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

Research Article

On the Study of Families of Linearized Polynomials over Finite Fields

Shalini Gupta*, Manpreet Singh, Mansi Harish

Department of Mathematics and Statistics, Himachal Pradesh University, Shimla-171005, India
E-mail: shalini.garga1970@gmail.com

Received: 8 May 2023; **Revised:** 28 July 2023; **Accepted:** 3 August 2023

Abstract: Linearized polynomials are gaining attention from many researchers because of their applications in the field of coding theory, cryptography and finite geometry. The linearized polynomials of the type $T_l^k(Z)$ and $S_l^k(Z)$ were recently introduced in the literature. The characterization of these linearized polynomials and patterns in their roots over finite fields have been extensively studied by various authors. In the present paper, we extend the study of families of linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ by taking k and l as prime powers and construct new families of linearized polynomials over finite fields. Further, we establish relation between linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ which may be helpful in determining zeros of these polynomials over finite fields.

***Keywords*:** finite fields, linearized polynomial, zeros

MSC: 11T06, 11D04

1. Introduction

Finite field is an important area of algebra which has many applications in network security, coding theory, elliptic curve cryptography etc., see [1-2]. Evariste Galois [3] introduced the finite field $GF(p^n)$, which is also called Galois field whose number of elements are p^n, where p is a prime and n is a positive integer. Any map from $\mathbb{F}_{q^n}$ to itself can be represented by a polynomial in $\mathbb{F}_{q^n}[x]$, where q is prime or prime power. Therefore, any polynomial in $\mathbb{F}_{q^n}[x]$ induces a map of $\mathbb{F}_{q^n}$ which corresponds to the linearized polynomial $L(X)=\Sigma_{i=0}^{k} a_k X^{q^i}$, see [4].

Solving linearized polynomials over finite fields and determining their zeros is the matter of concern of many researchers due to their vast applications in modern symmetric cryptosystem. The methods given in the literature for finding the number of zeros of linearized polynomials are not applicable to many specific linearized polynomials. Mesnager et al. [5] provided general method to get a more precise upper bound on the number of rational zeros of any linearized polynomial over finite fields. In [6], an explicit representation for the solutions of the equation $T_l^k(\mathrm{X})=\Sigma_{i=0}^{\frac{k}{l}-1} X^{2^{li}}=a$, for any given positive integers k, l and n with $l \mid k$, in the closed field $\mathbb{F}_2$ and in the finite field $\mathbb{F}_{2^n}$ were given. This study helped the authors to completely characterize the a's for which this equation has solution in $\mathbb{F}_{2^n}$. Further, the explicit representation of all solutions in $\mathbb{F}_{p^n}$ to the affine equations $T_l^k(X)=a$ and $S_l^k(X)=a$, $a \in \mathbb{F}_{p^n}$ were discussed in [7]. The solutions to these equations were determined by finding the kernel of $T_l^k(X)$ and $S_l^k(X)$ over $\mathbb{F}_{p^n}$.

DOI: https://doi.org/10.37256/cm.4320232999

Various authors contributed in the characterization of linearized polynomials and worked towards their applicability in areas such as coding theory and cryptography. In [8], the study of isomorphism among different types of algebra such as $\mathcal{L}_n(\mathbb{F}_{q^n})$, composition algebra $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ and Dickson matrix algebra was carried out. Chou et al. discussed cardinalities of the subfield value set of linearized polynomials, power polynomials and Dickson polynomials over finite fields in [9]. Reis in [10] introduced the class of nilpotent linearized polynomials over the finite field $\mathbb{F}_{q^n}$. Martínez-Peñas introduced the linearized Reed solomon codes using linearized polynomials in [11]. The distinct roots of q-polynomials over $\mathbb{F}_{q^n}$ were found using the maximum kernel method introduced by Csajbók et al. in [12]. Batoli and Bonini [13] constructed the planar polynomial from linearized polynomials of the type $f_{A,B}(x) = x(x^{q^2} + Ax^q + Bx)$ over the field $\mathbb{F}_{q^3}$. Permutation polynomials of the form $f(L(x)+kL(x))\times M(x)$ were constructed from linearized decomposition by Reis and Wang [14].

In the present paper, we extend the study of linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ by taking k and l as prime powers. Further, we construct new families of linearized polynomials over $\mathbb{F}_{p^n}$ by using $T_l^k(Z)$. In addition to this, we derive interesting relation between linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ over finite field $\mathbb{F}_{p^n}$. With the help of this relation, we construct a new family of linearized polynomials using $S_l^k(Z)$.

