Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 907–930
DOI : 10.47974/JDMSC-2192

Some classes of permutation polynomials of the form $x(x^{s_1(q+1)} + bx^{s_2(q+1)} + a)$ over $\mathbb{F}_{q^2}$

Shalini Gupta *
Manpreet Singh †
Sagar Vinayak §
Department of Mathematics & Statistics
Himachal Pradesh University
Summer Hill
Shimla 171005
Himachal Pradesh
India

Abstract

Permutation polynomials hold significant relevance in the practical applications of finite fields. Presently, they constitute a pivotal focus in contemporary research endeavors. This paper undertakes the classification of permutation binomials and trinomials of the form $x(x^{s_1(q+1)} + b^{s_2(q+1)} + a)$ over $\mathbb{F}_{q^2}$, with $s_1 = 3$. We explore these polynomials with variations in b, considering the cases where $b = 0$ or $b \neq 0$ with $s_2 = 1$ and $s_2 = 2$.

Subject Classification: *11T06, 11T55, 05A05.*

Keywords: *Finite fields, Permutation polynomial, Permutation binomial, Permutation trinomial.*

1. Introduction

Consider the finite field $\mathbb{F}_q$ contains q elements. The polynomials over finite field attract many researchers due to their applications in

* *ORCID-ID:* **0000-0001-7743-0744**
† *ORCID-ID:* **0000-0002-3961-3571**
§ *ORCID-ID:* **0009-0001-4543-975X**

* *E-mail:* **shalini.garga1970@gmail.com (Corresponding Author)**
† *E-mail:* **ms44167@gmail.com**
§ *E-mail:* **sagarvinayak0001@gmail.com**

engineering and technology. Various types of polynomials such as linearized polynomials, irreducible polynomials, normal polynomials and skew polynomials are discussed in literature, one may refer to [3], [10], [20], [38], [39], [48], [58]. A polynomial is a permutation polynomial if the mapping function $f:\mathbb{F}_q \mapsto \mathbb{F}_q$ is one-one and onto that is a bijection. Permutation polynomials find extensive applications in various fields, including cryptography, coding theory and combinatorial design, see [11], [12], [28], [35], [47]. The study of permutation polynomials has gained significant attention in recent research. For a comprehensive understanding of permutation polynomials(PPs) and their latest advancements, one may refer to [25], [36], [37], [40], [41], [55].

Permutation binomials and permutation trinomials possess a compact and concise structure, making them suitable for implementation in cryptography and coding theory. Recent research by various authors has focused on PPs of the type $x^r g(x^{\frac{q-1}{d}})$ satisfies $d|(q-1)$ over $\mathbb{F}_q$. The polynomial $xg(x^{q-1})$, with $g(x) = \alpha + x^2$, $\alpha + x^3$ and $\alpha + x^5$ to be permutation over $\mathbb{F}_{q^2}$ respectively are determined by Hou [21], Hou and Lappano [26], and Lappano [30] respectively. Continuing this work, Hou [22], [23] has provided a complete characterization of polynomials in the type $xh(x^{q-1})$, where $\alpha + \beta x + x^2$ over $\mathbb{F}_{q^2}$. The permutation polynomial and complete permutation polynomials from linearized polynomials are discussed in [50].

Akbary et al. [1], initially introduced the concept of the index of a polynomial in the context of the distribution of permutation polynomials over finite fields. This parameter has been proved useful in studying various properties, including Carlitz rank [27], character sum bounds [42] and value set size bounds [53]. Instead of classifying permutation polynomials by their degrees, researchers have explored their classification based on indices [4], [5], [13], [16], [18], [24], [31], [32], [33], [51], [56], [57], [61], [62]. Several authors have proposed criteria for polynomials of the form $x^r f(x^s)$ to be permutation polynomial, see [52, 46, 2, 54, 63] for further details. Gupta and Sharma [18] have constructed four new classes of the form $x^r g(x^{q-1})$ to be permutation over $\mathbb{F}_{2^{2m}}$ along with related conjectures concerning permutation polynomials over finite fields with even characteristic, which are subsequently proved by Zha et al. [62].

Özbudak and Temür [44], [45] classified the polynomials $x^3(x^{3q-3} + bx^{q-1} + c)$, $x^3(1 + ax^{q-1} + bx^{2(q-1)})$ and $x^3(1 + bx^{2q-2} + cx^{3q-3})$ to be permutation over $\mathbb{F}_{q^2}$.

The sparse polynomials is of the type $x^r g(x^{\frac{q^n-1}{q-1}})$ with index $q-1$. Recent studies have explored the possibility of sparse polynomials being permutation polynomials by various authors in [8], [9], [59], [60], [65]. The problems related to complete permutation monomial of sparse polynomials are studied in [6], [7], [8], [9], [15], [59], [60]. Sharma and Gupta [49] have determined PPs of the type $x^r g(x^{p^k+1})$ over $\mathbb{F}_{p^{2k}}$, considering $g(x)$ of degree 1 and 2, and different values of r, with certain restrictions on coefficients. Furthermore, Gupta et al. [19] have identified permutation binomials and trinomials over $\mathbb{F}_{q^n}$.

Li et al. have provided an explanation of PPs of degree six or seven over $\mathbb{F}_{2^k}$ in [29]. Fan [14] classified the PPs of degree 7 over $\mathbb{F}_{p^k}$, where p is an odd prime, employing exceptional polynomials.

Motivated by the aforementioned research, this paper focuses on the study of PPs of the type $G(x) = x(x^{s_1(q+1)} + bx^{s_2(q+1)} + a)$ over $\mathbb{F}_{q^2}$. To establish the permutation property of the polynomial, we utilize PPs of degree seven over $\mathbb{F}_{p^k}$ as introduced by Fan [14]. The paper is organized into five sections. The subsequent section provides an overview of the necessary preliminaries for this study. In Section 3, we set $b=0$ in $G(x)$, resulting in the binomial $A(x) = xh(x^{q+1})$, where $h(x) = x^{s_1} + a$ over $\mathbb{F}_{q^2}$. Here, we investigate $A(x)$ over $\mathbb{F}_{2^{2k}}$ to satisfy permutation property and subsequently investigate $A(x)$ as a permutation binomial over finite fields with $q > 409$. Section 4 discusses the classification of $G(x) = x(x^{s_1(q+1)} + bx^{s_2(q+1)} + a)$ as a permutation trinomial of two types: (i) when $s_1 = 3$ and $s_2 = 1$ (ii) when $s_1 = 3$ and $s_2 = 2$. Finally, Section 5 concludes work done in the paper.

2. Preliminaries

Throughout the paper, we use the symbol $\equiv$ for equivalent polynomials, the symbol $\cong$ for linearly related polynomials and PP stands for permutation polynomial.

Lemma 2.1: [29] *Let* $2^k \geq 8$. *If* $k \equiv 0 (\mathrm{mod}\, 3)$, *then there does not exist PPs over* $\mathbb{F}_{2^k}$ *of degree 7. Otherwise, every PP of degree 7 over* $\mathbb{F}_{2^t}$ *is equivalent to* x^7 *or to* $x^7 + x^5 + x$. *When* $k = 4$, *then PP is equivalent to one of the given below:*

$$x^7 + \gamma^3 x^4 + \gamma^6 x,$$
$$x^7 + x^5 + x^4,$$
$$x^7 + x^5 + \gamma x^4 + \gamma^{14} x^3 + \gamma^{12} x^3 + \gamma^8 x,$$
$$x^7 + x^5 + \gamma^5 x^4 + \gamma^2 x^3 + \gamma^{12} x^2 + \gamma^5 x,$$
$$x^7 + x^5 + \gamma^7 x^4 + \gamma^5 x^2 + \gamma^3 x,$$

where γ *satisfies* $x^4 + x + 1 \in \mathbb{F}_2[x]$.

