On the Primitivity of Trinomials over Small Finite Fields

Li Yujuan[1†], Zhao Jinhua[2], Wang Huaifu[3], Ma Jing[4 *]

. Science and Technology on Information Assurance Laboratory, Beijing, 100072, P.R. China

Abstract: In this paper, we explore the primitivity of trinomials over small finite fields. We extend the results of the primitivity of trinomials $x^n + ax + b$ over $\mathbb{F}_4$ [1] to the general form $x^n + ax^k + b$. We prove that for given n and k, one of all the trinomials $x^n + ax^k + b$ with b being the primitive element of $\mathbb{F}_4$ and $a + b \neq 1$ is primitive over $\mathbb{F}_4$ if and only if all the others are primitive over $\mathbb{F}_4$. And we can deduce that if we find one primitive trinomial over $\mathbb{F}_4$, in fact there are at least four primitive trinomials with the same degree. We give the necessary conditions if there exist primitive trinomials over $\mathbb{F}_4$. We study the trinomials with degrees $n = 4^m + 1$ and $n = 21 \cdot 4^m + 29$, where m is a positive integer. For these two cases, we prove that the trinomials $x^n + ax + b$ with degrees $n = 4^m + 1$ and $n = 21 \cdot 4^m + 29$ are always reducible if $m > 1$. If some results are obviously true over $\mathbb{F}_3$, we also give it.

Keywords: finite fields; primitive polynomials; trinomials

1 Introduction

As usual, denote $\mathbb{F}_q$ the finite field of q elements and let $\mathbb{F}_q[x]$ be the ring of polynomials in one variable x with coefficients in $\mathbb{F}_q$. Trinomials in $\mathbb{F}_q[x]$ are polynomials of the form $x^n + ax^k + b (n > k > 0, ab \neq 0)$. Irreducible and primitive trinomials have many important applications in the theory of finite fields, cryptography, and coding theory [2-4]. Hence, there are many results on the factorizations of trinomials and existence or non-existence of irreducible or primitive trinomials. For detail results one can see [5] [6] [7] [8] . However, these results on trinomials are mainly related to binary field and many basic questions concerning trinomials remain unanswered. For example, to this day no one has proved that there are infinite primitive trinomials over finite field $\mathbb{F}_q$.

In this paper, we mainly explore the primitivity of trinomials $x^n + ax^k + b$ over finite field $\mathbb{F}_4$. First we remark that we only consider the trinomials of odd degrees. This is because the only primitive trinomials of even degree over $\mathbb{F}_4$ are of the form $x^2 + ax + b$ [6] . In next section, we extend the results of the primitivity of trinomials $x^n + ax + b$ over $\mathbb{F}_4$ [1] to the general form $x^n + ax^k + b$. As a consequence, We prove that for given n and k, one of all the trinomials $x^n + ax^k + b$ with b being the primitive element of $\mathbb{F}_4$ and $a + b \neq 1$ is primitive over $\mathbb{F}_4$ if and only if all the others are primitive over $\mathbb{F}_4$. And we can deduce that if we find one primitive trinomial over $\mathbb{F}_4$, in fact there are at least four trinomials with the same degree. We give a table of necessary conditions for the existence of primitive trinomials and other interesting results. In section 3, we discuss the primitivity of trinomials with special degrees over $\mathbb{F}_4$ and if some results are obviously true over $\mathbb{F}_3$, we also give it.

2 The general form

In [1], we have given some results on the primitivity of trinomials of the special form $x^n + ax + b$ over $\mathbb{F}_4$. In this section, we extend these results to the general form $x^n + ax^k + b$. These new results are mainly included in the following theorem 1 and theorem 2. To prove theorem 1 and theorem 2, we first give some lemmas.

Lemma 1 [3]. If $f(x) \in \mathbb{F}_q[x]$ is a polynomial of positive degree with $f(0) \neq 0$, and if r is a prime not dividing q, then $ord(f(x^r)) = rord(f(x))$.

Lemma 2. If $f(x) \in \mathbb{F}_q[x]$ is a polynomial of positive degree with $f(0) \neq 0$ and $f(x)$ has no multiple roots, then for each $a \in \mathbb{F}_q^*$, $ord(f(x))$ divides $ord(a) \cdot ord(f(ax))$.

