*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 3, pp. 1073–1085
DOI : 10.47974/JDMSC-1836

# On permutation and complete permutation binomials and trinomials from linearized polynomials over finite fields

Manpreet Singh
Shalini Gupta *
P. L. Sharma
*Department of Mathematics and Statistics*
*Himachal Pradesh University*
*Shimla 171005*
*Himachal Pradesh*
*India*

**Abstract**

In recent years, researchers have shown considerable interest in linearized polynomials and permutation polynomials over finite fields primarily because of their wide-ranging applications in fields such as cryptography, coding theory and communications theory. With their compact algebraic form and remarkable properties, permutation binomials and trinomials find extensive applications in the realms of mathematics and engineering. In this paper, we present a class of linearized polynomials over finite fields to construct permutation and complete permutation binomials and trinomials over $\mathbb{F}_{p^n}$ subject to certain conditions.

***Subject Classification:*** *(2010) 12E05, 12E20.*

***Keywords:*** *Linearized polynomial, Permutation polynomial, Complete permutation polynomial, Binomial, Trinomial.*

## 1. Introduction

Linearized polynomial was introduced by Ore [18] in 1933. Linearized polynomial is an active area of research in recent years [11, 17]. The main task is to determine the count of zeros of linearized polynomials. The results related to zeros of linearized polynomials of type $T_l^k(X)$ and $S_l^k(X)$ are discussed in [14, 15, 16]. The polynomials over finite fields play an important role in coding theory and cryptography. In [2], authors explored

* *E-mail:* **shalini.garga1970@gmail.com**

© Taru Publications

the matroidal root structure of skew polynomials over finite fields. Yi et al. [23] introduced and executed a hardware architecture for Gaussian elimination in finite fields aiming to enhance MQ cryptographic systems on Internet of Things (IoT) devices. The number of zeros of linearized polynomial plays a vital role in cryptography. Linearized polynomial which has only one zero and is bijective also gives us permutation polynomial, see [11].

Permutation polynomial(PP) over finite fields finds numerous uses in the fields of coding theory, cryptography, combinatorics, etc. Construction and applications of PPs are discussed in [11, 17]. PPs are used to encrypt and decrypt the data while sending the messages from one person to another. Various types of PPs are investigated in recent years. Charpin and Kyureghyan [3] examined polynomials of the form $F(X) = G(X) + \gamma \mathrm{Tr}(H(X))$, demonstrating that if $G(X)$ is a PP or linearized polynomial, then $F(X)$ is a PP. This result is used to presents six classes of such PPs. Zieve in [25] discussed the conditions for the polynomial of the form $X^r H(X^{(q-1)/d})$ to be PP. Additionally, an in-depth overview of recent progress in PP over finite fields was given by Hou in [10] where the author discussed permutation binomial(PB), permutation trinomial(PT), PP defined by functional equations and various PPs from linearized polynomials. Zeng [24] demonstrated that two newly defined polynomials of the form $(X^{2^k} + X + \delta)^s + X$ over $\mathbb{F}_{p^n}$, satisfying specific conditions, are PPs.

Due to their compact structure binomials and trinomials are used in various fields like cryptography and coding theory. Several types of PBs and PTs are investigated by number of researchers in recent times. Hou [7] derived certain conditions for the binomial of the type $f = tX + X^{2q-1}$ to be a PB over finite fields. Hou [9] explored the conditions under which the polynomial $f(X) = aX + X^{3q-2}$ is a PB over the finite field $\mathbb{F}_{q^2}$. Li et al. [12] discussed some novel classes of PBs and PTs over finite fields. Tu and Zeng [20] presented the polynomial $g(X) = X + a_1 X^{q(q-1)+1} + a_2 X^{2(q-1)+1}$ over $\mathbb{F}_{q^2}$, where $q$ is an odd prime, and they identified the set of pairs $(a_1, a_2)$ for which $g(X)$ forms a permutation over $\mathbb{F}_{q^2}$. Wu et al. [21] described the determination of PP over $\mathbb{F}_{p^{2m}}$ and proved some conjectures related to PP. It was shown by Ding et al. [4] that the trinomial $f(X) = X + X^{2^{(m-1)/2}} + X^{2^m - 2^{(m+1)/2}+1}$ is a PP. Gupta and Sharma [5] discussed four classes of PTs of the form $X^r H(X^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$. The trinomial $f(X) = X + tX^q + X^{2q-1}$ is categorized as a PT if and only if it meets the specified conditions outlined in [8].