This paper is organised in six sections. The following Section overviews the preliminaries which are required for the study of this paper. In Section 3, construction of new families of linearized polynomials using $T_l^k(Z)$ is proposed. Relation between the linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ is discussed in Section 4. The construction of a new family of linearized polynomial using $S_l^k(Z)$ is presented in Section 5. We finally conclude our results in Section 6.

2. Preliminaries

In this paper, we use the following symbols:

· n-a positive integer.

· p and r-prime numbers.

· a and b-positive integers with $a \geq b$.

Let $F = \mathbb{F}_q$ is a finite field with q elements where $q = p^s$, p is a prime and s is a positive integer.

Definition 2.1 [1] A polynomial of the form

$$L(X) = \sum_{i=0}^{n} a_i X^{q^i}$$

with coefficients in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called a q-polynomial over $\mathbb{F}_{q^m}$. 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

$$L(\beta+\gamma) = L(\beta)+L(\gamma) \quad \text{for all } \beta,\ \gamma \in F$$

$$\text{and} \quad L(c\beta) = cL(\beta) \quad \text{for all } c \in \mathbb{F}_q \text{ and for all } \beta \in F.$$

Definition 2.2 [1] The polynomials $l(X) = \Sigma_{i=0}^{n} a_i X^i$ and $L(X) = \Sigma_{i=0}^{n} a_i X^{q^i}$ over $\mathbb{F}_{q^m}$ are called q-associates of each other. More specifically, $l(X)$ is the conventional q-associate of $L(X)$ and $L(X)$ is the linearized q-associate of $l(X)$.

Lemma 2.1 [1] Let $L_1(X)$ and $L_2(X)$ be q-polynomials over $\mathbb{F}_q$ with conventional q-associates $l_1(X)$ and $l_2(X)$. Then $l(X) = l_1(X)l_2(X)$ and $L(X) = L_1(X) \otimes L_2(X)$ are q-associates of each other.

Definition 2.3 [7] Let k and l be positive integers such that $l \mid k$. Define p-polynomial over $\mathbb{F}_p$ as

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

Definition 2.2 implies that

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

is the conventional p-associate of $T_l^k(X)$, where p is a prime.

Definition 2.4 [7] Let k and l be positive integers such that $l \mid k$. Define p-polynomial over $\mathbb{F}_p$ as

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

Definition 2.2 implies that

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

is the conventional p-associate of $S_l^k(X)$, where p is a prime.

3. Construction of new families of linearized polynomials using $T_l^k(Z)$ over $\mathbb{F}_{p^n}$

The linearized polynomial $T_l^k(Z)$ over $\mathbb{F}_{p^n}$ can be expressed according to definition 2.3. Furthermore, when considering a prime number r and positive integers a and b, where $a \geq b$, the polynomial $T_{r^b}^{r^a}(Z)$ is defined as follows:

$$T_{r^b}^{r^a}(Z) = \sum_{i=0}^{r^{a-b}-1} Z^{p^{(r^b)i}}. \tag{1}$$

In this section, we first prove some identities related to composition of the linearized polynomial $T_{r^b}^{r^a}(Z)$. Further, we construct families of linearized polynomials using $T_l^k(Z)$ over $\mathbb{F}_{p^n}$ for different values of l and k.

Proposition 3.1 For a, b, c, a', b' with $c \geq a \geq b$ and $a' \geq b'$, the following identities hold:

(a) $T_{r^b}^{r^a} \circ T_{r^{b'}}^{r^{a'}} = T_{r^{b'}}^{r^{a'}} \circ T_{r^b}^{r^a}$

(b) $T_{r^b}^{r^a} \circ T_{r^a}^{r^c} = T_{r^b}^{r^c}$

(c) $T_{r^a}^{r^a}(Z) = Z$

(d) $T_{r^a}^{r^{2a}}(Z) = Z + Z^{p^{r^a}}$

Proof. Using equation (1) results from (*a*) to (*d*) can be easily proved over $\mathbb{F}_{p^n}$. □

Theorem 3.1 Consider the linearized polynomial $T_{r^b}^{r^a}(Z)$, where $a = m$ and $b = 1$. Then, the family of linearized polynomials of degree $p^{r^{m+1}-r}$ given by

$$T_r^{r^m}(Z) + (p-1)T_r^{r^{m+1}}(Z)$$

is expressed as

$$(p-1)\sum_{i=r^{m-1}}^{i=r^m-1} Z^{p^{ri}}$$

over $\mathbb{F}_{p^n}$.

