Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

Research Article

Two Classes of Irreducible Polynomials over Finite Fields

Wensi An, Hongfeng Wu*

College of Science, North China University of Technology, Beijing 100144, China
E-mail: whfmath@ncut.edu.cn

Received: 25 July 2025; **Revised:** 7 November 2025; **Accepted:** 24 November 2025

Abstract: Let p be a prime, q be a power of p and t be a positive integer. In this paper, we construct stable polynomials of the form $(X+\zeta)^t-\zeta \in \mathbb{F}_q[X]$ over $\mathbb{F}_q$ by Capelli's lemma. We also solve the problem by establishing equivalent conditions for the irreducibility of the trinomial $X^{p^t}+mX+s \in \mathbb{F}_q[X]$, thereby characterizing its inverse stability over $\mathbb{F}_q$. Moreover, when p is odd and $t>s\geq 0$, we prove that the trinomial $X^{p^t}+aX^{p^s}+b \in \mathbb{F}_q[X]$ is not stable over $\mathbb{F}_q$.

Keywords: stable polynomials, finite fields, irreducible polynomials, sequences over finite fields

MSC: 11T06, 11B37, 11L40, 12E20

1. Introduction

Finding stable polynomials and inversely stable polynomials is an efficient way to construct irreducible polynomials over finite fields [1–5]. To define these two classes of polynomials, iteration is a key ingredient. Let p be a prime, and $q=p^e$, $e\in\mathbb{N}$. We define the sequence of iterations of $f(X)\in\mathbb{F}_q[X]$:

$$f^{(0)}(X)=X, \quad f^{(n)}(X)=f\left(f^{(n-1)}(X)\right), \quad n=1,\,2,\,\ldots.$$

Following [6], we say that $f(X)$ is stable if all polynomials $f^{(n)}(X)$ are irreducible over $\mathbb{F}_q$. The study of the stability of polynomials has attracted much attention (see for example, [1, 5–7]). However, we only have a few results. In 1985, Odoni [7] obtained that if p and ζ satisfy certain conditions, then $(X+\zeta)^p-\zeta$ is stable over $\mathbb{F}_q$. In [6], Ahmadi et al. obtained that there are no stable shifted linearised polynomials over finite fields, which leads to the conclusion that there are no stable quadratic polynomials over finite fields of characteristic 2. In the same year, Jones and Boston [8] proved the stability of quadratic polynomials over finite fields of odd characteristic. Lin and Wang [9] constructed stable polynomials of the form $b^{m-1}(X+a)^m+c(X+a)+d$ over the finite field $\mathbb{F}_q$ for $m=2,\,3,\,4$. In particular, when constructing stable polynomials for $m=4$, these authors make use of the X^4-b stable equivalence condition. Recently, in [10], the authors studied the stability of the binomials X^t-b over $\mathbb{F}_q$.

DOI: https://doi.org/10.37256/cm.7320267952

For inversely stable polynomials. First, let $\psi(X)$ be an arbitrary polynomial in $\mathbb{F}_q[X]$, and define $\Psi(X) = \dfrac{1}{\psi(X)}$. Let $\Psi^{(n)}(X) = \dfrac{\mu_n(X)}{\omega_n(X)}$ where $\mu_n(X)$ and $\omega_n(X)$ are coprime polynomials over $\mathbb{F}_q$ with $\omega_n(X)$ monic. Then $\psi(X)$ is an inversely stable polynomial over $\mathbb{F}_q$ if $\omega_n(X)$ is irreducible and distinct over $\mathbb{F}_q$ for each n. In 2023, Cheng introduced the concept of inversely stable polynomials and constructed a class of inversely stable polynomials of the form $X^p - X + s \in \mathbb{F}_p[X]$ [11]. There was also an open question. This open problem is to determine the identity of $X^{p^t} + mX + s \in \mathbb{F}_q[X]$ that is inversely stable over $\mathbb{F}_q$, where t is a positive integer. Last year Cheng discussed in detail the case that $e \geq t = 1$ and $m = -1$ [2]. Furthermore, when $e = t \geq 2$, Theorems 5.2.2 and 5.2.3 in [12] imply that $\psi(X)$ can never be inversely stable over $\mathbb{F}_q$ for any $m,\ s \in \mathbb{F}_q$.

The present paper concludes with two main parts. First, we address the stability of the polynomials of the form $f(X) = (X+\zeta)^t - \zeta$, in the cases where t is odd and where t is even, respectively. It turns out that under the condition of ensuring that $f(X)$ is irreducible, $f(X)$ is "not far" from being stable. To be explicit, if t is odd, being stable is exactly equivalent to being irreducible; while if t is even, $f(X)$ is stable if and only if it is irreducible and $-\zeta$ is rad(t)-free. These results are contained in Section 3.

In Section 4, we completely solve the open problem proposed by Cheng [11], which requires to characterizing the inverse stability of the class of polynomials $X^{p^t} + mX + s \in \mathbb{F}_q[X]$. The cases that $t = 1$ and $t \geq 2$ are treated separately. It is worth noting that in the discussion of the cases, we prove the following proposition (i.e., Proposition 3):

Proposition 1 Let $f(X) = X^{p^t} + mX + s$ be an irreducible polynomial over $\mathbb{F}_q$, with a zero γ in $\overline{\mathbb{F}_q}$. For any $a,\ b,\ c,\ d \in \mathbb{F}_q$ with c and d not both zero, the following statements hold:

(i) If $c = 0$, then $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = 0$ if $p \geq 3$, $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = \dfrac{a}{d}\cdot m$ if $p = 2$, $t = 1$ and $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = 0$ if $p = 2,\ t \geq 2$;

(ii) If $c \neq 0$, then

$$\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a\gamma+b}{c\gamma+d}\right) = \frac{m(ad-bc)}{c^2\left(s - \left(\dfrac{d}{c}\right)^{p^t} - m\cdot\dfrac{d}{c}\right)}.$$

Let m and s be nonzero elements in $\mathbb{F}_q$, such that there exists a $m_0 \in \mathbb{F}_q^*$ satisfying $m = -m_0^{p^t-1}$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\dfrac{s}{m_0^{p^t}}\right) \neq 0$. Define three sequences $\{a_n\}$, $\{c_n\}$ and $\{d_n\}$ in $\mathbb{F}_q$ as follows:

(1) $a_1 = s$, $a_2 = m$, and $a_{n+1} = ma_nd_n$ for $n \geq 2$;

(2) $c_1 = 1$, $c_2 = s$, and $c_{n+1} = c_n^2\left(s - \left(\dfrac{d_n}{c_n}\right)^{p^t} - m\cdot\dfrac{d_n}{c_n}\right)$ for $n \geq 2$;

(3) $d_1 = 0$, $d_2 = -1$, and $d_{n+1} = -c_n^2$ for $n \geq 2$.

To see that the sequence $\{c_n\}$ is well-defined, one needs to check that $c_n \neq 0$ for all $n \in \mathbb{N}^+$. The leading terms c_1 and c_2 are clearly nonzero. Suppose that $c_n \neq 0$ for some $n \geq 2$. If $c_{n+1} = 0$, then $s - \left(\dfrac{d_n}{c_n}\right)^{p^t} - m\cdot\dfrac{d_n}{c_n} = 0$, which implies that

$$\frac{s}{m_0^{p^t}} = \left(\frac{d_n}{m_0c_n}\right)^{p^t} - \frac{d_n}{m_0c_n}.$$

This is a contradiction with the condition that $\mathrm{Tr}_{\mathbb{F}_q}\left(\dfrac{s}{m_0^{p^t}}\right) \neq 0$. Then by induction the c_n's are nonzero.

We present a concrete criterion for $X^{p^t}+mX+s$ to be inversely stable over $\mathbb{F}_q$. The main result of Section 4 can be summarized into the following theorem (i.e., Theorem 7).

Theorem 1 Let p be a prime and $q=p^e$ with a positive integer e. Let $\psi(X)=X^{p^t}+mX+s\in\mathbb{F}_q[X]$ with t being a positive integer.

When $t=1$, $\psi(X)$ is inversely stable over $\mathbb{F}_q$ if and only if the following hold:

(i) there exists $m_0\in\mathbb{F}_q^*$ such that $m=-m_0^{p-1}$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^p}\right)\neq 0$;

(ii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^p c_n}\right)\neq 0$ for any positive integer n, where the sequences $\{a_n\}$, $\{c_n\}$ are defined as in Section 4.

When $t\geq 2$, $\psi(X)$ is inversely stable over $\mathbb{F}_q$ if and only if the following hold:

(i) $p=t=2$ and $2\nmid e$;

(ii) there exists $m_0\in\mathbb{F}_q^*$ such that $m=m_0^3$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^4}\right)\neq 0$;

(iii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^4 c_n}\right)\neq 0$ for any positive integer n, where the sequences $\{a_n\}$, $\{c_n\}$ are defined as in Section 4.

In Section 5, we prove that if $\mathbb{F}_q$ is of odd characteristic p, then no polynomial of the form $X^{p^t}+aX^{p^s}+b$ is stable over $\mathbb{F}_q$.

