AIMS Mathematics, 8(12): 29182–29220.
DOI: 10.3934/math.20231495
Received: 03 July 2023
Revised: 15 September 2023
Accepted: 25 September 2023
Published: 26 October 2023

http://www.aimspress.com/journal/Math

Research article

A recent survey of permutation trinomials over finite fields

Varsha Jarali[1], **Prasanna Poojary**[2] **and G. R. Vadiraja Bhatta**[1,*]

[1] Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India; varshapjarali@gmail.com; vadiraja.bhatta@manipal.edu

[2] Department of Mathematics, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India; poojary.prasanna@manipal.edu; poojaryprasanna34@gmail.com

* **Correspondence:** Email: grvbhatta@gmail.com.

Abstract: Constructing permutation polynomials is a hot topic in the area of finite fields, and permutation polynomials have many applications in different areas. Recently, several classes of permutation trinomials were constructed. In 2015, Hou surveyed the achievements of permutation polynomials and novel methods. But, very few were known at that time. Recently, many permutation binomials and trinomials have been constructed. Here we survey the significant contribution made to the construction of permutation trinomials over finite fields in recent years. Emphasis is placed on significant results and novel methods. The covered material is split into three aspects: the existence of permutation trinomials of the respective forms $x^r h(x^s)$, $\lambda_1 x^a + \lambda_2 x^b + \lambda_3 x^c$ and $x + x^{s(q^m-1)+1} + x^{t(q^m-1)+1}$, with Niho-type exponents s, t.

Keywords: permutation polynomial; trinomial permutations; Niho-type exponents; binomial permutations
Mathematics Subject Classification: 05A05, 11T06

1. Introduction

Let F_q be the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer. A polynomial $f(x) \in F_q[x]$ is called a permutation polynomial over F_q if it is a bijection of F_q into itself. The study of permutation polynomials on finite fields began by Hermite [27], Dickson [15] and Carlitz [12] has since been carried out by many other researchers [1, 3–5, 8, 9, 35, 87]. The study of permutation polynomials over finite fields has been attracting researcher interest for many years due to their wide applications in cryptography [36, 59, 61, 62], coding theory [17, 18] and combinatorial designs [16]. In many cases, compositional inverses of permutation polynomials are necessary. In block ciphers, substitution boxes, which form the confusion layer during encryption, are often designed

by using permutation polynomials and their compositional inverses. Very important progress has been achieved in the area of the construction of permutation polynomials and their compositional inverses (see [55, 77–79]).

Permutation polynomials with fewer terms are particularly desirable due to their good algebraic structure over finite fields. The three most basic types of polynomials are monomials, binomials and trinomials. Permutation polynomials of the monomial or binomial type have been widely investigated in recent decades. However, much less is known about polynomials with more than two terms, such as trinomials and quadrinomials. The monomial x^r is a permutation polynomial over F_q if and only if $\gcd(r, q-1) = 1$. It is challenging to ascertain the conditions on a, b, n, m and q under which the binomials $ax^n + bx^m$ are permutations on F_q.

In 2015, Hou [32] briefly surveyed the known classes of permutation binomials and trinomials, but very few classes were known at that time. The purpose of the present paper is to review some of the recent contributions to the area while providing more details and background. Our primary focus is on the results of permutation trinomials that have appeared in the last decade. In addition, we will present the reader with a selection process for recently developed approaches and methods.

An old and yet very useful result on the theory of permutation polynomials is the following theorem, proved by Hermite [27] for prime fields, and Dickson [15] in the general case.

Lemma 1.1. *(Hermite-Dickson criterion) [27] Let F_q be a finite field of characteristic p. Then, $f(x) \in F_q[x]$ is a permutation polynomial of F_q if and only if the following two conditions hold:*

(1) $f(x)$ has exactly one root in F_q;
(2) For each integer t with $1 \le t \le q-2$ and $t \not\equiv 0 \pmod p$, the reduction of $f(x^t) \pmod{x^q - x}$ has a degree $\le q-2$.

The following Lemma 1.2 shows that polynomials of the form $x^r h(x^{(q-1)/d})$ over F_q have a close connection with the d-order subgroup μ_d of F_q^*.

Indeed, there have been many construction results that were obtained by using the method of constructing permutation polynomials over μ_d to obtain permutation polynomials over the original finite field. It was first stated by Wan and Lidl [69], and later modified by Wang [70] and Zieve [87].

Lemma 1.2. *[69, 70, 87] Let $d, r > 0$ with $d|(q-1)$ and $h(x) \in F_q[x]$. Then, $f(x) = x^r h(x^{(q-1)/d})$ permutes F_q if and only if*

(1) $\gcd(r, (q-1)/d) = 1$,
(2) $x^r h(x)^{(q-1)/d}$ permutes μ_d.

Theorem 1.1. *[47] Let p be a prime and $n, r_1, r_2, \cdots, r_t$ be non-negative integers such that*

$$n = d_0 + d_1 p + d_2 p^2 + \cdots + d_s p^s \ \ (0 \le d_i \le p-1), \ \ \forall 0 \le i \le s,$$
$$r_j = d_{j0} + d_{j1} p + d_{j2} p^2 + \cdots + d_{js} p^s \ \ (0 \le d_{ji} \le p-1), \ \ \forall\ 0 \le j \le t, \forall\ 0 \le i \le s.$$

Then,

$$\binom{n}{r_1, r_2, \ldots, r_t} = \binom{d_0}{d_{10}, d_{20}, \ldots, d_{t0}} \cdots \binom{d_s}{d_{1s}, d_{2s}, \ldots, d_{ts}} \pmod p.$$

Further, it follows that $\binom{n}{r_1, r_2, \ldots, r_t} \not\equiv 0 \pmod p$ if and only if $\sum_{i=1}^{t} d_{ij} = d_j$, $\forall\ 0 \le j \le s$.

Definition 1.1. *[74] Two permutation polynomials $f(x)$ and $g(x)$ in $F_q[x]$ are called the quasi-multiplicative equivalence if there exists an integer $1 \leq d < q-1$ such that $\gcd(d, q-1) = 1$ and $f(x) = ag(cx^d)$, where $a, b \in F_q^*$.*

Definition 1.2. *[47] A polynomial $f(x) \in F_q[x]$ is said to be a complete permutation polynomial over F_q if both $f(x)$ and $f(x) + x$ are permutations of F_q.*

To check the permutation property of any given polynomial over a finite field, we can use Akbary, Ghioca, Wang(AGW) criterion. We make use of the subfield of the finite field and a known polynomial that permutes the subfield. For instance, a permutation polynomial over F_q can be used to check the constructed polynomial over F_{q^n}, regardless of whether it is a permutation polynomial or not.

Lemma 1.3. *[1] (AGW criterion) Let K, L and $\bar{L}$ be finite sets with $|L| = |\bar{L}|$, and let*

$$g : K \to K, \quad \bar{g} : L \to \bar{L}, \quad \omega : K \to L$$

and $\bar{\omega}$: $K \to \bar{L}$ be maps as shown in the Figure 1, such that $\bar{\omega} \circ g = \bar{g} \circ \omega$. If both ω and $\bar{\omega}$ are surjective, then the following statements are equivalent:

(1) g is a bijection from K to K;
(2) $\bar{g}$ is a bijection from L to $\bar{L}$ and g is injective on $\omega^{-1}(l)$ for each $l \in L$.