Proof. By using Definition 2.3 and equation (1), we compute

$$T_r^{r^m}(Z)+(p-1)T_r^{r^{m+1}}(Z)=\sum_{i=0}^{r^{m-1}-1}Z^{p^{ri}}+(p-1)\sum_{i=0}^{r^m-1}Z^{p^{ri}}$$

$$=[Z+Z^{p^r}+Z^{p^{2r}}+\cdots+Z^{p^{r^m-r}}]+(p-1)[Z$$

$$+Z^{p^r}+Z^{p^{2r}}+\cdots+Z^{p^{r^{m+1}-r}}]$$

$$=(p-1)\sum_{i=r^{m-1}}^{i=r^m-1}Z^{p^{ri}}.$$

Therefore, $T_r^{r^m}(Z)+(p-1)T_r^{r^{m+1}}(Z)$ represents a family of linearized polynomials $(p-1)\Sigma_{i=r^{m-1}}^{i=r^m-1}Z^{p^{ri}}$ of degree $p^{r^{m+1}-r}$ over $\mathbb{F}_{p^n}$. □

In the following theorems, we prove results related to $T_l^k(Z)$, where r is an even prime in Theorem 3.2 and r is an odd prime in Theorem 3.3.

Theorem 3.2 Consider the linearized polynomial $T_l^k(Z)$, where $l=2r$ and $k=r^m$. Then, the family of linearized polynomials of degree p^{2r^m-2r} given by

$$T_r^{r^m}(Z)+(p-1)T_r^{r^{m+1}}(Z)$$

is expressed as

$$(p-1)\sum_{i=r^{m-2}}^{i=r^{m-1}-1}Z^{p^{2ri}}$$

over $\mathbb{F}_{p^n}$, where r is an even prime.

Proof. By using Definition 2.3 and equation (1), we compute

$$T_{2r}^{r^m}(Z)+(p-1)T_{2r}^{r^{m+1}}(Z)=\sum_{i=0}^{\frac{r^m}{2r}-1}Z^{p^{2ri}}+(p-1)\sum_{i=0}^{\frac{r^{m+1}}{2r}-1}Z^{p^{2ri}}$$

$$=[Z+Z^{p^{2r}}+Z^{p^{4r}}+Z^{p^{6r}}+\cdots+Z^{p^{r^m-2r}}]$$

$$+(p-1)[Z+Z^{p^{2r}}+Z^{p^{2r.2}}+Z^{p^{2r.3}}+Z^{p^{2r.4}}+\cdots+Z^{p^{r^{m+1}-2r}}]$$

$$=(p-1)[Z^{p^{2r^{m-1}}}+\cdots+Z^{p^{2r^m-2r}}].$$

Therefore, $T_{2r}^{r^m}(Z)+(p-1)T_{2r}^{r^{m+1}}(Z)$ represents a family of linearized polynomials $(p-1)\sum_{i=r^{m-2}}^{i=r^{m-1}-1}Z^{p^{2ri}}$ of degree p^{2r^m-2r} over $\mathbb{F}_{p^n}$, where r is an even prime. □

Theorem 3.3 Consider the linearized polynomial $T_l^k(Z)$, where $k=r^m+r$ and $l=2r$. Then, a family of linearized

polynomials of degree $p^{r^{m+1}-r}$

$$T_{2r}^{r^m+r}(Z)+(p-1)T_{2r}^{r^{m+1}+r}(Z)$$

is expressed as

$$(p-1)\sum_{i=\frac{r^{m-1}+1}{2}}^{i=\frac{r^m-1}{2}} Z^{p^{2ri}}$$

over $\mathbb{F}_{p^n}$, where r is an odd prime.

