

New classes of permutation pentanomials over $\mathbb{F}_{5^{2n}}$

Shalini Gupta *

Sagar Vinayak †

Manpreet Singh §

Department of Mathematics & Statistics

Himachal Pradesh University

Shimla 171005

Himachal Pradesh

India

Abstract

Developing novel classes of permutation polynomials (PPs) has become a prominent focus in recent mathematical research. We introduce new classes of permutation pentanomials defined on $\mathbb{F}_{5^{2n}}$ through the strategic selection of coefficients expressed as $x^r h(x^{q-1})$, where $q = 5^n$. Over nine distinct classes are identified, with further generalizations achieved by varying the exponent r .

Subject Classification (2020): 11T55, 11T06, 05A05.

Keywords: Permutation polynomial, Permutation pentanomial, Finite field.

1. Introduction

Let $f(x) \in \mathbb{F}_q[x]$, where $\mathbb{F}_q$ denotes finite field containing q elements (with q being power of a prime), is a PP given that it maps $\mathbb{F}_q$ bijectively onto itself. These polynomials are of particular interest because they permute the elements of the field. The study of PPs has become a vibrant research domain with wide-ranging applicability, especially in areas such as error-correcting codes [6], cryptographic systems [22], and combinatorial constructions [7]. Their practical relevance has been demonstrated in several domains, leading to a surge of recent developments and results in this field.

The study of permutation polynomials (PPs) has deep historical roots, originating from foundational contributions by Hermite [15] and Dickson [4],[5].

* E-mail: shalini.garga1970@gmail.com (Corresponding Author)

† E-mail: sagarvinayak0001@gmail.com

§ E-mail: ms44167@gmail.com

Over time, significant attention has been directed towards the identification of structured families of PPs, especially those with minimal terms such as binomials, trinomials, quadrinomials [2],[9],[11],[25],[32],[33],[42] and more recently, pentanomials and hexanomials [36],[40],[41]. These polynomials, due to their algebraic simplicity and rich permutation behavior, have been widely explored using various mathematical frameworks including linearized polynomials, normal polynomials, trace functions, algebraic curve techniques, and fractional polynomial transformations [3],[12],[14],[29],[30]. Of particular interest is the class of polynomials expressed as $x^s g(x^{(q-1)/d})$ over $\mathbb{F}_{q^2}$, the bijective property of such polynomials is governed by the appropriate selection of parameters s , d , and structure of $g(x)$, making their classification both rich and complex, see [1],[20],[34],[35]. One may refer to following books [23],[26] and survey papers [16],[17] for better understanding.

Extensive studies have established criteria under which these forms permute the elements of finite fields, particularly over $\mathbb{F}_{q^2}$ for small r and low-degree $h(x)$. Numerous researchers have focused on constructing permutation trinomials and pentanomials over fields like $\mathbb{F}_{2^{2n}}$, $\mathbb{F}_{3^{2n}}$, and $\mathbb{F}_{5^{2n}}$, often with carefully chosen coefficients or by solving specific low-degree equations, see [8],[10],[13],[19],[21],[24],[28],[31],[37]. For instance in [27], polynomials structured as $x^3(x^{2(q-1)} + cx^{q-1} + d)$ and related structures have been shown to yield permutation behavior under certain conditions on the coefficients and field size. The AGW (Akbari–Ghioca–Wang) criterion [2] has been proven useful in verifying such properties and in generating new classes of permutation polynomials over finite fields. Recent works have even extended the investigation to hexanomials and more complex forms, revealing deeper algebraic patterns.

Despite these advancements, constructing generalized forms of PPs with broader algebraic configurations remains a challenging and open area of inquiry. Many existing constructions are confined to special cases where coefficients are fixed or constrained, leaving ample scope for discovering new families with greater flexibility. Continued exploration in this direction promises to uncover richer structural insights into polynomial functions over finite fields and may lead to novel theoretical breakthroughs in algebra and number theory.

This work seeks to advance the study of permutation polynomials by presenting novel classes of permutation pentanomials defined over $\mathbb{F}_{5^{2n}}$. The proposed approach builds upon existing constructions by easing certain restrictions on coefficients and examining how these changes affect the permutation behavior of the polynomials.

The organization of the manuscript is outlined here: Section 2 outlines the essential background, including key definitions and foundational results relevant to permutation polynomials in finite fields. Section 3 develops a set of lemmas that serve as the basis for construction of new permutation pentanomials. Additionally, we state and prove the main results concerning the permutation properties of some new classes of pentanomials over $\mathbb{F}_{5^{2n}}$. The concluding remarks are presented in Section 4, which also proposes prospective research directions for further investigation.

2. Preliminaries

Let us denote by μ_k the collection of all k -th roots of unity within the algebraic closure $\overline{\mathbb{F}}_q$ of the field $\mathbb{F}_q$.

The upcoming sections rely on the following lemmas to establish the main results.

Lemma 1: [39] *For $k, s > 0$ such that $k|(q-1)$, and consider $g(x) \in \mathbb{F}_q[x]$. The function*

$$F(x) = x^s g\left(x^{\frac{q-1}{k}}\right)$$

is a PP over $\mathbb{F}_q$ if and only if: $\gcd\left(s, \frac{q-1}{k}\right) = 1$, and the function $x \mapsto x^s g(x)^{\frac{q-1}{k}}$ is bijective on μ_k .

Lemma 2: [18] *Let $q = 5^n$, where n is an even integer. Then, ± 2 are square elements in $\mathbb{F}_{q^2}$. Moreover, $\sqrt{\pm 2} \in \mathbb{F}_q$.*

Several proofs require a detailed investigation of the solutions to polynomial systems. A fundamental algebraic tool utilized in such contexts is the resultant of two polynomials. We begin by recalling some essential properties of the resultant [23]. Let $\mathbb{F}$ be a field and consider two polynomials of degree s and t respectively, where $u_i, v_j \in \mathbb{F}$ for all i, j , and $u_s v_t \neq 0$ given by:

$$u(x) = \sum_{i=0}^s u_i x^i, v(x) = \sum_{j=0}^t v_j x^j.$$

The resultant, $\text{Res}(u, v) \in R$ of $u(x)$ and $v(x)$ is defined as the determinant of the Sylvester matrix. This matrix is of size $(s+t) \times (s+t)$ and is constructed from the coefficients of $u(x)$ and $v(x)$ as follows:

$$\text{Res}(u, v) = \det \begin{pmatrix} u_s & u_{s-1} & \cdots & u_0 & 0 & \cdots & 0 \\ 0 & u_s & u_{s-1} & \cdots & u_0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & u_s & u_{s-1} & \cdots & u_0 \\ v_t & v_{t-1} & \cdots & v_0 & 0 & \cdots & 0 \\ 0 & v_t & v_{t-1} & \cdots & v_0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & v_t & v_{t-1} & \cdots & v_0 \end{pmatrix}.$$

The top t rows consist of right-shifted copies of the coefficients of $u(x)$, while the bottom s rows are similarly constructed from the coefficients of $v(x)$. The vanishing of this determinant, $\text{Res}(u, v) = 0$, provides a necessary and sufficient condition for $u(x)$ and $v(x)$ to share a common non-trivial root in an algebraic closure of the coefficient field.

3. Main Results

The present section discusses Lemmas 1 to 5 which show that several degree 4 and 5 polynomials remain non-zero over μ_{q+1} for $q = 5^n$ under certain

constraints. Lemmas 6 to 11 further establish that specific fractional polynomials permute μ_{q+1} under particular conditions. Using these lemmas, we prove Theorems 1 to 9, which introduce various classes of permutation pentanomials over $\mathbb{F}_{5^{2n}}$.