So, if $\bar{g}$ is a bijection on L, we can make conclusions about the permutation of g over K.

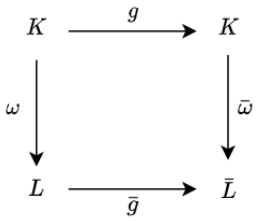

Figure 1. Commutative diagram.

There are several approaches that can be employed to decide whether $f(x)$ is a permutation polynomial. When investigating the permutational properties of a polynomial, a well-established connection with algebraic curves is provided by the following observation. For a given polynomial $f(x) \in F_q[x]$, let us consider the curve C_f with the affine equation

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

Deciding whether a polynomial is a permutation polynomial over any field is based on the investigation of the set of F_{q^2}-rational point of C_f. The Hermite-Dickson criteria [27] constitute another well-known tool for use in the construction of any type of permutation polynomial, and when using these criteria, one may use the Lucas sequence [47] to compute binomial coefficients in the polynomial expressions. Here, the main aim is to compute the sum $\sum_{x \in F_q} f(x)^s$ for the integer $0 \leq s \leq q-1$. However, computing the sum is a little lengthy and the toughest one. To overcome this difficulty, recent discoveries have been made, including Lemma 1.2. The main construction method involves the use of the multivariate

method [21] and discussions of the number of solutions of special equations $f(x) = d$. Recently, one more method has come into existence for the computation of the permutation binomials and trinomials, i.e., the computation of the fractional polynomials [39]. The AGW criterion is another significant technique to determine a polynomial's permutation property (see [1]).

In Section 2, we list all of the existing permutation trinomials, and those of the forms $x^r h(x^s)$, $\lambda_1 x^a + \lambda_2 x^b + \lambda_3 x^c$ and $x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$ with Niho-type exponents s, t are discussed in the Sections 3–5, respectively. In addition, in Sections 3–5, we provide a discussion about current conjectures and open problems that have been mentioned in the literature.

2. Permutation trinomials

There are compelling findings about both the existence and non-existence of permutation binomials, but there is not a comparable instance of non-existence in the case of permutation trinomials. Nonetheless, there have been numerous permutation trinomial discoveries from a variety of backgrounds. The Dickson polynomial of order five, i.e., $D_5(x, a) = x^5 + ax^3 - a^2x$, is a permutation trinomial over F_{3^m} with a wide range of uses; it also produces a family of ideal nonlinear functions for cryptography, as well as linear codes for data transmission and storage. Similarly, the Dickson polynomial $D_7(x, a) = x^7 + x^5 + x$ of degree 7 with $m \not\equiv 0 \pmod 3$ comprises permutation trinomials over F_{3^m}. In 1997, Lee and Park [38] investigated permutation trinomials; they assumed that $q \equiv 1 \pmod 3$ and there is a fixed primitive root g of F_q for $\alpha \in F_q^*$, and that $\log_g \alpha$ is the residue class $k \pmod{q-1}$ such that $\alpha = g^k$; here, $s = \frac{q-1}{3}$ and $\omega = g^s$, $h(x) = x^r f(x^s)$, where $f(x) = ax^2 + bx + c \in F_q[x]$. Similar to this, in [13, 21] both authors used two distinct concepts to investigate the permutation property of the trinomial

$$f(x) = x^{2^{(m+1)/2}} + x^{2^{(m+1)/2}+2} + x^{3\cdot 2^{(m+1)/2}+4}$$

over F_{2^m} when m is odd. Lee and Park [38] established the following theorem, which is the primary method of creating numerous permutation polynomials of the form $h(x) = x^r f(x)$.

Theorem 2.1. *[38] Let $h(x) = x^r f(x^s) \in F_q[x]$, where $f(x) = ax^2 + bx + c \in F_q[x]$ and $s = \frac{q-1}{d}$ with $d \mid (q-1)$. Then, $h(x)$ is a permutation polynomial over F_q if and only if the following conditions are satisfied:*

(1) $(r, s) = 1$,
(2) for $0 \le i \le 3$, $f(\omega^i) \neq 0$,
(3) $\log_g \frac{f(1)}{f(\omega)} \equiv \log_g \frac{f(\omega)}{f(\omega^2)} \not\equiv r \pmod 3$.

3. Polynomials of the form $x^r h(x^s)$

The permutation behavior of polynomials of the form $f(x) = x^r h(x^{(q-1)/d})$ over a finite field F_q has drawn the interest of many scholars since the majority of permutation polynomials can be expressed as $x^r h(x^s)$ over a finite field F_q. Over the past few years, a large number of permutation polynomials of this form have been discovered. Wan and Lidl [69] first investigated the permutation behavior of the form $f(x) = x^r h(x^{(q-1)/d})$, where $d|q-1$ and $1 < r < \frac{q-1}{d}$ over F_q. In this section, we list all of the permutation polynomials of the form $x^r h(x^s)$. In his contribution to the field of permutation,

Zieve [87] introduced a common method to find permutations of the type $f(x) = x^r h(x^{(q-1)/d})$ over F_q by exploiting the behavior of the permutations $g(x) = x^r h(x)^{q-1}$ in μ_{q+1}; as an added feature, and from this fact, Zieve [88] constructed several classes of permutation trinomials over F_{q^2}.

The approach involves rational functions over F_{q^2} that map μ_{q+1} to either μ_{q+1} or $F_q \cup \{\infty\}$. He first constructed a general polynomial of the form

$$f(x) = x^{n+k(q+1)} \cdot ((\gamma x^{q-1} - \beta)^n - \gamma(x^{q-1} - \gamma^q \beta)^n)$$

for $n > 0$, $k \geq 0$, $\beta, \gamma \in F_{q^2}$ with $\beta^{q+1} = 1$ and $\gamma^{(q+1)} \neq 1$, which permutes F_{q^2} if and only if $\gcd(n + 2k, q - 1) = 1$ and $\gcd(n, q + 1) = 1$. He also investigated polynomials of the form

$$f(x) = x^{n+k(q+1)} \cdot ((\delta x^{q-1} - \beta\delta^q)^n - \delta(x^{q-1} - \beta)^n)$$

with $\delta \in F_{q^2}$ but $\delta \notin F_q$; it is a permutation polynomial over F_{q^2} if and only if $\gcd(n(n+2k), q-1) = 1$. As a consequence of the above fact, he mentioned some trinomials in the following corollaries for $n = 3$ and certain values of β, δ, γ.

Corollary 3.1. *[88] Let q be a prime power and $k \geq 0$. The polynomial*

$$f(x) = x^{k(q+1)+3} + 3x^{k(q+1)+q+2} - x^{k(q+1)+3q}$$

permutes F_{q^2} if and only if $\gcd(2k + 3, q - 1) = 1$ *and* $3 \nmid q$.

For the values $k = q - 3$, $k = 1$ and $k = 0$, the above corollary reduces to the following corollary.

Corollary 3.2. *[88] Let q be a prime power with $3 \nmid q$. Then,*

(1) $x^q + 3x^{2q-1} - x^{q^2-q+1}$ *permutes* F_{q^2}.
(2) $x^{q+4} + 3x^{2q+3} - x^{4q+1}$ *permutes* F_{q^2} *if and only if* $q \not\equiv 1 \pmod 5$.
(3) $x^3 + 3x^{q+2} - x^{3q}$ *permutes* F_{q^2} *if and only if* $q \equiv 2 \pmod 3$.