Proof. By using Definition 2.3 and equation (1), we compute

$$T_{2r}^{r^m+r}(Z)+(p-1)T_{2r}^{r^{m+1}+r}(Z)=\sum_{i=0}^{i=\frac{r^m+r}{2r}-1} Z^{p^{2ri}}+(p-1)\sum_{i=0}^{i=\frac{r^{m+1}+r}{2r}} Z^{p^{2ri}}$$

$$=Z+Z^{p^{2r}}+Z^{p^{2r.2}}+Z^{p^{2r.3}}+Z^{p^{2r.4}}+\cdots+Z^{p^{r^m-r}}$$

$$+(p-1)[Z+Z^{p^{2r}}+Z^{p^{2r.2}}+Z^{p^{2r.3}}+Z^{p^{2r.4}}+\cdots+Z^{p^{r^{m+1}-r}}$$

$$=(p-1)[Z^{p^{r^m+r}}+\cdots+Z^{p^{r^{m+1}-r}}]$$

$$=(p-1)\sum_{i=\frac{r^{m-1}+1}{2}}^{i=\frac{r^m-1}{2}} Z^{p^{2ri}}.$$

Therefore, $T_{2r}^{r^m+r}(Z)+(p-1)T_{2r}^{r^{m+1}+r}(Z)$ represents a family of linearized polynomials $(p-1)\sum_{i=\frac{r^{m-1}+1}{2}}^{i=\frac{r^m-1}{2}} Z^{p^{2ri}}$ of degree $p^{r^{m+1}-r}$ over $\mathbb{F}_{p^n}$, where r is an odd prime. □

The following theorem provides some useful results related to the composition of linearized polynomials $T_l^k(Z)$ over $\mathbb{F}_{2^n}$

Theorem 3.4 The following results hold for the composition of linearized polynomials of the type $T_{r^b}^{r^a}(Z)$ over $\mathbb{F}_{2^n}$:

(a) $T_2^4 \circ T_2^{2^m}(Z)=T_{2^m}^{2^{m+1}}(Z)$

(b) $T_{2^{m-1}}^{2^m} \circ T_{2^{m-1}}^{2^m}(Z)=T_{2^m}^{2^{m+1}}(Z)$

(c) $T_2^4 \circ T_2^{2^m}(Z)=T_{2^{m-1}}^{2^m} \circ T_{2^{m-1}}^{2^m}(Z)$

Proof. (*a*) Since

$$t_2^4(Z)=1+Z^2$$

and

$$t_2^{2^m}(Z)=1+Z^2+Z^4+Z^6+\cdots+Z^{2^m-2}$$

are conventional associates of $T_2^4(Z)$ and $T_2^{2^m}(Z)$ respectively, then

$$t_2^4(Z)\cdot t_2^{2^m}(Z)=(1+Z^2)\cdot(1+Z^2+Z^4+Z^6+\cdots+Z^{2^m-2})$$

$$=1+Z^{2^m}$$

$$=t_2^{2^{m+1}}(Z).$$

So,

$$t_2^4(Z)\cdot t_2^{2^m}(Z)=1+Z^{2^m}.$$

Since product of conventional associates of $T_2^4(Z)$ and $T_2^{2^m}(Z)$ is equal to conventional associate of $T_2^{2^{m+1}}(Z)$, then by using Lemma 2.1, we can write

$$T_2^4\circ T_2^{2^m}(Z)=Z+Z^{2^{2^m}}$$

$$=\sum_{i=0}^{i=\frac{2^{m+1}}{2^m}-1}Z^{2^{2^m i}}$$

$$=T_{2^m}^{2^{m+1}}(Z).$$

Hence,

$$T_2^4\circ T_2^{2^m}(Z)=T_{2^m}^{2^{m+1}}(Z).$$

(*b*) Since conventional associate of $T_{2^{m-1}}^{2^m}(Z)$ is $t_{2^{m-1}}^{2^m}(Z)$, therefore

$$t_{2^{m-1}}^{2^m}(Z)\cdot t_{2^{m-1}}^{2^m}(Z)=(1+Z^{2^{m-1}})^2=1+Z^{2^m}$$

that is,

$$t_{2^{m-1}}^{2^m}(Z)\cdot t_{2^{m-1}}^{2^m}(Z)=1+Z^{2^m}.$$

Also,

$$T_{2^{m-1}}^{2^m}\circ T_{2^{m-1}}^{2^m}(Z)=1+Z^{2^{2^m}}$$

$$=\sum_{i=0}^{i=\frac{2^{m+1}}{2^m}-1}Z^{2^{2^m i}}$$

$$=T_{2^m}^{2^{m+1}}(\mathrm{Z})$$

Hence, we obtain

$$T_{2^{m-1}}^{2^m}\circ T_{2^{m-1}}^{2^m}(Z)=T_{2^m}^{2^{m+1}}(Z).$$

(*c*) From part (*a*) and part (*b*),

$$T_2^4\circ T_2^{2^m}(Z)=T_{2^m}^{2^{m+1}}(Z) \tag{2}$$

and

$$T_{2^{m-1}}^{2^m} \circ T_{2^{m-1}}^{2^m}(Z) = T_{2^m}^{2^{m+1}}(Z) \quad . \tag{3}$$

