Azerbaijan Journal of Mathematics
V. 16, No 2, 2026, July
ISSN 2218-6816
https://doi.org/10.59849/2218-6816.2026.2.130

An Investigation of Permutation Pentanomials Over $\mathbb{F}_{5^{2k}}$

P. Agarwal, S. Gupta, M. Singh, S. Vinayak, R. Efendiev*, S. Jain

Abstract. Permutation polynomials play a significant role in the finite field theory due to their wide applications in coding theory, cryptography and combinatorial designs. The permutation pentanomials, polynomials with five nonzero terms, offer an attractive balance between algebraic simplicity and functional richness making them suitable for practical implementation in computational and cryptographic systems. While numerous studies have been devoted to permutation binomials, trinomials and quadrinomials, systematic exploration of permutation pentanomials particularly over fields of characteristic five, remains limited. The present paper aims to construct new classes of permutation pentanomials over $\mathbb{F}_{5^{2k}}$. Specifically, we investigate pentanomials of the algebraic form $x^{4t+5}l(x^{q-1})$ over $\mathbb{F}_{q^2}$, where $q = 5^k$, k is a positive integer, and $l(x) = x^{2t}(x^5 + c_1x^4 + c_2x^s + c_3x + 1)$, for $c_i \in \mathbb{F}_5$, $i = 1, 2, 3$; $s \in \{2, 3\}$ and derive necessary and sufficient conditions under which these polynomials act as permutation over $\mathbb{F}_{5^{2k}}$. The permutation behaviour of the constructed pentanomials is verified through both theoretical proofs and computational experiments.
The study not only extends the existing body of knowledge on permutation polynomials but also provides generalized results. The findings may have further implications in the design of cryptographic functions, error correcting codes and pseudo-random sequence generators.

Key Words and Phrases: finite fields, permutation polynomial, permutation pentanomial.

2010 Mathematics Subject Classifications: 11T06, 11D04, 11T55

1. Introduction

Consider the finite field $\mathbb{F}_q$ which contains $q = p^n$ elements, where p is a prime and n is a positive integer. The polynomial $u(x)$ is said to be a permutation over $\mathbb{F}_q$ if the associated map $u : \mathbb{F}_q \to \mathbb{F}_q$ is a permutation. The study of permutation

*Corresponding author.

polynomials is an active research area in recent times due to their applications in the field of technology such as coding theory, cryptography and combinatorial design, see [10, 11, 26, 32, 38, 39].

The survey by Hou [25] gave a overview of recent development in the study and construction of permutation polynomials over finite fields, summarizing key results, methods, and open problems. Mullen [35] discussed the main properties of permutation polynomials, described various methods to construct them, and presented their important applications in coding theory, cryptography, and communication systems. In 2014, Mullen and Wang [36] presented a summary of permutation polynomials in one variable, explaining basic definitions, main results, and common construction techniques within finite field theory. Zieve [51] introduced several explicit families of polynomials over finite fields, using subgroup structures and algebraic conditions to make them permutation polynomials. Later, Zieve [52] extended this work by constructing permutation polynomials from subfield permutations and showing their connection with complete sets of mutually orthogonal Latin squares.

In recent years, authors focused in the polynomials of the form $x^r l(x^{q-1})$ to be a permutation over $\mathbb{F}_{q^2}$. But in these type of polynomials, researchers are concentrating only on $l(x)$ with few terms such as binomials and trinomials over finite field because binomials and trinomials have concise and compact structure and have various applications in the field of cryptography. In this regard, Hou [18, 19, 20, 23], Hou and Lappano [21] and Lappano [22], completely characterized the permutation binomials and trinomials of the type $xl(x^{q-1})$ over $\mathbb{F}_{q^2}$, where $l(x) = \alpha + x^2, \alpha + \beta x + x^2$ and $\alpha + x^t$ for $t = 5, 7$. Further, Gupta and Sharma [15] constructed permutation polynomials of the type $x^r l(x^{2^k-1})$ over $\mathbb{F}_{2^{2k}}$ and proposed two conjectures on permutation polynomials which were subsequently proved by Zha et al [48]. Gupta et al. [16] constructed several classes of permutation trinomials of the form $xh(x^{q+1})$ over $\mathbb{F}_{q^2}$. A comprehensive survey on permutation binomials and trinomials over finite fields was provided by Hou [24] and Jarali et al. [44].

Li et al. [30] constructed permutation trinomials using the fractional polynomials over finite fields with characteristic 2 and 3. The authors also presented conjuctures which were proved by Bartoli and Giulietti [5], and constructed permutation trinomials over finite field of characteristic five. The classification of permutation polynomials with Niho exponents were given by Bai and Xia [3] over $\mathbb{F}_{p^k}$ for $p = 3$ and 5. Some new classes of permutation trinomials with Niho exponents over $\mathbb{F}_{5^{2k}}$ were proposed by [46]. Further, several authors investigated permutation polynomials with Niho exponents in different years, one may refer to [7, 8, 12, 13, 14, 27, 28, 34, 37, 41, 42]. The permutation and complete permutation polynomials from linearized polynomials are discussed in [43].

Recently, various researchers have shown interest in permutation pentanomials over finite fields. Li et al. [29] and Xu et al. [47] constructed permutation pentanomials over $\mathbb{F}_{q^2}$ with even characteristic. Further, the new classes of permutation pentanomials and hexanomials over finite field $\mathbb{F}_{2^{2k}}$ were proposed by Zhang et al. [49]. Permutation pentanomials of the form $x^r h(x^{q-1})$ over $\mathbb{F}_{q^2}$ with characteristic 2 and 3 were constructed by Liu et al. [33]. Shen et al. [40] presented some new classes of permutation pentanomials and hexanomials over finite field $\mathbb{F}_{q^2}$ with characteristic five. Further, Gupta et al. [17] presented new classes of permutation trinomials and pentanomials over $\mathbb{F}_{3^{2k}}$.

The objective of the paper is to introduce new classes of permutation pentanomials over finite field with characteristic five. We construct several new classes of permutation pentanomials of the form $x^{4t+5}l(x^{5^k-1})$ over $\mathbb{F}_{5^{2k}}$, where $l(x) = x^{2t}(x^5 + c_1x^4 + c_2x^s + +c_3x + 1)$ for $c_i \in \mathbb{F}_5$, $i = 1, 2, 3$; $s \in \{2, 3\}$, by deriving necessary and sufficient conditions on t and k.

The paper is organized in four sections: The section 2 describes preliminaries and results which are helpful to explain the main results. Section 3 focuses on the construction of new classes of permutation pentanomials of the form $x^{4t+5}l(x^{5^k-1})$ over $\mathbb{F}_{5^{2k}}$. Lastly, section 4 concludes the paper.

2. Preliminaries

This section outlines key preliminary results that assist in the formulation and proof of the main results in the sections that follow.

Lemma 1. *.[[1, 2, 45, 50]] Let $s, r > 0$ with $s \mid (q-1)$ and $l(x) \in \mathbb{F}_q[x]$. Then, $g(x) = x^r l(x^{\frac{q-1}{s}})$ permutes $\mathbb{F}_q$ if and only if both the following conditions are satisfied*

i) $gcd(r, \frac{q-1}{s}) = 1$ and

ii) $x^r l(x)^{\frac{q-1}{s}}$ permutes μ_s.