Regarding the case of $q = 2^{2m+1}$, the first two parts of the above corollary were conjectured by Tu et al. [64]. Later, Zieve [88] provided the alternative proof for [28, Theorem 1] in [88, Theorem 5.1]. Using this, he further determined the permutation binomial for $h(x) = x^d + \beta^{-1}$ in the following corollary. The proof encompasses demonstrating that $h(x)$ has roots in μ_{q+1} if and only if $-\beta^{-1}$ is in $(\mu_{q+1})^d$, which equals $\mu_{(q+1)}/\gcd(q + 1, d)$.

Corollary 3.3. *[88] Let q be a prime power, let r and d be positive integers and let β be the $(q + 1)^{th}$ root of unity in F_{q^2}. Then, $x^{r+d(q-1)} + \beta^{-1}x^r$ permutes F_{q^2} if and only if all of the following conditions hold:*

(1) $\gcd(r, q - 1) = 1$,
(2) $\gcd(r - d, q + 1) = 1$,
(3) $(-\beta)^{(q+1)/\gcd(q+1,d)} \neq 1$.

There are numerous classes of permutation trinomials over finite fields in the literature, some of which have profound connections to other areas. Recently, a complete determination of the permutation trinomials of the type

$$f(x) = ax + bx^q + x^{2q-1} \in F_q[x]$$

over F_{q^2} was demonstrated in [29–31]. Trinomials of the form

$$f(x) = ax + bx^q + x^{2q-1} \in F_q[x]$$

were taken into consideration by Hou [29]. The main theme is dependent on the fact that

$$f \equiv (a + b + 1)x \pmod{x^q - x},$$

so $f(x)$ is a permutation polynomial of F_q if and only if $(a + b + 1) \neq 0$.

Motivated by the work of Fernando et al. [22] i.e., a study of permutation polynomial over finite fields defined by functional equations, which also detailed the discovery of a class of permutation binomials in [28] over F_{q^2}, in 2013, Hou [29] determined a class of permutation trinomials of the form

$$f(x) = -x + bx^q + x^{2q-1} \in F_q[x]$$

over F_{q^2} when $q > 2$. The following theorem is similar to the theorems mentioned in [28], but the method presented is different from that of [28].

Theorem 3.1. *[29] Let $q > 2$ be a prime power and $f(x) = -x + bx^q + x^{2q-1} \in F_q[x]$, where $b \in F_q^*$. Then, $f(x)$ is a permutation polynomial of F_{q^2} if and only if one of the following conditions applies:*

(1) q is even and $Tr_{q/2}\left(\frac{1}{b}\right) = 0$,
(2) $q \equiv 1 \pmod 8$ and $b^2 = -2$.

Regarding sufficiency, the author applied the existence of the solution $x \in F_{q^2}$ of the equation $f(x) = y$ for every $y \in F_{q^2}$, and, regarding the necessity

$$\sum_{x \in F_{q^2}} f(x)^s = 0$$

for $1 \leq s \leq q - 2$. The sum can be expressed as a double sum in terms of the binomial coefficients; it can be solved for $s = (q - 1)q$ and $s = 1 + (q - 2)q$. When $s = (q - 1)q$, the sum

$$\sum_{x \in F_{q^2}} f(x)^s = 0$$

gives $1 + 4b^{-2}$ as a square in F_q^*, and when $s = 1 + (q - 2)q$, the simplified sum implies that $b^2 = -2$.

Hou [30] used another approach that involves the use of $Tr(x)$ and $N(x)$. The idea behind this approach is that the polynomial $f(x) \in F_q[x]$ permutes F_{q^2} if and only if $f(x) = c$ has a unique solution in F_{q^2} for any $c \in F_{q^2}$. This can be achieved by proving that $f(F_{q^2} \backslash F_q) \subseteq F_{q^2} \backslash F_q$, followed by $c \in F_{q^2} \backslash F_q$. Then, it is sufficient to prove that $(Tr(x), N(x))$ is uniquely determined by c, since $(Tr(x), N(x))$ can be uniquely determined by the set $\{x, x^q\}$ and $f(x) \neq f(x^q) = f(x)^q$. Here, Hou [30] considered two cases on q and stated the following theorem.

Theorem 3.2. *[30] Let $f(x) = ax + bx^q + x^{2q-1} \in F_{q^2}[x]$. Then, $f(x)$ is a permutation polynomial of F_{q^2} if and only if one of the following conditions is satisfied when q is odd:*

(1) $a(a - 1)$ is a square in F_q^*, and $b^2 = a^2 + 3a$,

(2) $a = 1$ *and* $b^2 - 4$ *is a square in* F_q^*,
(3) $a = 3$, $b = 0$ *and* $q \equiv -1 \pmod 6$,
(4) $a = b = 0$ *and* $q \equiv 1, 3 \pmod 6$.

Alternatively, it is a permutation polynomial if and only if either condition is satisfied when q is even and $q > 2$*:*

(1) $a \neq 1$, $Tr_{q/2}\left(\frac{1}{a+1}\right) = 0$ *and* $b^2 = a^2 + a$,
(2) $a = 1$, $b \neq 0$ *and* $Tr_{q/2}\left(\frac{1}{b}\right) = 0$.

After the computation of permutation trinomials [30] of the form $f(x) = ax + bx^q + x^{2q-1} \in F_q[x]$ for all primes with $q > 2$, Hou [31] came up with certain new conditions to determine general permutation trinomials of the form $ax + bx^q + x^{2q-1}$ over F_{q^2}. The results cover two cases on q, odd and even, and the methodology is based on the method described in [30].

Theorem 3.3. *[31] Let* $f(x) = ax + bx^q + x^{2q-1} \in F_{q^2}[x]$ *and q be a prime power. Then,* $f(x)$ *is a permutation polynomial of* F_{q^2} *if and only if one of the following conditions is satisfied:*

(1) When q is odd:

(a) $a = b = 0$ *and* $q \equiv 1, 3 \pmod 6$,
(b) $(-a)^{(q+1)/2} = -1$ *or 3 and* $b = 0$,
(c) $ab \neq 0$, $a = b^{1-q}$ *and* $1 - \frac{4a}{b^2}$ *is a square of* F_q^*,
(d) $ab(a - b^{1-q}) \neq 0$, $1 - \frac{4a}{b^2}$ *is a square of* F_q^* *and* $b^2 - a^2b^{q-1} - 3a = 0$.

(2) When q is even:

(a) $a = b = 0$ *and* $q = 2^{2k}$,
(b) $ab \neq 0$, $a = b^{1-q}$ *and* $Tr_{q/2}(b^{-1-q}) = 0$,
(c) $ab(a - b^{1-q}) \neq 0$, $\frac{a}{b^2} \in F_q$, $Tr_{q/2}\left(\frac{a}{b^2}\right) = 0$ *and* $b^2 + a^2b^{q-1} + a = 0$.