2. Preliminaries

Let p be a prime number, and q be a power of p. Let $\mathbb{F}_q$ be a finite field with q elements. We denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements in $\mathbb{F}_q$.

Let n be a positive integer. For $\alpha\in\mathbb{F}_{q^n}$, the trace and the norm of α over $\mathbb{F}_q$ are defined respectively by

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=\sum_{i=0}^{n-1}\alpha^{q^i},$$

and

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=\prod_{i=0}^{n-1}\alpha^{q^i}.$$

In particular, the trace and the norm of α over the prime field $\mathbb{F}_p$ are called the absolute trace and the absolute norm of α, and are denoted simply by $\mathrm{Tr}_{\mathbb{F}_{q^n}}(\alpha)$ and $\mathrm{N}_{\mathbb{F}_{q^n}}(\alpha)$, respectively.

Lemma 1 [13] Let $\alpha\in\mathbb{F}_{q^n}$ and the minimal polynomial of α over $\mathbb{F}_q$ be

$$m(X)=X^d+c_1X^{d-1}+\cdots+c_d.$$

Then

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=-\frac{n}{d}\cdot c_1,\ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=(-1)^n c_d^{\frac{n}{d}}.$$

Let $f(X)=a_0+a_1X+\cdots+a_nX^n\in\mathbb{F}_q[X]$ with $a_0a_n\neq 0$. The reciprocal polynomial of $f(X)$ is defined by

$$\widetilde{f}(X) = X^n f\left(\frac{1}{X}\right) = a_0X^n + a_1X^{n-1} + \cdots + a_n.$$

It is obvious to see that $\widetilde{\widetilde{f}(X)} = f(X)$, and $f(X)$ is irreducible over $\mathbb{F}_q$ if and only if $\widetilde{f}(X)$ is.

Let m be a positive integer dividing $q-1$. A nonzero element α in $\mathbb{F}_q$ is said to be m-free if for any divisor d of m the equality $\alpha = \beta^d$ with $\beta \in \mathbb{F}_q$ implies that $d = 1$. For any positive integer n, denote by $\mathrm{rad}(n)$ the radical of n, i.e., the product of the distinct prime divisors of n. The following result is well-known.

Lemma 2 [10] Let t be a positive integer such that $\mathrm{rad}(t) \mid q-1$. Then an element $\alpha \in \mathbb{F}_{q^n}$ is $\mathrm{rad}(t)$-free if and only if $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ is $\mathrm{rad}(t)$-free in $\mathbb{F}_q$.

In the following, we list some criteria on the irreducibility of certain classes of polynomials over $\mathbb{F}_q$.

Lemma 3 [10] Let $t \geq 2$ be an integer and $\zeta \in \mathbb{F}_q^*$. Then the binomial $X^t - \zeta$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

(i) $\mathrm{rad}(t) \mid q-1$;

(ii) ζ is $\mathrm{rad}(t)$-free; and

(iii) $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.

Lemma 4 [13] For $a,\ b \in \mathbb{F}_q^*$, the trinomial $X^p - aX - b$ is irreducible over $\mathbb{F}_q$ if and only if $a = a_0^{p-1}$ for some $a_0 \in \mathbb{F}_q^*$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{b}{a_0^p}\right) \neq 0$.

Recall that a polynomial $L(X)$ in the form

$$L(X) = \sum_{i=0}^{v} l_i X^{p^i},\ l_i \in \mathbb{F}_q,$$

is called a linearized polynomial over $\mathbb{F}_q$. If $L(X)$ is a linearized polynomial and $b \in \mathbb{F}_q^*$, then $A(X) = L(X) - b$ is called an affine polynomial over $\mathbb{F}_q$. The criterion for an affine polynomial to be irreducible is given below.

Lemma 5 [13] Let $L(X) = \sum_{i=0}^{v} l_i X^{p^i}$ be a monic linearized polynomial over $\mathbb{F}_q$, where $v \geq 2$, and $A(X) = L(X) - b$, $b \in \mathbb{F}_q^*$, be an affine polynomial. Then $A(X)$ is irreducible over $\mathbb{F}_q$ if and only if $p = v = 2$ and $L(X)$ is of the form

$$L(X) = X(X + a_0)(X^2 + a_0X + b_0),$$

where $a_0,\ b_0 \in \mathbb{F}_q^*$ and the quadratic polynomials $X^2 + a_0X + b_0$ and $X^2 + b_0X + b$ are both irreducible over $\mathbb{F}_q$.

Finally, we record the Capelli's lemma, which characterizes the irreducibility of composed polynomials.

Lemma 6 [1, 10] (Capelli's lemma) Let K be a field, f and g be polynomials over K, and $\beta \in \overline{K}$ be any zero of g. The composed polynomial $g(f)$ is irreducible over K if and only if g is irreducible over K and $f - \beta$ is irreducible over $K(\beta)$.

At the end of this section we recall the sequence of iteration associated with a fraction of polynomials, and the definitions of stable polynomial and of inversely stable polynomial. Let $\varphi(X) = \dfrac{f(X)}{g(X)}$ where $f(X)$ and $g(X)$ are coprime polynomials over $\mathbb{F}_q$ with $g(X) \neq 0$. The sequence of iteration associated with $\varphi(X)$ is defined recurrently by

$$\varphi^{(n)}(X) = \varphi\left(\varphi^{(n-1)}(X)\right),\ n = 1,\ 2,\ \cdots,$$

with the leading term $\varphi^{(0)}(X) = X$. Clearly, every term in this sequence is a fraction of polynomials over $\mathbb{F}_q$.

Definition 1 (1) A polynomial $f(X)$ over $\mathbb{F}_q$ is said to be stable if all the terms $f^{(n)}(X)$ in the sequence of iteration associated with $f(X)$ are irreducible over $\mathbb{F}_q$.

(2) Let $f(X)$ be a nonzero polynomial over $\mathbb{F}_q$, and $F(X) = \dfrac{1}{f(X)}$. Let $F^{(n)}(X) = \dfrac{h_n(X)}{g_n(X)}$ where $h_n(X)$ and $g_n(X)$ are coprime polynomials over $\mathbb{F}_q$ with $g_n(X)$ monic. Then $f(X)$ is said to be inversely stable if all the terms $g_n(X)$ are pairwise distinct and irreducible.

Remark 1 Lemma 1 is applied in the proof of Proposition 3; Lemmas 2 and 3 are mainly used to establish Theorems 2 and 3; Lemma 4 contributes to the proof of Theorem 4; Lemma 5 is employed in the proofs of Theorem 5, Proposition 4, and Theorems 6, 8, and 9; Lemma 6 is also used in the proofs of Theorems 2 and 3.

Example 1 Let $q = 3$ and $f(X) = X^2 + X + 1$. Over $\mathbb{F}_q$, we have:

$$\begin{aligned}
f^{(2)}(X) =& X^4 + 2X^3 + X^2,\\
f^{(3)}(X) =& X^8 + X^7 + X^5 + 2X^4 + 2X^3 + X^2 + 1,\\
f^{(4)}(X) =& X^{16} + 2X^{15} + X^{14} + 2X^{13} + 2X^{11} + X^{10} + 2X^8 + X^7 + 2X^6 + X^5 + X^4,\\
f^{(5)}(X) =& X^{32} + X^{31} + 2X^{29} + 2X^{27} + 2X^{26} + 2X^{25} + 2X^{24}\\
&+ 2X^{23} + X^{22} + X^{19} + 2X^{18} + 2X^{17} + X^{16} + X^{13}\\
&+ X^{12} + 2X^{11} + 2X^9 + X^7 + 2X^6 + X^5 + X^4 + 1.
\end{aligned}$$

3. Stable polynomials of the form $(X+\zeta)^t - \zeta$

In this section we completely determine the stable polynomials of the form $f(X) = (X+\zeta)^t - \zeta$ over $\mathbb{F}_q$. If $t = 1$, then $f(X) = X$ is clearly not stable. In the following context we assume that $t \geq 2$. We treat the cases where t is odd and where t is even separately.

Let $f(X) = (X+\zeta)^t - \zeta \in \mathbb{F}_q[X]$. The change of variables $Y = X + \zeta$ yields $f(X) = Y^t - \zeta$, which implies that $f(X)$ is irreducible over $\mathbb{F}_q$ if and only if $Y^t - \zeta$ is. Using Lemma 3 we obtain the following conclusion.

Lemma 7 Let $t \geq 2$ be an integer and $\zeta \in \mathbb{F}_q^*$. Then the polynomial $(X+\zeta)^t - \zeta$ is irreducible over $\mathbb{F}_q$ if and only if the following conditions are satisfied:

(i) $\mathrm{rad}(t) \mid q-1$;

(ii) ζ is $\mathrm{rad}(t)$-free; and

(iii) $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.

Now we prove the main theorems in this section. First we consider the case where t is odd.

Theorem 2 Let $f(X) = (X+\zeta)^t - \zeta \in \mathbb{F}_q[X]$, where $t \geq 2$ is odd. Then $f(X)$ is stable over $\mathbb{F}_q$ if and only if the following conditions hold:

(i) $\mathrm{rad}(t) \mid q-1$;

(ii) ζ is $\mathrm{rad}(t)$-free.

