd(2p^t r^u d, 2^a)} = p^t r^u d$, this means that $\beta \in \langle \xi^{2^a} \rangle$, so there exist an positive integer z_k such that $\beta^k = \xi^{2^a z_k}$. Setting $\eta_k = \xi^{-z_k}$, we have $\eta_k^{2^a} \beta^k = 1$. It easy to see that we only have a unique element in $\mathbb{F}_q^*$ such that $\eta_k^{2^a} \beta^k = 1$. Now we can establish a isomorphism as follows:

$$\begin{aligned} \varphi_k : \mathbb{F}_q[x]/\langle x^{2^a} - 1 \rangle &\to \mathbb{F}_q[x]/\langle x^{2^a} - \eta_k \rangle \\ f(x) + \langle x^{2^a} - 1 \rangle &\mapsto f(x) + \langle x^{2^a} - \eta_k \rangle \end{aligned}$$

By Lemma 2, we know the irreducible factorization of $x^{2^a}-1$ over $\mathbb{F}_q$. Here we just discuss the condition when $1 \le a \le l$. Then we have:

$$x^{2^a}-1=(x+1)(x-1)\cdot\prod_{i=1}^{a-1}\prod_{h\in H_i}(x^2-2hx+1);$$

Using φ_k, we can get the irreducible factorization of $x^{2^a}-\beta^k$ over $\mathbb{F}_q$ where $1 \le a \le l$ as follows:

$$x^{2^a}-\beta^k=\beta^k(\eta_k x+1)(\eta_k x-1)\cdot\prod_{i=1}^{a-1}\prod_{h\in H_i}((\eta_k x)^2-2h\eta_k x+1); \tag{3}$$

Theorem 5. *Assume that $s=1$, $1 \le a \le l$ and $b \le t, c > u$, then the irreducible factorization of $x^{2^a p^b r^c}-1$ over $\mathbb{F}_q$ is given by:*

$$\begin{aligned}
&x^{2^a p^b r^c}-1\\
&=\prod_{k=0}^{p^b r^u-1}((x+\eta_k^{-1})(x-\eta_k^{-1})\cdot\prod_{m=1}^{a-1}\prod_{h\in H_m}(x^2-2h\eta_k^{-1}x+\eta_k^{-2}))\\
&\cdot\prod_{i=1}^{c-u}\prod_{j=1,r\dagger j}^{p^b r^u}((x^{r^i}+\eta_j^{-1})(x^{r^i}-\eta_j^{-1})\cdot\prod_{m=1}^{a-1}\prod_{h\in H_m}(x^{2r^i}-2h\eta_j^{-1}x^{r^i}+\eta_j^{-2})).
\end{aligned}$$

Proof. By Eq. (3), we have

$$x^{2^a}-\beta^j=\beta^j(\eta_j x+1)(\eta_j x-1)\prod_{i=1}^{a-1}\prod_{h\in H_i}((\eta_j x)^2-2h\eta_j x+1); \tag{4}$$

then

$$x^{2^a r^i}-\beta^j=\beta^j(\eta_j x^{r^i}+1)(\eta_j x^{r^i}-1)\prod_{i=1}^{a-1}\prod_{h\in H_i}(\eta_j^2 x^{2r^i}-2h\eta_j x^{r^i}+1); \tag{5}$$

By Lemma 1, $x^{r^i}+\eta_j^{-1}$ and $x^{r^i}-\eta_j^{-1}$are irreducible over $\mathbb{F}_q$.

Next we want to make sure that $x^{2r^i}-2h\eta_j^{-1}x^{r^i}+\eta_j^{-2}$ is irreducible over $\mathbb{F}_q$ where $1 \le j \le p^b r^u$, $r\dagger j$. We use Lemma 3 to prove this statement. Let $m=r^i, n=2, f(x)=x^2-2h\eta_j^{-1}x+\eta_j^{-2}$. For Eq. (4), we know that $f(x)$ is a irreducible factor of $x^{2^a}-\beta^j$. Obviously that $4\dagger r^i$, we just need to prove

the validity of condition(1)(2) in Lemma 3. Let μ be the root of $f(x)$, then $\mu^{2^a} = \beta^j$. Since β is a primitive $p^b r^u$-th root of unity and $\gcd(r, j) = 1$, then $r^i | \mathrm{ord}(\mu)$, i.e. $r^i | d$. Clearly $\gcd(q+1, r) = 1$, therefore $\gcd(r^i, \frac{q^2-1}{d}) = 1$. So we can get the result that $x^{2r^i} - 2h\eta_j^{-1} x^{r^i} + \eta_j^{-2}$ is irreducible. □

Here we can get the the irreducible factorization of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ in other conditions similarly.

In general, we have the following conclusions:

Theorem 6. *We denote $v_p(m)$ the degree of prime p in the standard decomposition of the positive integer m. Suppose that every prime factor of m divides $q-1$, one has (1) if $v_p(m) \leq v_p(q-1)$ holds true for every prime number $p | q-1$, then every irreducible factor of $x^m - 1$ in $\mathbb{F}_q$ is a binomial; (2) if $q \equiv 3 (\mathrm{mod}\ 4)$, then every irreducible factor of $x^m - 1$ is either a binomial or a trinomial.*

Proof. (1) Let ξ be the primitive element of $\mathbb{F}_q$ as before. Let $m = p_1^{e_1} \cdots p_s^{e_s}$, α is a element in E which is a extension field of $\mathbb{F}_q$, such that $\alpha^m = 1$, next we want to find the minimal polynomial of α over $\mathbb{F}_q$. Since $\mathrm{ord}(\alpha) | m$, set $\mathrm{ord}(\alpha) = p_1^{e_1'} \cdots p_t^{e_t'}$, $e_1' \leq e_1, \cdots, e_t' \leq e_t$, $t \leq s$,$q - 1 = p_1^{r_1} \cdots p_n^{r_n}$, $n \geq s$.