Lemma 3: *Given that $q = 5^n$ with even n , $x^5 + (c + d + 3)x^4 + ((d + 1)c + 1)x^3 + ((3d + 1)c - 2)x^2 + ((c - 2)(d + 3) + 3c)x + c - 2$ is non-zero in μ_{q+1} , where $c, d \in \{1, 3\}$.*

Proof: Let γ be a root of $x^5 + (c + d + 3)x^4 + ((d + 1)c + 1)x^3 + ((3d + 1)c - 2)x^2 + ((c - 2)(d + 3) + 3c)x + c - 2$. Then,

$$\gamma^5 + (c + d + 3)\gamma^4 + ((d + 1)c + 1)\gamma^3 + ((3d + 1)c - 2)\gamma^2 + ((c - 2)(d + 3) + 3c)\gamma + c - 2 = 0 \quad (1)$$

$$(\gamma^3 + c\gamma^2 + 3c\gamma + c - 2)(\gamma^2 + (d + 3)\gamma + 1) = 0 \quad (2)$$

which implies that either $(\gamma^3 + c\gamma^2 + 3c\gamma + c - 2) = 0$ or $(\gamma^2 + (d + 3)\gamma + 1) = 0$. Let us discuss the case when $(\gamma^2 + (d + 3)\gamma + 1) = 0$; on solving for the value of γ , we get $\gamma = -3 \pm 3\sqrt{2}$ or $3 \pm 3\sqrt{2}$. Since n is even and by Lemma 2, $\sqrt{\pm 2} \in \mathbb{F}_q$, which gives $\gamma \in \mathbb{F}_q$. Also, $\mathbb{F}_q \cap \mu_{q+1} = \{1, -1\}$ concludes contradiction as per the obtained values of γ . On the other hand, if $(\gamma^3 + c\gamma^2 + 3c\gamma + c - 2) = 0$, then on solving, we get $\gamma = 0, \pm 2$; all these cases contradict equation (2). Thus, for even values of n , $x^5 + (c + d + 3)x^4 + ((d + 1)c + 1)x^3 + ((3d + 1)c - 2)x^2 + ((c - 2)(d + 3) + 3c)x + c - 2$ is non-zero in μ_{q+1} .

Lemma 4: *Given that $q = 5^n$ with even n , $x^5 + (d + c - 3)x^4 + ((d + 4)c + 1)x^3 + ((2d + 1)c - 3)x^2 + ((d + 2)(c - 3) + 2c)x + c - 3$ is non-zero in μ_{q+1} , where $d, c \in \{2, 4\}$.*

Proof: Let δ be a root of $x^5 + (d + c - 3)x^4 + ((d + 4)c + 1)x^3 + ((2d + 1)c - 3)x^2 + ((d + 2)(c - 3) + 2c)x + c - 3$. Then,

$$\delta^5 + (d + c - 3)\delta^4 + ((d + 4)c + 1)\delta^3 + ((2d + 1)c - 3)\delta^2 + ((d + 2)(c - 3) + 2c)\delta + c - 3 = 0 \quad (4)$$

$$(\delta^3 + c\delta^2 + 2c\delta + c - 3)(\delta^2 + (d + 2)\delta + 1) = 0. \quad (5)$$

Equation (5) shows that either $(\delta^3 + c\delta^2 + 2c\delta + c - 3) = 0$ or $(\delta^2 + (d + 2)\delta + 1) = 0$. For the sake of simplicity, suppose $(\delta^3 + c\delta^2 + 2c\delta + c - 3) = 0$. On solving, we have $\delta = 0, \pm 1$, which gives a contradiction when substituted into equation (5). In the case of $(\delta^2 + (d + 2)\delta + 1) = 0$, we get $\delta = 3 \pm 3\sqrt{2}$ or $-3 \pm 3\sqrt{2}$. Since n is even and Lemma 2 implies $\sqrt{\pm 2} \in \mathbb{F}_q$, and we know $\mathbb{F}_q \cap \mu_{q+1} = \{1, -1\}$, the obtained values of δ lead to a contradiction. Therefore, for even values of n , $x^5 + (d + c - 3)x^4 + ((d +$

$4)c + 1)x^3 + ((2d + 1)c - 3)x^2 + ((d + 2)(c - 3) + 2c)x + c - 3$ is non-zero in μ_{q+1} , where $d, c \in \{2, 4\}$.

Lemma 5: For $q = 5^n$, the polynomials $x^4 + 4x^3 + 3x^2 + 4x + 1$, $x^4 + 2x^3 + 3x^2 + 2x + 1$ and $x^4 + x^3 + 3x^2 + x + 1$ are non-zero in μ_{q+1} .

Proof: Let β be a root of $x^4 + 4x^3 + 3x^2 + 4x + 1$. Thus, we obtain

$$\beta^4 + 4\beta^3 + 3\beta^2 + 4\beta + 1 = 0. \quad (6)$$

After factorizing we have, $(\beta^2 + \beta + 2)(\beta^2 + 3\beta + 3) = 0$. Solving for β , we get $\beta = 2 \pm 3\sqrt{-2}$ or $\beta = 1 \pm 3\sqrt{2}$. However, substituting these values in Equation (6) yields a contradiction. Thus, $x^4 + 4x^3 + 3x^2 + 4x + 1$ is non-zero in μ_{q+1} . Likewise, proof can be done for other parts.

Using the similar arguments, the following Lemma 6 can be derived.

Lemma 6: For $q = 5^n$ with even n , the polynomials $x^4 + x^3 + 4x^2 + 3x + 3$, $x^4 + 4x^3 + 4x^2 + 2x + 3$, $x^4 + 4x^3 + x^2 + 4x + 2$ and $x^4 + x^3 + x^2 + x + 2$ are non-zero in μ_{q+1} .

Lemma 7: Given that $c \in \{1, 3\}$, the fractional polynomial

$$I_1(x) = \frac{(c+3)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1}{x^5 + (c+4)x^4 + (2c+1)x^3 + (4c+3)x^2 + (2c+2)x + c + 3}$$

permutes $\mu_{5^{n+1}}$ if and only if n being even.

Proof: In first case, consider n as even and $c \in \{1, 3\}$, where

$$I_1(x) = \frac{(c+3)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1}{x^5 + (c+4)x^4 + (2c+1)x^3 + (4c+3)x^2 + (2c+2)x + c + 3}.$$

Further, by putting the value $d = 1$ in Lemma 3, we obtain $G(x) = x^5 + (c + 4)x^4 + (2c + 1)x^3 + (4c + 3)x^2 + (2c + 2)x + c + 3$, which is non-zero in $\mu_{5^{n+1}}$ for n as even. Therefore, $I_1(x)$ acts as a permutation on $\mu_{5^{n+1}}$ exactly when the fractional polynomial $I_1(x)$ is one-to-one on $\mu_{5^{n+1}}$.

If $x, y \in \mu_{5^{n+1}}$, consider $I_1(x) = I_1(y)$

$$\begin{aligned} & \frac{(c+3)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1}{x^5 + (c+4)x^4 + (2c+1)x^3 + (4c+3)x^2 + (2c+2)x + c + 3} \\ &= \frac{(c+3)y^5 + (2c+2)y^4 + (4c+3)y^3 + (2c+1)y^2 + (c+4)y + 1}{y^5 + (c+4)y^4 + (2c+1)y^3 + (4c+3)y^2 + (2c+2)y + c + 3}. \end{aligned} \quad (7)$$

On rearranging, we have

$$\begin{aligned} & ((c + 3)x^5 + (2c + 2)x^4 + (4c + 3)x^3 + (2c + 1)x^2 + (c + 4)x + 1) \\ & (y^5 + (c + 4)y^4 + (2c + 1)y^3 + (4c + 3)y^2 + (2c + 2)y + c + 3) \\ & - (x^5 + (c + 4)x^4 + (2c + 1)x^3 + (4c + 3)x^2 + (2c + 2)x + c + 3) \\ & ((c + 3)y^5 + (2c + 2)y^4 + (4c + 3)y^3 + (2c + 1)y^2 + (c + 4)y + 1) = 0. \end{aligned} \quad (8)$$

Utilizing the MAGMA software, equation (8) can be factorized as

$$C(x, y) := (x + \xi^{16})(x + \xi^8)(y + \xi^8)(y + \xi^{16})(x + 4y) \\ (xy + c^2x + 1)(xy + c^2y + 1). \quad (9)$$