Therefore, $f(X)$ is stable over $\mathbb{F}_q$ if and only if $f(X)$ is irreducible over $\mathbb{F}_q$.

Proof. Suppose that $f(X)$ is stable over $\mathbb{F}_q$, then it is automatically irreducible over $\mathbb{F}_q$. By Lemma 7 the conditions (i) and (ii) hold.

Conversely, suppose that (i) and (ii) are satisfied. If $f(X)$ is not stable over $\mathbb{F}_q$, there exists a minimal positive integer n such that $f^{(n)}(X)$ is reducible over $\mathbb{F}_q$. Since $f(X)$ is irreducible, $n \geq 2$. Let α_n be a zero of $f^{(n)}(X)$ lying in $\overline{\mathbb{F}_q}$. For $0 \leq i \leq n-1$ we define $\alpha_i = f^{(n-i)}(\alpha_n)$ and

$$f_i(X) = f(X) - \alpha_i = (X+\zeta)^t - (\alpha_i + \zeta).$$

It is straightforward to check that for any $0 \leq i \leq n-1$, α_i is a zero of $f^{(i)}(X)$, and $f(\alpha_{i+1}) = \alpha_i$. Thus α_{i+1} is a zero of $f_i(X)$.

We claim that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{n-1}) = \mathbb{F}_{q^{t^{n-1}}}$. As $f(\alpha_1) = f_0(\alpha_1) = 0$ and $f(X)$ is irreducible over $\mathbb{F}_q$, then

$$\mathbb{F}_q(\alpha_1) \simeq \mathbb{F}_q[X]/(f(X)) = \mathbb{F}_{q^t}.$$

Suppose that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{k-1}) = \mathbb{F}_{q^{t^{k-1}}}$ for $k \leq n-1$. Since $f^{(k)}(X)$ is irreducible over $\mathbb{F}_q$, by Capelli's lemma (Lemma 6) $f_{k-1}(X) = f(X) - \alpha_{k-1}$ is irreducible over $\mathbb{F}_{q^{t^{k-1}}}$. As α_k is a zero of $f_{k-1}(X)$, then it holds that

$$\mathbb{F}_q(\alpha_k) = \mathbb{F}_q(\alpha_1, \cdots, \alpha_k) = \mathbb{F}_{q^{t^{k-1}}}(\alpha_k) \simeq \mathbb{F}_{q^{t^{k-1}}}[X]/(f_{k-1}) = \mathbb{F}_{q^{t^k}}.$$

By induction one obtains that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{n-1}) = \mathbb{F}_{q^{t^{n-1}}}$.

Now as $f^{(n)}(X)$ is reducible and $f^{(n-1)}(X)$ is irreducible over $\mathbb{F}_q$, by Capelli's lemma the polynomial $f_{n-1}(X) = f(X) - \alpha_{n-1}$ is reducible over $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{n-1}) = \mathbb{F}_{q^{t^{n-1}}}$. Thus one obtains from Lemma 3 that $\alpha_{n-1} + \zeta \in \mathbb{F}_{q^{t^{n-1}}}$ is not $\mathrm{rad}(t)$-free, and from Lemma 2 that $\mathrm{N}_{\mathbb{F}_{q^{t^{n-1}}}/\mathbb{F}_q}(\alpha_{n-1}+\zeta)$ is not $\mathrm{rad}(t)$-free. By definition

$$\mathrm{N}_{\mathbb{F}_{q^{t^{n-1}}}/\mathbb{F}_q}(\alpha_{n-1}+\zeta) = (\alpha_{n-1}+\zeta)(\alpha_{n-1}+\zeta)^q \cdots (\alpha_{n-1}+\zeta)^{q^{t^{n-1}-1}}$$

$$= (\zeta + \alpha_{n-1})(\zeta + \alpha_{n-1}^q) \cdots (\zeta + \alpha_{n-1}^{q^{t^{n-1}-1}}).$$

On the other hand, since $f^{(n-1)}(X)$ is irreducible and α_{n-1} is a zero of $f^{(n-1)}(X)$, then

$$f^{(n-1)}(X) = \prod_{j=0}^{t^{n-1}-1} (X - \alpha_{n-1}^{q^j}).$$

Notice that $f^{(n-1)}(-\zeta) = -\zeta$, thus we have that

$$\mathrm{N}_{\mathbb{F}_{q^{t^{n-1}}}/\mathbb{F}_q}(\alpha_{n-1}+\zeta) = (-1)^{t^{n-1}} f^{(n-1)}(-\zeta) = (-1)^{t^{n-1}+1}\zeta = \zeta,$$

which contradicts the condition that ζ is $\mathrm{rad}(t)$-free. It follows that $f(X)$ is stable over $\mathbb{F}_q$.

Next we turn to the case that t is even. □

Theorem 3 Let $f(X) = (X+\zeta)^t - \zeta \in \mathbb{F}_q[X]$, where $t \geq 2$ is even. Then $f(X)$ is stable over $\mathbb{F}_q$ if and only if the following conditions hold:

(i) $\mathrm{rad}(t) \mid q-1$;

(ii) both ζ and $-\zeta$ are $\mathrm{rad}(t)$-free; and

(iii) $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.

Therefore, $f(X)$ is stable over $\mathbb{F}_q$ if and only if $f(X)$ is irreducible over $\mathbb{F}_q$ and $-\zeta$ is $\mathrm{rad}(t)$-free.

Proof. By Lemma 7, $f(X)$ is irreducible over $\mathbb{F}_q$ if and only if conditions (i) and (ii) hold, and ζ is $\mathrm{rad}(t)$-free.

Let $f(X)$ be stable over $\mathbb{F}_q$. Then $f(X)$ is irreducible over $\mathbb{F}_q$. Thus conditions (i) and (iii) and ζ is $\mathrm{rad}(t)$-free hold. So we only need to check whether $-\zeta$ is $\mathrm{rad}(t)$-free. Let α be a zero of $f(X)$ over $\mathbb{F}_{q^t}$. Since $f(X)$ is stable, $f^{(2)}(X)$ is irreducible over $\mathbb{F}_q$. Using Capelli's lemma, we see that $f(X)-\alpha = (X+\zeta)^t - (\alpha+\zeta)$ is irreducible over $\mathbb{F}_{q^t}$. Thus one obtains from Lemma 3 that $\alpha+\zeta \in \mathbb{F}_{q^t}$ is $\mathrm{rad}(t)$-free, and from Lemma 2 that $\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha+\zeta)$ is $\mathrm{rad}(t)$-free. By definition

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha+\zeta) = (\alpha+\zeta)(\alpha+\zeta)^q \cdots (\alpha+\zeta)^{q^{t-1}}$$

$$= (-1)^t(-\alpha-\zeta)(-\alpha^q-\zeta)\cdots(-\alpha^{q^{t-1}}-\zeta).$$

On the other hand, since $f(X)$ is irreducible and α is a zero of $f(X)$, then

$$f(X) = \prod_{j=0}^{t-1}(X-\alpha^{q^j}).$$

Notice that $f(-\zeta) = -\zeta$, thus we have that

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha+\zeta) = (-1)^t f(-\zeta) = (-1)^{t+1}\zeta = -\zeta.$$

So condition (ii) also holds.

Conversely, let the polynomial $f(X)$ satisfy the conditions (i), (ii) and (iii). So $f(X)$ is irreducible over $\mathbb{F}_q$. Assume that $f(X)$ is not stable over $\mathbb{F}_q$, then there exists the smallest positive integer $n \geq 2$ such that $f^{(n)}(X)$ is reducible over $\mathbb{F}_q$. Let α_n be a zero of $f^{(n)}(X)$ lying in $\overline{\mathbb{F}_q}$. For $0 \leq i \leq n-1$ we define $\alpha_i = f^{(n-i)}(\alpha_n)$ and

$$f_i(X) = f(X) - \alpha_i = (X+\zeta)^t - (\alpha_i+\zeta).$$

It is straightforward to check that for any $0 \leq i \leq n-1$, α_i is a zero of $f^{(i)}(X)$, and $f(\alpha_{i+1}) = \alpha_i$. Then α_{i+1} is a zero of $f_i(X)$.

If $n = 2$, then $f^{(2)}(X)$ is reducible over $\mathbb{F}_q$. Since $f(X)$ is irreducible over $\mathbb{F}_q$ and $f(\alpha_1) = 0$, we have that $\alpha_1 \in \mathbb{F}_{q^t}$ and $f_1(X) \in \mathbb{F}_{q^t}[X]$. By Capelli's lemma, $f_1(X)$ is reducible over $\mathbb{F}_{q^t}$. Since conditions (i) and (iii) hold. Using Lemma 2 and Lemma 3, we can see that $\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha_1+\zeta)$ is not $\mathrm{rad}(t)$-free. By definition

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha_1+\zeta) = (\alpha_1+\zeta)(\alpha_1+\zeta)^q \cdots (\alpha_1+\zeta)^{q^{t-1}}$$

$$= (-1)^t(-\alpha_1 - \zeta)(-\alpha_1^q - \zeta)\cdots(-\alpha_1^{q^{t-1}} - \zeta).$$

Moreover, since $f(X)$ is irreducible and α_1 is a zero of $f(X)$, then

$$f(X) = \prod_{j=0}^{t-1}(X - \alpha_1^{q^j}),$$

so that

$$\mathrm{N}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha_1 + \zeta) = (-1)^t f(-\zeta) = (-1)^{t+1}\zeta = -\zeta,$$

which contradicts the condition that $-\zeta$ is rad(t)-free. Then only the case $n-1 \geq 2$ needs to be considered.