Lemma 2. *.[[5]] Let $f(x)$ be a polynomial and C_f be the plane algebraic curve with the following form:*

$$C_f : \frac{f(x) - f(y)}{x - y} = 0,$$

then $f(x)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if C_f has no $\mathbb{F}_q$-rational point (a, b) with $a \neq b$.

Definition 1. *[9, 31] Let $p(x) = p_0x^n + p_1x^{n-1} + \cdots + p_n \in F[x]$ and $q(x) = q_0x^m + q_1x^{m-1} + \cdots + q_m \in F[x]$ be two polynomials of degree n and m respectively* *with $m, n \in \mathbb{N}$. Then, the resultant $R(p,q)$ of two polynomials is defined by the determinant*

$$R(p,q) = \begin{vmatrix} p_0 & p_1 & \dots & p_n & 0 & & \dots & 0 \\ 0 & p_0 & p_1 & \dots & p_n & 0 & \dots & 0 \\ \vdots & & & & & & & \\ 0 & \dots & 0 & p_0 & p_1 & & \dots & p_n \\ q_0 & q_1 & \dots & & q_m & 0 & \dots & 0 \\ 0 & q_0 & q_1 & \dots & & q_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & q_0 & q_1 & & \dots & q_m \end{vmatrix}$$

of order $m+n$. For a field F, $H_1(x,y)$ and $H_2(x,y) \in F[x,y]$ of positive degree in y, the resultant of H_1 and H_2 with respect to y is denoted by $Res(H_1,H_2,y)$. It is the resultant of H_1 and H_2 when considered as polynomials in the single variable y, that is, as elements in $R[y]$ with $R = F[x]$. Since $Res(H_1,H_2,y) \in F[x]$ is in the ideal generated by H_1 and H_2, therefore any pair (a,b) with $H_1(a,b) = H_2(a,b) = 0$ is such that $Res(H_1,H_2,y)(a) = 0$.

Lemma 3. *.[[33]] Let $q = p^k$, where p is a prime. Let r, i and j be positive integers, where $i \not\equiv p-1 \pmod{p}$ and $gcd(i+1, q+1) = 1$. Suppose that $l(x) \in \mathbb{F}_{q^2}[x]$ has no roots in μ_{p^k+1}. The polynomial $g(x) = x^r l(x)^{q-1}$ is a permutation polynomial over μ_{p^k+1} if and only if the polynomial $G(x) = x^{r+ij} L(x)^{q-1}$ is a permutation polynomial over μ_{p^k+1}, where $L(x) = (1 + x + x^2 + \dots + x^i)^j l(x)$.*

3. New Construction of Permutation Pentanomials over $\mathbb{F}_{5^{2k}}$

In this section, we construct permutation pentanomials of the type $x^{4t+5} l(x^{5^k-1})$ over $\mathbb{F}_{5^{2k}}$, where $l(x) = x^{2t}(x^5 + c_1 x^4 + c_2 x^s + +c_3 x + 1)$ for $c_i \in \mathbb{F}_5$, $i = 1,2,3$; $s \in \{2,3\}$. Here, new classes of permutation pentanomials over $\mathbb{F}_{5^{2k}}$ are constructed using the set of $(5^k+1)^{\text{th}}$ roots of unity and resultant of two polynomials. The following lemma is used in proving the main results.

Lemma 4. *The polynomial $x^5 + x^4 - x^s + x + 1$, where $s \in \{2,3\}$, has no roots in μ_{5^k+1}.*

Proof. Let $\lambda \in \mu_{5^k+1}$ be such that it satisfies the equation

$$x^5 + x^4 - x^s + x + 1 = 0.$$

Then, we have

$$\lambda^5 + \lambda^4 - \lambda^s + \lambda + 1 = 0. \tag{1}$$

Taking $(5^k)^{th}$ power of Eq. (1), and then multiplying by λ^5, we get

$$\lambda^5 + \lambda^4 - \lambda^{5-2s} + \lambda + 1 = 0. \tag{2}$$

Subtracting Eq. (1) from Eq. (2), we obtain

$$\lambda^s(\lambda^{5-2s} - 1) = 0. \tag{3}$$

For $s = 2$, Eq. (3) gives $\lambda = 0, 1$, but $\lambda = 0 \notin \mu_{5^k+1}$ and $\lambda = 1$ is a contradiction to Eq. (1). Similar argument holds for $s = 3$. Therefore, $x^5 + x^4 - x^s + x + 1$ has no roots in μ_{5^k+1}. Hence the result. ◀

Remark 1. *The polynomial $x^{2t}l(x)$, where $l(x) = x^5 + x^4 - x^s + x + 1$, $s \in \{2, 3\}$ and t is any integer, has no roots in μ_{5^k+1}.*

Lemma 5. *The polynomial $x^5 + (s+1)x^4 - x^s + (s-1)x + 1$, where $s \in \{2, 3\}$, has no roots in μ_{5^k+1}.*

Proof. Suppose $\lambda \in \mu_{5^k+1}$ satisfies the equation

$$x^5 + (s+1)x^4 - x^s + (s-1)x + 1 = 0.$$

Then, we have

$$\lambda^5 + (s+1)\lambda^4 - \lambda^3 + (s-1)\lambda + 1 = 0. \tag{4}$$

Taking $(5^k)^{th}$ power of Eq. (4), and then multiplying by λ^5, we get

$$\lambda^5 + (1-s)\lambda^4 - \lambda^2 + (1+s)\lambda + 1 = 0. \tag{5}$$

Subtracting Eq. (4) from Eq. (5), we obtain

$$2s\lambda(\lambda^3 - 1) + \lambda^s(\lambda^{5-2s} - 1) = 0. \tag{6}$$

Putting $s = 2$ in Eq. (6) yields $\lambda = 0, 1, 2, -2$. But $\lambda = 0 \notin \mu_{5^k+1}$ and $\lambda = 1, 2, -2$ is a contradiction to Eq. (1). Therefore, $x^5 + (s+1)x^4 - x^s + (s-1)x + 1$ has no roots in μ_{5^k+1}. Similar justification holds for the $s = 3$. Hence the result. ◀

Remark 2. *The polynomial $x^{2t}l(x)$, where $x^5 + (s+1)x^4 - x^s + (s-1)x + 1$, $s \in \{2, 3\}$ and t is any integer, has no roots in μ_{5^k+1}.*

Lemma 6. *The polynomial $x^5 + 4sx^4 + 2x^2 + sx + 1$, where $s \in \{2, 3\}$, has no roots in μ_{5^k+1}.*