Proof. Let β be a root of $f(x)$, then $a^{-1}\beta$ is a root of $f(ax)$ and $ord(\beta) = ord(a \cdot a^{-1}\beta)$. It is obvious that $ord(a \cdot a^{-1}\beta)$ can divide $ord(a) \cdot ord(a^{-1}\beta)$, so $ord(\beta)$ can divide $ord(a) \cdot ord(a^{-1}\beta)$. Since $f(0) \neq 0$ and $f(x)$ has no multiple roots, it is well known that the order of $f(x)$ is equal to the least common multiple of the orders of all its roots, hence according to the basic knowledge of the least common multiple, we have $ord(f(x))$ can divide $ord(a) \cdot ord(f(ax))$. □

Lemma 3. Let ω be a primitive element of $\mathbb{F}_4$. If $k \equiv 0 \mod 3$ or $n \equiv 0 \mod 3$, then for any $a \in \mathbb{F}_4^*$, the trinomial $x^n + ax^k + \omega$ can not be primitive over $\mathbb{F}_4$.

*Emails: [1]liyj@amss.ac.cn, [2]afogy@163.com, [3]wanghf@mmrc.iss.ac.cn, [4]xxbzsys@163.com,† Corresponding author

Proof. Let $g(x) = x^n + ax^k + \omega$. If $n \equiv 0 \mod 3$ and $k \equiv 1 \mod 3$ or $k \equiv 2 \mod 3$, one can easily check that $g(x)$ has at least one root in $\mathbb{F}_4$. So it is reducible over $\mathbb{F}_4$. And of course not primitive.

If $n \equiv 0 \mod 3$ and $k \equiv 0 \mod 3$, then $g(x) = (x^3)^{\frac{n}{3}} + a(x^3)^{\frac{k}{3}} + \omega$. According to lemma 1, we have

$$\begin{aligned} ord(g(x)) &= 3ord(x^{\frac{n}{3}} + ax^{\frac{k}{3}} + \omega) \\ &\leq 3(4^{\frac{n}{3}} - 1) \\ &< 4^n - 1. \end{aligned}$$

So $g(x)$ can not be primitive over $\mathbb{F}_4$.

If $k \equiv 0 \mod 3$ and $n \equiv 1 \mod 3$, since $a \in \mathbb{F}_4^*$, $a = 1, \omega$ or ω^2. For $a = 1$ and $a = \omega^2$, one can check that for each case $g(x) = x^n + ax^k + \omega$ has a root in $\mathbb{F}_4$. For $a = \omega$, note that $g(\omega x) = \omega(x^n + x^k + 1)$, $g(0) \neq 0$ and n is odd, so $g(x)$ has no multiple roots, then by lemma 2, $ord(g(x))$ can divide $ord(\omega) \cdot ord(g(\omega x))$, which is equal to $3ord(g(\omega x))$. Since $\omega^{-1}g(\omega x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$, we have $ord(g(\omega x)) = ord(\omega^{-1}g(\omega x)) \leq 2^n - 1$, then $ord(g(x)) \leq 3ord(g(\omega x)) \leq 3(2^n - 1) < 4^n - 1$. So $g(x)$ can not be primitive over $\mathbb{F}_4$ too.

If $k \equiv 0 \mod 3$ and $n \equiv 2 \mod 3$, for $a = 1$ and $a = \omega^2$, one can check that for each case $g(x) = x^n + ax^k + \omega$ has a root in $\mathbb{F}_4$. For $a = \omega$, the proof is similar to the case $k \equiv 0 \mod 3$, $n \equiv 1 \mod 3$ and $a = \omega$, we omit it. □

Corollary 1. Let ω be a primitive element of $\mathbb{F}_4$.

1. If $x^n + \omega x^k + \omega$ is primitive, then $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$.
2. If $x^n + x^k + \omega^{-1}$ is primitive, then $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$.