If $n-1 \geq 2$, by the minimality of n, $f^{(i)}(X)$ is irreducible over $\mathbb{F}_q$ for any $1 \leq i \leq n-1$. We claim that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{n-1}) = \mathbb{F}_{q^{t^{n-1}}}$. As $f(\alpha_1) = f_0(\alpha_1) = 0$ and $f(X)$ is irreducible over $\mathbb{F}_q$, then

$$\mathbb{F}_q(\alpha_1) \simeq \mathbb{F}_q[X]/(f(X)) = \mathbb{F}_{q^t}.$$

Suppose that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{k-1}) = \mathbb{F}_{q^{t^{k-1}}}$ for $k \leq n-1$. Since $f^{(k)}(X)$ is irreducible over $\mathbb{F}_q$, by Capelli's lemma $f_{k-1}(X) = f(X) - \alpha_{k-1}$ is irreducible over $\mathbb{F}_{q^{t^{k-1}}}$. As α_k is a zero of $f_{k-1}(X)$, then it holds that

$$\mathbb{F}_q(\alpha_k) = \mathbb{F}_q(\alpha_1, \cdots, \alpha_k) = \mathbb{F}_{q^{t^{k-1}}}(\alpha_k) \simeq \mathbb{F}_{q^{t^{k-1}}}[X]/(f_{k-1}) = \mathbb{F}_{q^{t^k}}.$$

By induction one obtains that $\mathbb{F}_q(\alpha_1, \cdots, \alpha_{n-1}) = \mathbb{F}_{q^{t^{n-1}}}$. Since $f^{(n)}(X)$ is reducible over $\mathbb{F}_q$, by Capelli's lemma, we see that $f_{n-1}(X)$ is reducible over $\mathbb{F}_{q^{t^{n-1}}}$. Thus it follows from Lemma 3 that $\alpha_{n-1} + \zeta \in \mathbb{F}_{q^{t^{n-1}}}$ is not rad(t)-free, and thus by Lemma 2, $\mathrm{N}_{\mathbb{F}_{q^{t^{n-1}}}/\mathbb{F}_q}(\alpha_{n-1} + \zeta)$ is not rad(t)-free.

On the other hand, since $f^{(n-1)}(X)$ is irreducible and α_{n-1} is a zero of $f^{(n-1)}(X)$, then

$$f^{(n-1)}(X) = \prod_{j=0}^{t^{n-1}-1}(X - \alpha_{n-1}^{q^j}).$$

Notice that $f^{(n-1)}(-\zeta) = -\zeta$, thus we have that

$$\mathrm{N}_{\mathbb{F}_{q^{t^{n-1}}}/\mathbb{F}_q}(\alpha_{n-1} + \zeta) = (\alpha_{n-1} + \zeta)(\alpha_{n-1} + \zeta)^q \cdots (\alpha_{n-1} + \zeta)^{q^{t^{n-1}-1}}$$

$$= (\alpha_{n-1} + \zeta)(\alpha_{n-1}^q + \zeta)\cdots(\alpha_{n-1}^{q^{t^{n-1}-1}} + \zeta)$$

$$= (-1)^{t^{n-1}} f^{(n-1)}(-\zeta)$$

$$= (-1)^{t^{n-1}+1}\zeta$$

$$= -\zeta,$$

which contradicts the condition that $-\zeta$ is rad(t)-free. Hence, no such n exists, proving that $f(X)$ is stable over $\mathbb{F}_q$. □

Example 2 Let $q = 7,\ t = 6,\ \zeta = 3$. For any element $\beta \in \mathbb{F}_7$, we have $\beta^2 \neq 3$ and $\beta^3 \neq 3$, and $\beta^6 = 1$. Thus, we obtain that 3 is rad(6)-free. Since $-3 = 4 = 2^2$, $-\zeta$ is not rad(6)-free. Let $f(X) = (X+\zeta)^t - \zeta$. By Lemma 7, $f(X) = (X+3)^6 - 3$ is irreducible over $\mathbb{F}_7$. We get

$$\begin{aligned} f^{(2)}(X) =& X^{36} + 3X^{35} + X^{29} + 3X^{28} + 6X^{22} + 4X^{21} + 4X^{15} + 5X^{14} + 6X^8 + 4X^7 + 5X + 5 \\ =& (X^{18} + 5X^{17} + 5X^{16} + 3X^{15} + 4X^{14} + 6X^{11} + 2X^{10} + 6X^8 + 6X^7 + 2X^4 + 3X^3 + 4X^2 + 5X + 5) \\ & \cdot (X^{18} + 5X^{17} + 5X^{16} + 3X^{15} + 4X^{14} + 6X^{11} + 2X^{10} + 4X^9 + 2X^8 + 2X^4 + 3X^3 + 2X^2 + 1). \end{aligned}$$

Thus, we know that $(X+3)^6 - 3$ is not stable over $\mathbb{F}_7$.

4. Inversely stable polynomials of the form $X^{p^t} + mX + s$

In [11], Cheng proposed the following problem:

Problem 1 Let p be a prime and $q = p^e$ with a positive integer e. Let $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$ with t being a positive integer. Determine when $\psi(X)$ is inversely stable over $\mathbb{F}_q$.

Cheng [11] provided a solution for the case $e = t = 1$, and later he dealt with the cases $e \geq t = 1$ and $m = -1$ in [2]. By Theorems 5.2.2 and 5.2.3 in [12], the polynomial $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$ is never inversely stable over $\mathbb{F}_q$ for $e = t \geq 2$. In this section, we consider the cases where $t = 1$ and where $t \geq 2$, respectively, and give a complete solution to Problem 1.

One easily checks that $\psi(X)$ is reducible over $\mathbb{F}_q$ if $s = 0$. From Lemma 3, $\psi(X)$ is also reducible over $\mathbb{F}_q$ if $m = 0$. Then $m,\ s \neq 0$ is a necessary condition for $\psi(X)$ to be irreducible over $\mathbb{F}_q$.

Let $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X],\ m,\ s \neq 0$, and $\Psi(X) = \dfrac{1}{\psi(X)}$. The fraction $\Psi(X)$ gives rise naturally to a map

$$\Psi : \overline{\mathbb{F}_q} \cup \{\infty\} \to \overline{\mathbb{F}_q} \cup \{\infty\}$$

as follows: For $\alpha \in \overline{\mathbb{F}_q}$, $\Psi(\alpha)$ is the evaluation of $\Psi(X)$ at α if α is not a zero of $\psi(X)$; while $\Psi(\alpha) = \infty$ if α is a zero of $\psi(X)$. And Ψ maps the point ∞ at infinity to 0. Moreover, for $n \geq 1$, the iteration $\Psi^{(n)}(X)$ induces a map $\Psi^{(n)}$ which is exactly the n-th power of Ψ.

Lemma 8 Assume that $\psi(X)$ has no zero in $\mathbb{F}_q$. Then for any positive integer n, $\Psi^{(n)}(0) \neq \infty$ and $\Psi^{(n)}(\infty) \neq \infty$.

Proof. Suppose that there exists a positive integer k such that $\Psi^{(k)}(0) = \infty$. By $\Psi(0) = s^{-1}$ and $\Psi^{(2)}(0) = \Psi(s^{-1}) \neq \infty$, we get $k > 2$. Observing further that $\Psi^{(k)}(0) = \Psi^{(k-1)}(s^{-1}) = \Psi(\Psi^{(k-2)}(s^{-1})) = \infty$, it is clear that $\Psi^{(k-2)}(s^{-1}) \in \mathbb{F}_q$, which combined with the fact that $\psi(X)$ has no zero in $\mathbb{F}_q$ yields a contradiction. Thus, for any positive integer n, we have $\Psi^{(n)}(0) \neq \infty$.

If there exists a positive integer k such that $\Psi^{(k)}(\infty) = \infty$. For $\Psi(\infty) = 0$, $k \geq 2$. Then we have $\Psi^{(k)}(\infty) = \Psi^{(k-1)}(0) = \infty$, a contradiction. So, for any positive integer n, $\Psi^{(n)}(\infty) \neq \infty$. □

Let n be any positive integer. Notice that $\Psi^{(n)}$ can be written as $\Psi^{(n)}(X) = \dfrac{\mu_n(X)}{\omega_n(X)}$ where $\mu_n(X)$ and $\omega_n(X)$ are coprime polynomials over $\mathbb{F}_q$ with $\omega_n(X)$ monic. Then, we obtain the following important proposition for $\Psi(X)$ and $\psi(X)$.