Complete permutation polynomial(CPP) has attracted the attention of authors in recent past. Wu et al. [22] discussed four classes of complete permutation monomials over finite fields of characteristic two. Tu et al. [19] investigated three classes of monomials and one class of trinomial over finite field of even characteristic. Three classes of complete permutation monomials over finite fields of odd characteristic are discussed by Guangkui and Cao [6]. Bassalygo and Zinoviev described CPP of the type $X^{q+2}+bX$ over $\mathbb{F}_{q^2}$ and $X^{q^2+q+2}$ over $\mathbb{F}_{q^3}$ in [1]. Ma et al. [12] derived four classes of complete permutation monomials and one class of complete permutation trinomial over finite fields.

Motivated by the above work, in this paper, we investigate the linearized binomials and trinomials of the type $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$ and derive restrictions for them to be PBs and PTs . Further, the conditions for permutation monomials, binomials and trinomials from $T_l^k(X)$ and $S_l^k(X)$ are derived to get complete permutation monomials, binomials and trinomials over $\mathbb{F}_{p^n}$.

This paper consists of five sections. The next section presents some fundamental concepts that will be helpful in the understanding of paper. In section 3 and section 4, we study the permutation behaviour of the linearized binomials and trinomials of the form $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$. Section 5 presents the conditions for the existence of complete permutation monomials, binomials and trinomials from linearized polynomials of type $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$.

## 2. Preliminaries

Consider a finite field denoted as $F=\mathbb{F}_q$, where $q$ represents the field's cardinality and is defined as $q=p^r$ with $p$ being a prime number and $r$ a positive integer. The linearized polynomial was first introduced by Ore. A lot of researchers have worked on linearized polynomials and their applications. The linearized polynomial is defined as follows:

**Definition 2.1:** A linearized polynomial or $q$ -polynomial over $\mathbb{F}_{q^m}$ is the polynomial of the form $L(X)=\sum_{i=0}^{n}\alpha_i X^{q^i}$, $\alpha_i\in\mathbb{F}_{q^m}$. The linearized polynomial satisfies the following properties.

If $F$ is an arbitrary extension field of $\mathbb{F}_{q^m}$ and $L(X)$ is a linearized polynomial over $\mathbb{F}_{q^m}$, then

$$L(\beta_1+\beta_2)=L(\beta_1)+L(\beta_2) \text{ for all } \beta_1,\beta_2\in F$$

$$L(a\beta) = aL(\beta) \text{ for all } a \in \mathbb{F}_q \text{ and for all } \beta \in F.$$

Every linearized polynomial has its conventional $q$ - associate. The conventional $q$ - associate of the linearized polynomial is defined as follows:

**Definition 2.2: [11]** The polynomial $l(X)$ represented as $\sum_{i=0}^{n} \alpha_i X^i$, and $L(X)$ expressed as $\sum_{i=0}^{n} \alpha_i X^{q^i}$ over $\mathbb{F}_{q^m}$, are referred as $q$ - associates. To be more precise, $l(X)$ is the conventional $q$ - associate of $L(X)$ and $L(X)$ is the linearized $q$ - associate of $l(X)$.

The linearized polynomial of the type $T_l^k(X)$ and $S_l^k(X)$ are given by Mesnager et al. in [15]. The definition of these polynomials are given below:

**Definition 2.3: [15]** A $p$ - polynomial $T_l^k(X)$ over $\mathbb{F}_p$ is defined as:

$$T_l^k(X) = \sum_{i=0}^{\frac{k}{l}-1} X^{p^{li}},$$

where $k$ and $l$ are positive integers such that $l \mid k$.

**Definition 2.4: [15]** A $p$ - polynomial $S_l^k(X)$ over $\mathbb{F}_p$ is defined as:

$$S_l^k(X) = \sum_{i=0}^{\frac{k}{l}-1} (-1)^i X^{p^{li}},$$

where $k$ and $l$ are positive integers such that $l \mid k$.

PP finds extensive applications in cryptography and coding theory. The criteria for a polynomial over $\mathbb{F}_q$ to be a PP are outlined as follows:

**Definition 2.5: [11]** A polynomial $f \in \mathbb{F}_q[x]$ is called a PP of $\mathbb{F}_q$ if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.