Proof. Let $\lambda \in \mu_{5^k+1}$ be such that it satisfies the equation

$$x^5 + 4sx^4 + 2x^s + sx + 1 = 0.$$

Then, we have

$$\lambda^5 + 4s\lambda^4 + 2\lambda^s + s\lambda + 1 = 0. \tag{7}$$

Taking $(5^k)^{th}$ power of Eq. (7), and then multiplying by λ^5, we obtain

$$\lambda^5 + s\lambda^4 + 2\lambda^{5-s} + 4s\lambda + 1 = 0. \tag{8}$$

Subtracting Eq. (7) from Eq. (8), we obtain

$$3s\lambda - 3s\lambda^4 + 2\lambda^s(\lambda^{5-2s} - 1) = 0. \tag{9}$$

Put $s = 2$ in Eq. (9), we obtain $\lambda(\lambda-1)(\lambda^2-\lambda+1) = 0$ which gives $\lambda = 0, 1$ and $\lambda^2 = \lambda - 1$. But $\lambda = 0 \notin \mu_{5^k+1}$ and $\lambda = 1$ is a contradiction to Eq. (7). The remaining factor $\lambda^2 = \lambda - 1$ implies that $\lambda^6 = 1$. Thus, $\lambda^{5^k+1} = 1$ and $\lambda^6 = 1$ gives $1 = \lambda^{\gcd(5^k+1,6)} = \lambda^2$ as k is an even integer. So, $\lambda = 1, -1$ contradicts the Eq. (7). Similar argument holds for $s = 3$. Thus, the polynomial $x^5 + 3x^4 + 2x^2 + 2x + 1$ has no roots in μ_{5^k+1}. ◄

Remark 3. *Let k be an even integer, the polynomial $x^{2t}l(x)$, where $l(x) = x^5 + 4sx^4 + 2x^2 + sx + 1$, $s \in \{2, 3\}$ and t is any integer, has no roots in μ_{5^k+1}.*

Theorem 1. *Let $q = 5^k$, where k is a positive integer and t is an integer such that $t \geq -1$. Then, the polynomial*

$$u_1(x) = x^{(5+2t)\cdot 5^k+2t} + x^{(4+2t)\cdot 5^k+2t+1} - x^{(s+2t)\cdot 5^k+2t+2} + x^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5}$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if $gcd(4t + 5, 5^k - 1) = 1$.

Proof. The polynomial

$$u_1(x) = x^{(5+2t)\cdot 5^k+2t} + x^{(4+2t)\cdot 5^k+2t+1} - x^{(s+2t)\cdot 5^k+2t+2} + x^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5}$$

can be expressed as $u_1(x) = x^{4t+5}l(x^{q-1})$, where $l(x) = x^{2t}(x^5 + x^4 - x^s + x + 1)$. According to Remark 1, $l(x)$ has no roots in μ_{5^k+1}. Using Lemma 1, the polynomial $u_1(x) = x^{4t+5}l(x^{q-1})$ is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if $\gcd(4t + 5, 5^k - 1) = 1$ and the polynomial $v_1(x) = x^{4t+5}l(x)^{q-1}$ permutes μ_{5^k+1}. Let $x \in \mu_{5^k+1}$, we have

$$v_1(x) = x^{4t+5}l(x)^{q-1}$$

$$
\begin{aligned}
&= x^{4t+5}(x^{2t}(x^5 + x^4 - x^s + x + 1))^{q-1} \\
&= x^{4t+5}\frac{(x^{2t}(x^5 + x^4 - x^s + x + 1))^q}{x^{2t}(x^5 + x^4 - x^s + x + 1)} \\
&= x^{4t+5}\frac{(x^{2tq}(x^{5q} + x^{4q} - x^{sq} + x^q + 1))}{x^{2t}(x^5 + x^4 - x^s + x + 1)} \\
&= x^{4t+5}\frac{(x^{-2t}(x^{-5} + x^{-4} - x^{-s} + x^{-1} + 1))}{x^{2t}(x^5 + x^4 - x^s + x + 1)} \\
&= \frac{x^5 + x^4 - x^{5-s} + x + 1}{x^5 + x^4 - x^s + x + 1}.
\end{aligned}
$$

By putting $s = 2$ in the above equation, we get the polynomial

$$v_1(x) = \frac{x^5 + x^4 - x^2 + x + 1}{x^5 + x^4 - x^3 + x + 1}.$$

We have to prove that $v_1(x) = \dfrac{x^5 + x^4 - x^2 + x + 1}{x^5 + x^4 - x^3 + x + 1}$ permutes μ_{5^k+1}. Let $x, y \in \mu_{5^k+1}$ such that

$$
\begin{gathered}
v_1(x) = v_1(y) \\
\frac{x^5 + x^4 - x^2 + x + 1}{x^5 + x^4 - x^3 + x + 1} = \frac{y^5 + y^4 - y^2 + y + 1}{y^5 + y^4 - y^3 + y + 1}.
\end{gathered}
$$

Here, we use algebraic curve method to prove that if $v_1(x) = v_1(y)$, then $x = y$. Consider the curve

$$
\begin{aligned}
A(x, y) = &(x^5 + x^4 - x^2 + x + 1)(y^5 + y^4 - y^3 + y + 1) \\
&-(x^5 + x^4 - x^3 + x + 1)(y^5 + y^4 - y^2 + y + 1).
\end{aligned}
$$

Utilizing Lemma 2, the polynomial $v_1(x)$ permutes μ_{5^k+1} if and only if the curve $A(x, y)$ does not have any points $(x, y) \in \mu^2_{5^k+1}$ off the line $x = y$. The factorization of the curve $A(x, y)$ using MAGMA [6] is given as

$$A(x, y) = (x - y)B(x, y)C(x, y),$$

where

$$B(x, y) = x^2y + xy^2 + 2xy + 2x + 2y + 3$$

and

$$C(x, y) = x^2y^2 + 4x^2y + 4xy^2 + 4xy + 2x + 2y.$$

The resultant$(B(x, y), x^2y^2B(\frac{1}{x}, \frac{1}{y}); y) = x^7 + 4x^6 + 4x^5 + 3x^4 + 4x^3 + 4x^2 + x$ and the resultant$(C(x, y), x^2y^2C(\frac{1}{x}, \frac{1}{y}); y) = x^7 + 4x^6 + 4x^5 + 3x^4 + 4x^3 + 4x^2 + x$. The factorization of the resultants $(B(x, y), x^2y^2B(\frac{1}{x}, \frac{1}{y}); y)$ and $(C(x, y), x^2y^2C(\frac{1}{x}, \frac{1}{y}); y)$

is given as $x(x+\alpha)(x+\alpha^5)(x+2)(x+3)(x+\alpha^9)(x+\alpha^{23})$, where α is such that $x^2+2x+3 \in \mathbb{F}_5[x]$. The roots of the resultant $(B(x,y), x^2y^2B(\frac{1}{x},\frac{1}{y}); y)$ are $x = 0, -\alpha, -\alpha^5, -2, -3, \alpha^9, \alpha^{23}$. But $x^q = x \neq \frac{1}{x}$, therefore there is no point $(x,y) \in \mu^2_{5^k+1}$ that satisfies $(B(x,y), x^2y^2B(\frac{1}{x},\frac{1}{y}); y) = 0$. Similar justification holds for the resultant $(C(x,y), x^2y^2C(\frac{1}{x},\frac{1}{y}); y)$. Therefore, we get $x = y$.