Remark 3.1. *In [30, 31], Hou considered the general trinomial*

$$f(x) = ax + bx^q + x^{2q-1}$$

over F_{q^2}. *The construction discussed in [31] included more general conditions on coefficients, including the conditions mentioned in [30].*

Using the criterion proposed by Akbary et al. [1], Tu et al. [65] determined the permutation trinomials over a finite field of even characteristics. They investigated whether, for a positive integer m and $v \in F_{2^m}^*$, the trinomial

$$f(x) = x^{2^{2m}+1} + x^{2^m+1} + vx$$

is a permutation polynomial over $F_{2^{3m}}$. Later, Wu and Lin [73] noticed that

$$f(x) = x^{2^{2m}+1} + x^{2^m+1} + vx$$

can be written as

$$f(x) = x(Tr_m^{3m}(x) + x) + vx;$$

using this, they derived complete permutation polynomials of the form

$$f(x) = x(Tr_m^{nm}(x) + x) + vx$$

over $F_{2^{nm}}$ for any $v \in F_{2^m} \backslash \{0, 1\}$.

By combining different techniques with the multivariate method proposed by Dobbertin [21], Ding et al. [19] constructed different types of permutation polynomials over F_{2^m} with non-zero trivial coefficients. Two classes of permutation polynomials have been constructed under the condition that m is odd. Both classes of trinomials are described in the following theorem.

Theorem 3.4. *[19] For any odd integer $m > 1$, the following trinomials are permutation polynomials over F_{2^m}:*

(1) $f(x) = x + x^{2^{(m+1)/2}-1} + x^{2^m-2^{(m+1)/2}+1}$,
(2) $f(x) = x + x^3 + x^{2^m-2^{(m+3)/2}+2}$.

And, using the fact that, for a positive integer m, the equation $x^2 + ux + v = 0$, where $u, v \in F_{2^m}$ and $u \neq 0$ has roots in F_{2^m} if and only if $Tr_{v/u^2} = 0$, they determined that the trinomial

$$f(x) = x + x^{2^{(m+2)/2}-1} + x^{2^m-2^{m/2}+1}$$

is a permutation polynomial over F_{2^m} for any even $m \geq 2$. They observed that one of these above classes works for any finite field F_{q^m} such that $q \not\equiv 0 \pmod 3$. Using the Dobbertin [21] multivariate methods, they obtained the general class of permutation trinomials listed below.

Theorem 3.5. *[19] Let k be a positive integer, q be a prime power with $q \not\equiv 0 \pmod 3$ and m be an even positive integer. Then,*

$$f(x) = x + x^{kq^{m/2}-(k-1)} + x^{(k+1)-kq^{m/2}}$$

is a permutation polynomial of F_{q^m} if and only if one of the following three conditions holds:

(1) $m \equiv 0 \pmod 4$,
(2) $q \equiv 1 \pmod 4$,
(3) $m \equiv 2 \pmod 4$, $q \equiv 2 \pmod 3$ *and* $exp_3(k) \geq exp_3(q^{m/2} + 1)$, *where exp_i denotes the exponent of three in the canonical factorization of i.*

Normally, it is hard to determine an explicit expression of the compositional inverse of a permutation polynomial. However, they obtained the compositional inverse of the permutation trinomial by substituting $k = 2$ and $q = 2$ in the above theorem. Similarly, for $q = 2$ and $k = 1$.

Motivated by the work of Ding et al. [19], Li et al. [40] constructed four classes of permutation trinomials over F_{2^m}. In the following theorems, they considered two classes of trinomials with non-zero trivial coefficients.

Theorem 3.6. *[40] Let $q = 2^{2k}$ and k be a positive integer. Then, $f(x) = x + x^{2^k} + x^{2^{2k-1}-2^{k-1}+1}$ is a permutation trinomial over F_q if and only if $k \not\equiv 0 \pmod 3$.*

They only mentioned a sufficient condition to be a permutation trinomial in the preceding Theorem 3.6. Later, Gupta and Sharma [26] observed that, as a consequence of Theorem 3.10, case 1 the above-mentioned Theorem 3.6 reduces to

$$f(x) = x + x^{2^k} + x^{2^{2k-1}-2^{k-1}+1},$$

which is a permutation trinomial over $F_{2^{2k}}$ if and only if $\gcd(m, 3) = 1$.

Theorem 3.7. *[40] Let $q = 2^{2k}$ and $k > 0$ be an odd integer. Then, $f(x) = x + x^{2^k+2} + x^{2^{2k-1}+2^{k-1}+1}$ is a permutation trinomial over F_q.*

Nevertheless, Gupta and Sharma [26] enhanced Theorem 3.7 by asserting that

$$f(x) = x + x^{2^k+2} + x^{2^{2k-1}+2^{k-1}+1}$$

is a permutation trinomial over F_q if and only if k is odd.

By constructing the fractional polynomial $g(x)$, Li et al. [39] observed that Theorem 3.7 can be improved for $q = 2^k$ and $\gcd(3, k) = 1$; then,

$$f(x)^2 = x^2(1 + x^{2q-2} + x^{1-q})$$

for $r = 2$ and $h(x) = 1 + x^2 + x^{-1}$; the fractional polynomial becomes

$$g(x) = \frac{x^4 + x^3 + x}{x^3 + x + 1},$$

which permutes μ_{q+1} when $k \not\equiv 0 \pmod 3$. In the next two theorems, they introduced two new classes of permutation trinomials of the form $f(x) = x + ax^\alpha + bx^\beta$ over F_q, where $a, b \in F_q^*$.

Theorem 3.8. *[40] Let $q = 2^{2k}$ and $k > 0$ be an integer:*

$$f(x) = x + ax^{2^{k+1}-1} + a^{2^{k-1}} x^{2^{2k}-2^k+1},$$

where $a \in F_q$ and the order of a is $2^k + 1$. Then, $f(x)$ is a permutation trinomial over F_q.

Theorem 3.9. *[40] Let*

$$q = 2^{2k+1}, \quad f(x) = x + ax^3 + a^{2^{2k+1}-2^{k+1}} x^{2^{2k+1}-2^{k+2}+2},$$

where $a \in F_q$. Then, $f(x)$ is a permutation trinomial over F_q.

Later, Gupta and Sharma [26] presented four new classes of permutation trinomials of the form $x^r h(x^{2^m-1})$ over $F_{2^{2m}}$. Among those four classes of permutation trinomials, two classes give necessity conditions for Theorem 3.6 and Theorem 3.7.

Theorem 3.10. *[26]*

(1) The polynomial $f(x) = x^4 + x^{2^m+3} + x^{3\cdot 2^m+1} \in F_{2^{2m}}[x]$ is a permutation polynomial over $F_{2^{2m}}$ if and only if $\gcd(m, 3) = 1$.

(2) The polynomial $f(x) = x^2 + x^{2\cdot 2^m} + x^{3\cdot 2^m-1} \in F_{2^{2m}}[x]$ is a permutation polynomial over $F_{2^{2m}}$ if and only if $\gcd(m, 3) = 1$.

(3) The polynomial $f(x) = x^5 + x^{2^m+4} + x^{4\cdot 2^m+1} \in F_{2^{2m}}[x]$ is a permutation polynomial over $F_{2^{2m}}$ if and only if m is odd.

(4) The polynomial $f(x) = x^3 + x^{3\cdot 2^m} + x^{2^{m+2}-1} \in F_{2^{2m}}[x]$ is a permutation polynomial over $F_{2^{2m}}$ if and only if m is odd.

In addition to the above four classes of permutation trinomials, they also stated the following two conjectures on permutation trinomials.

Conjecture 3.1. *[26] The polynomial*

$$f(x) = x^5 + x^{3\cdot 2^m+2} + x^{4\cdot 2^m+1} \in F_{2^{2m}}$$

is a permutation trinomial over $F_{2^{2m}}$ if and only if $m \equiv 2 \pmod 4$.