**Lemma 2.1: [11]** *The polynomial $g \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ if and only if one of the following conditions holds :*

(i) *the function $g : a \mapsto g(a)$ is onto;*

(ii) *the function $g : a \mapsto g(a)$ is one-to-one;*

(iii) *$g(X) = c$ has a solution in $\mathbb{F}_q$ for each $c \in \mathbb{F}_q$;*

(iv) *$g(X) = c$ has unique solution in $\mathbb{F}_q$ for each $c \in \mathbb{F}_q$.*

**Definition 2.6: [20]** A PP $G(X)$ over a finite field $\mathbb{F}_{p^n}$ is a called complete permutation, or a complete mapping , if $G(X)+X$ is also a PP over $\mathbb{F}_{p^n}$.

Mesnager et al. in [15] gave certain results for the linearized polynomials of the type $T_l^k(X)$ and $S_l^k(X)$ to be PP which are given in the following corollary and theorems.

**Corollary 2.1: [16]** *$T_l^k(X)$ is a PP over $\mathbb{F}_{2^n}$ if and only if $d|l$ and $\frac{k}{l}$ is odd.*

**Theorem 2.1: [15]** *Suppose that $\frac{k}{l}$ is odd. When $\frac{n}{d}$ is odd, $\{x \in \mathbb{F}_{p^n} | S_l^k = 0\} = \{0\}$ and consequently the cardinality of the set $\{x \in \mathbb{F}_{p^n} | S_l^k = 0\} = 1$.*

**Theorem 2.2: [15]** *The following is holding true:*

$$\{x \in \mathbb{F}_{p^n} | T_l^k = 0\} = \begin{cases} \mathbb{F}_{p^d}, & \text{if } p|\frac{k}{L} \\ S_e^{2e}(\mathbb{F}_{p^d}) & \text{otherwise.} \end{cases}$$

Consequently, the cardinality of set $\{x \in \mathbb{F}_{p^n} | T_l^k = 0\} = \begin{cases} p^d, & \text{if } p|\frac{k}{L} \\ p^{d-e} & \text{otherwise.} \end{cases}$

The above mentioned results for the linearized polynomials of the type $T_l^k(X)$ and $S_l^k(X)$ are used in proving our results presented in next sections.

## 3. Permutation Binomials from $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$

Polynomials which have only two terms are called binomials. In this section, we investigate linearized binomials of the type $T_l^k(X)$ and $S_l^k(X)$ and derive conditions for them to be PBs over $\mathbb{F}_{p^n}$.

The linearized polynomial of the type $T_l^k(X)$ is defined as

$$T_l^k(X) = \sum_{i=0}^{\frac{k}{l}-1} X^{p^{li}}. \tag{3.1}$$

By taking $k = 2l$ in equation 3.1 we have,

$$T_l^{2l}(X) = X + X^{p^l} \tag{3.2}$$

which is a linearized binomial of the type $T_l^k(X)$ over $\mathbb{F}_{p^n}$. In the following lemma, we show that the linearized binomial given by equation 3.2 is not a PB over $\mathbb{F}_{2^n}$.

**Lemma 3.1:** *The linearized binomial* $T_l^{2l}(X) = X + X^{2^l}$ *is not a linearized PB over* $\mathbb{F}_{2^n}$.

***Proof:*** Clearly, the linearized binomial $T_l^{2l}(X)$ is not linearized permutation binomial over $\mathbb{F}_{2^n}$.

Now, we check the linearized binomial $T_l^{2l}(X)$ for an odd prime $p$ and show that $T_l^{2l}(X)$ is a PB when we put certain restrictions on $n$ and $l$.

**Theorem 3.1:** *For any odd prime p, the linearized binomial* $T_l^{2l}(X) = X + X^{p^l}$ *is a PB if and only if* $d \mid l$, *where* $d = gcd(n, 2l)$.

***Proof:*** Let $d = gcd(n, 2l)$, $e = gcd(d, l)$ and $L = lcm[d, l]$. For equation 3.2 to be a PB, from Theorem 2.2, we must have the cardinality of the set $\{x \in \mathbb{F}_{p^n} \mid T_l^k = 0\} = 1$, which is possible only when $d = e$ and $p \nmid \frac{2l}{L}$. Since $d = gcd(n, 2l)$ and $e = gcd(d, l)$, therefore, for $d = e$, we have $d = gcd(d, l)$ and $L = l$. This implies that the condition $p \nmid \frac{2l}{L}$ is true only when $d \mid l$.