Case 1: $e_i \leq r_i, 1 \leq i \leq s$.

Under this condition, let $\beta = \xi^{\frac{q-1}{m}}$, then $\beta \in \mathbb{F}_q$ is a element of order m, α is a power of β. Hence $x^m - 1 = \prod_{i=0}^{m-1}(x - \beta^i)$ is a multiple of the minimal polynomial of α.

Case 2: $e_i \leq r_i, 1 \leq i \leq u < s$, but $e_{u+1} > r_{u+1}, \cdots, e_s > r_s$. Under this condition, let $\beta = \xi^{\frac{q-1}{p_1^{r_1} \cdots p_s^{r_s}}}$, then $\mathrm{ord}(\beta) = p_1^{r_1} \cdots p_s^{r_s}$. then we discuss this into two cases:

Case 2.1: $\mathrm{ord}(\alpha) = m$.

Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = v$, v is the minimal positive integer such that $q^v \equiv 1 (\mathrm{mod}\ m)$. Since $q^v \equiv 1 (\mathrm{mod}\ m)$ if and only if $q^v \equiv 1 (\mathrm{mod}\ p_i^{e_i})$, $i = 1, \cdots, s$. Since $q^v = (1 + p_1^{r_1} \cdots p_n^{r_n})^v = 1 + v p_1^{r_1} \cdots p_n^{r_n} + \cdots$, we have $v = p_{u+1}^{e_{u+1} - r_{u+1}} \cdots p_s^{e_s - r_s}$. So $\mathrm{ord}(\alpha^v) = \frac{m}{\gcd(m,v)} = p_1^{r_1} \cdots p_s^{r_s}$. That means that there exist a positive integer ℓ such that $\alpha^v = \beta^\ell$, $\gcd(\ell, \mathrm{ord}(\beta)) = 1$. By Lemma 1 we can see that $x^v - \beta^\ell$ is irreducible over $\mathbb{F}_q$, and it is just the minimal polynomial of α over $\mathbb{F}_q$.

Case 2.2: $\mathrm{ord}(\alpha) | m$, $\mathrm{ord}(\alpha) \neq m$.

Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = v'$, v' is a divisor of v. Taking the approach similar to case2.1 we can get the result.

(2) We can obtained the result directly from (1) and Lemma 2. This completes the proof of the theorem. □

4. Concluding Remarks

In this paper the irreducible factorization of $x^{2^a p^b r^c} - 1$ is given in a very explicit form, where p, r are prime divisors of $q-1$, and we can see that all the irreducible factors of $x^{2^a p^b r^c} - 1$ over $\mathbb{F}_q$ are either binomials or trinomials. And we show that the irreducible factors of $x^m - 1$ over $\mathbb{F}_q$ are either binomials or trinomials under some certain conditions. Let m be a positive integer, we can use the same method to deal with the irreducible factorization of $x^m - 1$ where every prime factor of m is a divisor of $q - 1$.

References

[1] E. R., Bit-serial Reed-Solomen encoders, *IEEE Trans. Inform. Theory*, **28** (1982), 869–874, http://dx.doi.org/10.119/TIT.1982.1056591.

[2] Blake I. F., Gao S., Mullin R. C., Explicit factorization of $x^{2^k} + 1$ over F_p with $p \equiv 3(\text{mod } 4)$, *Appl. Algebra Engrg. Comm. Comput.*, **4** (1993), 89–94. http://dx.doi.org/10.1007/BF01386832.

[3] Daykin D. E., The irreducible factors of $(cx + d)x^{q^m} - (ax + b)$ over $GF(q)$, *Quart. J. Math. Oxford Ser.*, **14** (1963), 61-64. http://dx.doi.org/10.1007/s10623-101-9647-159.

[4] Fitzgerald R. W., Yucas J. L., Generalized reciprocals, factors of Dickson polynomials and generalized cyclotomic polynomials over finite fields, *Finite Fields Appl.*, **13** (2007), 492-515. http://dx.doi.org/10.1007/978-3-540-73074-3-1.

[5] Golomb S ., Gong G ., Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar, Cambridge University Press, Cambridge (2005). http://dx.doi.org/10.1016/s1071-5797-2-2.

[6] Lidl R ., Niederreiter H., Finite Fields, Cambridge University Press, Cambridge (2008). http://dx.doi.org/10.1007/j.ffa.2008.01.008.

[7] Meyn H., Factorization of the cyclotomic polynomial $x^{2^n} + 1$ over finite fields, *Finite Fields Appl.*, **2** (1996), 439–442. http://dx.doi.org/10.1006/ffta.1996.0026.

[8] Benger N., Scott M., Constructing tower extensions of finite fields for implementation of pairing-based cryptography, in: Lecture Notes in Comput. *Sci. vol.*, **6087** (2010), 180–195. http:dx.doi.org/10.1007/978-3-642-13797-6-13.

[9] Stichtenoth H., Topuzoğlu A., Factorization of a class of polynomials over finite fields, *Finite Fields Appl.*, **18** (2012), 108–122. http://dx.doi.org/10.1016/j.ffa.2011.07.005.

[10] Chen B. C., Li L., Tuerhong, Explicit factorization of $x^{2^m p^n} - 1$ over finite field, *Finite fields Appl.*, **24** (2013): 95–104. http://dx.doi.org/10.1016/j.jja.2013.06.002.