From equation (2) and equation (3), we get,

$$T_2^4 \circ T_2^{2^m}(Z) = T_{2^{m-1}}^{2^m} \circ T_{2^{m-1}}^{2^m}(Z) \quad . \qquad \square$$

4. Relation between linearized polynomial $T_l^k(Z)$ and $S_l^k(Z)$ over $\mathbb{F}_{p^n}$

In this section, we establish interesting relation between linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ by performing computations over $\mathbb{F}_{p^n}$. Further, we prove this relation with the help of definitions and properties of $T_l^k(Z)$ and $S_l^k(Z)$ Results provided in this section are used to construct a new family of linearized polynomial using $S_l^k(Z)$. Also, the relation between $T_l^k(Z)$ and $S_l^k(Z)$ may be useful in finding the zeros of these polynomials.

Theorem 4.1 For any prime p, the linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$ satisfy the following relation

$$S_l^{2l}(Z) = (p-1)T_l^{2l}(Z) + (p+2)Z \ , \quad \text{for } k = 2l \tag{4}$$

and

$$S_l^k(Z) = \begin{cases} (p-1)T_l^k(Z) - (p-2)T_{2l}^k(Z), & \text{if } \dfrac{k}{l} \text{ is even} \\ (p-1)T_l^k(Z) - (p-2)T_{2l}^{k+l}(Z), & \text{if } \dfrac{k}{l} \text{ is odd.} \end{cases} \quad , \quad \text{for } k \neq 2l. \tag{5}$$

Proof. Case 1: For $k = 2l$

$$\begin{aligned} (p-1)T_l^{2l}(Z) + (p+2)Z &= (p-1)\sum_{i=0}^{2-1} Z^{p^{li}} + (p+2)Z \\ &= (p-1)[Z + Z^{p^l}] + (p+2)Z \\ &= Z + (p-1)Z^{p^l} \\ &= S_l^{2l}(Z) \end{aligned}$$

Therefore,

$$S_l^{2l}(Z) = (p-1)T_l^{2l}(Z) + (p+2)Z \ .$$

Case 2: For $k \neq 2l$,

(i) When $\frac{k}{l}$ is even, then

$$(p-1)T_l^k(Z) - (p-2)T_{2l}^k(Z) = (p-1)\sum_{i=0}^{\frac{k}{l}-1} Z^{p^{li}} - (p-2)\sum_{i=0}^{\frac{k}{2l}-1} Z^{p^{2li}}$$

$$
\begin{aligned}
&= (p-1)[Z + Z^{p^l} + Z^{p^{2l}} + Z^{p^{3l}} + Z^{p^{4l}} + \cdots + Z^{p^{k-3l}} \\
&\quad + Z^{p^{k-2l}} + Z^{p^{k-l}}] - (p-2)[Z + Z^{p^{2l}} + Z^{p^{4l}} + Z^{p^{6l}} \\
&\quad + Z^{p^{8l}} + \cdots + Z^{p^{k-4l}} + Z^{p^{k-2l}}] \\
&= Z + Z^{p^{2l}} + Z^{p^{4l}} + Z^{p^{6l}} + Z^{p^{8l}} + \cdots + Z^{p^{k-4l}} \\
&\quad + Z^{p^{k-2l}} - Z^{p^l} - Z^{p^{3l}} - \cdots - Z^{p^{k-l}} \\
&= S_l^k(Z)
\end{aligned}
$$