Hence, the linearized binomial

$$T_l^{2l}(X) = X + X^{p^l}$$

is a PB over $\mathbb{F}_{p^n}$ if and only if $d \mid l$.

**Corollary 3.1:** *If p is an odd prime and l is one or an odd prime then,* $T_l^{2l}(X) = X + X^{p^l}$ *is a linearized permutation binomial over* $\mathbb{F}_{p^n}$ *if n is odd.*

***Proof:*** Let $l$ is one or an odd prime and $d = gcd(n, 2l)$. If $n$ is even, then $d$ can only be 2 or $2l$ and $d$ does not divide $l$. Consequently, the linearized polynomial $T_l^{2l}(X) = X + X^{p^l}$ does not function as a PB over $\mathbb{F}_{p^n}$ for even $n$.

On the other hand, if $n$ is odd, then $d$ can be either 1 or $l$, and $d$ divides $l$. Hence, the linearized binomial $T_l^{2l}(X) = X + X^{p^l}$ is a PB over $\mathbb{F}_{p^n}$ for odd $n$.

**Corollary 3.2:** *If p is an odd prime, and l is either* 2 *or a composite number in the form* $l = 2^a q$, *where* $q(\neq 2)$ *is a prime, then the polynomial* $T_l^{2l}(X) = X + X^{p^l}$ *functions as a linearized permutation binomial over* $\mathbb{F}_{p^n}$ *if n is not a multiple of* $2^{a+1}$.

***Proof:*** Let $p$ be an odd prime and $l = 2$ or $l$ is a composite number of the type $l = 2^a q$ where $q(\neq 2)$ is a prime number. If $n = 2^{a+1}m$, then $d = 2^{a+1}$ and $d \nmid l$. Thererfore, $T_l^{2l}(X) = X + X^{p^l}$ is not a PB over $\mathbb{F}_{p^n}$ if $n = 2^{a+1}m$.

If $n \neq 2^{a+1}$, then $d = 2^a$ or 1 and $d \mid l$. Therefore, $T_l^{2l}(X) = X + X^{p^l}$ is a linearized permutation binomial over $\mathbb{F}_{p^n}$ if $n \neq 2^{a+1}m$.

Hence, when $p$ is an odd prime and $d = gcd(n, 2l)$ then, the linearized binomial $T_l^{2l}(X)$ is a PB when $d \mid l$.

The linearized polynomial of the type $S_l^k(X)$ is defined as

$$S_l^k(X) = \sum_{i=0}^{\frac{k}{l}-1} (-1)^i X^{p^{li}}. \tag{3.3}$$

By taking $k = 2l$ in the equation 3.3, we obtained

$$S_l^{2l}(X) = X - X^{p^l}. \tag{3.4}$$

When $p$ is even, $S_l^{2l}(X) = T_l^{2l}(X)$. Therefore, by Lemma 3.1 $S_l^{2l}(X)$ is not a PB over $\mathbb{F}_{2^n}$.

**Theorem 3.2:** *For an odd prime p, the linearized binomial of the type* $S_l^{2l}(X) = X - X^{p^l}$ *is not linearized permutation binomial over* $\mathbb{F}_{p^n}$.

***Proof:*** Clearly, $S_l^{2l}(X)$ is not a linearized permutation binomial over $\mathbb{F}_{p^n}$.

## 4. Permutation Trinomials from $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$

By taking $k = 3l$ in equation 3.1 and equation 3.3 we get linearized trinomials of the type $T_l^k(X)$ and $S_l^k(X)$ which are given as follows:

$$T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}} \tag{4.1}$$

and

$$S_l^{3l}(X) = X - X^{p^l} + X^{p^{2l}}. \tag{4.2}$$

In this section, we investigate the trinomials of the type $T_l^k(X)$ and $S_l^k(X)$. The linearized trinomial of the type $T_l^k(X)$ over $\mathbb{F}_{p^n}$ is given by $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$. Clearly, the linearized trinomial

$$T_l^{3l}(X) = X + X^{3^l} + X^{3^{2l}} \tag{4.3}$$

is not a PT over $\mathbb{F}_{3^n}$. Therefore, using Lemma 3.1 and the result stated in the equation 4.3, we conclude that linearized polynomial of the type

$T_l^k(X)$ over $\mathbb{F}_{p^n}$ with $p$ terms is not a PP which can be stated in the form of a corollary as follows:

**Corollary 4.1:** *For any prime p, the linearized polynomial* $T_l^{pl}(X) = X + X^{p^l} + X^{p^{2l}} + \cdots + X^{p^{(p-1)l}}$ *is not a linearized permutation polynomial over* $\mathbb{F}_{p^n}$.