Definition 2.1: [19] If there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfies

$$f(x) = Sg(Tx + U) + V.$$

Then, the polynomials $g(x)$ and $f(x)$ in $\mathbb{F}_q$ are said to be linearly related.

When $G(x)$ in $\mathbb{F}_q[x]$ is a PP over $\mathbb{F}_{q^k}$ for infinitely many *k*, then $G(x)$ is called an exceptional polynomial.

Lemma 2.2: [43] *Every exceptional polynomial* $g(x)$ *of degree 7 over* $\mathbb{F}_q$ *such that* $gcd(q, 7) = 1$, $(\cong)$ *is linearly related to*

$$x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x,$$

where $\beta \in \mathbb{F}_q^*$ *if* $q \not\equiv \pm 1 \pmod 7$ *or* $\beta = 0$ *if* $q \equiv -1 \pmod 7$.

Lemma 2.3: [17] *Every exceptional polynomial* $g(x)$ *of degree 7 over* $\mathbb{F}_{7^k}$ *is linearly related to* $(\cong) x^7$ *or to* $x(x^{\frac{6}{d}} - \beta)^d$ *where* $d \in \{1, 2, 3\}$ *and* $\beta \in \mathbb{F}_{7^k}^*$ *such that* $\beta^{d(\frac{7^k - 1}{6})} \neq 1$.

Lemma 2.4: [14] *If* $p^k \leq 409$, *then a non-exceptional PP of degree 7 exists over* $\mathbb{F}_{p^k}$.

Remark 2.1: In [14], if $k \geq 3$, then all the PPs of degree 7 are exceptional over $\mathbb{F}_{7^k}$.

Lemma 2.5: [64] *Let l be some positive integer such that l divides* $q-1$. *Then* $x^r g(x^{\frac{q-1}{l}})$ *is a PP over* $\mathbb{F}_q$ *if and only if gcd* $(r, \frac{q-1}{l})=1$ *and* $x^r g(x)^{\frac{q-1}{l}}$ *is a PP over* μ_l.

Corollary 2.1: [34] *If* $n>1$ *such that n divides* $q-1$, *then PP of degree n does not exist over* $\mathbb{F}_q$.

3. Classification of permutation binomial over $\mathbb{F}_{q^2}$

Consider the polynomial of the type

$$C(x)=x(x^{3q+3}+bx^{q+1}+a) \tag{1}$$

over finite fields $\mathbb{F}_{q^2}$ has been investigated in the present section.

Setting $b=0$ in equation (1), gives the binomial

$$C(x)=x(x^{3q+3}+a) \tag{2}$$

over $\mathbb{F}_{q^2}$. Because $\gcd(1,q+1)=1$. Using Lemma 2.5, $C(x)=x(x^{3q+3}+a)$ permutes $\mathbb{F}_{q^2}$ if and only if $C_1(x)=x(x^3+a)^{q+1}$ is a PP over $\mathbb{F}_q^*$ as $\mu_{q-1}=\mathbb{F}_q^*$.

We represent polynomial $C_1(x)=x(x^3+a)^{q+1}$ of degree 7 which is obtained as follows:

For $\alpha\in\mathbb{F}_q$, we have

$$\begin{aligned} C_1(\alpha) &= \alpha(\alpha^3+a)^{q+1} \\ &= \alpha(\alpha^6+(a^q+a)\alpha^3+a^{q+1}) \\ &= \alpha^7+(a^q+a)\alpha^4+a^{q+1}\alpha. \end{aligned}$$

Hence, $C_1(x)$ permutes $\mathbb{F}_q$ if and only if

$$C_2(x)=x^7+A_1x^4+A_2x \tag{3}$$

is a PP over $\mathbb{F}_q$, where $A_1=a^q+a$ and $C_2=a^{q+1}$.

Theorem 3.1: *Let k be a positive integer and* $q=2^k$. *Then, for* $a\in\mathbb{F}_{q^2}^*$,

$$C(x)=x(x^{3q+3}+a)$$

is a PP over $\mathbb{F}_{2^{2k}}$ *if and only if*

i) $a^2+a+1=0$, *when* $q=2$.

ii) $a \neq 1$ *when* $q = 4$.

iii) $a^{3q+2} + a^{2q+3} = 1$, *when* $q > 8$ *and* $m \not\equiv 0 \pmod 3$.

Proof: Since $\gcd(1, q+1) = 1$, by Lemma 2.5, $C(x) = x(x^{3(q+1)} + a)$ permutes $\mathbb{F}_q$ if and only if $C_2(x) = x^7 + A_1x^4 + A_2x$ is a PP over $\mathbb{F}_q$.

Case 1: For $q = 2$, $C_2(x) \equiv (1 + A_1 + A_2)\ x \pmod{x^2 + x}$. $C_2(x)$ permutes $\mathbb{F}_q$ if and only if $1 + A_1 + A_2 \neq 0$, this implies $1 + A_1 + A_2 = 1$, that is $a(a^2 + a + 1) = 0$. Since $a \neq 0$, therefore $a^2 + a + 1 = 0$.

Case 2: For $q = 4$, $C_2(x) \equiv (1 + A_1 + A_2)x \pmod{x^4 + x}$. $C_2(x)$ permutes $\mathbb{F}_q$ if and only if $1 + A_1 + A_2 \neq 0$, that is if and only if $a \neq 1$.

Case 3: For $q \geq 8$, if $k \equiv 0 \pmod 3$ then $7 \mid q - 1$, there does not exist PP of degree 7 by Corollary 2.1. So, for $q > 8$ and $k \not\equiv 0 \pmod 3$, by Lemma 2.1, the PP of degree 7 over $\mathbb{F}_q$ is equivalent to $x^7 + \gamma^3x^4 + \gamma^6x$, i.e.

$$C_2(x) \equiv x^7 + \gamma^3x^4 + \gamma^6x, \tag{4}$$

where γ satisfies $x^4 + x + 1 \in \mathbb{F}_2[x]$. Through comparing the coefficients in equation (3) and equation (4), we get $A_1 = \gamma^3$ and $A_2 = \gamma^6$. From the values of A_1 and A_2, we obtain the condition $a^{3q+2} + a^{2q+3} = 1$.

Theorem 3.2: *Let* $q = p^k > 409$ *such that* $q \not\equiv 0$ *or* $1 \pmod 7$. *For* $a \in \mathbb{F}_{q^2}^*$,

$$C(x) = x(x^{3(q+1)} + a)$$

is not a PP over $\mathbb{F}_{p^{2k}}$.

Proof: Utilizing Lemma 2.5, $C(x)$ is a PP over $\mathbb{F}_{q^2}$ if and only if $C_2(x)$ is a PP over $\mathbb{F}_q$. By Lemma 2.4, $C_2(x)$ permutes $\mathbb{F}_q$ if and only if the polynomial $C_2(x)$ is an exceptional in $\mathbb{F}_q$. By Lemma 2.2, $C_2(x)$ permutes $\mathbb{F}_q$ if and only if $C_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2x^3 - 7\beta^3x$ for some $\beta \in \mathbb{F}_q^*$ or x^7 when $q \equiv -1 \pmod 7$. Let us analyze the cases below:

Case 1: When $C_2(x) \cong x^7$, so there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy

$$C_2(x) = V + S(Tx + U)^7. \tag{5}$$

Through equating the corresponding coefficients in equation (3) and equation (4), we get

$$\begin{aligned} &ST^7 = 1,\ 7UT^6S = 0,\ 21T^5U^2S = 0,\ 35T^4U^3S = 0,\\ &35T^3U^4S = 0,\ 21T^2U^5S = 0,\ 7TSU^6 = 0,\ SU^7 + V = 0. \end{aligned} \tag{6}$$

Since $ST \neq 0$, therefore $7UT^6S = 0$ gives $7U = 0$. Also, $q \not\equiv 0 \pmod 7$, so $U = 0$. Substituting $U = 0$ in $A_2 = 7U^6TS$ shows that $a^{q+1} = 0$, which leads to the contradiction $a = 0$.