Let us denote $A(x, y)$ and $B(x, y)$ as

$$A(x, y) = xy + c^2x + 1 \quad (10)$$

and

$$B(x, y) = xy + c^2y + 1. \quad (11)$$

Therefore,

$$C(x, y) = (x + \xi^{16})(x + \xi^8)(y + \xi^8)(y + \xi^{16})(x + 4y)A(x, y)B(x, y),$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2n}}$ satisfies the equation $x^2 + 4x + 2 = 0$. The equation $C(x, y) = 0$ holds precisely when at least one of the factors $(x + 4y)$, $(x + \xi^8)$, $(x + \xi^{16})$, $(y + \xi^8)$, $(y + \xi^{16})$, $A(x, y)$, or $B(x, y)$ vanishes. Since in each of the cases $x = -\xi^8$ or $-\xi^{16}$, we have $x^{5^n} \neq \frac{1}{x}$. By employing the MAGMA program, the resultant of $A(x, y)$ and $xyA(x^{-1}, y^{-1})$ computed over y , for the case $c = 3$, is $(x + \xi^8)(x + \xi^{16})$. This indicates that any potential common solutions to the equations $A(x, y) = 0$ and $xyA(x^{-1}, y^{-1}) = 0$ are restricted along the straight lines defined by $x = -\xi^8$ and $x = -\xi^{16}$. However, at these specific points, the condition $x^{5^n} = x \neq 1/x$ holds, resulting in a contradiction. Consequently, no elements $(x, y) \in \mu_{5^{n+1}}^2$ simultaneously satisfy the equation $A(x, y) = 0$. Likewise, we conclude a contradiction in the case of $B(x, y)$. An analogous argument holds for the case $c = 1$, in which the resultant of $A(x, y)$ and $xyB(x^{-1}, y^{-1})$ computed over y is found to be $(x + \xi^4)(x + \xi^{20})$. This confirms that the function $I_1(x)$ indeed defines a permutation over $\mu_{5^{n+1}}$.

In contrast, consider $I_1(x)$ acts as a permutation on $\mu_{5^{n+1}}$ with n being odd. Then, $3|(5^n + 1)$, which means there exists $\rho \in \mu_3 \subset \mu_{5^{n+1}}$. Note that $I_1(-\rho) = I_1(-1)$, showing that $I_1(x)$ takes the same value at two distinct elements of $\mu_{5^{n+1}}$. This violates the condition of injectivity, contradicting our assumption. Hence, the result follows.

Theorem 1: For $c \in \{1, 3\}$, the polynomial $F_1(x) = x^5(x^{5 \cdot 5^n - 5} + (c + 4)x^{4 \cdot 5^n - 4} + (2c + 1)x^{3 \cdot 5^n - 3} + (4c + 3)x^{2 \cdot 5^n - 2} + (2c + 2)x^{5^n - 1} + c + 3)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.

Proof: Since $\gcd(5, 5^n - 1) = 1$ for all n , Lemma 2 ensures that the polynomial $x^5 + (c + 4)x^4 + (2c + 1)x^3 + (4c + 3)x^2 + (2c + 2)x + c + 3$ has non-zero roots in $\mu_{5^{n+1}}$ and Lemma 1 implies that the polynomial

$$x^5(x^{5 \cdot 5^n - 5} + (c + 4)x^{4 \cdot 5^n - 4} + (2c + 1)x^{3 \cdot 5^n - 3} + (4c + 3)x^{2 \cdot 5^n - 2} + (2c + 2)x^{5^n - 1} + c + 3)$$

is a permutation of $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{(c+3)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1}{x^5 + (c+4)x^4 + (2c+1)x^3 + (4c+3)x^2 + (2c+2)x + c + 3}$$

acts as a permutation on the set $\mu_{5^{n+1}}$. Since, Lemma 7 states that $I_1(x)$ permutes if and only if n being even. Thus, $F_1(x)$ defines a PP exactly when n is even.

Theorem 2 For $c \in \{1, 3\}$, the polynomial $F_2(x) = x^5((c+3)x^{5 \cdot 5^{n-5}} + (2c+2)x^{4 \cdot 5^{n-4}} + (4c+3)x^{3 \cdot 5^{n-3}} + (2c+1)x^{2 \cdot 5^{n-2}} + (c+4)x^{5^{n-1}} + 1)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.

Proof: Since $\gcd(5, 5^n - 1) = 1$ for all even n and substituting $d = 2$ into Lemma 4 guarantees that the polynomial $(c+3)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1$ is non-zero over $\mu_{5^{n+1}}$. Consequently, the polynomial $x^5((c+3)x^{5 \cdot 5^{n-5}} + (2c+2)x^{4 \cdot 5^{n-4}} + (4c+3)x^{3 \cdot 5^{n-3}} + (2c+1)x^{2 \cdot 5^{n-2}} + (c+4)x^{5^{n-1}} + 1)$ is a PP of $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{x^5 + (c+4)x^4 + (2c+1)x^3 + (4c+3)x^2 + (2c+2)x + c+3}{(3+c)x^5 + (2c+2)x^4 + (4c+3)x^3 + (2c+1)x^2 + (c+4)x + 1} = \frac{1}{I_1(x)}$$

acts as a permutation on the set $\mu_{5^{n+1}}$. According to Lemma 7, $I_1(x)$ defines a PP over $\mathbb{F}_{q^2}$ exactly when n is even. Thus, using [38, Theorem 5.1], $\frac{1}{I_1(x)}$ is a permutation over $\mu_{5^{n+1}}$ only when n is even. Hence, $F_2(x)$ permutes only when n is even.

Lemma 8: Given that $c \in \{2, 4\}$, the fractional polynomial

$I_2(x) = \frac{(c+2)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c+1)x + 1}{x^5 + (c+1)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c+2}$ permutes $\mu_{5^{n+1}}$ if and only if n is even.

Proof: In the first case, consider n as even and

$$I_2(x) = \frac{(c+2)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c-4)x + 1}{x^5 + (c-4)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c+2},$$

with $c \in \{2, 4\}$. Further, by putting $d = 4$ in Lemma 3, gives that $G(x) = x^5 + (c-4)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c+2$ is non-zero in $\mu_{5^{n+1}}$ for n as even. Therefore, $I_2(x)$ acts as a permutation on $\mu_{5^{n+1}}$ exactly when the fractional polynomial $I_2(x)$ is one-to-one on $\mu_{5^{n+1}}$.

If $x, y \in \mu_{5^{n+1}}$, consider $I_2(x) = I_2(y)$

$$\begin{aligned} & \frac{(c+2)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c-4)x + 1}{x^5 + (c-4)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c+2} \\ &= \frac{(c+2)y^5 + (3c+2)y^4 + (4c+2)y^3 + (3c+1)y^2 + (c-4)y + 1}{y^5 + (c-4)y^4 + (3c+1)y^3 + (4c+2)y^2 + (3c+2)y + c+2}. \end{aligned} \quad (12)$$

On rearranging, we obtain

$$\begin{aligned} & ((c+2)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c-4)x + 1) \\ & (y^5 + (c-4)y^4 + (3c+1)y^3 + (4c+2)y^2 + (3c+2)y + c+2) \\ & - (x^5 + (c-4)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c+2) \\ & ((c+2)y^5 + (3c+2)y^4 + (4c+2)y^3 + (3c+1)y^2 + (c-4)y + 1) = 0. \end{aligned} \quad (13)$$

By using the MAGMA implementation, the equation (13) is factorized as

$$\begin{aligned} C(x, y) := & (x + \xi^8)(x + \xi^{16})(y + \xi^8)(y + \xi^{16})(x + 4y) \\ & (xy - c^2x + 1)(xy - c^2y + 1). \end{aligned} \quad (14)$$

Let us denote $A(x, y)$ and $B(x, y)$ as

$$A(x, y) = xy - c^2x + 1 \quad (15)$$

and

$$B(x, y) = xy - c^2y + 1. \quad (16)$$

Therefore,

$$C(x, y) = (x + \xi^8)(x + \xi^{16})(y + \xi^8)(y + \xi^{16})(x + 4y)A(x, y)B(x, y), \quad (17)$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2n}}$ satisfies the equation $x^2 + 4x + 2 = 0$. It follows that $C(x, y) = 0$ holds precisely when at least one of the expressions $(x + 4y)$, $(x + \xi^8)$, $(x + \xi^{16})$, $(y + \xi^8)$, $(y + \xi^{16})$, $A(x, y)$, or $B(x, y)$ equals zero. In each case, when $x = -\xi^8$ or $x = -\xi^{16}$, it results in $x^{5^n} \neq \frac{1}{x}$, which leads to a contradiction.