**Theorem 4.1:** *The linearized trinomial* $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ *is a PT if and only if* $d \mid l$, *where* $d = \gcd(n, 3l)$, *for any prime* $p \neq 3$.

***Proof:*** Let $e = gcd(d, l)$ and $L = lcm[d, l]$. For equation 4.1 to be a PB, utilizing Theorem 2.2, we must have the cardinality of the set $\{x \in \mathbb{F}_{p^n} \mid T_l^k = 0\} = 1$, which is possible only when $d = e$ and $p \nmid \frac{3l}{L}$. Since $d = gcd(n, 3l)$ and $e = gcd(d, l)$, we get $d = gcd(d, l)$ and $L = l$. Now, $p \nmid \frac{3l}{L}$ holds only when $d \mid l$, which completes the proof.

**Corollary 4.2:** *If* $p \neq 3$ *is a prime and* $l \neq 3$ *is a prime or* 1, *then the linearized trinomial* $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ *over* $\mathbb{F}_{p^n}$ *is linearized permutation trinomial if n is not a multiple of* 3.

***Proof:*** Let $l \neq 3$ is a prime or 1, $d = gcd(n, 3l)$. If $n$ is a multiple of 3, then, either $d = 3$ or $3l$ and $d \nmid l$. So, the linearized polynomial $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ is not a PT over $\mathbb{F}_{p^n}$ if $n$ is a multiple of 3. If $n$ is not multiple of 3, then $d = 1$ or $l$ and $d \mid l$. So, the linearized trinomial

$$T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$$

is a PT over $\mathbb{F}_{p^n}$ if $n$ is not a multiple of 3.

**Corollary 4.3:** *Let* $p \neq 3$ *be a prime. If* $l = 3$ *or l is a composite number of the type* $l = 3^a q$ *where* $q(\neq 3)$ *is a prime number, then* $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ *is a linearized permutation trinomial over* $\mathbb{F}_{p^n}$ *if n is not a multiple of* $3^{a+1}$.

***Proof:*** Let $p \neq 3$ be a prime and $l = 3$ or $l$ is a composite number of type $l = 3^a q$ where $q \neq 3$ is prime number. If $n = 3^{a+1} m$ then $d = 3^{a+1}$ and $d \nmid l$. Thererfore, $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ is not a PT over $\mathbb{F}_{p^n}$ if $n = 3^{a+1} m$.

If $n \neq 3^{a+1}$ then $d = 3^a$ or 1 and $d \mid l$. Therefore, $T_l^{3l}(X) = X + X^{p^l} + X^{p^{2l}}$ is linearized permutation trinomial over $\mathbb{F}_{p^n}$ if $n \neq 3^{a+1} m$. Therefore, the linearized trinomial $T_l^{3l}(X)$ is a PT by putting some restrictions on $n, l$ when $d \mid l$.

Now, we investigate whether the trinomial of the type $S_l^k(X)$ is PT or not. The linearized trinomial of the type $S_l^k(X)$ over $\mathbb{F}_{p^n}$ as defined in equation 4.2. In the following theorem, we derive conditions for the linearized trinomial of the type $S_l^k(X)$ to be a PT.

**Theorem 4.2:** *The linearized trinomial* $S_l^{3l}(X) = X - X^{p^l} + X^{p^{2l}}$ *is PT over* $\mathbb{F}_{p^n}$, *if both l and n are odd .*

***Proof:*** If $l$ and $n$ are odd and, then $d = gcd(n, 3l)$ is odd . Therefore, $\frac{n}{d} = \text{odd}$.

Hence, by Theorem 2.1

$$S_l^{3l}(X) = X - X^{p^l} + X^{p^{2l}}$$

is linearized permutation trinomial over $\mathbb{F}_{p^n}$. The linearized trinomial of the type $S_l^k(X)$ is PT when both $n$ and $l$ are odd.