Proof. Let $T_1(x) = x^n + \omega x^k + \omega$ and $T_2(x) = x^n + x^k + \omega^{-1}$. Suppose that $T_1(x)$ is primitive. If $k \equiv 0 \mod 3$ or $n \equiv 0 \mod 3$, according to lemma 3, $T_1(x)$ can not be primitive over $\mathbb{F}_4$. If $n \equiv 1 \mod 3$, $k \equiv 1 \mod 3$ and if $n \equiv 2 \mod 3$, $k \equiv 2 \mod 3$, one can check that $T_1(x)$ has a root in $\mathbb{F}_4$ for each case. So if $T_1(x)$ is primitive, then $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$.

If $k \equiv 0 \mod 3$ or $n \equiv 0 \mod 3$, the same according to lemma 3, $T_2(x)$ can not be primitive over $\mathbb{F}_4$. If $n \equiv 1 \mod 3$, $k \equiv 1 \mod 3$, then $T_2(\omega^{-1}x) = \omega^{-1}(x^n + x^k + 1)$. So according to lemma 2, $ord(T_2(x))$ can divide $ord(\omega^{-1}) \cdot ord(T_2(\omega^{-1}x))$, which is equal to $3ord(T_2(\omega^{-1}x))$. Since $\omega T_2(\omega^{-1}x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$, we have $ord(T_2(\omega^{-1}x)) = ord(\omega g(\omega^{-1}x)) \leq 2^n - 1$, then $ord(T_2(x)) \leq 3ord(T_2(\omega^{-1}x)) \leq 3(2^n - 1) < 4^n - 1$. If $n \equiv 2 \mod 3$, $k \equiv 2 \mod 3$, the proof is the same as the case $n \equiv 1 \mod 3$, $k \equiv 1 \mod 3$. So if $T_2(x)$ is primitive, then also $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$. This completes the proof. □

Let ω be a primitive element of $\mathbb{F}_4$. In [1] we have proved that the trinomials of the special form $x^n + \omega x + \omega$ was primitive over $\mathbb{F}_4$ if and only if $x^n + x + \omega^{-1}$ was primitive over $\mathbb{F}_4$. In fact, it is also true for the trinomials of the general form.

Theorem 1. The trinomial $x^n + \omega x^k + \omega$ is primitive over $\mathbb{F}_4$ if and only if $x^n + x^k + \omega^{-1}$ is primitive over $\mathbb{F}_4$.

Proof. Let $T_1(x) = x^n + \omega x^k + \omega$ and $T_2(x) = x^n + x^k + \omega^{-1}$. Since $T_1(x)$ is primitive, then by corollary 1, $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$. Let ξ be a root of $T_1(x)$, then

$$\omega = \xi \cdot \xi^4 \cdots \xi^{4^{n-1}} = \xi^{\frac{4^n - 1}{3}}. \tag{1}$$

If $n \equiv 1 \mod 3$ and $k \equiv 2 \mod 3$, then

$$T_2(\omega\xi) = (\omega\xi)^n + (\omega\xi)^k + \omega^{-1} = \omega(\xi^n + \omega\xi^k + \omega) = 0.$$

Hence, $\omega\xi$ is a root of $x^n + x^k + \omega^{-1}$. By (1), we have $\omega\xi = \xi^{1 + \frac{4^n - 1}{3}}$. Note that

$$1 + \frac{4^n - 1}{3} = 1 + n + \sum_{k=0}^{n-2} C_n^k 3^{n-k-1}.$$

So 3 is not a divisor of $4^n - 1$ and $1 + \frac{4^n - 1}{3}$ if $n \equiv 1 \mod 3$. If p is a prime divisor of $4^n - 1$ and $p \neq 3$, obviously, it can not be a divisor of $1 + \frac{4^n - 1}{3}$. So $4^n - 1$ and $1 + \frac{4^n - 1}{3}$ are relatively prime. Then the order of $\omega\xi$ is also $4^n - 1$. Thus, $\omega\xi$ is a primitive element of $\mathbb{F}_{4^n}$. Since the degree of $x^n + x^k + \omega^{-1}$ is n, then it is the minimal polynomial of $\omega\xi$, hence $x^n + x^k + \omega^{-1}$ is primitive over $\mathbb{F}_4$. If $n \equiv 2 \mod 3$ and $k \equiv 1 \mod 3$, the proof is similar, we omit it.