Conjecture 3.2. *[26] The polynomial*

$$f(x) = x^5 + x^{2^m+4} + x^{5\cdot 2^m} \in F_{2^{2m}}$$

is a permutation trinomial over $F_{2^{2m}}$ if and only if $m \equiv 2 \pmod 4$.

Wu et al. [74] observed that the above Conjecture 3.2 can be written as

$$f(x) = x^{5+k(q+1)}(1 + x^{2^m-1} + x^{5\cdot(2^m-1)}),$$

which permutes $F_{2^{2m}}$ if and only if $\gcd(5 + 2k, 2^m - 1) = 1$ and $2/m$ for $m > 0, k > 0$. Using this, the authors determined some of the similar permutation trinomials. Later, Zha et al. [82] also proved the above two conjectures. Based on the work done by Gupta and Sharma [26], Zha et al. [82] investigated permutation trinomials of the form $x^r h(x^{2^m-1})$ over $F_{2^{2m}}$ by applying a bijection over the unit circle of $F_{2^{2m}}$ with order $2^m + 1$. And, from Conjecture 3.1, they derived new permutation trinomials.

Theorem 3.11. *[82] The trinomial*

$$f(x) = x^{2^m+4} + x^{2^{m+1}+3} + x^{5\cdot 2^m} \in F_{2^{2m}}$$

is a permutation trinomial over $F_{2^{2m}}$ if and only if $m \equiv 2 \pmod 4$.

Subsequently, they demonstrated that Conjecture 3.2 was correct, and they obtained the following classes of permutation trinomials from Conjecture 3.2.

Theorem 3.12. *[82]*

(1) $x^3 + x^{2^{m+1}+1} + x^{3\cdot 2^m} \in F_{2^{2m}}$ permutes $F_{2^{2m}}$ if and only if m is odd.
(2) $x^3 + x^{2^m+2} + x^{3\cdot 2^m} \in F_{2^{2m}}$ permutes $F_{2^{2m}}$ if and only if m is odd.
(3) $x^5 + x^{4\cdot 2^m+1} + x^{5\cdot 2^m} \in F_{2^{2m}}$ permutes $F_{2^{2m}}$ if and only if $m \equiv 2 \pmod 4$.
(4) The mapping $g_5(x) = x^5(1 + x + x^5)^{2^m-1}$ permutes μ_{2^m+1} if and only if m is even.

They established a connection between two families of permutation polynomials over $F_{2^{2m}}$ in the following theorem.

Theorem 3.13. *[82] Let r, l be integers and m be even with $\gcd(r, 2^m - 1) = 1$. Assume the following:*

$$h(x) \in F_{2^{2m}}[x] \text{ and } H(x) = (1 + x + x^2)^l h(x).$$

The polynomial

$$F(x) = x^{r+2l} H(x^{2^m-1})$$

permutes $F_{2^{2m}}$ if and only if $\gcd(r + 2l, 2^m - 1) = 1$ and the polynomial $f(x) = x^r h(x^{2^m-1})$ permutes $F_{2^{2m}}$.

Fernando [23] extracted permutation trinomials from reversed Dickson polynomials of the $(k + 1)^{th}$ kind when $n = p^l + 2$ and $p > 3$, where $l \in N$.

Theorem 3.14. *[23] Let $p > 3$ be an odd prime and $q = p^e$, where e is a non-negative integer. Let k be an integer such that $k \neq 0, 2, 4$ and $0 \leq k \leq p-1$. Let*

$$f(x) = (4-k)x^{\frac{p^l+1}{2}} + kx^{\frac{p^l-1}{2}} + (2-k)x.$$

Then, $f(x)$ is a permutation polynomial of F_q if and only if $l = 0$ and $k \neq 3$.

Through the study of the number of solutions of special equations, Ma et al. [52] constructed one class of complete permutation trinomials:

$$f(x) = -x + x^{\frac{p^{2m}+1}{2}} + x^{\frac{p^{2m}+1}{2}}p^m$$

for any odd prime p over $F_{p^{3m}}$. They also proved that

$$f(x) = -x + x^{\frac{p^{2m}+1}{2}} + x^{\frac{p^{2m}+1}{2}}p^m$$

is a permutation polynomial over $F_{p^{3m}}$ if and only if

$$h(x) = x + x^{p^m} - x^{1+p^m-p^{2m}}$$

applies over $F_{p^{3m}}$. Using the multivariate method introduced by Dobbertin [21], they constructed the two classes of trinomial permutations over F_{2^m} listed below.

Theorem 3.15. *[52] Let $m > 1$ be an odd integer, and write $k = \frac{m+1}{2}$. Then, for each $u \in F_{2^m}^*$, the following trinomials are permutation polynomials over F_{2^m} :*

(1) $f(x) = x + u^{2^{k-1}-1}x^{2^k-1} + u^{2^{k-1}}x^{2^k+1}$,
(2) $f(x) = x + ux^{2^k-1} + u^{2^k}x^{2^m-2^{k+1}+2}$.

For the field of characteristic 2, let $q = 2^k$ and $f(x) = x^r h(x^{q-1}) \in F_{q^2}$, where

$$h(x) = 1 + x^m + x^n (1 < m < n);$$

then, $f(x)$ permutes F_{q^2} if and only if $\gcd(r, q-1) = 1$ and $g(x) = x^r h(x)^{q-1}$ permutes μ_{q+1}. The fractional polynomial of $g(x)$ is

$$g(x) = x^r h(x)^{q-1} = x^r \frac{h(x)^q}{h(x)} = x^r \frac{1 + x^{mq} + x^{nq}}{1 + x^m + x^n} = x^{r-n} \frac{x^n + x^{n-m} + 1}{1 + x^m + x^n}; \tag{3.1}$$

using this specified equation, Li et al. [39] constructed several classes of permutation trinomials of the form $x^r h(x^{(p^m-1)/d})$ with $m = 2k$ and $d = p^k + 1$ for $p = 2, 3$, and they proposed Conjectures 3.3 and 3.4.

By construction of the fractional polynomial and Lemma 1.2 the next theorem was developed and it is a generalization of Corollary 3.2. For the next theorem, $r = 3 + (q+1)l$ in the first case and $r = 2 + (q+1)l$ in the second case were considered.

Theorem 3.16. *[39] Let $q = 2^k$; then, $f(x) = x^r h(x^{q-1}) = x^a + x^b + x^c$ is a permutation trinomial of F_{q^2} in the following cases:*

(1) $a = lq + l + 3$, $b = (l+4)q + l - 1$ *and* $c = (l-1)q + l + 4$, *when k is even and* $\gcd(2l+3, q-1) = 1$,

(2) $a = lq+l+2$, $b = (l+2)q+l$ *and* $c = (l-1)q+l+3$, *when* $k \not\equiv 0 \pmod 3$ *and* $\gcd(l+1, q-1) = 1$.

In the following theorem, they considered $f(x) = x^r h(x^{q-1})$, where $h(x) = 1 + x^4 + x^{-1}$ and $r = 2 + (q+1)l$, and they obtained new class of permutation trinomial.