## 5. Complete Permutation Monomials, Binomials and Trinomials from $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$

The PP $f(X)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ is defined as CPP if $f(X) + X$ is also a permutation polynomial.

In this section, we investigate the linearized permutation monomials, binomials and trinomials constructed in previous sections and derive conditions for them to be linearized complete permutation binomials and trinomials.

The linearized polynomial $T_l^k(X)$ is defined as in equation 3.1. For monomials, we take $k = l$ in the equation 3.1, therefore, we obtain $T_l^l(X) = X$ which is a permutation monomial over $\mathbb{F}_{p^n}$.

Now, $T_l^l(X) + X = 0$ over $\mathbb{F}_{2^n}$. Therefore, $T_l^l(X) + X$ is not a permutation monomial and $T_l^l(X)$ is not a complete permutation monomial over $\mathbb{F}_{2^n}$.

For an odd prime $p$, $T_l^l(X) + X = (p+2)X$ which is a PP over $\mathbb{F}_{p^n}$. Hence $T_l^l(X)$ is a complete permutation monomial over $\mathbb{F}_{p^n}$ when $p$ is an odd prime.

In the following theorem, we derive certain conditions for $T_l^{2l}(X)$ to be a complete permutation binomial as follows.

**Theorem 5.1:** *The linearized binomial* $T_l^{2l}(X) = X + X^{p^l}$ *in Theorem 3.1 is a linearized complete permutation binomial if there does not exist any even positive*

*integer i such that* $k(p^l-1)=\frac{p^n-1}{p-1}i$, *where* $\alpha^{\frac{p^n-1}{p-1}i}=-2$ *for some primitive element* $\alpha$ *of* $\mathbb{F}_{p^n}$ *and even integer i,* $1\le i\le p-1$.

***Proof:*** To prove $T_l^{2l}(X)=X+X^{p^l}$ to be a complete permutation binomial, we have to show that $T_l^{2l}(X)+X$ is a PB. Therefore, for every non zero element $\alpha^k$ of $\mathbb{F}_{p^n}$, we must have,

$$2(\alpha^k)+(\alpha^k)^{p^l}\neq 0. \tag{5.1}$$

For $p=3$ the linearized polynomial $T_l^{2l}(X)+X$ is not a PP as 0 and 1 are zeros of this polynomial.

Now for prime, by computations, it has been observed that

$$\alpha^{\frac{p^n-1}{p-1}i}=-2 \tag{5.2}$$

for some even positive integer *i*. Therefore, for $T_l^{2l}(X)+X$ to be a PP, from equation 5.1 and 5.2 we must not have any even positive integer *i* such that

$$k(p^l-1)=\frac{p^n-1}{p-1}i.$$

Then, $T_l^{2l}(X)+X$ is a PB when $k(p^l-1)\neq\frac{p^n-1}{p-1}i$.

Hence, $T_l^{2l}(X)$ is a linearized complete permutation binomial when $k(p^l-1)\neq\frac{p^n-1}{p-1}i$.

**Remark:** By Theorem 4.1, the linearized trinomial $T_l^{3l}(X)=X+X^{2^l}+X^{2^{2l}}$ is a PT over $\mathbb{F}_{2^n}$ with some given conditions. Since 0 and 1 are the zeros of the linearized polynomial $T_l^{3l}(X)+X$ over $\mathbb{F}_{2^n}$. Therefore, $T_l^{3l}(X)+X$ doesnot qualify as a PT and $T_l^{3l}(X)$ is not a complete linearized permutation trinomial over $\mathbb{F}_{2^n}$.

**Theorem 5.2:** *The linearized trinomial* $S_l^{3l}=X-X^{p^l}+X^{p^{2l}}$ *in Theorem 4.2 is a complete permutation trinomial if* $n=l$.

***Proof:*** According to Theorem 4.2, the linearized trinomial $S_l^{3l}(X)$ becomes a PP when both *n* and *l* are odd.

To establish that $S_l^{3l}(X)+X$ is also a PP, consider a non-zero element $\alpha^k$ in $\mathbb{F}_{p^n}$. For $S_l^{3l}(X)+X$ to be a PP, it is necessary that $2(\alpha^k)-(\alpha^k)^{p^l}+(\alpha^k)^{p^{2l}}\neq 0$.