Conversely, suppose that $T_2(x)$ is primitive, then by corollary 1, we also have that $n \equiv 1 \mod 3$, $k \equiv 2 \mod 3$ or $n \equiv 2 \mod 3$, $k \equiv 1 \mod 3$. And the proof of the left is similar to the proof of necessity, we omit it. □

Lemma 4 [3]. The monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $n > 1$ is a primitive polynomial over $\mathbb{F}_q$ if and only if $(-1)^n f(0)$ is a primitive element of $\mathbb{F}_q$ and the least positive integer r for which x^r is congruent $\bmod f(x)$ to some element of $\mathbb{F}_q$ is $r = \frac{q^n-1}{q-1}$. In case $f(x)$ is primitive over $\mathbb{F}_q$, we have $x^r \equiv (-1)^n f(0) \bmod f(x)$.

By lemma 4, when we check the primitivity of all trinomials $x^n + ax^k + b$ over $\mathbb{F}_4$. We only need to consider the trinomials with b being the primitive element of $\mathbb{F}_4$. Let ω be a primitive element of $\mathbb{F}_4$. Then $b = \omega$ or $b = \omega^2$. If $b = \omega$, $a = \omega^2$ or $b = \omega^2, a = \omega$, note that $\omega^2 + \omega + 1 = 0$, then 1 is the root of $x^n + ax^k + b$. Hence if $x^n + ax^k + b$ is primitive over $\mathbb{F}_4$, then $a = b = \omega$ or $a = b = \omega^2$ or $a = 1, b = \omega$ or $a = 1, b = \omega^2$, i.e., only the following four cases $g_1(x) = x^n + \omega x^k + \omega, g_2(x) = x^n + \omega^2 x^k + \omega^2, g_3(x) = x^n + x^k + \omega$ and $g_4(x) = x^n + x^k + \omega^2$ maybe primitive over $\mathbb{F}_4$. By theorem 1, $g_1(x)$ is primitive over $\mathbb{F}_4$ if and only if $g_4(x)$ is primitive over $\mathbb{F}_4$ and $g_2(x)$ is primitive over $\mathbb{F}_4$ if and only if $g_3(x)$ is primitive over $\mathbb{F}_4$. Note that $g_1^2(x) = g_2(x^2)$, then the squares of all the roots of $g_1(x)$ are just all the roots of $g_2(x)$ and the converse is true. So $g_1(x)$ is primitive over $\mathbb{F}_4$ if and only if $g_2(x)$ is primitive over $\mathbb{F}_4$. The above discussion means that for given n and k, one of all the trinomials $x^n + ax^k + b$ with b being the primitive element of $\mathbb{F}_4$ and $a + b \neq 1$ is primitive over $\mathbb{F}_4$ if and only if all the others are primitive over $\mathbb{F}_4$. And we can deduce that if we find one primitive trinomial over $\mathbb{F}_4$, in fact there are at least four trinomials with the same degree.

Lemma 5 [6]. Suppose $[K : \mathbb{F}_2]$ is even. Only two types of odd-degree trinomials have an even number of factors, namely,

1. $g(x) = x^n + ax^k + b, 2|k|2n$, if $t^2 + t + a^{\frac{2n}{k}} b^{2-\frac{2n}{k}}$ has no roots in K.
2. $g(x) = x^n + ax^k + b, n - k|n$, if $t^2 + t + a^{\frac{2n}{k}} b^{-2}$ has no roots in K.

Lemma 6. Let ω be a primitive element of $\mathbb{F}_4$ and let $T_1(x) = x^n + \omega x^k + \omega$. If $n > 2$, then $T_1(x)$ is reducible over $\mathbb{F}_4$ for the cases in table 1.