Therefore, when $\frac{k}{l}$ is even

$$S_l^k(Z) = (p-1)T_l^k(Z) - (p-2)T_{2l}^k(Z).$$

(ii) When $\frac{k}{l}$ is odd, then

$$
\begin{aligned}
(p-1)T_l^k(Z) - (p-2)T_{2l}^{k+l}(Z) &= (p-1)\sum_{i=0}^{\frac{k}{l}-1} Z^{p^{li}} - (p-2)\sum_{i=0}^{\frac{k+l}{2l}-1} Z^{p^{2li}} \\
&= (p-1)[Z + Z^{p^l} + Z^{p^{2l}} + Z^{p^{3l}} + Z^{p^{4l}} + Z^{p^{5l}} + \cdots + Z^{p^{k-l}}] \\
&\quad -(p-2)[Z + Z^{p^{2l}} + Z^{p^{4l}} + Z^{p^{6l}} + Z^{p^{8l}} + \cdots + Z^{p^{k+l-2l}}] \\
&= Z + Z^{p^{2l}} + Z^{p^{4l}} + \cdots + Z^{p^{k-l}} \\
&\quad -Z^{p^l} - Z^{p^{3l}} - Z^{p^{5l}} - \cdots - Z^{p^{k-2l}} \\
&= S_l^k(Z)
\end{aligned}
$$

Therefore,

$$S_l^k(Z) = (p-1)T_l^k(Z) - (p-2)T_{2l}^{k+l}(Z);\ \frac{k}{l} \text{ is odd.}$$

Hence, for $k = 2l$, we have

$$S_l^k(Z) = (p-1)T_l^k(Z) - (p-2)T_{2l}^{k+l}$$

and for $k \neq 2l$, we have

$$S_l^k(Z) = \begin{cases} (p-1)T_l^k(Z) - (p-2)T_{2l}^k(Z) & \text{if } \frac{k}{l} \text{ is even} \\ (p-1)T_l^k(Z) - (p-2)T_{2l}^{k+l}(Z) & \text{if } \frac{k}{l} \text{ is odd.} \end{cases}$$

□

The result discussed in Theorem 4.1 can be used to deduce relation between $T_{r^b}^{r^a}(Z)$ and $S_{r^b}^{r^a}(Z)$ as shown in the following corollary:

Corollary 4.1 Consider the linearized polynomials $T_{r^b}^{r^a}(Z)$ and $S_{r^b}^{r^a}(Z)$, then

$$S_{r^a}^{2r^a}(Z) = (p-1)T_{r^a}^{2r^a}(Z) + (p+2)Z \tag{6}$$

and

$$S_{r^b}^{r^a}(Z) = \begin{cases} (p-1)T_{r^b}^{r^a}(Z) - (p-2)T_{2r^b}^{r^a}(Z) & \text{if } r \text{ is even prime} \\ (p-1)T_{r^b}^{r^a}(Z) - (p-2)T_{2r^b}^{r^a+r^b}(Z) & \text{if } r \text{ is odd prime,} \end{cases} \tag{7}$$

where p is prime.

Example 4.1 When $k \neq 2l$, $l = r^a$ and $k = r^b$, then

$$S_{r^b}^{r^a}(Z) = \begin{cases} 2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a}(Z) & \text{if } r \text{ is even prime} \\ 2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a+r^b}(Z) & \text{if } r \text{ is odd prime} \end{cases} \tag{8}$$

over $\mathbb{F}_3$.

Case 1: When r is an even prime, then

$$2T_{2^b}^{2^a}(Z) - T_{2.2^b}^{2^a}(Z) = 2\sum_{i=0}^{2^{a-b}-1} Z^{p^{(2^b)i}} - \sum_{i=0}^{2^{a-b-1}-1} Z^{p^{(2^{b+1})i}}$$

$$= 2[Z + Z^{p^{2^b}} + Z^{p^{2^b\times 2}} + Z^{p^{2^b\times 3}} + \cdots + Z^{p^{2^a-2^b}}] - [Z +$$

$$Z^{p^{2^{b+1}}} + Z^{p^{2^{b+1}\times 2}} + Z^{p^{2^{b+1}\times 3}} + \cdots + Z^{p^{2^a-2^{b+1}}}]$$

$$= Z - Z^{p^{2^b}} + Z^{p^{2^b\times 2}} - Z^{p^{2^b\times 3}} + Z^{p^{2^b\times 4}} - \cdots + Z^{p^{2^a-2^{b+1}}} + Z^{p^{2^a-2^b}}$$

$$= S_{2^b}^{2^a}(Z).$$

So, we have

$$S_{2^b}^{2^a}(Z) = 2T_{2^b}^{2^a}(Z) - T_{2.2^b}^{2^a}(Z).$$

Case 2: When r is an odd prime, then

$$2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a+r^b}(Z) = 2\sum_{i=0}^{r^{a-b}-1} Z^{p^{(r^b)i}} - \sum_{i=0}^{\frac{r^a+r^b}{2r^b}-1} Z^{p^{(2r^b)i}}$$