Theorem 3.17. *[39] Let* $q = 2^k$. *Then,*

$$f(x) = x^{lq+l+2} + x^{(l+4)q+l-2} + x^{(l-1)q+l+3}$$

is a permutation trinomial over F_{q^2} *when* $k \equiv 2, 4 \pmod 6$ *and* $\gcd(l+1, q-1) = 1$.

In the following theorem, they considered $f(x) = x^r h(x^{q-1})$, where $h(x) = 1 + x^3 + x^{-1}$ and $r = 3 + (q+1)l$ in the first case and $r = 1 + (q+1)l$ in the second case.

Theorem 3.18. *[39] Let* $q = 2^k$; *then,* $f(x) = x^r h(x^{q-1}) = x^a + x^b + x^c$ *is a permutation trinomial over* F_{q^2} *in the following cases:*

(1) $k \not\equiv 2 \pmod 4$, $a = lq + l + 3$, $b = (l+3)q + l$, $c = (l-1)q + l + 4$ *and* $\gcd(2l+3, q-1) = 1$.
(2) k *is even,* $a = lq + l + 1$, $b = (l+3)q + l - 2$, $c = (l-1)q + l + 2$, $l \geq 0$ *is an integer and* $\gcd(2l+1, q-1) = 1$.

Theorem 3.19. *[39] Let* $q = 2^k$, $r = 1 + (q+1)l$, *where* $\gcd(2l+1, q-1) = 1$, *and* $h(x) = 1 + x^4 + x^{-2}$. *Then,*

$$f(x) = x^{lq+l+1} + x^{(l+4)q+l-3} + x^{(l-2)q+l+3}$$

is a permutation trinomial over F_{q^2} *if* $k \not\equiv 0 \pmod 3$.

Following the method described by Hou [30], Li et al. [39] obtained two permutation trinomials over $F_{3^{2k}}$ with fixed exponents by applying $Tr(x)$ and $N(x)$. Then, they generalized these trinomials to two classes of permutation trinomials with one parameter in each class.

They obtained the following two classes of trinomials over $F_{3^{2k}}$, of the form $f(x) = x^r h(x^{q-1})$, by using the fractional polynomial method. In the following theorem, the first case was considered for $h(x) = 1 - x^2 + x^{-2}$; they later computed the fractional polynomial $g(x)$, which permutes μ_{q+1} when $k \not\equiv 0 \pmod 4$, as does $f(x)$. Similarly, in the second case of $r = 1$, $h(x) = 1 + x^3 + x^{-1}$, and the fractional polynomial $g(x)$ permutes μ_{q+1} when k is odd; this is also true for $f(x)$.

Theorem 3.20. *[39] Let* $q = 3^k$. *Then,*

(1) when $k \not\equiv 0 \pmod 4$, $f(x) = x - x^{2q-1} + x^{q^2-2q+2}$ *is a permutation trinomial over* F_{q^2},
(2) when k *is odd,* $f(x) = x - x^{3q-2} + x^{q^2-q+1}$ *is a permutation trinomial over* F_{q^2}.

Together with the above classes of permutation trinomials over F_{q^2}, they also proposed the following two conjectures. They verified Conjecture 3.4 by using **MAGMA** for $1 \leq k \leq 6$, and they observed that, by using Lemma 1.2, one can prove Conjecture 3.4.

Conjecture 3.3. *[39]*

(1) Let $q = 3^k$, k *be even and* $f(x) = x^{lq+l+5} + x^{(l+5)q+l} - x^{(l-1)q+l+6}$, *where* $\gcd(5 + 2l, q-1) = 1$. *Then,* $f(x)$ *is a permutation polynomial over* F_{q^2}.

(2) Let $q = 3^k$ and $f(x) = x^{lq+l+1} - x^{(l+4)q+l-3} - x^{(l-2)q+l+3}$, where $\gcd(1 + 2l, q - 1) = 1$. *Then, $f(x)$ is a permutation polynomial over F_{q^2}.*

(3) Let $q = 3^k$ and $f(x) = x^{lq+l+1} + x^{(l+2)q+l-1} - x^{(l-2)q+l+3}$, where $\gcd(1 + 2l, q - 1) = 1$. *Then, $f(x)$ is a permutation polynomial over F_{q^2} if $k \not\equiv 2 \pmod 4$.*

Conjecture 3.4. *[39]*

(1) Let $q = 3^k$, k be even and $g(x) = \frac{-x^7+x^3+x}{x^6+x^4-1}$. Then, $g(x)$ permutes μ_{q+1}.

(2) Let $q = 3^k$ and $g(x) = \frac{x^6+x^4-1}{-x^7+x^3+x}$. Then, $g(x)$ permutes μ_{q+1}.

(3) Let $q = 3^k$ and $g(x) = \frac{-x^5+x^3+x}{x^4+x^2-1}$. Then, $g(x)$ permutes μ_{q+1} if $k \not\equiv 2 \pmod 4$.

Remark 3.2. *According to our observation, all three parts of Conjecture 3.4 have been resolved. In a way, Conjecture 3.3 can be considered to be resolved as well since it is equivalent to Conjecture 3.4 based on Lemma 1.2, although no direct proof is available in the literature.*

Using the approach involving the resultant of two polynomials and rational points on curves, Bartoli and Giulietti [5] proved the first part of Conjecture 3.4. Later, by analyzing the quadratic factors of the corresponding fifth and seventh-degree equations over $F_{3^{2k}}$, Li [41] proved the last two cases of Conjecture 3.4. He used the theory of the existence of a unique solution in μ_{q+1} for the equation $g(x) = t$ for any $t \in \mu_{q+1}$. Also, using the technique introduced in [39], Liu and Sun [49] partially settled parts (2) and (3) of Conjecture 3.4. To prove these two parts, the authors first determined two classes of permutation trinomials of the form $f(x) = xh(x)^{q-1}$ over F_{q^2}, which are listed below. They considered $f(x) = xh(x)^{q-1}$; in the first case of the below theorem, $f(x)$ can be written as $x(1 - x^4 + x^{-2})^{q-1}$, and the corresponding fractional polynomial is

$$g_1(x) = \frac{x^6 + x^4 - 1}{-x^7 + x^3 + x},$$

which permutes μ_{q+1} if $m \not\equiv 0 \pmod 3$. Similarly, in the second case of the below theorem, $f(x)$ can be written as $x(1 - x^2 + x^{-2})^{q-1}$; the corresponding fractional polynomial is

$$g_1(x) = \frac{-x^5 + x^3 + x}{x^4 + x^2 - 1},$$

which permutes μ_{q+1} if m is odd.

Theorem 3.21. *[49] Let $q = 3^m$. Then, the following holds:*

(1) The polynomial $f(x) = x - x^{4q-3} + x^{3-2q}$ is a permutation trinomial over F_{q^2} if $m \not\equiv 0 \pmod 3$.
(2) The polynomial $f(x) = x - x^{2q-1} + x^{3-2q}$ is a permutation trinomial over F_{q^2} if m is odd.

Bhattacharya and Sarkar [10] constructed permutation binomials and trinomials. They extracted permutation trinomials of the form

$$x^{2^s+1} + x^{2^{s-1}+1} + \alpha x \in F_{2^t}[x],$$

where s and t are positive integers from permutation binomials of the form

$$x^{\frac{2^n-1}{2^t-1}+1} + ax \in F_{2^n}[x], \;\; n = 2^s t, \;\; a \in F^*_{2^{2t}}.$$

They used Hermite-Dickson criteria, the Lucas theorem and Wan-Lidl criteria to get the following trinomial.