Proposition 2 Let $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$, where $m, s \neq 0$. Consider the mapping from $\overline{\mathbb{F}_q} \cup \{\infty\}$ to itself $\Psi(X) = \dfrac{1}{\psi(X)}$. The following statements hold:

(i) For any point γ other than 0 in $\overline{\mathbb{F}_q} \cup \{\infty\}$, the preimage $\Psi^{-1}(\gamma)$ contains p^t points.

(ii) For any positive integer n, if $\psi(X)$ has no zero in $\mathbb{F}_q$, then $\omega_n(X) \in \mathbb{F}_q[X]$ and its degree is p^{tn}.

Proof. Clearly, since the map $\Psi(X) = \dfrac{1}{\psi(X)}$ is $\overline{\mathbb{F}_q} \cup \{\infty\}$ to itself, the preimage of 0 is ∞. Let $\gamma \neq 0$ be any element of $\overline{\mathbb{F}_q}$. Since $gcd\left(\psi(X) - \dfrac{1}{\gamma}, \psi'(X)\right) = 1$, this means that $\Psi(X) = \gamma$ has p^t distinct zeros in $\overline{\mathbb{F}}_q$. So (i) holds.

Prove (ii) below. First, it is easy to see that $\omega_n(X) \in \mathbb{F}_q[X]$, and $deg(\omega_n(X)) \leq p^{tn}$. Next prove that $deg(\omega_n(X)) = p^{tn}$. We first define n sets:

$$\left(\Psi^{(i)}\right)^{-1}(\infty) := \left\{\alpha \in \overline{\mathbb{F}_q} \cup \{\infty\} : \Psi^{(i)}(\alpha) = \infty\right\}, 1 \leq i \leq n.$$

Then Lemma 8 shows that $\infty \notin \left(\Psi^{(i)}\right)^{-1}(\infty)$ for any $i (1 \leq i \leq n)$. And it follows from (i) that $\left|\left(\Psi^{(1)}\right)^{-1}(\infty)\right| = p^t$.

Next we consider the number of α satisfying $\Psi^{(i+1)}(\alpha) = \infty$. Let $\Psi^{(i+1)}(\alpha) = \infty$, $\Psi(\alpha) = \beta$, then $\Psi^{(i)}(\beta) = \infty$, and based on the definition of the set above, we can see that the number of β's that satisfy this equation is $\left|\left(\Psi^{(i)}\right)^{-1}(\infty)\right|$. By Lemma 8, we know that $\beta \neq 0, \infty$. Thus, combined with (i) it can be shown that for any $i (1 \leq i \leq n-1)$

$$\left|\left(\Psi^{(i+1)}\right)^{-1}(\infty)\right| = p^t \left|\left(\Psi^{(i)}\right)^{-1}(\infty)\right|.$$

This means that $\left|\left(\Psi^{(n)}\right)^{-1}(\infty)\right| = p^{tn}$. Thus $\omega_n(X)$ has p^{tn} distinct zeros in $\overline{\mathbb{F}_q}$, which in combination with $deg(\omega_n(X)) \leq p^{tn}$ shows that $deg(\omega_n(X)) = p^{tn}$. □

Proposition 3 Let $f(X) = X^{p^t} + mX + s$ be an irreducible polynomial over $\mathbb{F}_q$, with a zero γ in $\overline{\mathbb{F}_q}$. For any $a, b, c, d \in \mathbb{F}_q$ with c and d not both zero, the following statements hold:

(i) If $c = 0$, then $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = \dfrac{a}{d} \cdot m$ if $p = 2$, $t = 1$, $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = 0$ if $p = 2$, $t \geq 2$ and $\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\dfrac{a\gamma+b}{c\gamma+d}\right) = 0$ if $p \geq 3$;

(ii) If $c \neq 0$, then

$$\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a\gamma+b}{c\gamma+d}\right) = \frac{m(ad-bc)}{c^2\left(s - \left(\dfrac{d}{c}\right)^{p^t} - m \cdot \dfrac{d}{c}\right)}.$$

Proof. (i) Since $f(X)$ is irreducible, $\mathbb{F}_q(\gamma) \simeq \mathbb{F}_q[X]/(f(X)) = \mathbb{F}_{q^{p^t}}$, and therefore

$$\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a\gamma+b}{d}\right) = \frac{a}{d} \cdot \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}(\gamma) + p^t \cdot \frac{b}{d}$$

$$= \begin{cases} \frac{a}{d} \cdot m, & \text{if } p = 2,\ t = 1; \\ 0, & \text{if } p = 2,\ t \geq 2; \\ 0, & \text{if } p \geq 3. \end{cases}$$

(ii) By the same argument we have that $\mathbb{F}_q(\gamma) = \mathbb{F}_{q^{p^t}}$. Then by the linearity of trace it holds that

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a\gamma+b}{c\gamma+d}\right) &= \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a}{c} + \frac{bc^{-1}-adc^{-2}}{\gamma+c^{-1}d}\right) \\ &= p^t \cdot \frac{a}{c} + \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{bc^{-1}-adc^{-2}}{\gamma+c^{-1}d}\right) \\ &= c^{-2}(bc-ad) \cdot \mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{1}{\gamma+c^{-1}d}\right). \end{aligned}$$

As $f(X)$ is irreducible, then

$$f\left(X - \frac{d}{c}\right) = X^{p^t} + mX + s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c},$$

is irreducible over $\mathbb{F}_q$ with a zero $\gamma + \frac{d}{c}$. In particular, $s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c} \neq 0$. It follows that the reciprocal polynomial

$$X^{p^t} f\left(\frac{1}{X} - \frac{d}{c}\right) = \left(s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c}\right) X^{p^t} + mX^{p^t-1} + 1,$$

of $f\left(X - \frac{d}{c}\right)$ is irreducible over $\mathbb{F}_q$ with zero $\left(\gamma + \frac{d}{c}\right)^{-1}$. Thus, $X^{p^t} + m\left(s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c}\right)^{-1} X^{p^t-1} + \left(s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c}\right)^{-1}$ is the minimal polynomial of $\left(\gamma + \frac{d}{c}\right)^{-1}$. Applying Lemma 1 we obtain that

$$\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{1}{\gamma+c^{-1}d}\right) = -m\left(s - \left(\frac{d}{c}\right)^{p^t} - m \cdot \frac{d}{c}\right)^{-1}.$$

Now the conclusion follows immediately. □

Example 3 When $p = 2,\ t = 1,\ q = 8$, Lemma 4 shows that $X^2 + X + 1$ is irreducible over $\mathbb{F}_q$. Let γ be a zero of $X^2 + X + 1$ over $\overline{\mathbb{F}_q}$. $\gamma + 1$ is also a zero of $X^2 + X + 1$, so $\gamma + 1$ is the conjugate of γ. By the definition of trace we get

$$\mathrm{Tr}_{\mathbb{F}_q(\gamma)/\mathbb{F}_q}\left(\frac{a\gamma+b}{c\gamma+d}\right)=\frac{a\gamma+b}{c\gamma+d}+\left(\frac{a\gamma+b}{c\gamma+d}\right)^q=\frac{a\gamma+b}{c\gamma+d}+\frac{a\gamma^q+b}{c\gamma^q+d}=\frac{a\gamma+b}{c\gamma+d}+\frac{a(\gamma+1)+b}{c(\gamma+1)+d}=\frac{ad+bc}{c^2+cd+d^2}.$$

We begin with the case that $t=1$.

Theorem 4 Let $\psi(X)=X^p+mX+s\in\mathbb{F}_q[X]$. Then ψ is inversely stable over $\mathbb{F}_q$ if and only if the following two conditions hold:

(i) there exists an $m_0\in\mathbb{F}_q^*$ such that $m=-m_0^{p-1}$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^p}\right)\neq 0$;

(ii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^p c_n}\right)\neq 0$ for any positive integer n, where sequences $\{a_n\},\ \{c_n\}$ are defined as above.

Proof. First, we recall that $\Psi^{(n)}$ can be written as $\Psi^{(n)}(X)=\frac{\mu_n(X)}{\omega_n(X)}$, where $\mu_n(X)$ and $\omega_n(X)$ are coprime polynomials over $\mathbb{F}_q$ with $\omega_n(X)$ monic. Let $\psi(X)$ be inversely stable over $\mathbb{F}_q$. Then for every $n\in\mathbb{N}$, $\omega_n(X)$ is irreducible over $\mathbb{F}_q$. So $m,\ s\neq 0$. Then, by Lemma 4, condition (i) holds.