$$= 2[Z + Z^{p^{r^b}} + Z^{p^{r^b\times 2}} + Z^{p^{r^b\times 3}} + \cdots + Z^{p^{r^a-r^b}}] - [Z +$$

$$Z^{p^{2r^b}} + Z^{p^{4r^b}} + Z^{p^{6r^b}} + \cdots + Z^{p^{r^a+r^b-2r^b}}]$$

$$= Z - Z^{p^{r^b}} + Z^{p^{r^b\times 2}} - Z^{p^{r^b\times 3}} + Z^{p^{r^b\times 4}} - \cdots - Z^{p^{r^a-r^{b+1}}} + Z^{p^{r^a-r^b}}$$

$$= S_{r^b}^{r^a}(Z).$$

$$S_{r^b}^{r^a}(Z) = 2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a+r^b}(Z).$$

Hence, we obtain

$$S_{r^b}^{r^a}(Z) = \begin{cases} 2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a}(Z) & \text{if } r \text{ is even prime} \\ 2T_{r^b}^{r^a}(Z) - T_{2r^b}^{r^a+r^b}(Z) & \text{if } r \text{ is odd prime} \end{cases}$$

over $\mathbb{F}_3$.

5. Construction of a new family of linearized polynomials using $S_l^k(Z)$ over $\mathbb{F}_{p^n}$

Theorem 5.1 Consider the linearized polynomial $S_{r^b}^{r^a}(Z)$, where $a = m$ and $b = 1$. Then, the family of linearized polynomials of degree $p^{r^{m+1}-r}$ given by

$$S_r^{r^m}(Z) + (p-1)S_r^{r^{m+1}}(Z)$$

is expressed as

$$(p-1)\sum_{i=r^{m-1}}^{i=r^m-1}(-1)^i Z^{p^{ri}}.$$

over $\mathbb{F}_{p^n}$.

Proof. Case 1: When r is an even prime, then

$$\begin{aligned} S_2^{2^m}(Z) + (p-1)S_2^{2^{m+1}}(Z) &= (p-1)T_2^{2^m}(Z) - (p-2)T_{2.2}^{2^m}(Z) + (p-1)[(p-1)T_2^{2^{m+1}}(Z) - (p-2)T_{2.2}^{2^{m+1}}(Z)] \\ &= (p-1)[T_2^{2^m}(Z) + (p-1)T_2^{2^{m+1}}(Z)] - (p-2)[T_4^{2^m}(Z) + (p-1)T_4^{2^{m+1}}(Z)] \\ &= (p-1)(p-1)\sum_{i=2^{m-1}}^{i=2^m-1} Z^{p^{2i}} - (p-2)(p-1)\sum_{i=2^{m-2}}^{i=2^{m-1}-1} Z^{p^{4i}} \\ &= (p-1)(p-1)[Z^{p^{2.2^{m-1}}} + \cdots + Z^{p^{2(2^m-1)}}] - (p-2)(p-1)[Z^{p^{4.2^{m-2}}} + \cdots + Z^{p^{4(2^{m-1}-1)}}] \\ &= (p-1)[(p-1)[Z^{p^{2^m}} + \cdots + Z^{p^{2^{m+1}-2}}] - (p-2)[Z^{p^{2^m}} + \cdots + Z^{p^{2^{m+1}-4}}]] \\ &= (p-1)\sum_{i=2^{m-1}}^{i=2^m-1}(-1)^i Z^{p^{2i}}. \end{aligned}$$

Therefore,

$$S_2^{2^m}(Z) + (p-1)T_2^{2^{m+1}}(Z) = (p-1)\sum_{i=2^{m-1}}^{i=2^m-1}(-1)^i Z^{p^{2i}}.$$

