On the Primitivity of some Trinomials over Finite Fields

LI Yujuan & WANG Huaifu[†] & ZHAO Jinhua

Science and Technology on Information Assurance Laboratory, Beijing, 100072, P.R. China
email: liyj@amss.ac.cn, wanghf@mmrc.iss.ac.cn, afogy@163.com

Abstract In this paper, we give conditions under which the trinomials of the form $x^n + ax + b$ over finite field $\mathbb{F}_{p^m}$ are not primitive and conditions under which there are no primitive trinomials of the form x^n+ax+b over finite field $\mathbb{F}_{p^m}$. For finite field $\mathbb{F}_4$, We show that there are no primitive trinomials of the form $x^n + x + \alpha$, if $n \equiv 1 \mod 3$ or $n \equiv 0 \mod 3$ or $n \equiv 4 \mod 5$.

1 Introduction

As usual, let p be a prime and let m be a positive integer, denote $\mathbb{F}_q(q = p^m)$ 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 $x^n + ax^k + b(n > k > 0, ab \neq 0)$. They have many important applications in the theory of finite fields, cryptography, and coding theory[3, 5]. For example, they are used to represent the field. Choosing an irreducible trinomial to represent the field can make the implementation of the field arithmetic faster than other irreducible polynomials[1, 6]. Hence there are many results on the factorizations of trinomials and existence or non-existence of irreducible or primitive trinomials. For example, Swan [7] shows that $x^n + x^k + 1(n > k > 0)$ is reducible over $\mathbb{F}_2$ if $8 \mid n$, Vishne [8] extends this result to the trinomials over finite fields of characteristic 2 and gives some sufficient conditions for a trinomial being reducible. Using the classical results of Stickelberger and Swan, Gathen [2] gives a necessary condition for irreducibility of a trinomial over a finite field and applies it in the special case $\mathbb{F}_3$. Recently, Hanson, Panario and Thomson [4] have determined the parity of the number of irreducible factors of some trinomials over finite field $\mathbb{F}_q$ of odd characteristic by analying some special congruences.

In this paper, we explore the primitivity of the trinomials of the special form x^n+ax+b over finite field $\mathbb{F}_{p^m}$. Using the well known results of the polynomial characterization of primitive linear feedback shift register sequences (see lemma 2.1), we mainly get the following results

Theorem 1.1. Let m, n be positive integers and $m, n \geqslant 2$, then the trinomials of the form x^n+ax+b over finite field $\mathbb{F}_{p^m}$ are not primitive if $b^{1-n}a^n \in \mathbb{F}^*_{p^u}$, where $\mathbb{F}_{p^u}$ denotes the proper subfield of $\mathbb{F}_{p^m}$ with p^u elements and $\mathbb{F}^*_{p^u} = \mathbb{F}_{p^u} - \{0\}$.

Using theorem 1.1, we can have

Corollary 1.1. Let m, n be positive integers and $m, n \geqslant 2$, then there are no primitive trinomials of the form $x^n + jx + \lambda(j \in \mathbb{F}^*_{p^u} \subset \mathbb{F}^*_{p^m})$ over finite field $\mathbb{F}_{p^m}$ if $n \equiv 1 \mod (p^m - 1)$.

[†] Corresponding author

Specially in $\mathbb{F}_4$, we get

Theorem 1.2. If $n \equiv 1 \mod 3$ or $n \equiv 0 \mod 3$ or $n \equiv 4 \mod 5$, then there are no primitive trinomials of the form $x^n + x + \alpha$ over finite field $\mathbb{F}_4$.

2 Proof of main theorems

Since we need use the knowledge of linear feedback shift registers and the knowledge of primitive polynomials over finite fields to prove our main results, we first review the basic definitions and some of the basic results concerning linear feedback shift registers and primitive polynomials over finite fields.

Definition 2.1. Let n be a positive integer, $f(x) = x^n + c_1x^{n-1} + \cdots + c_n \in \mathbb{F}_q[x]$. Given any n-tuple $(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_q^n$, let $s^\infty = (a_0, a_1, \cdots)$ denote the infinite sequence of elements of $\mathbb{F}_q$ generated by the following linear recurrence relation

$$a_{i+n} = -(c_n a_i + c_{n-1}a_{i+1} + \cdots + c_1 a_{i+n-1}) \quad i = 0, 1, \cdots . \tag{1}$$

The above relation (1) is called a linear feedback shift register (LFSR) of stage n, and s^∞ is called the linear feedback shift register sequence of stage n over $\mathbb{F}_q$ determined by $f(x)$ and $(a_0, a_1, \cdots, a_{n-1})$. Let

$$s_k = (a_k, a_{k+1}, \cdots, a_{k+n-1}), k \geqslant 0 \tag{2}$$

The n-tuple s_k is called the state of LFSR, and $s_0 = (a_0, a_1, \cdots, a_{n-1})$ is called the initial state of s^∞ and the polynomial $f(x)$ is called the characteristic polynomial of LFSR. If $c_n \neq 0$, the LFSR is said to be non-degenerate.