Furthermore, using the MAGMA code for $c = 2$, the resultant of $A(x, y)$ and $xyA(x^{-1}, y^{-1})$ computed over y is found to be $(x + \xi^4)(x + \xi^{20})$. It follows that the simultaneous solutions of $A(x, y) = 0$ and $xyA(x^{-1}, y^{-1}) = 0$ are confined to the lines $x = -\xi^4$ and $x = -\xi^{20}$. However, for these values, we again observe that $x^{5^n} = x \neq \frac{1}{x}$, producing a contradiction. Consequently, no pair $(x, y) \in \mu_{5^{n+1}}^2$ satisfies $A(x, y) = 0$. A similar contradiction arises for the case of $B(x, y)$. An analogous argument applies when $c = 4$, wherein the resultant of $A(x, y)$ and $xyA(x^{-1}, y^{-1})$ computed over y is $(x + \xi^8)(x + \xi^{16})$. Therefore, $I_2(x)$ defines a permutation over $\mu_{5^{n+1}}$.

Alternatively, if $I_2(x)$ is bijective map on $\mu_{5^{n+1}}$ with n being odd. In this case, since $3|(5^n + 1)$, it follows that there exist some $\rho \in \mu_3 \subset \mu_{5^{n+1}}$. Now, observe that $I_2(\rho) = I_2(1)$, indicating that $I_2(x)$ maps two distinct elements of $\mu_{5^{n+1}}$ to the same value. This contradicts the injectivity of $I_2(x)$, and thus the assumption fails. Hence, the proof is established.

Theorem 3: For $c \in \{2, 4\}$, the polynomial $F_3(x) = x^5(x^{5 \cdot 5^n - 5} + (c + 1)x^{4 \cdot 5^n - 4} + (3c + 1)x^{3 \cdot 5^n - 3} + (4c + 2)x^{2 \cdot 5^n - 2} + (3c + 2)x^{5^n - 1} + c - 3)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.

Proof: Since $\gcd(5, 5^n - 1) = 1$ for all n and Lemma 4 establishes that the polynomial $x^5 + (c + 1)x^4 + (3c + 1)x^3 + (-c + 2)x^2 + (3c + 2)x + c - 3$ is non-zero in $\mu_{5^{n+1}}$. By using Lemma 1, it follows that the polynomial $x^5(x^{5 \cdot 5^n - 5} + (c + 1)x^{4 \cdot 5^n - 4} + (3c + 1)x^{3 \cdot 5^n - 3} + (4c + 2)x^{2 \cdot 5^n - 2} + (3c + 2)x^{5^n - 1} + c - 3)$ permutes $\mathbb{F}_{5^{2n}}$ exactly when

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

defines a permutation over $\mu_{5^{n+1}}$. As Lemma 8 shows that $I_2(x)$ is a PP only when n is even. Consequently, $F_3(x)$ defines a PP over $\mathbb{F}_{5^{2n}}$ precisely when n is even.

Theorem 4: For $c \in \{2, 4\}$, the polynomial $F_4(x) = x^5((c+2)x^{5 \cdot 5^n - 5} + (3c+2)x^{4 \cdot 5^n - 4} + (4c+2)x^{3 \cdot 5^n - 3} + (3c+1)x^{2 \cdot 5^n - 2} + (c+1)x^{5^n - 1} + 1)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.

Proof: As $\gcd(5, 5^n - 1) = 1$ for all n , and choosing $d = 3$ in Lemma 3 ensures that the polynomial $(c+2)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c+1)x + 1$ is non-zero in $\mu_{5^{n+1}}$. As a result, the polynomial

$$x^5((c+2)x^{5 \cdot 5^n - 5} + (3c+2)x^{4 \cdot 5^n - 4} + (4c+2)x^{3 \cdot 5^n - 3} + (3c+1)x^{2 \cdot 5^n - 2} + (c+1)x^{5^n - 1} + 1)$$

defines a permutation over $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{x^5 + (c+1)x^4 + (3c+1)x^3 + (4c+2)x^2 + (3c+2)x + c - 3}{(c-3)x^5 + (3c+2)x^4 + (4c+2)x^3 + (3c+1)x^2 + (c+1)x + 1} = \frac{1}{I_2(x)}$$

acts as a permutation on the set $\mu_{5^{n+1}}$. As stated in Lemma 8, this occurs exactly when n is even. Therefore, using [38, Theorem 5.1], $\frac{1}{I_2(x)}$ defines a PP on $\mathbb{F}_{5^{2n}}$ precisely when n is even. Hence, $F_4(x)$ permutes precisely when n is even.

Theorem 5: For $s \in \mathbb{Z}^+$ and $c \in \{\pm 1, 2\}$, the polynomial $F_5(x) = x^s(x^{4 \cdot 5^n - 4} + cx^{3 \cdot 5^n - 3} + 3x^{2 \cdot 5^n - 2} + cx^{5^n - 1} + 1)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if $\gcd(s, 5^n - 1) = 1 = \gcd(s - 4, 5^n + 1)$.

Proof: Assuming $\gcd(s, 5^n - 1) = 1$, noting that $x^4 + cx^3 + 3x^2 + cx + 1$ has non-zero roots in $\mu_{5^{n+1}}$ by Lemma 5. Thus, Lemma 1 implies that $x^s(x^{4 \cdot 5^n - 4} + cx^{3 \cdot 5^n - 3} + 3x^{2 \cdot 5^n - 2} + cx^{5^n - 1} + 1)$ defines a permutation over $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{x^s(x^4 + cx^3 + 3x^2 + cx + 1)^{5^n - 1}}{x^4 + cx^3 + 3x^2 + cx + 1} = x^{s-4}$$

defines a permutation over $\mu_{5^{n+1}}$. This, in turn, the result holds precisely when $\gcd(s - 4, 5^n + 1) = 1$, see [38, Theorem 5.1]. Therefore, the conclusion holds.

In general, by applying Theorem 5, we can derive numerous classes of permutation pentanomials expressed as $x^s G(x^{5^n - 1})$, where $G(x) = x^4 + cx^3 + 3x^2 + cx + 1$. By choosing different values of s in such a manner that $\gcd(s, 5^n - 1) = 1$ and $\gcd(s - 4, 5^n + 1) = 1$ with n as positive integer and $c \in \{\pm 1, 2\}$, we have derived families of PP over $\mathbb{F}_{5^{2n}}$. The constraints on greatest common divisors provide different conditions on n as shown in Table 1.

Table 1
Classes of PPs defined by $x^s h(x^{5^n-1})$ for several specific values of s .