For $s = 3$, we denote $v_1(x)$ by $v(x)$. Then,

$$\begin{aligned} v(x) &= \frac{x^5+x^4-x^3+x+1}{x^5+x^4-x^2+x+1} \\ &= \frac{1}{v_1(x)}. \end{aligned}$$

Here, $v(x)$ permutes μ_{5^k+1} because $v_1(x)$ permutes μ_{5^k+1}. Hence proved. ◀

By putting the values $t = -1, 0, 1$ and $s = 2$ in the Theorem 1, we get the following corollaries.

Corollary 1. *Let k be a positive integer, then*

1) *the polynomial $x^{3\cdot5^k-2} + x^{2\cdot5^k-1} - x^{5^k} + x^{-5^k+2} + x^{-2\cdot5^k+3}$ is a permutation over $\mathbb{F}_{5^{2k}}$.*

2) *the polynomial $x^{5^{k+1}} + x^{4\cdot5^k+1} - x^{3\cdot5^k+2} + x^{5^k+4} + x^5$ is a permutation polynomial over $\mathbb{F}_{5^{2k}}$.*

3) *the polynomial $x^{7\cdot5^k+2} + x^{6\cdot5^k+3} - x^{5^{k+1}+4} + x^{3\cdot5^k+6} + x^{2\cdot5^k+7}$ is a permutation polynomial if and only if k is an odd.*

Consider $p = 5, i = 2,\ j = 1, t = 0,\ s = 2$ and $l(x) = x^5+x^4-x^3+x+1$, then by utilizing the Lemma 3 and Theorem 1, we get the following corollary.

Corollary 2. *Let k is a positive integer. Then, the polynomial*

$$U(x) = x^{7\cdot5^k} + 2x^{6\cdot5^k+1} + x^{5^{k+1}+2} + 2x^{2\cdot5^k+5} + x^7$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if k is an even integer which satisfies $k \not\equiv 0$ (mod 6).

Proof. The polynomial $L(x) = (x^2+x+1)(x^5+x^4-x^3+x+1) \in \mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7L(x^{q-1})$. Let k is an even integer such that $k \not\equiv 0 \pmod 6$. This gives $\gcd(5^k+1, 3) = 1$ and $\gcd(5^k-1, 7) = 1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x) = x^5l(x^{q-1})$ permutes μ_{5^k+1}. According to Theorem 1, $V(x) = x^5l(x^{q-1})$ permutes μ_{5^k+1}.

For the converse part, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. Let k is an odd integer then $3 \mid (5^k+1)$ and ω is the primitive cube roots of unity. It can be observed that $V(\omega) = V(\omega^2) = 0$. This gives that $V(x)$ does not permute μ_{5^k+1}. If $k \equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$ which contradicts the fact that $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. ◀

By putting the values $t = -1, 0, 1$ and $s = 3$ in the Theorem 1, we get the following corollaries.

Corollary 3. *Let k be a positive integer, then*

1) *the polynomial $x^{3\cdot 5^k-2} + x^{2\cdot 5^k-1} - x + x^{-5^k+2} + x^{-2\cdot 5^k+3}$ is a permutation over $\mathbb{F}_{5^{2k}}$.*

2) *the polynomial $x^{5^{k+1}} + x^{4\cdot 5^k+1} - x^{2\cdot 5^k+3} + x^{5^k+4} + x^5$ is a permutation over $\mathbb{F}_{5^{2k}}$.*

3) *the polynomial $x^{7\cdot 5^k+2} + x^{6\cdot 5^k+3} - x^{4\cdot 5^k+5} + x^{3\cdot 5^k+6} + x^{2\cdot 5^k+7}$ is a permutation if and only if k is odd.*

Consider $p = 5, i = 2,\ j = 1, t = 0,\ s = 3$ and $l(x) = x^5 + x^4 - x^2 + x + 1$, then utilizing the Lemma 3 and Theorem 1, we get the following corollary.

Corollary 4. *Let k is a positive integer. Then, the polynomial*

$$U(x) = x^{7\cdot 5^k} + 2x^{6\cdot 5^k+1} + 2x^{5^{k+1}+2} + x^{2\cdot 5^k+5} + x^{5^k+6} + x^7$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if k is an even integer such that $k \not\equiv 0$ (mod 6).

Proof. The polynomial $L(x) = (x^2+x+1)(x^5+x^4-x^2+x+1) \in \mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7 L(x^{q-1})$. Let k is an even integer satisfying $k \not\equiv 0 \pmod 6$. This gives $\gcd(5^k+1, 3) = 1$ and $\gcd(5^k-1, 7) = 1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x) = x^5 l(x^{q-1})$ permutes μ_{5^k+1}. According to Theorem 1, $V(x) = x^5 l(x^{5^k-1})$ permutes μ_{5^k+1}.

Conversely, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. Let k is an odd integer, then $3 \mid (5^k+1)$ and ω is the primitive cube roots of unity. It can be observed that $V(\omega) = V(\omega^2) = 0$. This gives that $V(x)$ does not permute μ_{5^k+1}. If $k \equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$ which is a contradiction to the fact that $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. ◀

Theorem 2. *Let $q = 5^k$, where k is a positive integer and t is an integer such that $t \geq -1$. Then, the polynomial*

$$u_2(x) = x^{(5+2t)\cdot 5^k+2t} + (1+s)x^{(4+2t)\cdot 5^k+2t+1} - x^{(s+2t)\cdot 5^k+2t+3} - (1-s)x^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5}$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if $gcd(4t+5, 5^k-1) = 1$.

Proof. The polynomial

$$u_2(x) = x^{(5+2t)\cdot 5^k+2t} + (s+1)x^{(4+2t)\cdot 5^k+2t+1} - x^{(s+2)\cdot 5^k+2t+3} - (1-s)x^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5}$$

can be expressed as $u_2(x) = x^{4t+5}l(x^{q-1})$, where $l(x) = x^{2t}(x^5+(s+1)x^4-x^2(s-1)x+1)$. According to Remark 2, $l(x)$ has no roots in μ_{5^k+1}. Using Lemma 1, the polynomial $u_2(x) = x^{4t+5}l(x^{q-1})$ is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if $\gcd(4t+5, 5^k-1) = 1$ and the polynomial $v_2(x) = x^{4t+5}l(x)^{q-1}$ permutes μ_{5^k+1}. Let $x \in \mu_{5^k+1}$, we have

$$\begin{aligned}
v_2(x) &= x^{4t+5}l(x)^{q-1} \\
&= x^{4t+5}(x^{2t}(x^5+(s+1)x^4-x^s+(s-1)x+1))^{q-1} \\
&= x^{4t+5}\frac{(x^{2t}(x^5+(s+1)x^4-x^s+(s-1)x+1))^q}{x^{2t}(x^5+(s+1)x^4-x^s+(s-1)x+1)} \\
&= x^{4t+5}\frac{(x^{2tq}(x^{5q}+(s+1)x^{4q}-x^{sq}+(s-1))x^q+1))}{x^{2t}(x^5+(s+1)x^4-x^s+(s-1)x+1)} \\
&= x^{4t+5}\frac{(x^{-2t}(x^{-5}+(s+1)x^{-4}-x^{-s}+(s-1)x^{-1}+1))}{x^{2t}(x^5+(s+1)x^4-x^s+(s-1)x+1)} \\
&= \frac{x^5+(s-1)x^4-x^{5-s}+(s+1)x+1}{x^5+(s+1)x^4-x^s+(s-1)x+1}.
\end{aligned}$$

Put $s = 2$ in $v_2(x)$, we obtain, $v_2(x) = \dfrac{x^5-x^4-x^3+3x+1}{x^5+3x^4-x^2-x+1}$.