Table 1

$k \mod 15$	$n \mod 15$	$k \mod 15$	$n \mod 15$
1	2,8,14	2	1,4,13
4	2,8,11	8	1,4,7
7	8,11,14	11	4,7,13
13	2,11,14	14	1,7,13

Proof. For the case $k \mod 15 = 1$ and $n \mod 15 = 2$, let β be a root of $x^2 + \omega x + \omega$. Then $\beta^{15} = 1$ and one can check that β is also the root of $T_1(x)$. Since $x^2 + \omega x + \omega$ is irreducible over $\mathbb{F}_4$ and $n > 2$, we have $x^2 + \omega x + \omega$ is a factor of $T_1(x)$. The proofs of other cases are similar, we omit them and list an irreducible factor of degree 2 for each case in the following table 2. □

Table 2

$k \mod 15$	$n \mod 15$	a factor of $T_1(x)$	$k \mod 15$	$n \mod 15$	a factor of $T_1(x)$
1	2	$x^2 + \omega x + \omega$	2	1	$x^2 + \omega^2 x + 1$
	8	$x^2 + \omega x + 1$		4	$x^2 + \omega^2 x + \omega^2$
	14	$x^2 + x + \omega^2$		13	$x^2 + x + \omega$
4	2	$x^2 + \omega x + 1$	8	1	$x^2 + \omega^2 x + \omega^2$
	8	$x^2 + \omega x + \omega$		4	$x^2 + \omega^2 x + 1$
	11	$x^2 + x + \omega^2$		7	$x^2 + x + \omega$
7	8	$x^2 + \omega^2 x + \omega^2$	11	4	$x^2 + \omega x + \omega$
	11	$x^2 + \omega^2 x + 1$		7	$x^2 + x + \omega^2$
	14	$x^2 + x + \omega$		13	$x^2 + \omega x + 1$
13	2	$x^2 + \omega^2 x + \omega^2$	14	1	$x^2 + \omega x + \omega$
	11	$x^2 + x + \omega$		7	$x^2 + \omega x + 1$
	14	$x^2 + \omega^2 x + 1$		13	$x^2 + x + \omega^2$

Now we can prove the following further results.

Theorem 2. If trinomial $x^n + ax^k + b$ with b being the primitive element of $\mathbb{F}_4$ is primitive over $\mathbb{F}_4$ and $n > 2$, then n, k satisfy the conditions in the table below.

Proof. By theorem 1 and the arguments after lemma 4, we only need to suppose that the trinomial $x^n + \omega x^k + \omega$ is primitive over $\mathbb{F}_4$, then by corollary 1, we have $k \equiv 1 \mod 3, n \equiv 2 \mod 3$ or $k \equiv 2 \mod 3, n \equiv 1 \mod 3$.

Table 3

$k \mod 15$	1	2	4	5	7	8	10	11	13	14
$n \mod 15$	5,11	7,10	5,14	1,4,7,13	2,5	10,13	2,8,11,14	1,10	5,8	4,10

For $k \equiv 1 \mod 3$ and $n \equiv 2 \mod 3$, note that $k \equiv 1 \mod 3$ is equivalent to $k \equiv 1, 4, 7, 10, 13 \mod 15$. For $k \equiv 1, 4, 7, 13 \mod 15$, since $n > 2$, then by lemma 6, for the corresponding values of $n \mod 15$ in table 1, the trinomial $x^n + \omega x^k + \omega$ is reducible over $\mathbb{F}_4$. Checking all possible values of $n \mod 15$ and make sure $n \equiv 2 \mod 3$ for each $k \equiv 1, 4, 7, 13 \mod 15$, only for the values of $n \mod 15$ in table 3, we can not decide whether $x^n + \omega x^k + \omega$ is primitive or not and for all other cases, $x^n + \omega x^k + \omega$ can not be primitive. For $k \equiv 10 \mod 15$, if $n \equiv 5 \mod 15$, then 5 can divide n and k, by lemma 1, $ord(x^n + \omega x^k + \omega) = 5ord(x^{\frac{n}{5}} + \omega x^{\frac{k}{5}} + \omega) < 4^n - 1$. So $x^n + \omega x^k + \omega$ is not primitive over $\mathbb{F}_4$. Checking all possible values of $n \mod 15$ and make sure $n \equiv 2 \mod 3$, $x^n + \omega x^k + \omega$ can not be primitive except for $n \equiv 2, 8, 11, 14 \mod 15$. For $k \equiv 2 \mod 3$ and $n \equiv 1 \mod 3$, the proof is similar to the case $k \equiv 1 \mod 3$ and $n \equiv 2 \mod 3$. We omit the proof. □

Following from theorem 2, we can have

Corollary 2. For any $n(n > 2)$ there is no primitive trinomials $x^n + ax^2 + b$ over $\mathbb{F}_4$.