Theorem 3.22. *[10] Let s and t be positive integers. Then, the polynomial*

$$x^{2^s+1} + x^{2^{s-1}+1} + \alpha x \in F_{2^t}[x]$$

is a permutation polynomial over F_{2^t} if and only if $t\alpha = 1$, $s = \{1, 2\}$ and t is odd.

Wu et al. [74] explicitly determined all permutation trinomials over F_{2^m} from the results of Zieve's paper [88]; they also proved the conjecture proposed in [26]. All of the explicit trinomials were obtained from

$$f(x) = x^{n+k(q+1)} \cdot ((\gamma x^{q-1} - \beta)^n - \gamma(x^{q-1} - \gamma^q\beta)^n)$$

by simplifying the coefficients of $x^{(n-k)(q-1)}$ and $x^{k(q-1)}$ from the polynomial $(\gamma x^{q-1} - \beta)^n - \gamma(x^{q-1} - \gamma^q\beta)^n$. To construct the permutation polynomial f_1, they considered

$$n = \sum_{i=0}^{l} n_i p^i, \;\; 0 \le n_i \le p;$$

using the Lucas formula, they came to know that there are $\prod_{i=0}^{l}(n_i + 1)$ integers k with $0 \le k \le n$ and $\binom{n}{k} \not\equiv 0 \pmod{p}$. Then, by simplifying and considering all cases on γ in

$$f(x) = x^{n+k(q+1)} \cdot ((\gamma x^{q-1} - \beta)^n - \gamma(x^{q-1} - \gamma^q\beta)^n),$$

they ended up with conditions which are mentioned in the following theorem. Following a similar procedure for the polynomial

$$f(x) = x^{n+k(q+1)} \cdot ((\delta x^{q-1} - \beta\delta^q)^n - \delta(x^{q-1} - \beta)^n),$$

they obtained f_2.

Theorem 3.23. *[74] Let $m > 0$ and k be an integer, $q = 2^m$. Then, the polynomial*

$$f_1(x) = x^{3+k(q+1)}(x^{3(q-1)} + x^{q-1} + 1)$$

permutes $F^*_{q^2}$ if and only if $\gcd(3 + 2k, q - 1) = 1$. *The polynomial*

$$f_2(x) = x^{6+k(q+1)}(x^{6(q-1)} + x^{4(q-1)} + 1)$$

permutes $F^*_{q^2}$ if and only if $\gcd(6 + 2k, q - 1) = 1$.

Using Conjecture 3.2, Wu et al. determined some similar permutation trinomials in the following theorems.

Theorem 3.24. *[74] Let $m > 0, k > 0$ and $q = 2^m$. Then, the polynomials of the form*

$$f(x) = x^{n+k(q+1)}(1 + x^{l_1\cdot(2^m-1)} + x^{l_2\cdot(2^m-1)})$$

permute $F_{2^{2m}}$ if and only if $\gcd(n + 2k, 2^m - 1) = 1$, *when*

(1) $l_1 = 4$, $l_2 = 5$ *and* $2 \mid m$,
(2) $l_1 = 2$, $l_2 = 3$ *and* $3 \nmid m$,
(3) $l_1 = 1$, $l_2 = 3$ *and* $3 \nmid m$,

for $n = 5, 4, 2$, *respectively.*

Li et al. [43] constructed four classes of permutation trinomials over F_{q^2} using Lemma 1.2 and the fraction polynomial method. In the first case of the following theorem, they considered polynomials of the form

$$f(x) = x^{lq+l+3}h(x^{q-1}),$$

where $h(x) = 1 + x^6 + x^{-2}$, and, in the second case, they considered $f(x) = xh(x^{q-1})$, where

$$h(x) = 1 + x^{\frac{q-2}{3}} + x^{\frac{2q-1}{3}}.$$

Later, Zheng et al. [83] listed all of the necessary values of s for these classes of permutation trinomials.

Theorem 3.25. *[43] Let* $q = 2^k$. *Then the following holds:*

(1) If $k \geq 1$, l *is an integer and* $f(x) = x^{lq+l+3} + x^{(l+6)q+l-3} + x^{(l-2)q+l+5}$, *then* $f(x)$ *is a permutation trinomial over* F_{q^2} *if and only if* $\gcd(3 + 2l, q - 1) = 1$ *and* $k \not\equiv 0 \pmod 4$.
(2) If k *is odd and* $f(x) = x + x^{\frac{q^2-3q+5}{3}} + x^{\frac{2q^2-3q+4}{3}}$, *then* $f(x)$ *is a permutation trinomial over* F_{q^2}.
(3) If $k \not\equiv 1 \pmod 3$, *then* $f(x) = x + x^{q^2-q+q} + x^{q^3-q^2+q}$ *is a permutation trinomial over* F_{q^3}.
(4) If $k \not\equiv 1 \pmod 3$, *then* $f(x) = x + x^{q^2} + x^{q^3-q^2+q}$ *is a permutation trinomial over* F_{q^3}.

Using the Niho exponents, Bai and Xia [2] investigated permutation trinomials of the form

$$f(x) = x^{(p-1)q+1} + x^{pq} - x^{q+(p-1)}$$

for $p = 3, 5$ and a positive integer k. They verified that $(p-1)q+1$, pq and $q+(p-1)$ are Niho exponents over $F_{p^{2k}}$. They also considered general polynomials of the form

$$g(x) = x^{(q+1)l+(p-1)q+1} + x^{(q+1)l+pq} - x^{(q+1)l+q+(p-1)},$$

where l is a non-negative integer and $\gcd(2l + p, q - 1) = 1$. The authors concluded that the same two polynomials may not be permutation polynomials when $p > 5$. They proved the following theorems by using an idea that originated from [30] and was used in [39].

Theorem 3.26. *[2] Let* $q = p^k$ *and*

$$f(x) = x^{(p-1)q+1} + x^{pq} - x^{q+(p-1)}$$

be the trinomial. Then, for $p = 3$ *or* $p = 5$, $f(x)$ *is a permutation polynomial of* F_{q^2} *if and only if* k *is even.*

Theorem 3.27. *[2] Let* $q = p^k$ *with* $p \in \{3, 5\}$ *and* l *be a non-negative integer satisfying* $\gcd(2l + p, q - 1) = 1$. *Then,*

$$g(x) = x^{(q+1)l+(p-1)q+1} + x^{(q+1)l+pq} - x^{(q+1)l+q+(p-1)}$$

is a permutation polynomial of F_{q^2} *if and only if* k *is even.*

Bartoli and Giulietti [5] constructed permutation trinomials of the form $x^{2p^s+r} + x^{p^s+r} + \lambda x^r$ over F_{p^t}, for the case that $2p^s + r < p^t$, and it was an extension of Bhattacharya and Sarkar's [10] work when $p = 2$ and $r = 1$. The authors characterized certain classes of permutation trinomials when s and r are non-negative integers given that $\lambda \in F_{p^t}$ and $f_\lambda(x) = x^{2p^s+r} + x^{p^s+r} + \lambda x^r$ in $F_{p^t}[x]$. If $r = 0$, then $d = 0$. If $r \neq 0$, write $r = p^u v$ with $u \geq 0$ and $p \nmid v$; then, $d = 2p^{s-u} + v$ if $u \leq s$ and $d = 2 + p^{u-s}v$ if $u > s$, that is,

$$d = (2p^s + r)/p^m, \ m = max\{n \geq 0 : p^n|(2p^s + r), p^n|(p^s + r), p^n|r\}.$$

Theorem 3.28. *[5] Assume that $d^4 < p^t$. Then, $f_\lambda(x)$ is a permutation polynomial of F_{p^t} if and only if one of the following cases holds:*

(1) $p = 2$, t is odd and $f_\lambda(x) = x^3 + x^2 + x$ or $f_\lambda(x) = x^5 + x^3 + x$,
(2) $p \equiv 2 \pmod 3$, t is odd and $f_\lambda(x) = x^3 + x^2 + \frac{1}{3}x$.