Case 2: When $C_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x$, so there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy

$$C_2(x) = V + S(-7\beta^3(Tx+U) + 14\beta^2(Tx+U)^3 - 7\beta(Tx+U)^5 + (Tx+U)^7). \tag{7}$$

Through equating the corresponding terms in equation (3) and equation (7), we get

$$\begin{aligned} &ST^7 = 1, 7UT^6S = 0, 21T^5U^2S - 7S\beta T^5 = 0,\\ &A_1 = 35T^4U^3S - 35\beta T^4US, 35T^3U^4S - 70T^3U^2\beta S + 14\beta^2T^3S,\\ &21U^5ST^2 - 70U^3ST^2\beta + 42UST^2\beta^2 = 0,\\ &A_2 = 7TSU^6 - 35wTU^4S + 42TU^2S - 7\beta^3TS,\\ &SU^7 - 7\beta U^5S + 14\beta^2U^3S - 7\beta^3US + V = 0. \end{aligned} \tag{8}$$

Since $ST \neq 0$, therefore $7UT^6S = 0$ gives $7U = 0$. Also, $q \not\equiv 0 \pmod 7$, so $U = 0$. Insert $U = 0$ in $21T^5U^2S - 7S\beta T^5 = 0$, we obtain $\beta TS = 0$, which contradicts $\beta, T, S \in \mathbb{F}_q^*$.

4. Classification of permutation trinomials over $\mathbb{F}_{q^2}$

The polynomials of the type

$$C(x) = x(x^{3q+3} + bx^{q+1} + a)$$

and

$$D(x) = x(x^{3q+3} + bx^{2q+2} + a)$$

over $\mathbb{F}_{q^2}$ has been investigated in the present section.

First, take the trinomial

$$C(x) = x(x^{3q+3} + bx^{q+1} + a)$$

over $\mathbb{F}_{q^2}$. Utilizing Lemma 2.5 as $\gcd(1, q+1) = 1$, then $C(x) = x(x^{3(q+1)} + bx^{q+1} + a)$ permutes $\mathbb{F}_{q^2}$ if and only if and $C_1(x) = x(x^3 + bx + a)^{q+1}$ is a PP over $\mathbb{F}_q^*$ as $\mu_{q-1} = \mathbb{F}_q^*$.

The polynomial $C_1(x) = x(x^3 + bx + a)^{q+1}$ is represented in a simplified polynomial of degree 7 obtained as follows:

For $\alpha \in \mathbb{F}_q$, we have

$$\begin{aligned} C_1(\alpha) &= \alpha(\alpha^3 + b\alpha + a)^{q+1} \\ &= \alpha(\alpha^6 + (b^q + b)\alpha^4 + (a^q + a)\alpha^3 + b^{q+1}\alpha^2 + a^{q+1}) \\ &= \alpha^7 + (b^q + b)\alpha^5 + (a^q + a)\alpha^4 + b^{q+1}\alpha^3 + (ab^q + ba^q)\alpha^2 + a^{q+1}\alpha. \end{aligned}$$

By taking, $A_1 = b^q + b$, $A_2 = a^q + a$, $A_3 = b^{q+1}$, $A_4 = a^q b + b^q a$ and $A_5 = a^{q+1}$. So, $C_1(x)$ permutes $\mathbb{F}_q$ if and only if

$$C_2(x) = x^7 + A_1x^5 + A_2x^4 + A_3x^3 + A_4x^2 + A_5x \tag{9}$$

is a PP over $\mathbb{F}_q$.

Theorem 4.1: *Let $k \geq 1$ be a integer and $q = 2^k$, then for $a, b \in \mathbb{F}_{q^2}^*$, the trinomial*

$$C(x) = x(x^{3q+3} + bx^{q+1} + a)$$

is a PP over $\mathbb{F}_{q^2}$ if and only if

(i) Either $b = a$ or $(b+a)^2 + (b+a) + 1 = 0$, when $q = 2$.

(ii) $(a+b)^2 + (a+b+1)\gamma^4 = 0$ or $(b+a)^2 + (b+a+1)\gamma^{10} = \gamma^{13}$, where γ satisfies $x^4 + x + 1 \in \mathbb{F}_2[x]$, when $q > 8$ and $k \not\equiv 0 \pmod 3$..

Proof: $C(x) = x(x^{3(q+1)} + bx^{q+1} + a)$ permutes $\mathbb{F}_{q^2}$ if and only if $C_2(x)$ permutes $\mathbb{F}_q$.

Case 1: For $q = 2$, $C_2(x) \equiv (1 + A_1 + A_2 + A_3 + A_4 + A_5)x \pmod{x^2 + x}$ is a PP if and only if $A_5 + A_4 + A_3 + A_2 + A_1 + 1 \neq 0$, this implies $A_5 + A_4 + A_3 + A_2 + A_1 = 0$, that is $(1 + (b+a) + (b+a)^2)(b+a) = 0$. Therefore, either $b = a$ or $1 + (b+a) + (b+a)^2 = 0$.

Case 2: For $q = 4$, $C_2(x) \equiv A_3x^3 + (A_1 + A_4)x^2 + (A_5 + A_2)x \pmod{x^4 + x}$. As, then there is no PP of degree 3 over $\mathbb{F}_q$ by Corollary 2.1. So, $A_3 = 0$ implies that $b^{q+1} = 0$ i.e. $b = 0$, which contradicts $b \in \mathbb{F}_q^*$.

Case 3: For $q \geq 8$, if $k \equiv 0 \pmod 3$ then $7 \mid q-1$ there does not exist PP of degree 7 by Corollary 2.1. For $q > 8$ and $k \not\equiv 0 \pmod 3$, the PP of degree 7 is equivalent to one of the polynomials in Lemma 2.1.

Subcase 1: Consider $C_2(x) \equiv x^7 + \gamma^3 x^4 + \gamma^6 x$, it follows that $A_3 = 0$ that is $b = 0$, which contradicts $b \in \mathbb{F}_q^*$.

Subcase 2: Consider $C_2(x) \equiv x^7 + x^5 + x^4$. Consequently, $A_3 = 0$ i.e. $b = 0$, which contradicts $b \in \mathbb{F}_q^*$.

Subcase 3: Consider $C_2(x) \equiv x^7 + x^5 + \gamma x^4 + \gamma^{14} x^3 + \gamma^{12} x^2 + \gamma^8 x$, where γ satisfies $x^4 + x + 1 \in \mathbb{F}_2[x]$.

By comparing terms with identical powers, we obtain

$$A_1 = 1, A_2 = \gamma, A_3 = \gamma^{14}, A_4 = \gamma^{12}, A_5 = \gamma^8$$

$$a^q b + b^q a = \gamma^{12}. \tag{10}$$

Thus,

$$b^q + b = 1, \tag{11}$$

$$a^q + a = \gamma. \tag{12}$$

Multiplying equation (11) with a and equation (12) with b and adding the resulting equations, we arrive at

$$ab^q + a^q b = a + b\gamma. \tag{13}$$

Using equation (16), we get

$$a + b\gamma = \gamma^{12}. \tag{14}$$

From the values of A_3 and A_5, we obtain

$$b^2 + b = \gamma^{14} \text{ and } a^2 + a\gamma = \gamma^8. \tag{15}$$

Adding equation (14) and equation (15)

$$(a+b)^2 + (a+b+1)\gamma^4 = 0.$$

Subcase 3: Consider $C_2(x) \equiv x^7 + x^5 + \gamma x^4 + \gamma^{14} x^3 + \gamma^{12} x^2 + \gamma^8 x$, where γ satisfies $x^4 + x + 1 \in \mathbb{F}_2[x]$.