Permutation Pentanomial	Coefficient s	Conditions on n
$x^{4 \cdot 5^n+1} + cx^{3 \cdot 5^n+2} + 3x^{2 \cdot 5^n+3} + cx^{5^n+4} + x^5$	5	for all n
$x^{4 \cdot 5^n+3} + cx^{3 \cdot 5^n+4} + 3x^{2 \cdot 5^n+5} + cx^{5^n+6} + x^7$	7	$n \equiv 2 \text{ or } 4 \pmod{6}$
$x^{4 \cdot 5^n+7} + cx^{3 \cdot 5^n+8} + 3x^{2 \cdot 5^n+9} + cx^{5^n+10} + x^{11}$	11	$n \not\equiv 0 \pmod{5}$, $n \not\equiv 3 \pmod{6}$
$x^{4 \cdot 5^n+9} + cx^{3 \cdot 5^n+10} + 3x^{2 \cdot 5^n+11} + cx^{5^n+12} + x^{13}$	13	n is even, $n \not\equiv 0 \pmod{4}$
$x^{4 \cdot 5^n+11} + cx^{3 \cdot 5^n+12} + 3x^{2 \cdot 5^n+13} + cx^{5^n+14} + x^{15}$	15	n being odd
$x^{4 \cdot 5^n+13} + cx^{3 \cdot 5^n+14} + 3x^{2 \cdot 5^n+15} + cx^{5^n+16} + x^{17}$	17	$n \not\equiv 0 \pmod{16}$, $n \not\equiv 2 \pmod{4}$
$x^{4 \cdot 5^n+15} + cx^{3 \cdot 5^n+16} + 3x^{2 \cdot 5^n+17} + cx^{5^n+18} + x^{19}$	19	n being even, $n \not\equiv 0 \pmod{9}$
$x^{4 \cdot 5^n+17} + cx^{3 \cdot 5^n+18} + 3x^{2 \cdot 5^n+19} + cx^{5^n+20} + x^{21}$	21	n being odd
$x^{4 \cdot 5^n+19} + cx^{3 \cdot 5^n+20} + 3x^{2 \cdot 5^n+21} + cx^{5^n+22} + x^{23}$	23	$n \not\equiv 0 \pmod{22}$
$x^{4 \cdot 5^n+21} + cx^{3 \cdot 5^n+22} + 3x^{2 \cdot 5^n+23} + cx^{5^n+24} + x^{25}$	25	n is even
$x^{4 \cdot 5^n+23} + cx^{3 \cdot 5^n+24} + 3x^{2 \cdot 5^n+25} + cx^{5^n+26} + x^{27}$	27	$n \not\equiv 11 \pmod{22}$
$x^{4 \cdot 5^n+25} + cx^{3 \cdot 5^n+26} + 3x^{2 \cdot 5^n+27} + cx^{5^n+28} + x^{29}$	29	$n \not\equiv 0 \pmod{28}$
$x^{4 \cdot 5^n+27} + cx^{3 \cdot 5^n+28} + 3x^{2 \cdot 5^n+29} + cx^{5^n+30} + x^{31}$	31	n is even, $n \not\equiv 0 \pmod{3}$

Lemma 9: The fractional polynomial $I_3(x) = \frac{3x^5+3x^4+4x^3+x^2+x}{x^4+x^3+4x^2+3x+3}$ permutes μ_{5^n+1} if and only if n being even.

Proof: Initially, let us consider the case with n even and

$$I_3(x) = \frac{3x^5+3x^4+4x^3+x^2+x}{x^4+x^3+4x^2+3x+3}.$$

Further, Lemma 6 confirms that $G(x) = x^4 + x^3 + 4x^2 + 3x + 3$ is non-zero in μ_{5^n+1} for even values of n . Therefore, $I_3(x)$ acts as a permutation on μ_{5^n+1} exactly when $I_3(x)$ is one-to-one over μ_{5^n+1} .

If $x, y \in \mu_{5^n+1}$, consider $I_3(x) = I_3(y)$

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

that is,

$(3x^5 + 3x^4 + 4x^3 + x^2 + x)(y^4 + y^3 + 4y^2 + 3y + 3)$
 $-(x^4 + x^3 + 4x^2 + 3x + 3)(3y^5 + 3y^4 + 4y^3 + y^2 + y) = 0.$
 Employing the MAGMA code, equation (18) is factorized as

$$C(x, y) := (x + \xi^4)(x + \xi^{20})(y + \xi^4)(y + \xi^{20})(x + 4y) \\ (xy + \xi^3x + \xi^{15}y + 1)(xy + \xi^3y + \xi^{15}x + 1). \quad (19)$$

Let us denote $A(x, y)$ and $B(x, y)$ as

$$A(x, y) = xy + \xi^3x + \xi^{15}y + 1 \quad (20)$$

and

$$B(x, y) = xy + \xi^3y + \xi^{15}x + 1, \quad (21)$$

which gives

$$C(x, y) = (x + 4y)(x + \xi^4)(x + \xi^{20})(y + \xi^4)(y + \xi^{20})A(x, y)B(x, y),$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2m}}$ satisfies the equation $x^2 + 4x + 2 = 0$. We observe that $C(x, y) = 0$ holds precisely when at least one of the expressions vanishes: $(x + 4y)$, $(x + \xi^4)$, $(x + \xi^{20})$, $(y + \xi^4)$, $(y + \xi^{20})$, $A(x, y)$, or $B(x, y)$. It is important to note that when $x = -\xi^4$ or $x = -\xi^{20}$, we obtain $x^{5^n} \neq \frac{1}{x}$ does not hold. Also, we can observe that

$$xy(A(x, y))^{5^n} = xy(x^{5^n}y^{5^n} + (\xi^3)^{5^n}x^{5^n} + (\xi^{15})^{5^n}y^{5^n} + 1) \\ = xy\left(\frac{1}{xy} + (4\xi^{5^n} + 3)\frac{1}{x} + (\xi^{5^n} + 2)\frac{1}{y} + 1\right). \quad (22)$$

Since for even n , $\xi^{5^n} = \xi$, therefore

$$xy(A(x, y))^{5^n} = B(x, y).$$

Thus, $A(x, y) = 0$ holds precisely when $B(x, y) = 0$. Consider $x, y \in \mu_{5^{n+1}}$ satisfy both $A(x, y) = 0 = B(x, y)$. Hence, solving equations (20) and (21), we get

$$A(x, y) - B(x, y) = (3\xi + 1)(x + 4y) = 0.$$

As $3\xi + 1 = 0$ gives $\xi = 3 \notin \mu_{5^{n+1}}$. Thus, $3\xi + 1 = 0$ is not possible and based on the assumption $x \neq y$, therefore we arrive at a contradiction. So, the only possible reason for $C(x, y) = 0$ exactly when $x = y$. As a result, given fractional polynomial $I_3(x)$ is one-to-one over $\mu_{5^{n+1}}$.

Alternatively, consider $I_3(x)$ as a permutation over $\mu_{5^{n+1}}$ with odd n . Under this assumption, we have $3 \mid (5^n + 1)$, which implies that there exists $\rho \in \mu_3$ and hence $\rho \in \mu_{5^{n+1}}$. Noting that $I_3(\rho) = I_3(1)$, we find that $I_3(x)$ takes the same value at two distinct elements of $\mu_{5^{n+1}}$. This violates the condition of injectivity, contradicting our assumption. Therefore, the claim follows.

Theorem 6: *The polynomial $F_6(x) = x^5(x^{4 \cdot 5^n - 4} + x^{3 \cdot 5^n - 3} + 4x^{2 \cdot 5^n - 2} + 3x^{5^n - 1} + 3)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.*

Proof: Since $\gcd(5, 5^n - 1) = 1$ for every n , it follows from Lemma 6 that the polynomial

$$x^4 + x^3 + 4x^2 + 3x + 3$$

is non-zero on $\mu_{5^{n+1}}$. Hence, by Lemma 1, the polynomial

$$x^5(x^{4 \cdot 5^{n-4}} + x^{3 \cdot 5^{n-3}} + 4x^{2 \cdot 5^{n-2}} + 3x^{5^{n-1}} + 3)$$

is a permutation polynomial over $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{3x^5 + 3x^4 + 4x^3 + x^2 + x}{x^4 + x^3 + 4x^2 + 3x + 3}$$

permutes $\mu_{5^{n+1}}$. As Lemma 9 states that $I_3(x)$ permutes only when n is even. Consequently, $F_6(x)$ is a PP exactly when n is even.

Lemma 10: *The fractional polynomial $I_4(x) = \frac{3x^5 + 2x^4 + 4x^3 + 4x^2 + x}{x^4 + 4x^3 + 4x^2 + 2x + 3}$ permutes $\mu_{5^{n+1}}$ if and only if n being even.*

Proof: Firstly, consider the case where n is even and

$$I_4(x) = \frac{3x^5 + 2x^4 + 4x^3 + 4x^2 + x}{x^4 + 4x^3 + 4x^2 + 2x + 3}.$$

Further, Lemma 6 confirms that $G(x) = x^4 + 4x^3 + 4x^2 + 2x + 3$ is non-zero in μ_{q+1} for even values of m . Therefore, $I_4(x)$ acts as a permutation on $\mu_{5^{n+1}}$ exactly when the fractional polynomial $I_4(x)$ is one-to-one over $\mu_{5^{n+1}}$.