We have to prove that $v_2(x) = \dfrac{x^5-x^4-x^3+3x+1}{x^5+3x^4-x^2-x+1}$ permutes μ_{5^k+1}. Let $x, y \in \mu_{5^k+1}$ such that

$$v_2(x) = v_2(y)$$

$$\frac{x^5-x^4-x^3+3x+1}{x^5+3x^4-x^2-x+1} = \frac{y^5-y^4-y^3+3y+1}{y^5+3y^4-y^2-y+1}.$$

Here, we use algebraic curve method to prove that $v_2(x) = v_2(y)$ whenever $x = y$. Consider the curve

$$A(x,y) = (x^5 - x^4 - x^3 + 3x + 1)(y^5 + 3y^4 - y^2 - y + 1) -$$
$$(x^5 + 3x^4 - x^2 - x + 1)(y^5 - y^4 - y^3 + 3y + 1).$$

Utilizing Lemma 2, the polynomial $v_1(x)$ permutes μ_{5^k+1} if and only if the curve $A(x,y)$ does not have any points $(x,y) \in \mu^2_{5^k+1}$ off the line $x = y$. The factorization of the curve $A(x,y)$ using the MAGMA [6], we get

$$A(x,y) = (x-y)(y+2)(x+2)(y+3)(x+3)B(x,y)C(x,y),$$

where

$$B(x,y) = xy + 4y + 1$$

and

$$C(x,y) = xy + 4x + 1.$$

Since $x = -2, 2$ and $y = -2, 2$, consequently, $x^{q+1} \neq 1$ and $y^{q+1} \neq 1$. This gives us $x, y \notin \mu_{5^k+1}$. We are left with the factors $B(x,y) = xy + 4y + 1$ and $C(x,y) = xy + 4x + 1$. The resultant$(B(x,y), xyB(\frac{1}{x}, \frac{1}{y}); y) = 2x$ and the resultant$(C(x,y), xyC(\frac{1}{x}, \frac{1}{y}); y) = x + 2$. But $x = 0, -2 \notin \mu_{5^k+1}$, therefore there is no point $(x,y) \in \mu^2_{5^k+1}$ which satisfies $(B(x,y), xyB(\frac{1}{x}, \frac{1}{y}); y) = 0$. Similar justification holds for the resultant $(C(x,y), xyC(\frac{1}{x}, \frac{1}{y}); y)$. Therefore, we get $x = y$. For $s = 3$, we denote $v_2(x)$ by $v(x)$, we get

$$v(x) = \frac{x^5 + 3x^4 - x^2 - x + 1}{x^5 - x^4 - x^3 + 3x + 1} = \frac{1}{v_2(x)}.$$

Here, $v(x)$ permutes μ_{5^k+1} because $v_2(x)$ permutes μ_{5^k+1}. Hence proved. ◀

By putting the values $t = -1, 0, 1$ and $s = 2$ in the Theorem 2, we get the following corollaries.

Corollary 5. *Let k be a positive integer, then*

1) *the polynomial $x^{3\cdot 5^k-2} + 3x^{2\cdot 5^k-1} - x - x^{-5^k+2} + x^{-2\cdot 5^k+3}$ is a permutation over $\mathbb{F}_{5^{2k}}$.*

2) *the polynomial $x^{5^{k+1}} + 3x^{4\cdot 5^k+1} - x^{2\cdot 5^k+3} - x^{5^k+4} + x^5$ is a permutation over $\mathbb{F}_{5^{2k}}$.*

3) *the polynomial $x^{7\cdot 5^k+2} + 3x^{6\cdot 5^k+3} - x^{4\cdot 5^k+5} - x^{3\cdot 5^k+6} + x^{2\cdot 5^k+7}$ is a permutation if and only if k is odd.*

Consider $p = 5, i = 2$ and $j = 1, t = 0$, $s = 3$ and $l(x) = x^5 + 3x^4 - x^2 + x + 1$, then utilizing the Lemma 3 and Theorem 2, we get the following corollary.

Corollary 6. *Let k is a positive integer. Then, the polynomial*

$$U(x) = x^{7\cdot 5^k} + x^{6\cdot 5^k+1} + 2x^{5^{k+1}+2} + 2x^{4\cdot 5^k+3} + 3x^{5^k+6} + x^7,$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if k is an even integer such that $k \not\equiv 0$ (mod 6).

Proof. The polynomial $L(x) = (x^2+x+1)(x^5+3x^4-x^2+x+1) \in \mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7 L(x^{5^k-1})$. Let k is an even integer such that $k \not\equiv 0 \pmod 6$. This gives $\gcd(5^k+1, 3) = 1$ and $\gcd(5^k-1, 7) = 1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x) = x^5 l(x^{5^k-1})$ permutes μ_{5^k+1}. According to Theorem 2, $V(x) = x^5 l(x^{5^k-1})$ permutes μ_{5^k+1}.

For the converse part, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$ and k is an odd integer then $3 \mid (5^k + 1)$ and ω is the primitive cube roots of unity. It can be observed that $V(\omega) = V(\omega^2) = 0$. This gives that $V(x)$ does not permute μ_{5^k+1}. If $k \equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$, which is a contradiction to the hypothesis. ◀

By putting the values $t = -1, 0, 1$ and $s = 3$ in the Theorem 2, we get the following corollaries.

Corollary 7. *Let k be a positive integer, then*

1) *the polynomial $x^{3\cdot 5^k-2} - x^{2\cdot 5^k-1} - x^{5^k} + 3x^{-5^k+2} + x^{-2\cdot 5^k+3}$ is a permutation over $\mathbb{F}_{5^{2k}}$.*
2) *the polynomial $x^{5^{k+1}} - x^{4\cdot 5^k+1} - x^{3\cdot 5^k+2} + 3x^{5^k+4} + x^5$ is a permutation over $\mathbb{F}_{5^{2k}}$.*
3) *the polynomial $x^{7\cdot 5^k+2} - x^{6\cdot 5^k+3} - x^{5^{k+1}+4} + 3x^{3\cdot 5^k+6} + x^{2\cdot 5^k+7}$ is a permutation if and only if k is odd.*

Consider $p = 5, i = 2$, $j = 1, t = 0, s = 3$ and $l(x) = x^5 - x^4 - x^3 + 3x + 1$, then utilizing the Lemma 3 and Theorem 2, we get the following corollary.

Corollary 8. *Let k is a positive integer. Then, the polynomial*

$$U(x) = x^{7\cdot 5^k} - x^{5^{k+1}+2} - 2x^{4\cdot 5^k+3} + 2x^{3\cdot 5^k+4} - x^{2\cdot 5^k+5} - x^{5^k+6} + x^7,$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if k is an even integer such that $k \not\equiv 0$ (mod 6).