By comparing terms with identical powers, we obtain

$$A_1 = 1, A_2 = \gamma^5, A_3 = \gamma^2, A_4 = \gamma^{12}, A_5 = \gamma^5$$

$$a^q b + b^q a = \gamma^{12}. \tag{16}$$

Thus,

$$b^q + b = 1, \tag{17}$$

$$a^q + a = \gamma^5. \tag{18}$$

Multiplying equation (17) with a and equation (18) with b and adding the resulting equations, we arrive at

$$ab^q + a^q b = a + b\gamma. \tag{19}$$

Using equation (16), we get

$$a + b\gamma^5 = \gamma^{12}. \tag{20}$$

From the values of A_3 and A_5, we obtain

$$b^2 + b = \gamma^2 \text{ and } a^2 + a\gamma^5 = \gamma^5. \tag{21}$$

Adding equation (20) and equation (21)

$$(a+b)^2 + (a+b+1)\gamma^{10} = \gamma^{13}.$$

Subcase 5: Consider $C_2(x) \equiv x^7$. Here, we conclude that $A_3 = 0$ and $A_5 = 0$, consequently, $a = 0$ and $b = 0$, which is a contradiction.

Subcase 6: Consider $C_2(x) \equiv x^7 + x^5 + x$. Then, $A_3 = 0$ implies that $b = 0$, which is a contradiction.

Theorem 4.2: *Let* $q = p^k > 409$ *such that* $q \not\equiv 0$ *or* $1 \pmod 7$. *For* $a, b \in \mathbb{F}_{q^2}^*$,

$$C(x) = x(x^{3(q+1)} + bx^{q+1} + a)$$

is not a PP over $\mathbb{F}_{q^2}$.

Proof: For $q = p^k > 409$, with $q \neq 0,1 \pmod 7$, Utilizing Lemma 2.5, $C(x)$ is a PP over $\mathbb{F}_{q^2}$ if and only if $C_2(x)$ permutes $\mathbb{F}_q$. Further, using Lemma 2.4,

$C_2(x)$ permutes $\mathbb{F}_q$ if and only if the polynomial $C_2(x)$ is an exceptional in $\mathbb{F}_q$.

Also, using Lemma 2.2, $C_2(x)$ permutes $\mathbb{F}_q$ if and only if $C_2(x) \cong x^7$ or $q \not\equiv -1 \pmod 7$ or $C_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x$, for some $\beta \in \mathbb{F}_q^*$.

Case 1: When $C_2(x) \cong x^7$, then there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisify

$$C_2(x) = V + S(Tx + U)^7.$$

By comparing terms with identical powers, we obtain

$$\begin{aligned} &ST^7 = 1, 7UST^6 = 0, A_1 = 21U^2ST^5, A_2 = 35U^3ST^4, \\ &A_3 = 35U^4ST^3, A_4 = 21U^5ST^2, A_5 = 7U^6ST, U^7S + V = 0. \end{aligned}$$

Since $ST \neq 0$, then $7UST^6 = 0$ implies that $7U = 0$. Also, $q \not\equiv 0 \pmod 7$, therefore $U = 0$. By putting $U = 0$ in A_5, we get $a = 0$, which is a contradiction.

Case 2: $C_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x$, $\beta \in \mathbb{F}_q^*$. Then, there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy

$$C_2(x) = V + S(-7\beta^3(Tx + U) + 14\beta^2(Tx + U)^3 - 7\beta(Tx + U)^5 + (Tx + U)^7).$$

By comparing terms with identical powers, we obtain

$$\begin{aligned} &ST^7 = 1, 7UT^6 = 0, A_1 = 21U^2ST^5 - 7ST^5\beta, \\ &A_2 = 35U^3ST^4 - 35UST^4\beta, \\ &A_3 = 35U^4ST^3 - 70U^2StT^3\beta - 14ST^3\beta^2, \\ &A_4 = 21U^5ST^2 - 70U^3ST^2\beta + 42UST^2\beta^2, \\ &A_5 = 7U^6ST - 35U^4ST\beta + 42U^2ST\beta^2 - 7ST\beta^3, \\ &V + U^7S - 7\beta U^5S + 14\beta^2U^3S - 7\beta^3US = 0. \end{aligned} \tag{22}$$

Given that $ST \neq 0$, therefore $7UST^6 = 0$ implies that $7U = 0$. Also, $q \not\equiv 0 \pmod 7$, therefore $U = 0$. By putting $U = 0$ in $A_4 = 0$ and $A_2 = 0$, we get

$$\begin{aligned} ab^q + a^q b &= 0, \\ a^q + a &= 0. \end{aligned} \tag{23}$$

From equation (23), we get $(b^q - b)\, a = 0$. Also, $a \neq 0$ gives $b^q = b$. Further, from $A_3 = 14ST^3\beta^2$ and $b^q = b$, we obtain

$$b^2 = 14ST^3\beta^2. \tag{24}$$

From $A_1 = -7ST^5\beta$ and $b^q = b$, we get $2b = -7st^5w$. Thus,

$$4b^2 = 49S^2T^{10}w^2. \tag{25}$$

From equation (24) and equation (25)

$$4 \cdot 14ST^3\beta^2 = 49S^2T^{10}\beta^2,$$

$$ST^3\beta^2(8 - 7ST^7) = 0.$$

Since $stw \neq 0$, it follows that $7ST^7 = 8$. Also, $ST^7 = 1$, from equation (22). Therefore, we arrive at contradiction $8 = 7$.

Theorem 4.3: *Let* $q = 7^k$ *such that* $k \geq 3$. *For* $a, b \in \mathbb{F}_{q^2}^*$,

$$C(x) = x(x^{3q+3} + bx^{q+1} + a)$$

is a PP over $\mathbb{F}_{q^2}$ *if and only if*

(i) $A_2 \neq 0, (A_2)^{\frac{q-1}{3}} \neq 1, A_4 = \frac{3A_3^2}{A_2}$ and $A_5 = 2A_2^2 - \frac{3A_3^3}{A_2^2}$.

(ii) A_1 is not a square in $\mathbb{F}_q, A_3 = \frac{5A_1^3 - A_2^2}{A_1}, A_4 = \frac{3A_1^3A_2 + 4A_2^3}{A_1^2}$ and $A_5 = -\frac{(A_1^6 - 2A_1^3A_2^2 + A_2^4)}{A_2^3}$.

Proof: As discussed in previous theorem, $C(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $C_2(x) \cong x^7$ or $x(x^{\frac{6}{s}} - \beta)^s$, $s \in \{1, 2, 3\}$ with $\beta^{\frac{s(q-1)}{6}} \neq 1$.

Case 1: When $C_2(x) \cong x^7$, then there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfies

$$C_2(x) = V + S(U + Tx)^7.$$

By comparing terms with identical powers, we obtain

$$A_1 = A_2 = A_3 = A_4 = A_5 = 0. \tag{26}$$

Now, $A_2 = 0$ and $A_5 = 0$ implies that $a = 0$ and $b = 0$, which leads to a contradiction.

Case 2: Consider $C_2(x) \cong x^7 - \beta x$ satisfies $\beta^{\frac{q-1}{6}} \neq 1$. Then, there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy

$$\begin{aligned} C_2(x) &= V + S((U+Tx)^7 - \beta(U+Tx)) \\ &= ST^7x^7 - S\beta Tx + SU^7 - S\beta U + V. \end{aligned}$$

By comparing terms with identical powers, we obtain

$$ST^7 = 1, A_1 = 0, A_2 = 0, A_3 = 0, A_4 = 0, A_5 = -S\beta T, SU^7 - S\beta U + V = 0. \quad (27)$$

Now, $A_3 = 0$ establishes $b = 0$ which contradicts the fact that $b \neq 0$.