From now on, we assume that the LFSR (1) is non-degenerate, i.e., $c_n \neq 0$. Let M_f be the companion matrix of polynomial $f(x)$, i.e.,

$$M_f = \begin{pmatrix} 0 & & & & -c_n \\ 1 & 0 & & & -c_{n-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -c_2 \\ & & & 1 & -c_1 \end{pmatrix} \tag{3}$$

Obviously, because $c_n \neq 0$, M_f is a permutation and $s_{k+1} = s_k M_f, k \geqslant 0$. It is well known that the period of a sequence generated by the above non-degenerate LFSR is equal to the length of the cycle of the complete factorization of M_f into disjoint cycles which the initial state lies in. Let $p(s^\infty)$ denote the period of the sequence s^∞ generated by M_f and initial state s_0, and let $p_{M_f}(s_0) = \min\{l | s_0 M_f^l = s_0\}$, then $p(s^\infty) = p_{M_f}(s_0)$. If $f(x)$ is irreducible, then for any nonzero initial state, the periods of the sequences generated by (1) are the same and equal to the order of $f(x)$. We say that a LFSR of stage n over $\mathbb{F}_q$ is primitive if for any choice of a nonzero initial state, the sequence generated by relation (1) is periodic of period $q^n - 1$, or equivalently, for any $s_0 \neq 0$, $p_{M_f}(s_0) = q^n - 1$.

Lemma 2.1. A linear feedback shift register of stage n over $\mathbb{F}_q$ is primitive if and only if its characteristic polynomial is a primitive polynomial of degree n in $\mathbb{F}_q[x]$.

Lemma 2.2.[5] The monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$ 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 mod $f(x)$ to some element of $\mathbb{F}_q$ is $r = \frac{q^n-1}{q-1}$. In case f is primitive over $\mathbb{F}_q$, we have $x^r \equiv (-1)^n f(0) \mod f(x)$.

Lemma 2.3.[5] Let f^* be the reciprocal polynomial of the monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$, then $ord(f) = ord(f^*)$. In particular, the monic polynomial $f \in \mathbb{F}_q[x]$ of degree $n \geqslant 1$ is primitive if and only if its reciprocal polynomial f^* is primitive.

By lemma 2.3, the trinomials of the form $x^n + ax + b$ over $\mathbb{F}_{p^m}$ are primitive if and only if the trinomials of the form $g(x) = x^n + \alpha x^{n-1} + \beta$ over $\mathbb{F}_{p^m}$ are primitive, where $\beta = b^{-1}, \alpha = b^{-1}a$. So we only consider the form $g(x) = x^n + \alpha x^{n-1} + \beta$. And note that the condition $b^{1-n}a^n \in \mathbb{F}^*_{p^u}$ is equivalent to the condition $\beta^{-1}\alpha^n \in \mathbb{F}^*_{p^u}$.

The main idea to prove our results is to show that there exists a nonzero initial state such that the period of LFSR sequence generated by $g(x)$ and this initial state can not reach $q^n - 1$, so the linear feedback shift register is not primitive, and then according to the lemma 2.1, we have $g(x) = x^n + \alpha x^{n-1} + \beta$ is not primitive.

Let M_g denote the matrix determined by $g(x) = x^n + \alpha x^{n-1} + \beta$ like (3), We first give a lemma for convenience of the proofs below.

Lemma 2.4. Suppose that $\beta^{-1}\alpha^n \in \mathbb{F}^*_{p^u}$, and let $s_0 = \alpha^{(n-1)t}(j_0 w, j_1 \alpha w, \ldots, j_{n-1}\alpha^{n-1}w)$ for some $t(0 \leqslant t \leqslant p^m - 2)$, $j_i \in \mathbb{F}_{p^u}(0 \leqslant i \leqslant n-1)$ and $w \in \mathbb{F}_{p^m}$. Then there exist $z_0, \ldots, z_{n-1} \in \mathbb{F}_{p^u}$ such that the n tuple

$$s_0 M_g^{n-1} = \alpha^{(n-1)(t+1)}(z_0 w, z_1 \alpha w, \ldots, z_{n-1}\alpha^{n-1}w).$$