Proof. Let ω be a primitive element of $\mathbb{F}_4$. By theorem 1 and the arguments after lemma 4, we only need to consider the case $a = b = \omega$. According to corollary 1, $x^n + \omega x^2 + \omega$ can not be primitive over $\mathbb{F}_4$ if $n \equiv 0 \mod 3$ and $n \equiv 2 \mod 3$. In fact, one can directly check that $x^n + ax^2 + \omega$ has a root in $\mathbb{F}_4$. If $n \equiv 1 \mod 3$, since $[\mathbb{F}_4 : \mathbb{F}_2] = 2$, $t^2 + t + \omega^{\frac{2n}{2}} \omega^{2 - \frac{2n}{2}} = t^2 + t + \omega^2$ has no roots in $\mathbb{F}_4$. Then by lemma 5, we have $x^n + \omega x^2 + \omega$ is reducible over $\mathbb{F}_4$. □

3 The special form

In this section, we go on to consider the primitivity of trinomials of the special form $x^n + ax + b$. By theorem 2 we know that there is no primitive trinomials over $\mathbb{F}_4$ except for $n \equiv 5 \mod 15$ and $n \equiv 11 \mod 15$. Hence we consider the primitivity of trinomial $x^n + ax + b$ when $n \equiv 5 \mod 15$ and $n \equiv 11 \mod 15$. We mainly study the trinomials with degrees $n = 4^m + 1$ and $n = 21 \cdot 4^m + 29$, where m is a positive integer. It is easy to check that if $n = 4^m + 1$, then $n \equiv 5 \mod 15$ for m is odd and if $n = 21 \cdot 4^m + 29$, then $n \equiv 5 \mod 15$ for m is even. For these two cases, we prove that the trinomials $x^n + ax + b$ with degrees $n = 4^m + 1$ and $n = 21 \cdot 4^m + 29$ are always reducible if $m > 1$. If some results are obviously true over $\mathbb{F}_3$, we also give them.

Theorem 3. Let m be a positive integer. Suppose that $a, b \in \mathbb{F}_q^*$ and

$$(\lambda_i, \lambda_{i+1}) = (1, -a) \cdot \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}^i, i = 0, 1, \cdots, q-2. \tag{2}$$

If $\lambda_i \neq 0$ for $1 \leq i \leq q-1$ and $\lambda_{q-2} b + \lambda_{q-1} a = 0$, then all irreducible factors of $x^{q^m+1} + ax + b$ have degrees dividing $(q+1)m$, and therefore, periods dividing $q^{(q+1)m} - 1$.

Proof. Let $\varphi(x) = x^{q^m+1} + ax + b$ and

$$\Phi(x) = \lambda_{q-1} \varphi(x) + \sum_{i=0}^{q-2} \lambda_i x^{q^{(q-2-i)m} + \cdots + q^m + 1} \varphi^{q^{(q-1-i)m}}(x). \tag{3}$$

By (2), we have that

$$(\lambda_{i+1}, \lambda_{i+2}) = (\lambda_i, \lambda_{i+1}) \cdot \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}, i = 0, 1, \cdots, q-3.$$

Then $\lambda_{i+2} + \lambda_i b + \lambda_{i+1} a = 0, 0 \leq i \leq q-3$. So by simple calculation and the condition that $\lambda_i \neq 0, 1 \leq i \leq q-1, \lambda_{q-2} b + \lambda_{q-1} a = 0$, we can deduce that

$$\Phi(x) = x^{q^{qm} + \cdots + q^m + 1} + \lambda_{q-1} b.$$

Note that $\varphi(x)$ can divide $\Phi(x)$. So $\varphi(x)$ can divide $\Phi(x) = x^{q^{qm} + \cdots + q^m + 1} + \lambda_{q-1} b$, which can divide $x^{(q-1)(q^{qm} + \cdots + q^m + 1)} - 1$. Notice that for any positive integer m, $q-1$ divides $q^m - 1$, and $(q^m - 1)(q^{qm} + \cdots + q^m + 1) = q^{(q+1)m} - 1$. So $(q-1)(q^{qm} + \cdots + q^m + 1)$ is a divisor of $q^{(q+1)m} - 1$. So $\varphi(x)$ divides $x^{q^{(q+1)m} - 1} - 1$. Hence all irreducible factors of $\varphi(x)$ have degrees dividing $(q+1)m$, and therefore, periods dividing $q^{(q+1)m} - 1$.