Case 3: $C_2(x) \cong x(x^3 - \beta)^2$ satisfies $\beta^{\frac{q-1}{3}} \neq 1$. Then, there exist U, V and non-zero $S, T \in \mathbb{F}$ satisfy $C_2(x) = V + S(Tx+U)((Tx+U)^3 - \beta)^2$.

By comparing terms with identical powers, we obtain

$$\begin{aligned} &ST^7 = 1, A_1 = 0, A_2 = 5ST^4\beta, A_3 = 6UST^3\beta, A_4 = 2U^2ST^2\beta, \\ &A_5 = 5\beta^2\beta T - U^3T, V + U^7S - 2\beta U^4S + US\beta^2 = 0. \end{aligned} \quad (28)$$

Using $ST^7 = 1$, eliminate S in the above set of equations to obtain

$$\begin{aligned} &A_1 = 0, 2\beta + T^3A_2 = 0, U\beta + T^4A_3 = 0, U^2\beta + 3T^5A_4 = 0, \\ &U^3\beta + T^6A_5 = 0, VT^7 + U^7 + 5U^4\beta + U\beta^2 = 0. \end{aligned}$$

Now, eliminating U using $U\beta + T^4A_3 = 0$ in the above set of equations, we conclude

$$\begin{aligned} &A_1 = 0, 2\beta T^3A_2 = 0, T^3A_3^2 + 3A_4\beta = 0, \\ &T^{12}A_3^3 - T^6A_5\beta^2 + \beta^4 = 0, \\ &VT^3\beta^7 - T^{24}A_3^7 + 5T^{12}A_3^4\beta^4 - A_3\beta^8 = 0. \end{aligned}$$

Since $A_2 \neq 0$, using $2\beta + T^3 = 0$, we obtain

$$A_2 \neq 0, A_4 = \frac{3A_3^2}{A_2} \text{ and } A_5 = 2A_2^2 - \frac{3A_3^3}{A_2^2}.$$

In converse part, assume that (i) is satisfied. So, for $T = S = 1$, $U = \frac{2A_3}{A_2}$, $\beta = 3A_2$, $V = \frac{4A_3^7}{A_2^7} + \frac{2A_3^4}{A_2^3} + 4A_2A_3$, we obtain

$$C_2(x) = S(Tx+U)(-\beta+(Tx+U)^3)^2+V.$$

Case 4: $C_2(x) \cong x(x^2-w\beta)^3$ satisfies $\beta^{\frac{q-1}{2}} \neq 1$. Then, there exist U, V and non-zero $S, T \in \mathbb{F}_q$ and satisfy

$$\begin{aligned} &ST^7 = 1, A_1 = 4ST^5\beta, A_2 = 6UST^4\beta, A_3 = 5U^2ST^3\beta - 3ST^3\beta^2, \\ &A_4 = 5U^3ST^2\beta + 2\beta^2UST^2, A_5 = 6U^4ST\beta + 2\beta^2U^2ST - \beta^3ST, \\ &V + U^7S + 4U^5S\beta + 3U^3S\beta^2 - US\beta^3 = 0. \end{aligned} \tag{29}$$

Now, eliminate S, utilizing $ST^7 = 1$, we obtain

$$\begin{aligned} &T^2A_1 + 3\beta = 0, U\beta T^3A_2 = 0, U^2\beta + 4T^4A_3 + 2\beta^2 = 0 \\ &U^3\beta + 6U\beta^2 + 4T^5A_4 = 0, U^4\beta + 5U^2\beta^2 + T^6A_5 + w\beta^3 = 0, \\ &VT^7 + U^7 + 4U^5\beta + 3U^3\beta^2 - U\beta^3 = 0. \end{aligned}$$

Here, eliminate U, in the above set of equations by using $U\beta + T^3A_2 = 0$, we get

$$\begin{aligned} &T^2A_1 + 3\beta = 0, T^6A_2^2 + 4TA_3\beta + 2\beta^3 = 0, \\ &T^6A_2^3 + 3T^2A_4\beta^2 + 6A_2\beta^3 = 0, T^{12}A_2^4 + 5T^6A_2^2\beta^3 + T^6A_5\beta^3 + \beta^6 = 0, \\ &VT^4\beta^7 + 6T^{18}A_2^7 + 3T^{12}A_2^5\beta^3 + 4T^6A_2^3\beta^6 + A_2\beta^9 = 0. \end{aligned}$$

Eliminate β, using $T^2A_1 + 3\beta = 0$ in above set of equations, which gives

$$\begin{aligned} &A_1^3 + 4A_1A_3 + 4A_2^2 = 0, \\ &A_1^3A_2 + 2A_1^2A_4 + 6A_2^3 = 0, \\ &A_1^6 + 5A_1^3A_2^2 + A_1^3A_5 + A_2^4 = 0, \\ &vA_1^7 + 4A_1^9A_2 + 2A_1^6A_2^3 + 5A_1^3A_2^5 + 3A_2^7 = 0. \end{aligned} \tag{30}$$

From the above set of equations, we obtain

$$\begin{aligned} &A_1 \text{ is not a square in } \mathbb{F}_q, \\ &A_3 = \frac{5A_1^3 - A_2^2}{A_1}, A_4 = \frac{3A_1^3A_2 + 4A_2^3}{A_1^2} \\ &\text{and } A_5 = -\frac{(A_1^6 - 2A_1^3A_2^2 + A_2^4)}{A_2^3}. \end{aligned}$$

In Converse part, assume that (*ii*) is satisfied. So, for $T = S = 1$, $U = \frac{3A_2}{A_1}$, $\beta = 2A_1$, $V = \frac{4A^7}{A_1^7} + \frac{2A_2^5}{A_1^4} + \frac{5A_2^3}{A_1} + 3A_1^2A_2$, we get

$$C_2(x) = V + S((-\beta + Tx + U)^2)^3(Tx + U).$$

As of now, we examine the trinomial

$$D(x) = x(x^{3q+1} + bx^{q+1} + a)$$

over $\mathbb{F}_{q^2}$.

Because $\gcd(1, q+1) = 1$ and utilizing Lemma 2.5, the $D(x) = x(x^{3(q+3)} + bx^{q+1} + a)$ permutes $\mathbb{F}_{q^2}$ if and only if and $D_1(x) = x(x^3 + bx^2 + a)^{q+1}$ is a PP over $\mathbb{F}_q^*$ as $\mu_{q-1} = \mathbb{F}_q^*$.

We represent $D_1(x) = x(x^3 + bx^2 + a)^{q+1}$ in a simplified polynomial of degree 7 which is obtained as follows:

Let $\alpha \in \mathbb{F}_q$

$$\begin{aligned} D_1(\alpha) &= \alpha(\alpha^3 + b\alpha^2 + a)^{q+1} \\ &= \alpha(\alpha^6 + (b^q + b)\alpha^5 + b^{q+1}\alpha^4 + (a^q + a)\alpha^3 + (a^q b + ab^q)\alpha^2 + a^{q+1}) \\ &= \alpha^7 + (b^q + b)\alpha^6 + b^{q+1}\alpha^5 + (a^q + a)\alpha^4 + (a^q b + ab^q)\alpha^3 + a^{q+1}\alpha. \end{aligned}$$

By taking, $A_1 = b^q + b, A_2 = b^{q+1}, A_3 = a^q + a, A_4 = a^q b + ab^q$ and $A_5 = a^{q+1}$. So, $D_1(x)$ permutes $\mathbb{F}_q$ if and only if

$$D_2(x) = x^7 + A_1x^6 + A_2x^5 + A_3x^4 + A_4x^3 + A_5x$$

is a PP over $\mathbb{F}_q$.