Below we prove condition (ii). Let n be any positive integer. By Proposition 2, we know $deg(\omega_n(X))=p^n$. Let $\beta_n\in\overline{\mathbb{F}}_q$ be a zero of $\omega_n(X)$. Thus, $p^n=[\mathbb{F}_q(\beta_n):\mathbb{F}_q]$. For each $1\leq i\leq n-1$, define $\beta_i:=\Psi^{(n-i)}(\beta_n)$. One finds that

$$\beta_1{}^p+m\beta_1+s=0, \tag{1}$$

and for $i\geq 2$

$$\beta_i^p+m\beta_i+\frac{s\beta_{i-1}-1}{\beta_{i-1}}=0. \tag{2}$$

The finite field sequence, denoted by $\{K_i\}_{i=0}^n$, is to be defined as

$$K_0:=\mathbb{F}_q,\ K_i:=K_0(\beta_1,\ \beta_2,\ \cdots,\ \beta_i),\ 1\leq i\leq n.$$

Let $h_1(X)=X^p+mX+s$ and $h_i(X)=X^p+mX+\frac{s\beta_{i-1}-1}{\beta_{i-1}}$ $(2\leq i\leq n)$. Clearly, $h_i(X)\in K_{i-1}[X]$ and $h_i(\beta_i)=0$, $1\leq i\leq n$. It follows that $[K_i:K_{i-1}]\leq p$, $1\leq i\leq n$. Considering the conclusion drawn above, we get that

$$p^n=[\mathbb{F}_q(\beta_n):\mathbb{F}_q]=[K_n:K_0]=\prod_{i=1}^n[K_i:K_{i-1}]\leq p^n.$$

So $[K_i:K_{i-1}]=p$ for any $1\leq i\leq n$. It implies that $h_i(X)$ is irreducible over K_{i-1} for each $1\leq i\leq n$. Thus $h_n(X)=X^p+mX+\frac{s\beta_{n-1}-1}{\beta_{n-1}}$ is irreducible over K_{n-1}. By Lemma 4, we have that

$$\mathrm{Tr}_{K_{n-1}}\left(\frac{s\beta_{n-1}-1}{m_0^p\beta_{n-1}}\right)\neq 0.$$

Let $\{a_n\},\ \{c_n\}$ and $\{d_n\}$ be the sequences over $\mathbb{F}_q$ defined as above. By iterative use of Proposition 3, we then get

$$\mathrm{Tr}_{K_{n-1}/K_{n-2}}\left(\frac{s\beta_{n-1}-1}{m_0^p\beta_{n-1}}\right)=\frac{1}{m_0^p}\cdot\frac{a_2\beta_{n-2}}{c_2\beta_{n-2}+d_2},$$

$$\mathrm{Tr}_{K_{n-2}/K_{n-3}}\left(\frac{1}{m_0^p}\cdot\frac{a_2\beta_{n-2}}{c_2\beta_{n-2}+d_2}\right)=\frac{1}{m_0^p}\cdot\frac{a_3\beta_{n-3}}{c_3\beta_{n-3}+d_3},$$

$$\vdots$$

$$\mathrm{Tr}_{K_2/K_1}\left(\frac{1}{m_0^p}\cdot\frac{a_{n-2}\beta_2}{c_{n-2}\beta_2+d_{n-2}}\right)=\frac{1}{m_0^p}\cdot\frac{a_{n-1}\beta_1}{c_{n-1}\beta_1+d_{n-1}},$$

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{1}{m_0^p}\cdot\frac{a_{n-1}\beta_1}{c_{n-1}\beta_1+d_{n-1}}\right)=\frac{1}{m_0^p}\cdot a_nc_n^{-1}.$$

Then, the transitivity of trace leads to

$$\mathrm{Tr}_{K_0}\left(\frac{1}{m_0^p}\cdot a_nc_n^{-1}\right)=\mathrm{Tr}_{K_{n-1}}\left(\frac{s\beta_{n-1}-1}{m_0^p\beta_{n-1}}\right)\neq 0.$$

Instead, assume conditions (i) and (ii) hold. Let n be any given positive integer. From Proposition 2, we get that $deg(\omega_n(X))=p^n$. Our aim now is to prove $\omega_n(X)$ is irreducible over $\mathbb{F}_q$.

Define β_i, K_i and $h_i(X)$ as in the proof above. Clearly, $h_1(X)$ is irreducible over K_0. Using Lemma 4, we obtain that $h_i(X)$ is irreducible over K_{i-1} for each $2\leq i\leq n$ if and only if

$$\mathrm{Tr}_{K_{i-1}}\left(\frac{s\beta_{i-1}-1}{m_0^p\beta_{i-1}}\right)\neq 0, \tag{3}$$

for each $2\leq i\leq n$.

We prove this by mathematical induction on i. First, since $h_1(X)$ is irreducible over K_0 and $h_1(\beta_1)=0$, by (ii) of Proposition 3, we have that

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{s\beta_1-1}{m_0^p\beta_1}\right)=\frac{a_2}{m_0^pc_2},$$

and

$$\mathrm{Tr}_{K_1}\left(\frac{s\beta_1-1}{m_0^p\beta_1}\right)=\mathrm{Tr}_{K_0}\left(\frac{a_2}{m_0^pc_2}\right)\neq 0.$$

It follows that (3) holds for $i=2$.

Next, let r be a positive integer with $r \geq 2$. Assuming that (3) holds for all i with $i \leq r-1$. By Lemma 4, $h_i(X)$ is irreducible over K_{i-1} for each $1 \leq i \leq r-1$. Note that $K_i = K_{i-1}(\beta_i)$ and $h_i(\beta_i) = 0$ for any $1 \leq i \leq r-1$. Using Proposition 3 iteratively again, we get

$$\mathrm{Tr}_{K_{r-1}/K_{r-2}}\left(\frac{s\beta_{r-1}-1}{m_0^p\beta_{r-1}}\right) = \frac{1}{m_0^p}\cdot\frac{a_2\beta_{r-2}}{c_2\beta_{r-2}+d_2},$$

$$\mathrm{Tr}_{K_{r-2}/K_{r-3}}\left(\frac{1}{m_0^p}\cdot\frac{a_2\beta_{r-2}}{c_2\beta_{r-2}+d_2}\right) = \frac{1}{m_0^p}\cdot\frac{a_3\beta_{r-3}}{c_3\beta_{r-3}+d_3},$$

$$\vdots$$

$$\mathrm{Tr}_{K_2/K_1}\left(\frac{1}{m_0^p}\cdot\frac{a_{r-2}\beta_2}{c_{r-2}\beta_2+d_{r-2}}\right) = \frac{1}{m_0^p}\cdot\frac{a_{r-1}\beta_1}{c_{r-1}\beta_1+d_{r-1}},$$

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{1}{m_0^p}\cdot\frac{a_{r-1}\beta_1}{c_{r-1}\beta_1+d_{r-1}}\right) = \frac{1}{m_0^p}\cdot a_r c_r^{-1}.$$

By the transitivity of trace, we have that

$$\mathrm{Tr}_{K_0}\left(\frac{1}{m_0^p}\cdot a_r c_r^{-1}\right) = \mathrm{Tr}_{K_{r-1}}\left(\frac{s\beta_{r-1}-1}{m_0^p\beta_{r-1}}\right) \neq 0.$$

As a result, (3) holds for $i = r$. Then for any $2 \leq i \leq n$, (3) holds. Thus, each $h_i(X)$ is the minimal polynomial of β_i over K_{i-1}. Thus, for all $1 \leq i \leq n$, $[K_i : K_{i-1}] = p$. So we obtain

$$[K_n : K_0] = \prod_{i=1}^{n}[K_i : K_{i-1}] = p^n.$$

From (2) it follows that $K_n = K_0(\beta_n)$. Recall that $\omega_n(X) \in K_0[X]$ with $\omega_n(\beta_n) = 0$ and $deg(\omega_n(X)) = p^n$. Therefore, $\omega_n(X)$ is irreducible over $K_0 = \mathbb{F}_q$. □

Next, consider the case $t \geq 2$.

Theorem 5 Let p be odd and $t \geq 2$ be an integer. Then $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$ is not inversely stable over $\mathbb{F}_q$.

Proof. When $m = 0$ or $s = 0$, the result is obvious. Let $m, s \neq 0$. By Lemma 5, if $\psi(X)$ is irreducible over $\mathbb{F}_q$, then $p = t = 2$. Since p is odd, it follows that $\psi(X)$ is reducible over $\mathbb{F}_q$, which indicates that $\psi(X)$ is not inversely stable over $\mathbb{F}_q$. □

In summary, it is sufficient to consider $p = t = 2$. In this case, $\psi(X) = X^4 + mX + s \in \mathbb{F}_{2^e}[X]$. For $X^4 + mX + s$, we get the following proposition.

Proposition 4 For $m, s \in \mathbb{F}_{2^e}$, the trinomial $X^4 + mX + s$ is irreducible over $\mathbb{F}_{2^e}$ if and only if $m = m_0^3$ for some $m_0 \in \mathbb{F}_{2^e}^*$, e is odd and $\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\frac{s}{m_0^4}\right) \neq 0$.