Proof. For convenience, we denote $s_0 = (a_0, \ldots, a_{n-1})$, i.e., $a_k = \alpha^{(n-1)t} j_k \alpha^k w, 0 \leqslant k \leqslant n-1$. According to relation (1) and $g(x) = x^n + \alpha x^{n-1} + \beta$, we have

$$a_{n+i} = -\beta a_i - \alpha a_{n+i-1}, i \geqslant 0.$$

And so

$$s_0 M_g^{n-1} = (a_{n-1}, \ldots, a_{2n-2}).$$

We prove that $a_{n-1+i} = \alpha^{(n-1)(t+1)}\alpha^i j_{n-1} w (0 \leqslant i \leqslant n-1))$ by deduction. For $i = 0$, since $a_{n-1} = \alpha^{(n-1)t}\alpha^{n-1}j_{n-1}w = \alpha^{(n-1)(t+1)}j_{n-1}w$, let $z_0 = j_{n-1}$, then $a_{n-1} = \alpha^{(n-1)(t+1)}z_0 w$. Suppose that the k-th component of $s_0 M_g^{n-1}$, $a_{n-1+k}(0 \leqslant k \leqslant n-1)$, is equal to $\alpha^{(n-1)(t+1)}\alpha^k z_k w$ for some $z_k \in \mathbb{F}_{p^u}$, let $l = \beta^{-1}\alpha^n \in \mathbb{F}^*_{p^u}$ and $z_{k+1} = -l^{-1}j_k - z_k \in \mathbb{F}_{p^u}$, by the condition of the lemma that $a_k = \alpha^{(n-1)t}\alpha^k j_k w$, then we have

$$\begin{aligned} a_{n+k} &= -\beta a_k - \alpha a_{n-1+k} \\ &= -\alpha^n l^{-1} \alpha^{(n-1)t}(\alpha^k j_k w) - \alpha(\alpha^{(n-1)(t+1)}\alpha^k z_k w) \\ &= \alpha^{(n-1)(t+1)}(-\alpha^{k+1} l^{-1} j_k w - \alpha^{k+1} z_k w) \\ &= \alpha^{(n-1)(t+1)}\alpha^{k+1} w(-l^{-1} j_k - z_k) \\ &= \alpha^{(n-1)(t+1)}\alpha^{k+1} z_{k+1} w \end{aligned}$$

i.e., the $(k+1)$-th component of $s_0 M_g^{n-1}$ is equal to $\alpha^{(n-1)(t+1)}\alpha^{k+1}z_{k+1}w$ for some $z_{k+1} \in \mathbb{F}_{p^u}$. Therefore, by the conditions of the lemma, there exist $z_0, \ldots, z_{n-1} \in \mathbb{F}_{p^u}$ such that

$$s_0 M_g^{n-1} = \alpha^{(n-1)(t+1)}(z_0 w, z_1 \alpha w, \ldots, z_{n-1}\alpha^{n-1}w).$$

Thus, the proof is complete. □

Proof of Theorem 1.1. Let w be any nonzero element of $\mathbb{F}_{p^m}$ and $s_0 = (j_0 w, 0, \ldots, 0) \in \mathbb{F}_{p^m}^n, j_0 \in \mathbb{F}_{p^u}^*$. Obviously, s_0 satisfies the condition of lemma 2.4 and $s_0 \neq 0$, thus the n-tuple $s_0 M_g^{n-1}$ satisfies that the i-th component is $\alpha^{n-1}\alpha^i z_{1,i} w$ for some $z_{1,i} \in \mathbb{F}_{p^u}$, $0 \leqslant i \leqslant n-1$, deductively, for any $l \geqslant 0$, the n-tuple $s_0 M_g^{l(n-1)}$ satisfies that the i-th component is $\alpha^{(n-1)l}\alpha^i z_{l,i} w$ for some $z_{l,i} \in \mathbb{F}_{p^u}$, $0 \leqslant i \leqslant n-1$. Then we can have at least $(p^m-1)(p^{un}-1)+1$ ones of such nonzero n tuples.

$$s_0 M_g^{l(n-1)}, 0 \leqslant l \leqslant (p^m-1)(p^{un}-1)$$

However, since $\alpha \in \mathbb{F}_{p^m}^*$, the total number of the elements of the set $\{\alpha^{(n-1)l} | l \in \mathbb{Z}, l \geqslant 0\}$ is at most $p^m - 1$. And the number of all the different nonzero n tuples with the property that the i-th component is $\alpha^i j_i w$ for some $j_i \in \mathbb{F}_{p^u}(0 \leqslant i \leqslant n-1)$, is $p^{un}-1$, so the number of all the different nonzero n tuples

$$\alpha^{(n-1)l}(j_0 w, j_1 \alpha w, \ldots, j_{n-1}\alpha^{n-1} w), (l \in \mathbb{Z}, l \geqslant 0, (j_0, \ldots, j_{n-1}) \in \mathbb{F}_{p^u}^n - \{0\})$$