If $x, y \in \mu_{5^{n+1}}$, consider $I_4(x) = I_4(y)$

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

that is

$$(3x^5 + 2x^4 + 4x^3 + 4x^2 + x)(y^4 + 4y^3 + 4y^2 + 2y + 3) - (x^4 + 4x^3 + 4x^2 + 2x + 3)(3y^5 + 2y^4 + 4y^3 + 4y^2 + y) = 0. \quad (23)$$

Employing the MAGMA program, equation (23) is factorized as

$$C(x, y) := (x + \xi^8)(x + \xi^{16})(y + \xi^8)(y + \xi^{16})(x + 4y)(xy + \xi^3x + \xi^{15}y + 1)(xy + \xi^3y + \xi^{15}x + 1). \quad (24)$$

Let us denote $A(x, y)$ and $B(x, y)$ as

$$A(x, y) = xy + \xi^3x + \xi^{15}y + 1 \quad (25)$$

and

$$B(x, y) = xy + \xi^3y + \xi^{15}x + 1 \quad (26)$$

which gives

$$C(x, y) = (x + \xi^8)(x + \xi^{16})(x + 4y)(y + \xi^8)(y + \xi^{16})A(x, y)B(x, y),$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2n}}$ satisfies the equation $x^2 + 4x + 2 = 0$. It follows that $C(x, y) = 0$ holds true exactly when one of the following expressions vanishes: $(x + 4y)$, $(x + \xi^8)$, $(x + \xi^{16})$, $(y + \xi^8)$, $(y + \xi^{16})$, $A(x, y)$, or $B(x, y)$. In each case where $x = -\xi^8$ or $x = -\xi^{16}$, we observe that $x^{5^n} \neq \frac{1}{x}$, which implies that $-\xi^8, -\xi^{16} \notin \mu_{5^{n+1}}$. Also, we can observe that

$$\begin{aligned}
xy(A(x, y)^{5^n}) &= xy(x^{5^n}y^{5^n} + (\xi^3)^{5^n}x^{5^n} + (\xi^{15})^{5^n}y^{5^n} + 1) \\
&= xy\left(\frac{1}{xy} + (4\xi^{5^n} + 3)\frac{1}{x} + (\xi^{5^n} + 2)\frac{1}{y} + 1\right).
\end{aligned} \tag{27}$$

When n is even, we have $\xi^{5^n} = \xi$, thus

$$xy(A(x, y))^{5^n} = B(x, y).$$

Clearly, $A(x, y) = 0$ precisely when $B(x, y) = 0$. Suppose $x, y \in \mu_{5^{n+1}}$ satisfying $A(x, y) = 0 = B(x, y)$. Hence, solving equations (25) and (26), we get

$$A(x, y) - B(x, y) = (3\xi + 1)(x + 4y) = 0.$$

Since $3\xi + 1 = 0$ implies $\xi = -\frac{1}{3} = 3 \notin \mu_{5^{n+1}}$, the equation $3\xi + 1 = 0$ cannot hold. Moreover, under the assumption $x \neq y$, this leads to a contradiction. Hence, $C(x, y) = 0$ occurs precisely when $x = y$. Thus, $I_4(x)$ is one-to-one over $\mu_{5^{n+1}}$.

Now, we examine the case when $I_4(x)$ is a bijective map on $\mu_{5^{n+1}}$, assuming that n is odd. Under this condition, the divisibility $3|(5^n + 1)$ ensures that the cube root of unity ρ belongs to $\mu_{5^{n+1}}$. However, since $I_4(-\rho) = I_4(-1)$, the function assigns the same output to two distinct inputs from $\mu_{5^{n+1}}$. This contradicts the premise that $I_4(x)$ is injective, and thus such a case cannot occur. The argument is therefore complete.

Theorem 7: *The polynomial $F_7(x) = x^5(x^{4 \cdot 5^{n-4}} + 4x^{3 \cdot 5^{n-3}} + 4x^{2 \cdot 5^{n-2}} + 2x^{5^{n-1}} + 3)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.*

Proof: Notice that $\gcd(5, 5^n - 1) = 1$ holds for all values of n , and by Lemma 6, the polynomial $x^4 + 4x^3 + 4x^2 + 2x + 3$ is non-zero over $\mu_{5^{n+1}}$. Hence, by Lemma 1, the polynomial

$$x^5(x^{4 \cdot 5^{n-4}} + 4x^{3 \cdot 5^{n-3}} + 4x^{2 \cdot 5^{n-2}} + 2x^{5^{n-1}} + 3)$$

is a permutation over $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{3x^5 + 2x^4 + 4x^3 + 4x^2 + x}{x^4 + 4x^3 + 4x^2 + 2x + 3}$$

defines a permutation over $\mu_{5^{n+1}}$. As demonstrated by Lemma 10, $I_4(x)$ permutes only when n is even. Consequently, $F_7(x)$ defines a PP over $\mathbb{F}_{5^{2n}}$ precisely when n is even.

Lemma 11: *The fractional polynomial $I_5(x) = \frac{2x^5 + x^4 + x^3 + x^2 + x}{x^4 + x^3 + x^2 + x + 2}$ permutes $\mu_{5^{n+1}}$ if and only if n being even.*

Proof: Firstly, consider the case when n is even and $I_5(x) = \frac{2x^5 + x^4 + x^3 + x^2 + x}{x^4 + x^3 + x^2 + x + 2}$. Further, Lemma 6 confirms that $G(x) = x^4 + x^3 + x^2 + x + 2$ is non-zero in $\mu_{5^{n+1}}$ for even n . Therefore, $I_5(x)$ acts as a permutation on $\mu_{5^{n+1}}$ exactly when the fractional polynomial $I_5(x)$ is one-to-one in $\mu_{5^{n+1}}$.

If $x, y \in \mu_{5^{n+1}}$, consider $I_5(x) = I_5(y)$

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

that is,

$$(2x^5+x^4+x^3+x^2+x)(y^4+y^3+y^2+y+2) - (x^4+x^3+x^2+x+2)(2y^5+y^4+y^3+y^2+y) = 0. \quad (28)$$

Using MAGMA, the factorization of equation (28) can be carried out as

$$C(x, y) := (xy + \xi^{14}x + \xi^{22}y + 1)(xy + \xi^{22}x + \xi^{14}y + 1)(x + 4y) \\ (xy + \xi^{19}x + \xi^{23}y + 1)(xy + \xi^{19}y + \xi^{23}x + 1). \quad (29)$$

Let us denote $A(x, y)$, $B(x, y)$, $D(x, y)$ and $E(x, y)$ as

$$A(x, y) = xy + \xi^{14}x + \xi^{22}y + 1 \quad (30)$$

and

$$B(x, y) = xy + \xi^{14}y + \xi^{22}x + 1 \quad (31)$$

$$D(x, y) = xy + \xi^{19}y + \xi^{23}x + 1 \quad (32)$$

$$E(x, y) = xy + \xi^{23}y + \xi^{19}x + 1. \quad (33)$$

Therefore,

$$C(x, y) = (x + 4y)A(x, y)B(x, y)D(x, y)E(x, y),$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2n}}$ satisfies the equation $x^2 + 4x + 2 = 0$. The condition $C(x, y) = 0$ is satisfied exactly when one of the following factors is zero: $(x + 4y)$, $A(x, y)$, $B(x, y)$, $D(x, y)$, or $E(x, y)$. We can observe that

$$xy(A(x, y)^{5^n}) = xy(x^{5^n}y^{5^n} + (\xi^{14})^{5^n}x^{5^n} + (\xi^{22})^{5^n}y^{5^n} + 1) \\ = xy\left(\frac{1}{xy} + (4\xi^{5^n} + 2)\frac{1}{x} + (\xi^{5^n} + 1)\frac{1}{y} + 1\right). \quad (34)$$

Since for even n , $\xi^{5^n} = \xi$, then

$$xy(A(x, y))^{5^n} = B(x, y).$$

In a similar manner, one can verify that $xy(D(x, y))^{5^n} = E(x, y)$. This follows that $A(x, y) = 0$ holds true exactly when $B(x, y) = 0$. Suppose $x, y \in \mu_{5^{n+1}}$ satisfying both $A(x, y) = 0 = B(x, y)$. Hence, solving equations (30) and (31), we obtain

$$A(x, y) - B(x, y) = (3\xi + 1)(x + 4y) = 0.$$

The expression $3\xi + 1 = 0$ gives $\xi = 3$, which is not an element of $\mu_{5^{n+1}}$. Therefore, this case is invalid. Given that $x \neq y$, we reach a contradiction. Likewise, $D(x, y) = 0 = E(x, y)$ concludes a contradiction. It deduces that $C(x, y) = 0$ precisely when $x = y$. Thus, fractional polynomial $I_5(x)$ is one-to-one on $\mu_{5^{n+1}}$.