Proof. Denote $\psi(X) = X^4 + mX + s$. Assume $\psi(X)$ is irreducible over $\mathbb{F}_{2^e}$. So $m,\ s \neq 0$. By Lemma 5, there exist $m_0,\ r_0 \in \mathbb{F}_{2^e}^*$ such that

$$X^4+mX = X(X+m_0)(X^2+m_0X+r_0).$$

Expanding the right-hand side, we get

$$X(X+m_0)(X^2+m_0X+r_0) = X^4+(m_0^2+r_0)X^2+m_0r_0X.$$

Equating coefficients with X^4+mX, ones get that $m=m_0^3$. Substitute $Y=\dfrac{X}{m_0}$, we have

$$\psi(X) = (m_0Y)^4+m_0^3(m_0Y)+s = m_0^4\left(Y^4+Y+c\right), \quad \text{where} \quad c=\frac{s}{m_0^4}.$$

Irreducibility of $\psi(X)$ implies that $\upsilon(Y)=Y^4+Y+c$ is irreducible over $\mathbb{F}_{2^e}$. Using Lemma 5 again, $\upsilon(Y)$ is irreducible if and only if both quadratics X^2+X+1 and X^2+X+c are irreducible over $\mathbb{F}_{2^e}$. Thus, e is odd and $\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\dfrac{s}{m_0^4}\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}}(c)\neq 0$.

Conversely, assume e is odd, $m=m_0^3$ for some $m_0\in\mathbb{F}_{2^e}^*$, and $\mathrm{Tr}_{\mathbb{F}_{2^e}}\left(\dfrac{s}{m_0^4}\right)\neq 0$. Let $c=\dfrac{s}{m_0^4}$. Then X^2+X+1 and X^2+X+c are irreducible over $\mathbb{F}_{2^e}$. By Lemma 5, $\upsilon(Y)=Y^4+Y+c$ is irreducible over $\mathbb{F}_{2^e}$. Substituting $X=m_0Y$:

$$\psi(X) = m_0^4\upsilon(Y).$$

Thus, $\psi(X)$ is irreducible over $\mathbb{F}_{2^e}$. □

Theorem 6 Let $t\geq 2$ and t,e be positive integers. Then $\psi(X)=X^{2^t}+mX+s$ is inversely stable over $\mathbb{F}_{2^e}$ if and only if the following three conditions hold:

(i) $t=2$ and $2\nmid e$;

(ii) there exists $m_0\in\mathbb{F}_{2^e}^*$ such that $m=m_0^3$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\dfrac{s}{m_0^4}\right)\neq 0$;

(iii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\dfrac{a_n}{m_0^4c_n}\right)\neq 0$ for any positive integer n, where the sequences $\{a_n\}$, $\{c_n\}$ are defined as above.

Proof. Assume $\psi(X)$ is inversely stable over $\mathbb{F}_{2^e}$. Then $\psi(X)$ is irreducible over $\mathbb{F}_{2^e}$. Thus, by Lemma 5 and Proposition 4, conditions (i) and (ii) hold, and $\psi(X)=X^4+mX+s$. Similar to the proof of the first part of Theorem 4, we have that for every $n\in\mathbb{N}$, $\omega_n(X)$ is irreducible over $\mathbb{F}_{2^e}$. By Proposition 2, $deg(\omega_n(X))=4^n$. Let $\beta_n\in\overline{\mathbb{F}}_{2^e}$ be a zero of $\omega_n(X)$. Thus, $4^n=[\mathbb{F}_{2^e}(\beta_n):\mathbb{F}_{2^e}]$. For each $1\leq i\leq n-1$, define $\beta_i:=\Psi^{(n-i)}(\beta_n)$. One finds that

$$\beta_1{}^4+m\beta_1+s=0, \tag{4}$$

and for $i\geq 2$

$$\beta_i^4+m\beta_i+\frac{s\beta_{i-1}-1}{\beta_{i-1}}=0. \tag{5}$$

The finite field sequence, denoted by $\{K_i\}_{i=0}^{n}$, is to be defined as

$$K_0 := \mathbb{F}_{2^e},\ K_i := K_0(\beta_1,\ \beta_2,\ \cdots,\ \beta_i),\ 1 \le i \le n.$$

Let $h_1(X) = X^4 + mX + s$ and $h_i(X) = X^4 + mX + \dfrac{s\beta_{i-1} - 1}{\beta_{i-1}} (2 \le i \le n)$. Clearly, $h_i(X) \in K_{i-1}[X]$ and $h_i(\beta_i) = 0$ for $1 \le i \le n$. Then $[K_i : K_{i-1}] \le 4$, $1 \le i \le n$. Considering the conclusion drawn above, we get that

$$4^n = [\mathbb{F}_q(\beta_n) : \mathbb{F}_q] = [K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}] \le 4^n.$$

Hence $[K_i : K_{i-1}] = 4$ for any $1 \le i \le n$. It implies that $h_i(X)$ is irreducible over K_{i-1} for each $1 \le i \le n$. In particular, $h_n(X) = X^4 + mX + \dfrac{s\beta_{n-1} - 1}{\beta_{n-1}}$ is irreducible over K_{n-1}. By Proposition 4, we have that

$$\mathrm{Tr}_{K_{n-1}}\left(\frac{s\beta_{n-1} - 1}{m_0^4 \beta_{n-1}}\right) \ne 0.$$

By iterative use of Proposition 3, we then get

$$\mathrm{Tr}_{K_{n-1}/K_{n-2}}\left(\frac{s\beta_{n-1} - 1}{m_0^4 \beta_{n-1}}\right) = \frac{1}{m_0^4} \cdot \frac{a_2\beta_{n-2}}{c_2\beta_{n-2} + d_2},$$

$$\mathrm{Tr}_{K_{n-2}/K_{n-3}}\left(\frac{1}{m_0^4} \cdot \frac{a_2\beta_{n-2}}{c_2\beta_{n-2} + d_2}\right) = \frac{1}{m_0^4} \cdot \frac{a_3\beta_{n-3}}{c_3\beta_{n-3} + d_3},$$

$$\vdots$$

$$\mathrm{Tr}_{K_2/K_1}\left(\frac{1}{m_0^4} \cdot \frac{a_{n-2}\beta_2}{c_{n-2}\beta_2 + d_{n-2}}\right) = \frac{1}{m_0^4} \cdot \frac{a_{n-1}\beta_1}{c_{n-1}\beta_1 + d_{n-1}},$$

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{1}{m_0^4} \cdot \frac{a_{n-1}\beta_1}{c_{n-1}\beta_1 + d_{n-1}}\right) = \frac{1}{m_0^4} \cdot a_n c_n^{-1}.$$

Then, the transitivity of trace leads to

$$\mathrm{Tr}_{K_0}\left(\frac{1}{m_0^4} \cdot a_n c_n^{-1}\right) = \mathrm{Tr}_{K_{n-1}}\left(\frac{s\beta_{n-1} - 1}{m_0^4 \beta_{n-1}}\right) \ne 0.$$

Conversely, assume conditions (i), (ii) and (iii) hold. Let n be any given positive integer. By Proposition 2, $deg(\omega_n(X)) = 4^n$. We shall show that $\omega_n(X)$ is irreducible over $\mathbb{F}_q$.

Define β_i, K_i and $h_i(X)$ as in the proof above. By Proposition 4, $h_1(X)$ is clearly irreducible over K_0, and we obtain that $h_i(X)$ is irreducible over K_{i-1} for each $2 \leq i \leq n$ if and only if

$$\mathrm{Tr}_{K_{i-1}}\left(\frac{s\beta_{i-1}-1}{m_0^4\beta_{i-1}}\right) \neq 0, \tag{6}$$

for each $2 \leq i \leq n$.

We proceed by induction on i. Note that $h_1(X)$ is irreducible over K_0 and $h_1(\beta_1) = 0$. From Proposition 3, we get that

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{s\beta_1-1}{m_0^4\beta_1}\right) = \frac{a_2}{m_0^4 c_2},$$

and

$$\mathrm{Tr}_{K_1}\left(\frac{s\beta_1-1}{m_0^4\beta_1}\right) = \mathrm{Tr}_{K_0}\left(\frac{a_2}{m_0^4 c_2}\right) \neq 0.$$

It follows that (6) holds for $i = 2$.