Proof. The polynomial $L(x) = (x^2+x+1)(x^5-x^4-x^3+3x+1) \in \mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7L(x^{5^k-1})$. Let k is an even integer such that $k \not\equiv 0 \pmod 6$. This gives $\gcd(5^k+1, 3) = 1$ and $\gcd(5^k-1, 7) = 1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x) = x^5l(x^{5^k-1})$ permutes μ_{5^k+1}. According to Theorem 2, $V(x) = x^5l(x^{5^k-1})$ permutes μ_{5^k+1}.

Conversely, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$ and k is an odd integer, then $3 \mid (5^k + 1)$ and ω is the primitive cube roots of unity. It can be observed that $V(\omega) = V(\omega^2) = 0$. This gives that $V(x)$ does not permute μ_{5^k+1}. If $k \equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$ which contradicts the fact that $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. ◄

Theorem 3. *Let $q = 5^k$, where k is a positive even integer and t is an integer such that $t \geq -1$. Then, the polynomial*

$$u_5(x) = x^{(5+2t)\cdot 5^k+2t} + 4sx^{(4+2t)\cdot 5^k+2t+1} + 2x^{(s+2t)\cdot 5^k+2t+3} + sx^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5}$$

is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if gcd$(4t+5, 5^k-1) = 1$.

Proof. The polynomial

$$u_3(x) = x^{(5+2t)\cdot 5^k+2t} + 4sx^{(4+2t)\cdot 5^k+2t+1} + 2x^{(s+2t)\cdot 5^k+2t+3} + \\ + sx^{(1+2t)\cdot 5^k+2t+4} + x^{(2t)\cdot 5^k+2t+5},$$

can be expressed as $u_3(x) = x^{4t+5}l(x^{q-1})$, where $l(x) = x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1)$. According to Remark 3, $l(x)$ has no roots in μ_{5^k+1}. Using Lemma 1, the polynomial $u_3(x) = x^{4t+5}l(x^{q-1})$ is a permutation over $\mathbb{F}_{5^{2k}}$ if and only if $\gcd(4t+5, 5^k-1) = 1$ and the polynomial $v_3(x) = x^{4t+5}l(x)^{q-1}$ permutes μ_{5^k+1}. Let $x \in \mu_{5^k+1}$, we have

$$\begin{aligned}
v_3(x) &= x^{4t+5}l(x)^{q-1} \\
&= x^{4t+5}(x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1))^{q-1} \\
&= x^{4t+5}\frac{(x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1))^q}{x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1)} \\
&= x^{4t+5}\frac{(x^{2tq}(x^{5q} + 4sx^{4q} + 2x^{sq} + sx^q + 1))}{x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1)} \\
&= x^{4t+5}\frac{(x^{-2t}(x^{-5} + 4sx^{-4} + 2x^{-s} + sx^{-1} + 1))}{x^{2t}(x^5 + 4sx^4 + 2x^s + sx + 1)} \\
&= \frac{x^5 + sx^4 + 2x^{5-s} + 4sx + 1}{x^5 + 4sx^4 + 2x^s + sx + 1}.
\end{aligned}$$

Put $s=2$ in $v_3(x)$, we obtain $v_3(x)=\dfrac{x^5+2x^4+2x^3+3x+1}{x^5+3x^4+2x^2+2x+1}$.

We have to prove that $v_3(x)=\dfrac{x^5+2x^4+2x^3+3x+1}{x^5+3x^4+2x^2+2x+1}$ permutes μ_{5^k+1}. Let $x,y\in\mu_{5^k+1}$ such that

$$v_3(x)=v_3(y)$$
$$\frac{x^5+2x^4+2x^3+3x+1}{x^5+3x^4+2x^2+2x+1}=\frac{y^5+2y^4+2y^3+3y+1}{y^5+3y^4+2y^2+2y+1}.$$

Here, we use algebraic curve method to prove that if $v_3(x)=v_3(y)$, then $x=y$. Consider the curve

$$\begin{aligned}A(x,y)&=(x^5+2x^4+2x^3+3x+1)(y^5+3y^4+2y^2+2y+1)\\&\quad-(x^5+3x^4+2x^2+2x+1)(y^5+2y^4+2y^3+3y+1).\end{aligned}$$

Utilizing Lemma 2, the polynomial $v_1(x)$ permutes μ_{5^k+1} if and only if the curve $A(x,y)$ does not have any points $(x,y)\in\mu^2_{5^k+1}$ off the line $x=y$.
The factorization of the curve $A(x,y)$ using the MAGMA [6], we get

$$A(x,y)=(x-y)(y+\alpha^8)(y+\alpha^{16})(x+\alpha^8)(x+\alpha^{16})B(x,y)C(x,y),$$

where

$$B(x,y)=xy+4y+1,$$
$$C(x,y)=xy+4x+1,$$

and α satisfies $x^2+2x+3\in\mathbb{F}_5[x]$. Since $x=-\alpha^8,-\alpha^{16}$ and $y=-\alpha^8,-\alpha^{16}$ this implies that $x^{q+1}\neq 1$ and $y^{q+1}\neq 1$. This gives us $x,y\notin\mu_{5^k+1}$. We are left with the factors $B(x,y)=xy+4y+1$ and $C(x,y)=xy+4x+1$. The resultant$(B(x,y),xyB(\frac{1}{x},\frac{1}{y});y)=\alpha^{19}x$ and the resultant$(C(x,y),xyC(\frac{1}{x},\frac{1}{y});y)=x+\alpha^8$. But $x=0,-\alpha^8\notin\mu_{5^k+1}$, therefore there is no point $(x,y)\in\mu^2_{5^k+1}$ that satisfies $(B(x,y),xyB(\frac{1}{x},\frac{1}{y});y)=0$. Similar justification holds for the $(C(x,y),xyC(\frac{1}{x},\frac{1}{y});y)$. Therefore, we get $x=y$.

For $s=3$, we denote $v_3(x)$ by $v(x)$, we get

$$v(x)=\frac{x^5+3x^4+2x^2+2x+1}{x^5+2x^4+2x^3+3x+1}=\frac{1}{v_3(x)}.$$

Here, $v(x)$ permutes μ_{5^k+1} since $v_3(x)$ permutes μ_{5^k+1}. ◄

By putting the values $t=-1,0$ and $s=2$ in the Theorem 3, we get the following corollaries.

Corollary 9. *Let k be an even positive integer, then*

1) *the polynomial* $x^{3\cdot 5^k-2}+3x^{2\cdot 5^k-1}+2x+2x^{-5^k+2}+x^{-2\cdot 5^k+3}$ *is a permutation over* $\mathbb{F}_{5^{2k}}$.

2) *the polynomial* $x^{5^{k+1}}+3x^{4\cdot 5^k+1}+2x^{2\cdot 5^k+3}+2x^{5^k+4}+x^5$ *is a permutation over* $\mathbb{F}_{5^{2k}}$.

Considering $p=5, i=2, j=1, t=0$ and $l(x)=x^5+3x^4+2x^2+2x+1$ and utilizing the Lemma 3 and Theorem 3, we get the following corollary.