Now, we examine when $I_5(x)$ is a bijective map on $\mu_{5^{n+1}}$ with n being odd. This implies that $3 \nmid 5^n + 1$, so ρ , a cube root of unity, lies in $\mu_{5^{n+1}}$. Now, observe that $I_5(-\rho) = I_5(-1)$, meaning the function takes the same value at two distinct elements of $\mu_{5^{n+1}}$. This contradicts the injectivity of $I_5(x)$. Hence, our assumption must be false, completing the proof.

Theorem 8: *The polynomial $F_8(x) = x^5(x^{4 \cdot 5^{n-4}} + x^{3 \cdot 5^{n-3}} + x^{2 \cdot 5^{n-2}} + x^{5^{n-1}} + 2)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.*

Proof: Note that $\gcd(5, 5^n - 1) = 1$ holds for all values of n , and by Lemma 6, the polynomial $x^4 + x^3 + x^2 + x + 2$ is non-zero over $\mu_{5^{n+1}}$. Hence, by Lemma 1, the polynomial

$$x^5(x^{4 \cdot 5^{n-4}} + x^{3 \cdot 5^{n-3}} + x^{2 \cdot 5^{n-2}} + x^{5^{n-1}} + 2)$$

permutes $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{2x^5 + x^4 + x^3 + x^2 + x}{x^4 + x^3 + x^2 + x + 2}$$

acts as a permutation on $\mu_{5^{n+1}}$. Since Lemma 11 demonstrates that $I_5(x)$ permutes $\mu_{5^{n+1}}$ only when n is even. Consequently, $F_8(x)$ defines a PP over $\mathbb{F}_{5^{2n}}$ precisely when n is even.

Lemma 12: *The fractional polynomial $I_6(x) = \frac{2x^5 + 4x^4 + x^3 + 4x^2 + x}{x^4 + 4x^3 + x^2 + 4x + 2}$ permutes $\mu_{5^{n+1}}$ if and only if n being even.*

Proof: Firstly, consider n is even and $I_6(x) = \frac{2x^5 + 4x^4 + x^3 + 4x^2 + x}{x^4 + 4x^3 + x^2 + 4x + 2}$. Further, Lemma 6 confirms that $G(x) = x^4 + 4x^3 + x^2 + 4x + 2$ is non-zero in $\mu_{5^{n+1}}$ for even values of n . Therefore, $I_6(x)$ acts as a permutation on $\mu_{5^{n+1}}$ exactly when the fractional polynomial $I_6(x)$ is one-to-one in $\mu_{5^{n+1}}$.

If $x, y \in \mu_{5^{n+1}}$, consider $I_6(x) = I_6(y)$

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

that is,

$$(2x^5 + 4x^4 + x^3 + 4x^2 + x)(y^4 + 4y^3 + y^2 + 4y + 2) - (x^4 + 4x^3 + x^2 + 4x + 2)(2y^5 + 4y^4 + y^3 + 4y^2 + y) = 0. \quad (35)$$

Using MAGMA implementation, the factorization of equation (35) can be carried out as

$$C(x, y) := (x + 4y)(xy + \xi^2 x + \xi^{10} y + 1)(xy + \xi^{10} x + \xi^2 y + 1)(xy + \xi^{11} x + \xi^7 y + 1)(xy + \xi^{11} y + \xi^7 x + 1). \quad (36)$$

Let us denote $A(x, y)$, $B(x, y)$, $D(x, y)$ and $E(x, y)$ as

$$A(x, y) = xy + \xi^2 x + \xi^{10} y + 1 \quad (37)$$

and

$$B(x, y) = xy + \xi^{10} x + \xi^2 y + 1 \quad (38)$$

$$D(x, y) = xy + \xi^{11} x + \xi^7 y + 1 \quad (39)$$

$$E(x, y) = xy + \xi^{11} y + \xi^7 x + 1. \quad (40)$$

Therefore,

$$C(x, y) = (x + 4y)A(x, y)B(x, y)D(x, y)E(x, y),$$

where $\xi \in \mathbb{F}_{5^2}^* \subset \mathbb{F}_{5^{2n}}$ satisfies the equation $x^2 + 4x + 2 = 0$. It follows that $C(x, y) = 0$ precisely when one of the following expressions vanishes: $(x + 4y)$, $A(x, y)$, $B(x, y)$, $D(x, y)$, or $E(x, y)$. We observe that

$$\begin{aligned} xy(A(x, y)^{5^n}) &= xy(x^{5^n}y^{5^n} + (\xi^2)^{5^n}x^{5^n} + (\xi^{10})^{5^n}y^{5^n} + 1) \\ &= xy\left(\frac{1}{xy} + (\xi^{5^n} + 3)\frac{1}{x} + (-\xi^{5^n} - 1)\frac{1}{y} + 1\right). \end{aligned} \quad (41)$$

Since for even n , $\xi^{5^n} = \xi$, then

$$xy(A(x, y))^{5^n} = B(x, y).$$

In a similar manner, we verify that $xy(D(x, y))^{5^n} = E(x, y)$. Consequently, $A(x, y) = 0$ precisely when $B(x, y) = 0$. Assume $x, y \in \mu_{5^{n+1}}$ satisfying $A(x, y) = 0 = B(x, y)$ are satisfied, solving equations (37) and (38) leads to

$$A(x, y) - B(x, y) = (2\xi - 1)(x + 4y) = 0.$$

Since $2\xi - 1 = 0$ implies $\xi = \frac{1}{2} = 3$, and $3 \notin \mu_{5^{n+1}}$, the equation $2\xi - 1 = 0$ cannot hold. Moreover, we have assumed $x \neq y$, which leads to a contradiction. Similarly, assuming $D(x, y) = 0 = E(x, y)$ also results in a contradiction. Therefore, $C(x, y) = 0$ exactly when $x = y$. This establishes that $I_6(x)$ is one-to-one over $\mu_{5^{n+1}}$.

Alternatively, consider $I_6(x)$ is a permutation over $\mu_{5^{n+1}}$ with n being odd. Accordingly, since $3 \mid 5^n + 1$, so ρ , a cube root of unity, lies in $\mu_{5^{n+1}}$. Notice that $I_6(\rho) = I_6(1)$, indicating that two distinct elements of $\mu_{5^{n+1}}$ are mapped to the same image. This contradicts the injectivity of $I_6(x)$. Therefore, the assumption cannot hold, which completes the argument.

Theorem 9: *The polynomial $F_9(x) = x^5(x^{4 \cdot 5^n - 4} + 4x^{3 \cdot 5^n - 3} + x^{2 \cdot 5^n - 2} + 4x^{5^n - 1} + 2)$ defines a PP over $\mathbb{F}_{5^{2n}}$ if and only if n being even.*

Proof: As $\gcd(5, 5^n - 1) = 1$ holds for all values of n , and by Lemma 6, the polynomial $x^4 + 4x^3 + x^2 + 4x + 2$ is non-zero over $\mu_{5^{n+1}}$. Hence, by Lemma 1, the polynomial

$$x^5(x^{4 \cdot 5^n - 4} + 4x^{3 \cdot 5^n - 3} + x^{2 \cdot 5^n - 2} + 4x^{5^n - 1} + 2)$$

is a permutation over $\mathbb{F}_{5^{2n}}$ exactly when

$$\frac{2x^5 + 4x^4 + x^3 + 4x^2 + x}{x^4 + 4x^3 + x^2 + 4x + 2}$$

acts as a permutation on $\mu_{5^{n+1}}$. Since, Lemma 12 demonstrates $I_6(x)$ permutes only when n being even. Consequently, $F_9(x)$ defines a PP on $\mathbb{F}_{5^{2n}}$ precisely when n is even.