Next, let r be a positive integer with $r \geq 2$. Suppose (6) holds for all i with $i \leq r-1$. Proposition 4 implies that $h_i(X)$ is irreducible over K_{i-1} for each $1 \leq i \leq r-1$. Note that $K_i = K_{i-1}(\beta_i)$ and $h_i(\beta_i) = 0$ for any $1 \leq i \leq r-1$. Using Proposition 3 iteratively again, we get

$$\mathrm{Tr}_{K_{r-1}/K_{r-2}}\left(\frac{s\beta_{r-1}-1}{m_0^4\beta_{r-1}}\right) = \frac{1}{m_0^4}\cdot\frac{a_2\beta_{r-2}}{c_2\beta_{r-2}+d_2},$$

$$\mathrm{Tr}_{K_{r-2}/K_{r-3}}\left(\frac{1}{m_0^4}\cdot\frac{a_2\beta_{r-2}}{c_2\beta_{r-2}+d_2}\right) = \frac{1}{m_0^4}\cdot\frac{a_3\beta_{r-3}}{c_3\beta_{r-3}+d_3},$$

$$\vdots$$

$$\mathrm{Tr}_{K_2/K_1}\left(\frac{1}{m_0^4}\cdot\frac{a_{r-2}\beta_2}{c_{r-2}\beta_2+d_{r-2}}\right) = \frac{1}{m_0^4}\cdot\frac{a_{r-1}\beta_1}{c_{r-1}\beta_1+d_{r-1}},$$

$$\mathrm{Tr}_{K_1/K_0}\left(\frac{1}{m_0^4}\cdot\frac{a_{r-1}\beta_1}{c_{r-1}\beta_1+d_{r-1}}\right) = \frac{1}{m_0^4}\cdot a_r c_r^{-1}.$$

By the transitivity of trace, we have that

$$\mathrm{Tr}_{K_0}\left(\frac{1}{m_0^4}\cdot a_r c_r^{-1}\right) = \mathrm{Tr}_{K_{r-1}}\left(\frac{s\beta_{r-1}-1}{m_0^4\beta_{r-1}}\right) \neq 0.$$

Thus (6) holds for $i = r$. Then for any $2 \le i \le n$, (6) holds. Hence, each $h_i(X)$ is the minimal polynomial of β_i over K_{i-1}. It follows that $[K_i : K_{i-1}] = 4$ for all $1 \le i \le n$. So we obtain

$$[K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}] = 4^n.$$

By (5), $K_n = K_0(\beta_n)$. Since $\omega_n(X) \in K_0[X]$ is a monic polynomial of degree 4^n satisfying $\omega_n(\beta_n) = 0$, $\omega_n(X)$ is the minimal polynomial of β_n over $K_0 = \mathbb{F}_q$. Hence it is irreducible over $\mathbb{F}_q$. □

To summarize what we have proved, we give a complete answer to the Problem 1.

Theorem 7 Let p be a prime and $q = p^e$ with a positive integer e. Let $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$ with t being a positive integer.

When $t = 1$, $\psi(X)$ is inversely stable over $\mathbb{F}_q$ if and only if the following hold:

(i) there exists $m_0 \in \mathbb{F}_q^*$ such that $m = -m_0^{p-1}$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^p}\right) \neq 0$;

(ii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^p c_n}\right) \neq 0$ for any positive integer n, where the sequences $\{a_n\},\ \{c_n\}$ are defined as above.

When $t \ge 2$, $\psi(X)$ is inversely stable over $\mathbb{F}_q$ if and only if the following hold:

(i) $p = t = 2$ and $2 \nmid e$;

(ii) there exists $m_0 \in \mathbb{F}_q^*$ such that $m = m_0^3$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^4}\right) \neq 0$;

(iii) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^4 c_n}\right) \neq 0$ for any positive integer n, where the sequences $\{a_n\},\ \{c_n\}$ are defined as above.

The inverse stability criteria for $\psi(X) = X^{p^t} + mX + s \in \mathbb{F}_q[X]$ are summarized in the following table.

Table 1. The inverse stability criteria for $\Psi(X)$

Value of t	Conditions for inverse stability
$t = 1$	(1) There exists $m_0 \in \mathbb{F}_q^*$ such that $m = -m_0^{p-1}$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^p}\right) \neq 0$(2) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^p c_n}\right) \neq 0$ for any positive integer n
$t = 2$	(1) $p = 2$ and $2 \nmid e$ (2) There exists $m_0 \in \mathbb{F}_q^*$ such that $m = m_0^3$ and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{s}{m_0^4}\right) \neq 0$(3) $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^4 c_n}\right) \neq 0$ for any positive integer n
$t \ge 3$	No inversely stable polynomial

Example 4 Let $p = 2,\ t = 1,\ e = 3$, and $f(X) = X^2 + X + 1$. By definition, it is clear that for any positive integer n, we have $a_n = c_n = d_n = 1$, and $\mathrm{Tr}_{\mathbb{F}_q}\left(\frac{a_n}{m_0^p c_n}\right) = 1 \neq 0$. From Theorem 4, we know $f(X)$ is inversely stable over $\mathbb{F}_{2^3}$. Let $F(X) = \dfrac{1}{X^2 + X + 1}$. We list the cases of $F^{(n)}(X)$ for $n = 2,\ 3,\ 4$:

$$F^{(2)}(X) = \frac{X^4 + X^2 + 1}{X^4 + X + 1},$$

$$F^{(3)}(X) = \frac{X^8 + X^2 + 1}{X^8 + X^6 + X^5 + X^4 + X^3 + X + 1},$$

$$F^{(4)}(X)=\frac{X^{16}+X^{12}+X^{10}+X^8+X^6+X^2+1}{X^{16}+X^{14}+X^{13}+X^{11}+X^9+X^7+X^6+X+1}.$$

Then, we have that $\mu_n(X),\ \omega_n(X)$ are pairwise coprime, and $\omega_2(X),\ \omega_3(X)$ and $\omega_4(X)$ are distinct and irreducible over $\mathbb{F}_{2^3}$.

5. Reducibility of iteration of polynomials of the form $X^{p^t}+aX^{p^s}+b$ for odd p

Let p be the characteristic of $\mathbb{F}_q$ and p be odd. In this section, we show that polynomials of the form $X^{p^t}+aX^{p^s}+b\in\mathbb{F}_q[X]$ are not stable over $\mathbb{F}_q$ when p is odd and $t>s\geq 0$, due to the fact that some of their iterates are reducible. Lemma 5 is the main tool of our proof.

Theorem 8 If $a,\ b\in\mathbb{F}_q^*$, then the trinomial

$$X^p+aX+b,$$

is not stable over $\mathbb{F}_q$ for its quadratic iterate is reducible over $\mathbb{F}_q$.

Proof. We have

$$f^{(2)}(X)=X^{p^2}+(a^p+a)X^p+a^2X+b(b^{p-1}+a+1).$$

It is clear that $f^{(2)}(X)$ is reducible for $b^{p-1}+a+1=0$. For $b^{p-1}+a+1\neq 0$, using Lemma 5 and p is odd, we obtain $f^{(2)}(X)$ is reducible over $\mathbb{F}_q$. So $f(X)$ is not stable over $\mathbb{F}_q$. □

Moreover, when $t\geq 2$, by Lemma 5 and p is odd, we get that polynomials of the form $X^{p^t}+a_{t-1}X^{p^{t-1}}+\cdots+a_0\in\mathbb{F}_q[X]$ where $a_0\in\mathbb{F}_q^*$, are reducible over $\mathbb{F}_q$. Combining the Theorem 8, we obtain the following theorem.

Theorem 9 If $t>s\geq 0$ and $a,b\in\mathbb{F}_q^*$, then the trinomial $X^{p^t}+aX^{p^s}+b$ is not stable over $\mathbb{F}_q$.

Example 5 Over $\mathbb{F}_3$, the polynomial $f(X)=X^9+X^3+1$ factors as $(X+2)^3(X^2+X+2)^3$. This indicates that $f(X)$ is not stable over $\mathbb{F}_3$.

Acknowledgments

The authors thank the anonymous referees for their helpful comments that improved the quality of the manuscript. This work was supported by Natural Science Foundation of Beijing Municipal (M23017).

Conflict of interest

The authors declare no competing financial interest.

References

[1] Ahmadi O, Monsef-Shokri K. A note on the stability of trinomials over finite fields. *Finite Fields and Their Applications*. 2020; 63: 101649.

[2] Cheng K. Infinite families of irreducible polynomials over finite fields. *arXiv:2412.04985*. 2024. Available from: https://doi.org/10.48550/arXiv.2412.04985.

[3] Cohen SD. The explicit construction of irreducible polynomials over finite fields. *Designs, Codes and Cryptography*. 1992; 2(2): 169–174.
[4] Fein B, Schacher M. Properties of iterates and composites of polynomials. *Journal of the London Mathematical Society*. 1996; 54(3): 489–497.
[5] Gómez-Pérez D, Nicolás AP, Ostafe A, Sadornil D. Stable polynomials over finite fields. *Revista Matemática Iberoamericana*. 2014; 30(2): 523–535.
[6] Ahmadi O, Luca F, Ostafe A, Shparlinski IE. On stable quadratic polynomials. *Glasgow Mathematical Journal*. 2012; 54(2): 359–369.
[7] Odoni RWK. The Galois theory of iterates and composites of polynomials. *Proceedings of the London Mathematical Society*. 1985; s3-51(3): 385–414.
[8] Jones R, Boston N. Settled polynomials over finite fields. *Proceedings of the American Mathematical Society*. 2011; 140(6): 1849–1863.
[9] Lin T, Wang Q. On the stable polynomials of degrees 2, 3, 4. *Finite Fields and Their Applications*. 2024; 99: 102474.
[10] Fernandes A, Panario D, Reis L. Stable binomials over finite fields. *Finite Fields and Their Applications*. 2025; 101: 102520.
[11] Cheng K. A new direction on constructing irreducible polynomials over finite fields. *Finite Fields and Their Applications*. 2024; 95: 102368.
[12] Gao S. *Normal Bases over Finite Fields*. Waterloo: University of Waterloo; 1993.
[13] Wan ZX. *Lectures on Finite Fields and Galois Rings*. Singapore: World Scientific; 2003.