Theorem 4.4: *Let $q = 2^k$, where k is a positive integer, Then, $a, b \in \mathbb{F}_{2^{2k}}^*$, the polynomial*

$$D(x) = x(x^{3q+3} + bx^{2q+2} + a)$$

is a PP over $\mathbb{F}_{2^{2k}}$ if and only if

(i) *either $a = b$ or $(a+b)^2 + (a+b) + 1 = 0$, whenever $q = 2$.*

(ii) *$a^4 + a + 1 = 0$ whenever $q = 4$.*

(iii) *$a = 1$ and $b = 1$ whenever $q > 8$ and $k \not\equiv 0 \pmod 3$.*

Proof: Because $\gcd(1, q+1) = 1$ and by utilizing Lemma 2.5, the trinomial $D(x) = x(x^{3q+3} + bx^{2q+2} + a)$ permutes $\mathbb{F}_{2^{2k}}$ if and only if $D_1(x) = x(x^3 + bx^2 + a)^{q+1}$ is a PP over $\mathbb{F}_{2^k}$.

Also, $D_1(x)$ permutes $\mathbb{F}_{2^k}$ if and only if $D_2(x)$ permutes $\mathbb{F}_{2^k}$. The PP of degree 7 over $\mathbb{F}_{2^k}$ is equivalent to one of the given polynomial in Lemma 2.1.

Case 1: For $q=2$, $D_2(x) \equiv (1+A_1 + A_2 + A_3 + A_4 + A_5)x \pmod{x^2+x}$ is a PP if and only if $A_5 + A_4 + A_3 + A_2 + A_1 1 + \neq 0$, this implies $A_5 + A_4 + A_3 + A_2 + A_1 = 0$, that is $(1+(b+a) + (b+a)^2)\ (b+a) = 0$. Therefore, either $1 + (b+a) + (b+a)^2 = 0$ or $b = a$

Case 2: For $q=4$, $D_2(x) \equiv A_1x^3 + A_2x^2 + (A_3+1)x \pmod{x^4+x}$. Because 3 divides $q-1$, then PP of degree 3 does not exist $\mathbb{F}_{2^k}$ by Corollary 2.1. So, $A_1 = 0$, which gives $b^q = b$ and $D_2(x) \equiv b^2x^2 + (a^4+a+1)x$.

For $D_2(x)$ to be normalised PP, when $a^4+a+1=0$.

Case 3: For $q \geq 8$, if $m \equiv 0 \pmod 3$ then $7 \mid q-1$ there does not exist PP of degree 7 by Corollary 2.1. For $q > 8$ and $k \not\equiv 0 \pmod 3$, the PP of degree 7 is equivalent to the polynomial given in Lemma 2.1.

Subcase 1: Consider $D_2(x) \equiv x^7$. By comparing terms with identical powers, we obtain

$$A_1 = A_2 = A_3 = A_4 = A_5 = 0.$$

Since $A_2 = 0$ and $A_5 = 0$, so $a=0$ and $b=0$, which is a contradiction.

Subcase 2: Consider $D_2(x) \equiv x^7 + x^5 + x$.

By comparing terms with identical powers, we obtain

$$A_1 = 0, A_2 = 1, A_3 = 0, A_4 = 0, A_5 = 1$$

which gives $b^q = b, b^2 = 1, a^q = a, a^2 = 1$. Therefore, $a=1$ and $b=1$, when $q > 8$.

Theorem 4.5: *Let* $q = p^k > 409$, *such that* $q \not\equiv 0$ or $1 \pmod 7$ *and* 7 *is not a square in* $\mathbb{F}_q$. *For* $a, b \in \mathbb{F}_{q^2}^*$,

$$D(x) = x(x^{3q+3} + bx^{2q+2} + a)$$

is a PP over $\mathbb{F}_{p^{2k}}$ *if and only if*

$$A_1 = A_3 = 0, A_2 \neq 0, A_4 = \frac{2}{7}A_2^2, A_5 = \frac{1}{49}A_2^3.$$

Proof: For $q = p^k > 409$ and $q \not\equiv 0 \text{ or } 1 \pmod 7$. Utilizing Lemma 2.5, $D(x)$ is a PP over $\mathbb{F}_{q^2}$ if and only if $D_1(x)$ permutes $\mathbb{F}_q$. $D_1(x)$ permutes $\mathbb{F}_q$ if and only if the polynomial $D_2(x)$ is an exceptional in $\mathbb{F}_q$ by utilizing Lemma 2.4,

By Lemma 2.2, $D_2(x)$ permutes $\mathbb{F}_q$ if and only if $D_2(x) \cong x^7$ or $q \not\equiv -1 \pmod 7$ or $D_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x$, for some $\beta \in \mathbb{F}_q^*$.

Case 1: When $D_2(x) \cong x^7$, then there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy $D_2(x) = V + S(Tx + U)^7$. By comparing terms with identical powers, we obtain

$$ST^7 = 1, A_1 = 7UST^6, A_2 = 35U^3ST^4, A_3 = 21U^2ST^5,$$
$$A_4 = 35U^4ST^3, A_5 = 7U^6ST, SU^7 + V = 0.$$

Since $ST \neq 0$, therefore $21U^5ST^2 = 0$ which implies that $21u^5 = 0$. Also, $q \not\equiv 0 \pmod 7$ therefore, either $p = 3$ or $U = 0$. If $p = 3$, then $A_2 = 0$ establishes $b = 0$, this goes against the fact that $b \neq 0$. Similarly for $U = 0$ gives $A_2 = 0$ which establishes that $b = 0$, leads to a contradiction.

Case 2: When $D_2(x) \cong x^7 - 7\beta x^5 + 14\beta^2 x^3 - 7\beta^3 x$ for some $\beta \in \mathbb{F}_q^*$. Then, there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy

$$D_2(x) = V + S(-7\beta^3(Tx + U) + 14\beta^2(Tx + U)^3 - 7\beta(Tx + U)^5 + (Tx + U)^7).$$

By comparing terms with identical powers, we obtain

$$ST^7 = 1, A_1 = 7UST^6, A_2 = 21U^2ST^5 - 7ST^5\beta,$$
$$A_3 = 35U^3ST^4 - 35UST^4\beta,$$
$$A_4 = 35U^4ST^3 - 70U^2ST^3\beta + 14ST^3\beta^2,$$
$$A_5 = 7U^6ST - 35U^4ST\beta + 42U^2ST\beta^2 - 7ST\beta^3,$$
$$V + U^7S - 7U^5S\beta + 14U^3S\beta^2 - 7US\beta^3 = 0,$$
$$21U^5ST^2 - 70U^3ST^2\beta + 42UST^2\beta^2 = 0.$$

Since $ST \neq 0$ and $q \not\equiv 0 \pmod 7$, therefore $21U^5ST^2 - 70U^3ST^2\beta + 42UST^2\beta^2 = 0$ implies that $U(3U^4 + 4U^2\beta + 6\beta^2) = 0$. Thus, $U = 0$ or $3U^4 - 10U^2\beta + 6\beta^2 = 0$.