Corollary 10. *Let k is an even positive integer. Then, the polynomial*

$$U(x)=x^{7\cdot 5^k}-x^{6\cdot 5^k+1}-x^{5^{k+1}+2}-x^{3\cdot 5^k+4}-2x^{5^k+6}+x^7,$$

is a permutation over $\mathbb{F}_{5^{2k}}$ *if and only if* $k\not\equiv 0 \pmod 6$.

Proof. The polynomial $L(x)=(x^2+x+1)(x^5+3x^4+2x^2+2x+1)\in\mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7L(x^{5^k-1})$. Let $k\not\equiv 0 \pmod 6$ and it is given that k is an even integer. Therefore, $\gcd(5^k+1,3)=1$ and $\gcd(5^k-1,7)=1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x)=x^5l(x^{5^k-1})$ permutes μ_{5^k+1}. According to Theorem 3, $V(x)=x^5l(x^{5^k-1})$ permutes μ_{5^k+1}.

Conversely, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. If $k\equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$ which contradicts the hypothesis. ◄

By putting the values $t=-1,0$ and $s=3$ in the Theorem 3, we get the following corollaries.

Corollary 11. *Let k be an even positive integer, then*

1) *the polynomial* $x^{3\cdot 5^k-2}+2x^{2\cdot 5^k-1}+2x^{5^k}+2x^{-5^k+2}+3x^{-2\cdot 5^k+3}$ *is a permutation over* $\mathbb{F}_{5^{2k}}$.

2) *the polynomial* $x^{5^{k+1}}+2x^{4\cdot 5^k+1}+2x^{3\cdot 5^k+2}+3x^{5^k+4}+x^5$ *is a permutation over* $\mathbb{F}_{5^{2k}}$.

Consider $p=5, i=2, j=1, t=0$ and $l(x)=x^5+2x^4+2x^3+3x+1$, then utilizing the Lemma 3 and Theorem 3, we get the following corollary.

Corollary 12. *Let k is an even positive integer. Then, the polynomial*

$$U(x)=x^{7\cdot 5^k}-2x^{6\cdot 5^k+1}-x^{4\cdot 5^k+3}-x^{2\cdot 5^k+5}-x^{5^k+6}+x^7,$$

is a permutation over $\mathbb{F}_{5^{2k}}$ *if and only if* $k\not\equiv 0 \pmod 6$.

Proof. The polynomial $L(x) = (x^2 + x + 1)(x^5 + 2x^4 + 2x^3 + 3x + 1) \in \mathbb{F}_{5^{2k}}$, and the polynomial $U(x)$ can be expressed as $x^7 L(x^{5^k-1})$. Let $k \not\equiv 0 \pmod 6$ and it is given that k is an even integer. Therefore, $\gcd(5^k + 1, 3) = 1$ and $\gcd(5^k - 1, 7) = 1$. Utilizing Lemma 3, the polynomial $U(x)$ permutes μ_{5^k+1} if and only if $V(x) = x^5 l(x^{5^k-1})$ permutes μ_{5^k+1}. According to Theorem 3, $V(x) = x^5 l(x^{5^k-1})$ permutes μ_{5^k+1}.

Conversely, let $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. If $k \equiv 0 \pmod 6$, then we deduce that $V(x)$ is not a permutation over μ_{5^k+1} using Lemma 1. Therefore, $U(x)$ is not a permutation over $\mathbb{F}_{5^{2k}}$ which contradicts the fact that $U(x)$ is a permutation over $\mathbb{F}_{5^{2k}}$. ◀

4. Conclusion

In this paper, we constructed permutation pentanomials of the form $x^{4t+5} l(x^{5^k-1})$ over $\mathbb{F}_{5^{2k}}$, where $l(x) = x^{2t}(x^5 + c_1 x^4 + c_2 x^s + c_3 x + 1)$, for $c_i \in \mathbb{F}_5$, $i = 1, 2, 3$; $s \in \{2, 3\}$. This work advances the study of permutation polynomials over finite fields by introducing and analyzing new classes of permutation pentanomials over $\mathbb{F}_{5^{2k}}$. It establishes specific conditions under which these pentanomials act as permutations of field elements. The results extend previous research on permutation trinomials and quadrinomials to higher-degree forms, thereby broadening the understanding of polynomial mappings over finite fields. Despite its novel contributions, the study does not investigate the cryptographic strength or resistance of the obtained polynomials against the algebraic or differential attacks, which would require a separate line of analysis.

However, the present work can be extended by exploring permutation pentanomials over finite fields of other characteristics and higher extensions. Future studies may also generalize the proposed construction techniques to higher degree sparse polynomials such as hexanomials and septanomials. Additionally, the cryptographic properties of the obtained pentanomials such as nonlinearity, differential uniformity and implementation efficiency can be analyzed to assess their suitability for practical applications in cryptography and coding theory.

Acknowledgement

The third author thankfully acknowledge the financial support of UGC India.

References

[1] Akbary, A., Ghioca, D., Wang, Q. (2011) *On constructing permutations of finite fields*, Finite Fields Appl., **17(1)**, 51–67.

[2] Akbary, A., Wang, Q. (2007) *On polynomials of the form* $x^r f\left(x^{\frac{q-1}{l}}\right)$, Int. J. Math. Math. Sci., **2007**, Article ID 23408. https://doi.org/10.1155/2007/23408

[3] Bai, T., Xia, Y. (2018) *A new class of permutation trinomials constructed from Niho exponents*, Cryptogr. Commun., **10**, 1023–1036.

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

[5] Bartoli, D., Giulietti, M. (2018) *Permutation polynomials, fractional polynomials, and algebraic curves*, Finite Fields Appl., **51**, 1–16.

[6] Bosma, W., Cannon, J., Playoust, C. (1997) *The Magma algebra system I: The user language*, J. Symbolic Comput., **24(3–4)**, 235–265.

[7] Cao, X., Hou, X.D., Mi, J., Xu, S. (2020) *More permutation polynomials with Niho exponents which permute* $\mathbb{F}_{q^2}$, Finite Fields Appl., **62**, Article 101626.

[8] Celik, S. (2025) *Commutator of maximal operator on Carleson curves in local generalized weighted Morrey spaces*, J. Contemp. Appl. Math., **15(2)**, 142-158. https://doi.org/10.62476/jcam.151.21

[9] Cox, D., Little, J., O'Shea, D., Sweedler, M. (1997) *Ideals, Varieties, and Algorithms*, Vol. 3, Springer.

[10] Ding, C., Yuan, J. (2006) *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A, **113(7)**, 1526–1535.

[11] Ding, C., Helleseth, T. (2013) *Optimal ternary cyclic codes from monomials*, IEEE Trans. Inf. Theory, **59(9)**, 5898–5904.

[12] Farzalieva, U.M. (2021) *Existence and uniqueness of a solution to the optimal control problem with Lions type functional for the linear nonstationary quasi-optics equation*, J. Contemp. Appl. Math., **11(2)**, 38-52.

[13] Gasimova, A.R., Ibrahimova, S.S. (2025) *On homogeneous limit integral equations of Fredholm type in spaces of bounded functions*, J. Contemp. Appl. Math., **15(2)**, 77-93.

[14] Grassl, M., Özbudak, F., Özkaya, B., Temür, B.G. (2024) *Complete characterization of a class of permutation trinomials in characteristic five*, Cryptogr. Commun., **16**, 825–841.