Upon substituting $l = n$, we obtain:

$$2 - (\alpha^k)^{p^n-1} + (\alpha^k)^{p^{2n}-1} = 1 + (\alpha^k)^{p^{2n}-1} \neq 0$$

since $(\alpha^k)^{p^{2n-1}} \neq -1$. Consequently, the linearized polynomial $S_l^{3l}(X) + X$ is a PP, and the linearized polynomial $S_l^{3l}(X)$ becomes a PP if $n = l$.

**References**


[1] Bassalygo, L. A. and Zinoviev, V. A., Permutation and complete permutation polynomials, *Finite Fields and Their Applications*, 33:2, 198-211 (2015).

[2] Baumbaugh, T. and Manganiello, F., Matroidal root structure of skew polynomials over finite fields, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:3, 377-389 (2019), DOI: 10.1080/09720529.2019.1600845.

[3] Charpin, P. and Kyureghyan, G. M., On a class of permutation polynomials over $\mathbb{F}_{2^n}$, International Conference on Sequences and their Applications, Springer, Berlin, Heidelberg, 368-376 (2008).

[4] Ding, C., Qu, L., Wang, Q., Yuan, J. and Yuan, P., Permutation trinomials over finite fields with even characteristic, *SIAM Journal of Discrete Mathematics*, 29:1, 79-92 (2015).

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

[6] Guangkui, X. and Cao, X., Complete permutation polynomials over finite fields of odd characteristic, *Finite Fields and Their Applications*, 31, 228-240 (2015).

[7] Hou, X. D., A class of permutation binomials over finite fields, *Journal of Number Theory*, 133:10, 3549-3558 (2013).

[8] Hou, X. D., A class of permutation trinomials over finite fields (2013), arXiv:1303.0568.

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

[10] Hou, X. D., Permutation polynomials over finite fields - a survey of recent advances, *Finite Fields and Their Applications*, 32, 82-119 (2015).

[11] Lidl R. and Niederreiter H., Finite Fields, Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, MA, Vol. 20 (1983).

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

[13] Ma, J., Zhang, T., Feng, T. and Ge, G., Some new results on permutation polynomials over finite fields, *Design Codes and Cryptography*, 83:2, 425-443 (2017).

[14] Mesnager, S., Kim, K. H. and Jo, H. S., On the number of rational zeros of linearized polynomials and the second order non linearity of cubic boolean functions, *Cryptography and Communications*, 12:4, 659-674 (2020).

[15] Mesnager, S., Kim, K. H., Choe, J. H. and Lee, D. N., Solving some affine equation over finite fields, *Finite Fields and Their Applications*, 68, 101746 (2020).

[16] Mesnager, S., Kim, K. H., Choe, J. H., Lee, D. N. and Go, D. S., Solving $x+x^{2^l}+\cdots+x^{2^{ml}}=a$ over $\mathbb{F}_{2^n}$, *Cryptography and Communications*, 12:4, 809-817 (2020).

[17] Mullen, G. L. and Panario D., Handbook of finite fields, Chapman and Hall, London (2013).

[18] Ore, O., On a special class of polynomials, *Transactions of the American Mathematical Society*, 34, 559-584 (1933).

[19] Tu, Z., Zeng, X. and Hu, L., Several classes of complete permutation polynomials, *Finite Fields and Their Applications*, 25, 182-193 (2014).

[20] Tu, Z. and Zeng, X., A class of permutation trinomials over finite fields of odd characteristic, *Cryptography and Communications*, 11, 563-58 (2019).

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

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

[23] Yi, H. B., Nie, Z. and Li, B., Efficient implementations of Gaussian elimination in finite fields on ASICs for MQ cryptographic systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 21:3, 797-802 (2018), DOI: 10.1080/09720529.2018.1449354.

[24] Zeng, X., Zhu, X. and Hu, L., Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over $\mathbb{F}_{2^n}$, *Applicable Algebra in Engineering, Communication and Computing,* 21:2, 145-150 (2010).

[25] Zieve, M., On some permutation polynomials over $F_q$ of the form $x^r h(x^{(q-1)/d})$, *Proceedings of the American Mathematical Society,* 137:7, 2209-2216 (2009).

*Received December, 2022*