Corollary 3. Let $q = 3, 4$ and let m be a positive integer. Suppose that $a, b \in \mathbb{F}_q^*$ and $b \neq a^2$, then all irreducible factors of $x^{q^m+1} + ax + b$ have degrees dividing $(q+1)m$.

Proof. For the case $q = 3$, let $g(x) = x^{3^m+1} + ax + b$. According to the condition that $b \neq a^2$ and since $\mathbb{F}_3 = \{0, 1, -1\}$, we have $b = -1, a = 1$ or $b = -1, a = -1$. Let $\lambda_0 = 1, \lambda_1 = -a$. Then $\lambda_2 = a^2 - b$ according to theorem 3 and one can check that $\lambda_1 b + \lambda_2 a = 0$ whatever $b = -1, a = 1$ or $b = -1, a = -1$. So by theorem 3, all irreducible factors of $x^{3^m+1} + ax + b$ have degrees dividing $4m$.

For the case $q = 4$, the proof is similar. Let ω be a primitive element of $\mathbb{F}_4$. Then $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ and $1 + \omega + \omega^2 = 0$. Since $b \neq a^2$, if $b = 1$, then $a \neq 1$, i.e., $a = \omega$ or $a = \omega^2$, if $b = \omega$, then $a = 1$ or $a = \omega$, if $b = \omega^2$, then $a = 1$ or $a = \omega^2$. Let $\lambda_0 = 1, \lambda_1 = a$. Then $\lambda_2 = a^2 - b, \lambda_3 = 1$. According to theorem 3 and one can check that for $b = 1, a = \omega$ or $a = \omega^2$, $b = \omega, a = 1$ or $a = \omega$ and $b = \omega^2, a = 1$ or $a = \omega^2$, we all have that $a^2 b + b^2 + a = 0$ and this is equivalent to $\lambda_2 b + \lambda_3 a = 0$. Hence by theorem 3, all irreducible factors of $x^{4^m+1} + ax + b$ have degrees dividing $5m$. □

By corollary 3, we can deduce that trinomial $x^{q^m+1} + ax + b$ is reducible if $m > 1$. Before we give corollary 4, we first need a lemma.

Lemma 7 [2]. Let $\mathbb{F}_q$ be a finite field and let m be a positive integer. Then the degree of every irreducible factor of $x^{q^m+1} + x + 1$ over $\mathbb{F}_q$ divides $3m$.

Corollary 4. Suppose that $q = 3, 4$ and m is a positive integer. Then all irreducible factors of $x^{q^m+1} + ax + b$ have degrees dividing $(q+1)m$ or dividing $3m$.

Proof. For the case $q = 3$, let $g(x) = x^{3^m+1} + ax + b$. According to theorem 3, all irreducible factors of $g(x) = x^{3^m+1} + ax + b$ dividing $4m$ when $b = -1$. If $b = 1, a = 1$, then by lemma 7, the degree of every irreducible factor of $x^{q^m+1} + x + 1$ over $\mathbb{F}_q$ divides $3m$. If $b = 1, a = -1$, then $g(x) = x^{3^m+1} - x + 1$. Let $g_1(x) = g(-x)$, then $g_1(x) = x^{3^m+1} + x + 1$, it is well known that the transformation from $g(x)$ to $g_1(x)$ preserves degrees of factors. So the degree of every irreducible factor of $g(x)$ is the same as the degree of some irreducible factor of $g_1(x)$, hence divides $3m$.