[15] Gupta, R., Sharma, R.K. (2016) *Some new classes of permutation trinomials over finite fields with even characteristic*, Finite Fields Appl., **41**, 89–96.

[16] Gupta, S., Singh, M., Vinayak, S. (2025) *Some classes of permutation polynomials of the form* $x(x^{s_1(q+1)} + bx^{s_2(q+1)} + a)$ *over* $\mathbb{F}_{q^2}$, J. Discrete Math. Sci. Cryptogr., **28(3)**, 907–930.

[17] Gupta, S., Vinayak, S., Nayyar, A., Singh, M. (2025) *On some new classes of permutation trinomials and pentanomials over* $\mathbb{F}_{3^{2m}}$, J. Appl. Math. Comput., **71**, 5259–5277.

[18] Hou, X.D. (2013) *A class of permutation binomials over finite fields*, J. Number Theory, **133(10)**, 3549–3558.

[19] Hou, X.D. (2014) *Determination of a type of permutation trinomials over finite fields*, Acta Arith., **166(3)**, 253–278.

[20] Hou, X.D. (2015) *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl., **35**, 16–35.

[21] Hou, X.D., Lappano, S.D. (2015) *Determination of a type of permutation binomials over finite fields*, J. Number Theory, **147**, 82–119.

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

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

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

[25] Hou, X.D. (2015) *Permutation polynomials over finite fields—A survey of recent advances*, Finite Fields Appl., **32**, 82–119.

[26] Laigle-Chapuy, Y. (2007) *Permutation polynomials and applications to coding theory*, Finite Fields Appl., **13(1)**, 58–70.

[27] Li, N., Helleseth, T. (2017) *Several classes of permutation trinomials from Niho exponents*, Cryptogr. Commun., **9**, 693–705.

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

[29] Li, K., Qu, L., Wang, Q. (2018) *New constructions of permutation polynomials of the form* $x^r h\big(x^{q-1}\big)$ *over* $\mathbb{F}_{q^2}$, Des. Codes Cryptogr., **86**, 2379–2405.

[30] Li, K., Qu, L., Li, C., Fu, S. (2018) *New permutation trinomials constructed from fractional polynomials*, Acta Arith., **183**, 101–116.

[31] Lidl, R., Niederreiter, H. (1997) *Finite Fields*, 2nd ed., Cambridge University Press, Cambridge.

[32] Lidl, R., Müller, W.B. (1984) *Permutation polynomials in RSA-cryptosystems*, In: *Advances in Cryptology (CRYPTO '83)*, Plenum Press, New York, 293–301.

[33] Liu, Q., Chen, G., Liu, X., Zou, J. (2023) *Several classes of permutation pentanomials with the form* $x^r h(x^{p^m-1})$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl., **92**, Article 102307.

[34] Ma, J., Ge, G. (2017) *A note on permutation polynomials over finite fields*, Finite Fields Appl., **48**, 261–270.

[35] Mullen, G.L. (1993) *Permutation polynomials over finite fields*, In: *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Las Vegas, NV, 1991), Lecture Notes Pure Appl. Math., **141**, 131–151.

[36] Mullen, G.L., Wang, Q. (2014) *Permutation polynomials of one variable*, In: *Handbook of Finite Fields*, CRC Press, Boca Raton, FL, Section 8.1.

[37] Rai, A., Gupta, R. (2023) *Further results on a class of permutation trinomials*, Cryptogr. Commun., **15(4)**, 811–820.

[38] Rehan, M., Vinayak, S., Gupta, S. (2023) *Randomness of sequences of numbers using permutation polynomials over prime finite fields*, Contemp. Math., **4(3)**, 453–466.

[39] Schwenk, J., Huber, K. (1998) *Public key encryption and digital signatures based on permutation polynomials*, Electron. Lett., **34(8)**, 759–760.

[40] Shen, R., Liu, X., Xu, X. (2024) *More constructions of permutation pentanomials and hexanomials over* $\mathbb{F}_{p^{2m}}$, Appl. Algebra Eng. Commun. Comput., **2024**, 1–23.

[41] Jain, S., Hashemi, F., Alimohammady, M., Cesarano, C., Agarwal, P. (2024) *Complex solutions in magnetic Schrödinger equations with critical nonlinear terms*, J. Contemp. Appl. Math., **14(2)**, 61-71.

[42] Sultanova, V. (2021) *Problems for the first-order differential equations with discrete additive and discrete multiplicative derivatives*, J. Contemp. Appl. Math., **11(2)**, 3-10.

[43] Singh, M., Gupta, S., Gupta, S., Sharma, P.L. (2024) *On permutation and complete permutation binomials and trinomials from linearized polynomials over finite fields*, J. Discrete Math. Sci. Cryptogr., **27(3)**, 1073–1085.

[44] Jarali, V., Poojary, P., Bhatta, G.V. (2023) *A recent survey of permutation trinomials over finite fields*, AIMS Math., **8(12)**, 29182–29220.

[45] Wan, D., Lidl, R. (1991) *Permutation polynomials of the form $x^r f\left(x^{\frac{q-1}{d}}\right)$ and their group structure*, Monatsh. Math., **112**, 149–163.

[46] Wu, G., Li, N. (2019) *Several classes of permutation trinomials over $\mathbb{F}_{5^n}$ from Niho exponents*, Cryptogr. Commun., **11**, 313–324.

[47] Xu, G., Cao, X., Ping, J. (2018) *Some permutation pentanomials over finite fields with even characteristic*, Finite Fields Appl., **49**, 212–226.

[48] Zha, Z., Hu, L., Fan, S. (2017) *Further results on permutation trinomials over finite fields with even characteristic*, Finite Fields Appl., **45**, 43–52.

[49] Zhang, T., Zheng, L., Hao, X. (2023) *More classes of permutation hexanomials and pentanomials over finite fields with even characteristic*, Finite Fields Appl., **91**, Article 102250.

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

[51] Zieve, M.E. (2008) *Some families of permutation polynomials over finite fields*, Int. J. Number Theory, **4(5)**, 851–857.

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

Praveen Agarwal
Department of Mathematical Science, Saveetha School of Engineering, Chennai, Tamilnadu, 602105 India.
Department of Computer Sciences, Faculty of Science, Karadeniz Technical University, Trabzon 61080, Türkiye.
Scientific Research Centre, Baku Engineering University, Baku AZ0102, Azerbaijan.
E-mail: goyal.praveen2011@gmail.com

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

Manpreet Singh
Department of Mathematics & Statistics, Himachal Pradesh University, Shimla-171005, India
E-mail: ms44167@gmail.com

Sagar Vinayak
Department of Mathematics & Statistics, Himachal Pradesh University, Shimla-171005, India
E-mail: sagarvinayak0001@gmail.com

Rakib Efendiev
Department of Mathematics and Computer Science, Baku Engineering University, Baku, Azerbaijan
E-mail: refendiyev@beu.edu.az

Shilpi Jain
Department of Mathematics, Poornima College of Engineering, Jaipur-302022, India
E-mail: shilpijain1310@gmail.com

Received 15 January 2026
Accepted 14 May 2026