If $U=0,$ then

$$A_1=0, A_2=-7ST^5, A_3=0, A_4=14ST^3\beta^2, A_5=-7ST\beta^3, V=0.$$

Eliminating S using $ST^7=1$ in the above set of equations, we get

$$A_2T^2+7\beta=0, A_4T^4-14\beta^2=0, A_5t^6+7\beta^3=0.$$

Using $A_2T^2+7\beta=0,$ eliminate β to obtain

$$A_1=A_3=0, A_2\neq 0, A_4=\frac{2}{7}A_2^2, A_5=\frac{1}{49}A_2^3.$$

If $3U^4-10U^2\beta+6\beta^2=0,$ then $\beta=\frac{(5\pm\sqrt{7})U^2}{6}$, but 7 is a square element $\mathbb{F}_q$ and this leads a contradiction. Conversly, suppose the given condition holds. Then, for $S=T=1,\ U=0,\ V=0,\ \beta=-\frac{A_2}{7},$ we get

$$D_2(x)=V+S(-7\beta^3(U+Tx)+14\beta^2(U+Tx)^3-7\beta(U+Tx)^5+(U+Tx)^7).$$

Hence proved.

Theorem 4.6: *Let* $q=7^k$ *with* $k\geq 3$. *For* $a,b\in\mathbb{F}_{q^2}^*$,

$$D(x)=x(x^{3q+3}+bx^{2q+2}+a)$$

is not a PP over $\mathbb{F}_{q^2}$.

Proof: As discussed in the previous theorem, $D(x)$ permutes $\mathbb{F}_q$ if and only if $D_2(x)\cong x^7$ or $x(x^{\frac{6}{s}}-\beta)^s$, $s\in\{1,2,3\}$ with $\beta^{\frac{q-1}{s}}\neq 1$.

Case 1: When $D_2(x)\cong x^7$. Then, there exist U,V and non-zero $S,T\in\mathbb{F}_q$ satisfy

$$D_2(x)=V+S(Tx+U)^7.$$

By comparing terms with identical powers, we conclude

$$A_1=A_2=A_3=A_4=A_5=0.$$

Here, $A_3=0$ establishes $b=0,$ leads to a contradiction.

Case 2: When $D_2(x)\cong x^7-\beta x,$ satisfies $\beta^{\frac{q-1}{6}}\neq 1,$ then there exist U,V and non-zero $S,T\in\mathbb{F}$ satisfy $F(x)=V+S((Tx+U)^7-\beta(Tx+U))$.

By comparing terms with identical powers, we obtain $A_3 = 0$ which gives $b = 0$ and that contradicts $b \neq 0$.

Case 3: When $D_2(x) \cong x(x^3 - \beta)^2$ satisfies $\beta^{\frac{q-1}{3}} \neq 1$, so there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy $D_2(x) = V + S(U + Tx)\ ((U + Tx)^3 - \beta)^2$.

By comparing terms with identical powers, we obtain

$$ST^7 = 1, A_1 = 0, A_3 = 0.$$

Now, $A_3 = 0$ establishes $b = 0$, this goes against the fact that $b \neq 0$.

Case 4: When $D_2(x) \cong x(x^2 - \beta)^3$ satisfies $\beta^{\frac{q-1}{2}} \neq 1$, so there exist U, V and non-zero $S, T \in \mathbb{F}_q$ satisfy $D_2(x) = V + S(U + Tx)\ ((U + Tx)^2 - \beta)^3$.

By comparing terms with identical powers, we obtain

$$\begin{aligned}
&ST^7 = 1, A_1 = 0, A_2 = 4ST^5\beta, A_3 = 6UST^4\beta,\\
&A_4 = 5U^2ST^3\beta + 3ST^3\beta^2,\\
&A_5 = 6U^4ST\beta + 2U^2ST\beta^2 - ST\beta^3,\\
&5U^3ST^2 + 2UST^2\beta^2 = 0,\\
&UT^7 + U^7 4T^5\beta + 3U^3\beta^2 - 4\beta^3 = 0.
\end{aligned}$$

Since $ST\beta \neq 0$, therefore $5U^3ST^2 + 2UST^2\beta^2 = 0$ implies that either $U = 0$ or $U^2 = \beta$. By putting $U = 0$ in A_3 gives $b = 0$, this goes against the fact that $b \neq 0$. If $U^2 = \beta$, then $T^6A_5 = 0$. Since $T \neq 0$, therefore $A_5 = 0$ implies that $a = 0$, but this is a condratiction to $a \neq 0$. Hence, $g(x) = x(x^{3q+3} + + a)$ is not a PP.

5. Conclusion

In this manuscript, we classified the PPs of the type $xh(x^{q+1})$ where $h(x) = x^{s_1} + bx^{s_2} + a$ over $\mathbb{F}_{q^2}$. We investigated the existence of permutation binomials and trinomials of the above type over $\mathbb{F}_{q^2}$ with some restrictions on coefficients.

Acknowledgements

The second author acknowledges UGC India's financial assistance.

References

[1] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Their Appl.*, vol. 15, no. 2, pp. 195-206 (2009).

[2] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{\frac{q-1}{l}})$, *Int. J. Math. Math. Sci.*, vol. 2007, no. 1, 23408 (2007), https://doi.org/10.1155/2007/23408.

[3] M. Alizadeh, M. R. Darafsheh, and S. Mehrabi, On the *k*-normal elements and polynomials over finite fields, *Ital. J. Pure Appl. Math.*, vol. 39, pp. 451-464 (2018).

[4] D. Bartoli, Permutation trinomials over $\mathbb{F}_{q^3}$, *Finite Fields Their Appl.*, vol. 61, 101597 (2020).

[5] D. Bartoli and M. Timpanella, A family of permutation trinomials over $\mathbb{F}_{q^2}$, *Finite Fields Their Appl.*, vol. 70, 101781 (2021).

[6] D. Bartoli, M. Giulietti, and G. Zini, On monomial complete permutation polynomials, *Finite Fields Their Appl.*, vol. 41, pp. 132-158 (2016).

[7] D. Bartoli, M. Giulietti, L. Quoos, and G. Zini, Complete permutation polynomials from exceptional polynomials, *J. Number Theory*, vol. 176, pp. 46-66 (2017).

[8] L. A. Bassalygo and V. A. Zinoviev, On one class of permutation polynomials over finite fields of characteristic two, *Mosc. Math. J.*, vol. 15, pp. 703-713 (2015).

[9] L. A. Bassalygo and V. A. Zinoviev, Permutation and complete permutation polynomials, *Finite Fields Their Appl.*, vol. 33, pp. 198-211 (2015).

[10] T. Baumbaugh and F. Manganiello, Matroidal root structure of skew polynomials over finite fields, *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 3, pp. 377-389 (2019), https://doi.org/10.1080/09720529.2019.1600845

[11] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Comb. Theory - A*, vol. 113, no. 7, pp. 1526-1535 (2006).

[12] C. Ding and T. Helleseth, Optimal ternary cyclic codes from monomials, *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5898-5904 (2013).

[13] C. Ding, L. Qu, Q. Wang, J. Yuan, and P. Yuan, Permutation trinomials over finite fields with even characteristic, *SIAM J. Discrete Math.*, vol. 29, no. 1, pp. 79-92 (2015).

[14] X. Fan, A classification of permutation polynomial of degree 7 over finite fields, *Finite Fields Their Appl.*, vol. 59, pp. 1-21 (2019).

[15] X. Feng, , D. Lin, , L. Wang, and Q. Wang, Further results on complete permutation monomials over finite fields, *Finite Fields Their Appl.*, vol. 57, pp. 47-59 (2019).

[16] N. Fernando, A Note on Permutation Binomials and Trinomials over Finite Fields, *N. Z. J. Math.*, vol. 48, pp. 25-29 (2018).

[17] M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, *Isr. J. Math.*, vol. 82, pp. 157-225 (1993).

[18] R. Gupta and R. K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Their Appl.*, vol. 41, pp. 89-96 (2016).

[19] R. Gupta, L. Quoos, and Q. Wang, Some classes of permutation binomials and trinomials of index $q-1$ over $\mathbb{F}_{q^n}$, *Cryptogr. Commun.*, vol. 16, no. 2, pp. 387-402 (2023).