Conclusion

This paper introduces new classes of permutation pentanomials over the finite field $\mathbb{F}_{5^{2n}}$. By fixing specific coefficients in the polynomial $h(x)$, we constructed PPs of the form $x^r h(x^{5^n-1})$. Through this approach, we discovered more than nine distinct classes of permutation pentanomials. In Theorem 5, we further generalized the exponent r enabling the creation of additional classes by varying r . A significant avenue for future research is to explore whether these results extend to arbitrary finite fields of the form $\mathbb{F}_{q^2}$, where $q = p^n$ for a prime p .

Declarations

Ethics Approval: This research does not involve human subjects or animals.

Funding Statement: No particular grants or funds were allocated for this research.

References

- [1] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Their Appl.*, vol. 15, no. 2, pp. 195-206 (2009).
- [2] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.*, vol. 2007, no. 1, 023408 (2007), <https://doi.org/10.1155/2007/23408>.
- [3] D. Bartoli and M. Giulietti, Permutation polynomials, fractional polynomials, and algebraic curves, *Finite Fields Their Appl.*, vol. 51, pp. 1-16 (2018).
- [4] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. Math.*, vol. 11, pp. 65-120 (1896).
- [5] L. E. Dickson, History of the Theory of Numbers, vol. 3, Carnegie Institute, Washington, D.C., 1923, Dover, New York (2005).
- [6] C. Ding and T. Helleseeth, Optimal ternary cyclic codes from monomials, *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5898-5904 (2013).
- [7] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory Ser. A*, vol. 113, no. 7, pp. 1526-1535 (2006).
- [8] C. Ding, L. Qu, Q. Wang, J. Yuan, and P. Yuan, Permutation trinomials over finite fields with even characteristic, *SIAM J. Discrete Math.*, vol. 29, no. 1, pp. 79-92 (2015).

- [9] R. Gupta, Several new permutation quadrinomials over finite fields of odd characteristic, *Des. Codes Cryptogr.*, vol. 88, no. 1, pp. 223–239 (2020).
- [10] R. Gupta and R. K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.*, vol. 41, pp. 89–96 (2016).
- [11] R. Gupta and A. Rai, A note on a class of permutation trinomials, *J. Algebra Appl.*, vol. 22, no. 08, p. 2350163 (2023).
- [12] S. Gupta, M. Singh, and M. Harish, On the study of families of linearized polynomials over finite fields, *Contemp. Math.*, vol. 4, no. 3, pp. 518–529 (2023).
- [13] S. Gupta, S. Vinayak, A. Nayyar, and M. Singh, On some new classes of permutation trinomials and pentanomials over $\mathbb{F}_{3^{2m}}$, *J. Appl. Math. Comput.*, vol. 71, pp. 5259–5277 (2025), doi: 10.1007/s12190-025-02433-z.
- [14] M. Harish, S. Vinayak, and S. Gupta, Randomness of sequences of numbers using permutation polynomials over prime finite fields, *Contemp. Math.*, vol. 4, no. 3, pp. 453–466 (2023).
- [15] C. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris*, vol. 57, pp. 750–757 (1863).
- [16] X. D. Hou, Permutation polynomials over finite fields – a survey of recent advances, *Finite Fields Appl.*, vol. 32, pp. 82–119 (2015).
- [17] X. D. Hou, A survey of permutation binomials and trinomials over finite fields, *Contemp. Math.*, vol. 632, pp. 177–191 (2015).
- [18] J. Ma and G. Ge, A note on permutation polynomials over finite fields, *Finite Fields Appl.*, vol. 48, pp. 261–270 (2017).
- [19] K. Li, L. Qu, and X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Appl.*, vol. 43, pp. 69–85 (2017).
- [20] K. Li, L. Qu, and Q. Wang, New constructions of permutation polynomials of the form $x^r h(x^{q-1})$ over $\mathbb{F}_{q^2}$, *Des. Codes Cryptogr.*, vol. 86, pp. 2379–2405 (2018).
- [21] N. Li and T. Helleseht, Several classes of permutation trinomials from Niho exponents, *Cryptogr. Commun.*, vol. 9, pp. 693–705 (2017).
- [22] R. Lidl and W. B. Müller, Permutation polynomials in RSA-cryptosystems, *Advances in Cryptology: Proc. Crypto*, vol. 83, pp. 293–301, Boston, MA, USA: Springer US (1984).

- [23] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, Second Edition, (1997).
- [24] Q. Liu, G. Chen, X. Liu, and J. Zou, Several classes of permutation pentanomials with the form $x^r h(x^{pm-1})$, *Finite Fields Appl.*, vol. 92, p. 102307 (2023).
- [25] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.*, vol. 361, pp. 4169–4180 (2009).
- [26] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Boca Raton, FL, USA: Taylor & Francis (2013).
- [27] F. Özbudak and B. G. Temür, Complete characterization of some permutation polynomials of the form $x^r (1 + ax^{s_1(q-1)} + bx^{s_2(q-1)})$, *Cryptogr. Commun.*, vol. 15, no. 4, pp. 775–793 (2023).
- [28] A. Rai and R. Gupta, Further results on a class of permutation trinomials, *Cryptogr. Commun.*, vol. 15, no. 4, pp. 811–820 (2023).
- [29] M. Singh, S. Gupta, and P. L. Sharma, On permutation and complete permutation binomials and trinomials from linearized polynomials over finite fields, *J. Discrete Math. Sci. Cryptogr.*, vol. 27, pp. 1073–1085 (2024).
- [30] P. L. Sharma, Ashima, and A. K. Sharma, Recursive construction of normal polynomials over finite fields, *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 8, pp. 2645–2660 (2022), doi: 10.1080/09720529.2021.1897215.
- [31] R. Shen, X. Liu, and X. Xu, More constructions of permutation pentanomials and hexanomials over $\mathbb{F}_{p_{2m}}$, *Appl. Algebra Eng. Commun. Comput.*, pp. 1–23 (2024), doi: 10.1007/s00200-024-00673-3.
- [32] Z. Tu, X. Zeng, and L. Hu, A class of binomial permutation polynomials (2013), <https://arxiv.org/pdf/1310.0337v1.pdf>.
- [33] Z. Tu, X. Zeng, C. Li, and T. Helleseeth, A class of new permutation trinomials, *Finite Fields Appl.*, vol. 50, pp. 178–195 (2018).
- [34] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, sequences, subsequences, and consequences, (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), in *Lect. Notes Comput. Sci.*, vol. 4893, pp. 119–128, Springer, Berlin (2007).
- [35] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure, *Monatsh. Math.*, vol. 112, pp. 149–163 (1991).

- [36] G. Xu, X. Cao, and J. Ping, Some permutation pentanomials over finite fields with even characteristic, *Finite Fields Appl.*, vol. 49, pp. 212–226 (2018).
- [37] A. A. Yadav, I. Gupta, H. Singh, and A. Yadav, Several new classes of permutation polynomials over finite fields $\mathbb{F}_{52m}$, *Appl. Algebra Eng. Commun. Comput.* (2025), <https://doi.org/10.1007/s00200-025-00696-4>.
- [38] M. E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from bijective R edei functions on subgroups of the multiplicative group of $\mathbb{F}_q$ (2013), <https://arxiv.org/abs/1310.0776>.
- [39] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^{h(x^{\frac{q-1}{d}})}$, *Proc. Amer. Math. Soc.*, vol. 137, no. 7, pp. 2209–2216 (2009).
- [40] T. Zhang, L. Zheng, and X. Hao, More classes of permutation hexanomials and pentanomials over finite fields with even characteristic, *Finite Fields Appl.*, vol. 91, p. 102250 (2023).
- [41] T. Zhang, L. Zheng, and H. Zhao, More classes of permutation pentanomials over finite fields with characteristic two, *Finite Fields Appl.*, vol. 98, p. 102468 (2024).
- [42] Z. Zha, L. Hu, and S. Fan, Further results on permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.*, vol. 45, pp. 43–52 (2017).

Received August, 2025