Case 2: When r is an odd prime, then

$$S_r^{r^m}(Z)+(p-1)S_r^{r^{m+1}}(Z)=(p-1)T_r^{r^m}(Z)-(p-2)T_r^{r^m+r}(Z)+(p-1)[(p-1)T_r^{r^{m+1}}(Z))-(p-2)T_{2r}^{r^{m+1}}(Z)]$$

$$=(p-1)[T_r^{r^m}(Z)+(p-1)T_r^{r^{m+1}}(Z)]-(p-2)[T_{2r}^{r^m+r}(Z)+(p-1)T_{2r}^{r^m+r}(Z)]$$

$$=(p-1)(p-1)\sum_{i=r^{m-1}}^{i=r^m-1}Z^{p^{ri}}-(p-2)(p-1)\sum_{i=\frac{r^{m-1}+1}{2}}^{i=\frac{r^m-1}{2}}Z^{p^{2ri}}$$

$$=(p-1)[(p-1)[Z^{p^{r\times r^{m-1}}}+\cdots+z^{p^{r\times(r^m-1)}}]-(p-2)[Z^{p^{r^m+r}}+\cdots+Z^{p^{r\times(r^m-1)}}]]$$

$$=(p-1)[(p-1)-(p-2)][Z^{p^{r^m+r}}+\cdots+Z^{p^{r^{m+1}-r}}]+(p-1)[Z^{p^{r^m}}+\cdots+Z^{p^{r\times r^{m+1}-r}}]]$$

$$=(p-1)\sum_{i=r^{m-1}}^{i=r^m-1}(-1)^iZ^{p^{ri}}.$$

Therefore, $S_r^{r^m}(Z)+(p-1)S_r^{r^{m+1}}(Z)$ represents a family of linearized polynomials $(p-1)\Sigma_{i=r^{m-1}}^{i=r^m-1}(-1)^iZ^{p^{ri}}$ of degree $p^{r^{m+1}-r}$over $\mathbb{F}_{p^n}$. □

6. Conclusion

In this paper, we extended the study of families of linearized polynomials of types $T_l^k(Z)$ and $S_l^k(Z)$ by taking l and k as prime powers and constructed families of linearized polynomials using $T_l^k(Z)$ over finite fields. Further, we established relation between $T_l^k(Z)$ and $S_l^k(Z)$, and constructed a new family of linearized polynomial over $\mathbb{F}_{p^n}$ using $S_l^k(Z)$. The results derived in the manuscript are helpful in the characterization of families of linearized polynomials $T_l^k(Z)$ and $S_l^k(Z)$. Also, the construction of new families of linearized polynomials have added to the literature of linearized polynomials over finite fields.

Conflict of interest

The authors declare no conflict of interest.

References

[1] Lidl R, Niederreiter H. *Finite Fields: Second Edition*. Cambridge University Press; 1983.

[2] Mullen GL, Panario D. *Handbook of Finite Fields*. CRC Press; 2013.

[3] Galois E. *On the Theory of Numbers*. Bulletin Des Sciences Mathematiques XIII, reprinted in Eeris et Memories Mathematics. Evariste Galois; 1830. p.428-435.

[4] Ore O. On a special class of polynomials. *Transactions of the American Mathematical Society*. 1933; 34(5): 559-584.

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

[6] Mesnager S, Kim KH, Choe JH, Lee DN, Go DS. Solving $x+x^{2^l}+\cdots+x^{2^{ml}}=a$ over $\mathbb{F}_{2^n}$. *Cryptography and Communications*. 2020; 12(4): 809-817.

[7] Mesnager S, Kim KH, Choe JH, Lee DN. Solving some affine equation over Finite Fields. *Finite Fields and Their Applications*. 2020; 68: 101746.
[8] Wu B, Liu Z. Linearized polynomials over finite fields revisited. *Finite Fields and Their Applications*. 2013; 22: 79-100.
[9] Chou WS, Gomez-Calderon J, Mullen GL, Panario D, Thomson D. Subfield value sets of polynomials over finite fields. *Functiones et Approximatio Commentarii Mathematici*. 2013; 48(1): 147-165.
[10] Reis L. Nilpotent linearized polynomials over finite fields and applications. *Finite Fields and Their Applications*. 2018; 50: 279-292.
[11] Martínez-Peñas U. Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*. 2018; 504: 587-612.
[12] Csajbók B, Marino G, Polverino O, Zullo F. A characterization of linearized polynomials with maximum kernel. *Finite Fields and Their Applications.* 2019; 56: 109-130.
[13] Bartoli D, Bonini M. Planar polynomials arising from linearized polynomials. *Journal of Algebra and Its Applications*. 2022; 21(1): 2250002.
[14] Reis L, Wang Q. *Permutation polynomials from a linearized decomposition*. 2021. Available fom: https://doi.org/10.48550/arXiv.2104.13234.