[20] S. Gupta, M. Singh, and M. Harish, On the Study of Families of Linearized Polynomials over Finite Fields, *Contemp. Math.*, vol. 4, no. 3, 518-529 (2023).

[21] X. D. Hou, A class of permutation binomials over finite fields, *J. Number Theory*, vol. 133, no. 10, pp. 3549-3558 (2013).

[22] X. D. Hou, Determination of a type of permutation trinomials over finite fields, *Acta Arith.*, vol. 3, no. 166, pp. 253-278 (2014).

[23] X. D. Hou, Determination of a type of permutation trinomials over finite fields, II, *Finite Fields Their Appl.*, vol. 35, pp. 16-35 (2015).

[24] X. D. Hou, A survey of permutation binomials and trinomials over finite fields, *Contemp. Math.*, vol. 632, pp. 177-191 (2015).

[25] X. D. Hou, Permutation polynomials over finite fields'a survey of recent advances, *Finite Fields Their Appl.*, vol. 32, pp. 82-119 (2015).

[26] X. D. Hou and S. D. Lappano, Determination of a type of permutation binomials over finite fields, *J. Number Theory*, vol. 147, pp. 14-23 (2015).

[27] L. Işık and A. Winterhof, Carlitz rank and index of permutation polynomials, *Finite Fields Their Appl.*, vol. 49, pp. 156-165 (2018).

[28] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Their Appl.*, vol. 13, no. 1, pp. 58-70 (2007).

[29] J. Li, , D. B. Chandler, and Q. Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, *Finite Fields Their Appl.*, vol. 16, no. 6, pp. 406-419 (2010).

[30] S. D. Lappano, A note regarding permutation binomials over $\mathbb{F}_{q^2}$, *Finite Fields Their Appl.*, vol. 34, pp. 153-160 (2015).

[31] N. Li and T. Helleseth, Several classes of permutation trinomials from Niho exponents, *Cryptogr. Commun.*, vol. 9, pp. 693-705 (2017).

[32] K. Li, , L. Qu, and X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Their Appl.*, vol. 43, pp. 69-85 (2017).

[33] N. Li and T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *Cryptogr. Commun.*, vol. 11, pp. 129-136 (2019).

[34] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, Second Edition, (1983).

[35] R. Lidl and W. B. Muller, Permutation polynomials in RSA-cryptosystems, in *Advances in Cryptology*, Plenum, New York, pp. 293-301 (1984).

[36] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Am. Math. Mon.*, vol. 95, no. 3, pp. 243-246, (1988).

[37] R. Lidi and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, II, *Am. Math. Mon.*, vol. 100, no. 1, pp. 71-74 (1993).

[38] R. Kim and H. S. Son, Recursive constructions of k-normal polynomials using some rational transformations over finite fields, *J. Algebra Appl.*, vol. 19, no. 11, 2050210 (2020).

[39] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $GF(2^s)$, *Finite Fields Their Appl.*, vol. 8, pp. 52-68 (2002).

[40] G. L. Mullen, Permutation polynomials over finite fields, Finite fields, coding theory, and advances in communications and computing, in *Lecture Notes in Pure and Applied Mathematics,* vol. 141, pp. 131-151 Marcel Dekker, New York, (1993).

[41] G. L. Mullen and Q. Wang, Permutation polynomials of one variable, in *Handbook of Finite Fields*, CRC, (2014).

[42] G. L. Mullen, D. Wan, and Q. Wang, An index bound on value sets of polynomial maps over finite fields, in Proceedings of workshop on the occasion of Harald Niederreiter's 70th Birthday: *J. Algebra Appl. Math.*, pp. 280-296 (2014).

[43] P. Müller, A Weil-bound free proof of Schur's conjecture, *Finite Fields Their Appl.*, vol. 3, no. 1, pp. 25-32 (1997).

[44] F. Özbudak and B. G. Temür, Classification of permutation polynomials of the form $x^3 g(x^{q-1})$ of $\mathbb{F}_{q^2}$ where $g(x) = x^3 + bx +$ c and b, c is an element of $\mathbb{F}_q^*$, *Des. Codes Cryptogr.*, vol. 90, no. 7, pp. 1537-1556 (2022).

[45] F. Özbudak and B. G. Temür, Complete characterization of some permutation polynomials of the form $x^r(1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$ over $\mathbb{F}_{q^2}$, *Cryptogr. Commun.*, vol. 15, pp. 775-793 (2023).

[46] Y. H. Park and J. B. Lee, Permutation polynomials and group permutation polynomials, *Bull. Aust. Math. Soc.*, vol. 63, no. 1, pp. 67-74 (2001).

[47] J. Schwenk and K. Huber, Public key encryption and digital signatures based on permutation polynomials, *Electron. Lett.*, vol. 34, no. 8, pp. 759-760 (1998).

[48] P. L. Sharma, Ashima, and A. K. Sharma, Recursive construction of normal polynomials over finite fields, *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 8, pp. 2645-2660 (2022).

[49] R. K. Sharma and R. Gupta, Determination of a type of permutation binomials and trinomials, *Appl. Algebra Eng. Commun. Comput.*, vol. 31, no. 1, pp. 65-86 (2020).

[50] M. Singh, S. Gupta, and P. L. Sharma, On permutation and complete permutation binomials and trinomials from linearized polynomials over finite fields, *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 3, pp. 1073-1085 (2024).

[51] Z. Tu, X. Zeng, C. Li, and T. Helleseth, A class of new permutation trinomials, *Finite Fields Their Appl.*, vol. 50, pp. 178-195 (2018).

[52] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure, *Monatshefte für Mathematik*, vol. 112, pp. 149-163 (1991).

[53] D. Wan and Q. Wang, Index bounds for character sums of polynomials over finite fields, *Des. Codes Cryptogr.*, vol. 81, pp. 459-468 (2016).

[54] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, sequences, subsequences, and consequences, (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), in *Lect. Notes Comput. Sci.*, vol. 4893, pp. 119-128, Springer, Berlin, (2007).

[55] Q. Wang, Polynomials over finite fields: an index approach, in *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, Degruyter, vol. pp. 319-348 (2019).

[56] Y. Wang, W. Zhang, and Z. Zha, Six New Classes of Permutation Trinomials over $\mathbb{F}_{2^n}$, *SIAM J. Discrete Math.*, vol. 32, no. 3, pp. 1946-1961 (2018).

[57] Y. Wang, Z. Zha, and W. Zhang, Six new classes of permutation trinomials over $\mathbb{F}_{3^{3k}}$, *Appl. Algebra Eng. Commun. Comput.*, vol. 29, pp. 479-499 (2018).

[58] B. Wu and Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields Their Appl.*, vol. 22, pp. 79-100 (2013).

[59] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Their Appl.*, vol. 28, pp. 148-165 (2014).

[60] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of complete permutation polynomials over $\mathbb{F}_q$, *Sci. China Math.*, vol. 58, no. 10, pp. 1-14 (2015).

[61] D. Wu, P. Yuan, C. Ding, and Y. Ma, Permutation trinomials over $\mathbb{F}_{q^2}$, *Finite Fields Their Appl.*, vol. 46, pp. 38-56 (2017).

[62] Z. Zha, L. Hu, and S. Fan, Further results on permutation trinomials over finite fields with even characteristic, *Finite Fields Their Appl.*, vol. 45, pp. 43-52 (2017).

[63] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{\frac{q-1}{d}})$, *Proc. Am. Math. Soc.*, vol. 137, pp. 2209-2216 (2009).

[64] M. E. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory*, vol. 4, no. 5, pp. 851-857 (2008).

[65] M. E. Zieve, Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, arXiv:1312.1325, (2013).

Received January, 2024