is at most $(p^m-1)(p^{un}-1)$, then there exists $l_0 (1 \leqslant l_0 \leqslant (p^m-1)(p^{un}-1))$ such that

$$s_0 M_g^{l_0(n-1)} = s_0.$$

Since $m \geqslant 2, \mathbb{F}_{p^u}$ is the proper subfield of $\mathbb{F}_{p^m}$, we have $u | m, u < m$, then $u \leqslant \frac{m}{2}$. Since $s_0 = (j_0 w, 0, \ldots, 0)$, we have $s_0 M_g \neq s_0$. Notice that $n - 1 \leqslant p^{\frac{m}{2}(n-2)}$ for $m, n, p \geqslant 2$, thus we can get

$$\begin{aligned}
1 &< p_{M_g}(s_0) \leqslant l_0(n-1) \\
&\leqslant (p^m-1)(p^{un}-1)(n-1) \\
&< p^m(p^{m+\frac{m}{2}n}-1)(n-1) \\
&< p^{m+\frac{m}{2}n+\frac{m}{2}(n-2)} - 1 \\
&= p^{mn} - 1.
\end{aligned}$$

then the linear feedback shift register sequence generated by $g(x)$ and the initial state s_0 has period smaller than $p^{mn}-1$, so the linear feedback shift register is not primitive, and then according to lemma 2.1, $g(x) = x^n + \alpha x^{n-1} + \beta$ is not primitive. □

Proof of Corollary 1.1. Since for any $\lambda \in \mathbb{F}_{p^m}^*$, we have $\lambda^{p^m-1} = 1$, and according to the condition that $n \equiv 1 \mod (p^m-1)$, then $\lambda^{n-1} = 1 \in \mathbb{F}_{p^u}^*$, and for any $j \in \mathbb{F}_{p^u}^*$, j^n still belongs to $\mathbb{F}_{p^u}^*$, therefore, $\lambda^{1-n} j^n \in \mathbb{F}_{p^u}^*$. Thus by theorem 1.1, we have $g(x) = x^n + jx + \lambda (j \in \mathbb{F}_{p^u}^*)$ is not primitive, i.e., there are no primitive trinomials of the form $x^n + jx + \lambda (j \in \mathbb{F}_{p^u}^*)$ over finite field $\mathbb{F}_{p^m}$ if $n \equiv 1 \mod (p^m-1)$. □

Proof of theorem 1.2. For trinomial $x^n + x + \alpha$, by lemma 2.3, we also consider its reciprocal polynomial $g(x) = x^n + \alpha^{-1}x^{n-1} + \alpha^{-1}$. By lemma 2.2, we only need consider the case α^{-1} is a primitive element of $\mathbb{F}_4$. If α^{-1} is a primitive element of $\mathbb{F}_4$, then α^{-1} satisfies $\alpha^{-2} + \alpha^{-1} + 1 = 0$. For $n \equiv 1 \mod 3$, it is the particular case of corollary 1.1 with $m = 2, p = 2$, so the proof is omitted. For $n \equiv 0 \mod 3$, let $n = 3z$, the trinomial $x^n + x + \alpha = x^{3z} + x + \alpha$. It is easy to verify that $\alpha + 1$ is one solution of $x^{3z} + x + \alpha$ over $\mathbb{F}_4$, then it is not primitive over $\mathbb{F}_4$. For $n \equiv 4 \mod 5$, let x_0 be any nonzero element of $\mathbb{F}_4$ and $\nu = (x_0, x_0, \alpha^{-1}x_0, 0, \alpha^{-1}x_0), s_0 = (\nu, \nu, \ldots, \nu, x_0, x_0, \alpha^{-1}x_0, 0)$. For simple calculation using linear recurrence (1), we can have

$5 = p_{M_g(s_0)} < 2^{2n} - 1$. So for $n \equiv 1 \mod 3$, $n \equiv 0 \mod 3$, $n \equiv 4 \mod 5$ and for any $\alpha \in \mathbb{F}_{p^m}^*$, there is always some initial state such that the sequence generated by $x^n + \alpha^{-1}x^{n-1} + \alpha^{-1}$ and this initial state has period smaller than $2^{2n} - 1$, thus there are no primitive trinomials of the form $x^n + x + \alpha$ over finite field $\mathbb{F}_4$ under the conditions of $n \equiv 1 \mod 3$, $n \equiv 0 \mod 3$ and $n \equiv 4 \mod 5$. □

References

[1] Deschamps, J.P., Imana, J.L., Sutter, G.D.: Hardware Implementation of Finite-Field Arithmetic. McGraw-Hill, 2009.

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

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

[4] 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.

[5] Lidl R., Neiderreiter, Finite Fields, Cambridge University Press, Cambridge (1997).

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

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

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