For the case $q = 4$, let $h(x) = x^{4^m+1} + ax + b$. According to theorem 3, all irreducible factors of $h(x) = x^{4^m+1} + ax + b$ dividing $5m$ when $b \neq a^2$. If $b = a^2$, the first case if $b = a = 1$, then by lemma 7, we know that the degree of every irreducible factor of $x^{q^m+1} + x + 1$ over $\mathbb{F}_q$ divides $3m$. Let ω be the primitive element of $\mathbb{F}_q$. The second case if $a = \omega$, then $b = \omega^2$ and $h(x) = x^{4^m+1} + \omega x + \omega^2$. Let $h_1(x) = h(\omega x)$, then $h_1(x) = \omega(x^{4^m+1} + x + 1)$, of course the transformation from $h(x)$ to $h_1(x)$ also preserves degrees of factors. So the degree of every irreducible factor of $h(x)$ is the same as the degree of some irreducible factor of $h_1(x)$, hence divides $3m$. The third case if $a = \omega^2$, then $b = \omega$ and $h(x) = x^{4^m+1} + \omega^2 x + \omega$. The proof of this case is similar to the second case, we omit it. □

Theorem 4. The trinomial $x^{21 \cdot 4^m+29} + ax + b$ always has a root in $\mathbb{F}_{4^3}$ for any positive integer m.

Proof. First one can verify that $x^{50} + ax + b$ always has a root in $\mathbb{F}_{4^3}$. For $m \equiv 0 \mod 3$, if β is a root of $x^{50} + ax + b$ in $\mathbb{F}_{4^3}$, then it is also the root of $x^{21 \cdot 4^m+29} + ax + b$. For $m \equiv 1 \mod 3$ and $m \equiv 1 \mod 3$, note that $21 \cdot 4 + 29 = 63 + 50$ and $21 \cdot 16 + 29 = 63 \cdot 5 + 50$, so the roots of $x^{50} + ax + b$ in $\mathbb{F}_{4^3}$ are also the roots of $x^{21 \cdot 4^m+29} + ax + b$. This completes the proof. □

Reference

[1] Li Yujuan, Wang Huaifu,Zhao Jinhua. On the primitivity of some trinomials over finite fields. Advances in mathematics(China), accepted, 2013.

[2] S.W.Golomb. Shift register sequence. Revised edition, Aegean Park Press,1982.

[3] Lidl R., Neiderreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[4] Savas,E., Koc,C.K.: Finite field arithmetic for cryptography. IEEE Circuits and Systems Magazine, 10(2), 40-56, 2010.

[5] Richard G. Swan . Factorization of polynomials over Finite Fields. Pacific Journal of Mathematics 12(2), 1099-1106, 1962.

[6] Uzi Vishne . Factorization of Trinomials over Galois Fields of Characteristic 2. Finite Fields and Their Applications 3(4), 370-377, 1997.

[7] J. von zur Gathen, Irreducible trinomials over Finite Fields, Mathematics of Computation, 72, 1987-2000, 2003.

[8] B. Hanson, D.Panario and D.Thomson, Swan-like results for binomials and trinomials over finite fields of odd characteristic. Designs. Codes and Cryptography, 61(3), 273-283, 2011.

小的有限域上三项式的本原性研究

李玉娟[1]，赵进华[2]，王怀富[3]，马婧[4]

. 信息保障技术重点实验室, 北京市 100072

摘　要: 在这篇文章中，我们研究小的有限域上三项式的本原性。我们把关于$\mathbb{F}_4$上特殊形式的三项式$x^n + ax + b$ 本原性的结果推广到了一般的形式$x^n + ax^k + b$ 。证明了对给定的n 和k，所有三项式$x^n + ax^k + b(a + b \neq 1, b$是$\mathbb{F}_4$的本原元)中的一个三项式在$\mathbb{F}_4$上本原，则所有其它的在$\mathbb{F}_4$上都本原，由此可推出如果找到$\mathbb{F}_4$上的一个本原三项式，那么事实上至少存在四个次数与其相同的本原三项式。给出了在$\mathbb{F}_4$ 上存在本原三项式的必要条件。研究了次数为$n = 4^m + 1$和$n = 21 \cdot 4^m + 29$ 的三项式$x^n + ax + b$ ，证明了当$m > 1$ 时，这两种次数的三项式$x^n + ax + b$总是可约的。如果一些结果在$\mathbb{F}_3$ 上也成立，也一并给出。

关键词: 有限域；本原多项式；三项式