There are some papers that make considerable use of the methodology based on the relationship between permutation polynomials and algebraic curves; however, the most challenging aspect of such a methodology is the investigation of the singular points of the curves. However, difficulty can be minimized by considering the algebraic curve C: $F(X, Y) = 0$, defined over F_q, and demonstrating that C has no completely irreducible components over F_q. Using this technique, Bartoli and Timpanella [7] determined permutation trinomials of the form

$$F_{A,B,m,n}(X) = X^{n+m}(1 + AX^{m(q-1)} + BX^{n(q-1)})$$

over F_{q^2}, where $q = 2^{2s+1}$ and n and m are odd.

To show that C has no absolutely irreducible components over F_q, Bartoli and Timpanella investigated singular points of C, and they proved that C splits into two components that share no common irreducible components whose degrees are close enough. By finding the lower bound on $(degA)(degB)$, later, by using Bezout's theorem [24, 57], they arrived at the final conclusion by contradiction.

Theorem 3.29. *[7] Let $(m, q + 1) = 1$. Suppose that $F_{A,B,m,n}(X)$ is a permutation polynomial of F_{q^2}. Let $n \equiv i \pmod 8$ and $m \equiv j \pmod 8$. Then, one of the following conditions is satisfied:*

(1) $2(n + m) \geq d < \sqrt[4]{q}$,
(2) $B \in F_q$,
(3) $A^2 + B^{q+1} \neq 0$, $B \notin F_q$ and $n < 5m$,
(4) $A^2 + B^{q+1} = 0$, $B \notin F_q$, $(i, j) \in \{(1, 5), (3, 7), (5, 1), (7, 3)\}$ and $n < 38m$,
(5) $A^2 + B^{q+1} = 0$, $B \notin F_q$ and $(i, j) \notin \{(1, 5), (3, 7), (5, 1), (7, 3)\}$.

Kyureghyan and Zieve [37] determined permutation polynomials of the form $x + \gamma Tr_{q^2/q}(x^{(q^2+1)/4})$ over F_{q^2}, where $\gamma \in F_{q^2}$ satisfies $(2\gamma)^{(q+1)/2} = 1$, which is equivalent to

$$x\left(\gamma^{-1} + x^{\frac{q+3}{4}(q-1)} + x^{\left(\frac{q^2+3q}{4}+1\right)(q-1)}\right).$$

Similarly, following Theorem 4.3, Qin and Yan [58] constructed permutation trinomials with the index $q+1$ over F_{q^2} by using monomials of $\mu_{(q+1)/2}$ and $-\mu_{(q+1)/2}$ to study the permutation property of $x^r h(x)^{q-1}$ on μ_{q+1}. In the following theorem, they characterized more generalized permutation trinomials over F_{q^2}.

Theorem 3.30. *[58] Let $c \in F_{q^2}$ satisfy that $(c/2)^{(q+1)/2} = 1$, and let k be an integer. Let* $\gcd(r, q^2-1) = 1$ *and* $\gcd(2r-2k-1, (q+1)/2) = 1$. *Then, the polynomial $x^r(c + x^s + x^{qs-1})$ is a permutation trinomial in the following cases:*

(1) $s = \frac{q^2+2q-3+4k(q-1)}{4}$,
  (a) $q \equiv 1 \pmod 4$,
  (b) $q \equiv 1 \pmod 8$ *and k is an odd integer.*
(2) $s = \frac{3q^2+2q-5+4k(q-1)}{4}$,
  (a) $q \equiv 1 \pmod 4$,
  (b) $q \equiv 5 \pmod 8$ *and k is an odd integer.*

Furthermore, motivated by the idea of Li et al. [43], Qin and Yan [58] determined several classes of permutation trinomials of the form $x^r(1 + x^{s_1(q-1)} + x^{s_2(q-1)})$ over F_{q^2} with the index $q + 1$, where $q = 2^k$ and k is odd. In addition, they considered another kind of permutation trinomial of the form $x^r(c - x^{s_1(q-1)} + x^{s_2(q-1)})$ over F_{q^2}, which is listed below.

Theorem 3.31. *[58] Let $c \in F_{q^2}$ and k be an odd integer. Let* $\gcd(r, q^2-1) = 1$ *and* $\gcd(2r-2k-1, (q+1)/2) = 1$. *Then, the polynomial $x^r(c - x^{s_1(q-1)} + x^{s_2(q-1)})$ is a permutation trinomial in the following cases:*

(1) $s_1 = \left(\frac{q+3}{4} + k\right)$, $s_2 = \left(\frac{q^2+3q}{4} + k + 1\right)$ *and* $(c/2)^{(q+1)/2} = 1$, $q \equiv 5 \pmod 8$,
(2) $s_1 = \left(\frac{3q+5}{4} + k\right)$, $s_2 = \left(\frac{3q^2+5q}{4} + k + 1\right)$ *and* $(c/2)^{(q+1)/2} = 1$, $q \equiv 5 \pmod 8$,
(3) $s_1 = \left(\frac{3q+5}{4} + k\right)$, $s_2 = \left(\frac{q^2+3q}{4} + k + 1\right)$ *and* $(-c/2)^{(q+1)/2} = 1$, $q \equiv 1 \pmod 8$,
(4) $s_1 = \left(\frac{3q+5}{4} + k\right)$, $s_2 = \left(\frac{3q^2+5q}{4} + k + 1\right)$ *and* $(-c/2)^{(q+1)/2} = 1$, $q \equiv 1 \pmod 8$.

Theorem 3.32. *[58] Let $c \in F_{q^2}^*$ and k be an integer. Let* $\gcd(r, q^2 - 1) = 1$. *Then, the polynomial $x^r(c - x^{s_1(q-1)} + x^{s_2(q-1)})$ is a permutation trinomial in the following cases:*

(1) $s_1 = \left(\frac{q+3}{4} + k\right)$, $s_2 = \left(\frac{3q^2+5q}{4} + k + 1\right)$ *and* $q \equiv 1 \pmod 4$,
(2) $s_1 = \left(\frac{3q+5}{4} + k\right)$, $s_2 = \left(\frac{q^2+3q}{4} + k + 1\right)$ *and* $q \equiv 1 \pmod 4$.

4. Polynomials of the form $\lambda_1 x^a + \lambda_2 x^b + \lambda_3 x^c$

The permutation polynomials of the form $\lambda_1 x^a + \lambda_2 x^b + \lambda_3 x^c$ are included in this section. One can see that the majority of polynomials of any form can be expressed in the form of $x^r h(x^s)$. In this case, there are also a lot of polynomials of the form $\lambda_1 x^a + \lambda_2 x^b + \lambda_3 x^c$ that can be expressed in the form of $x^r h(x^s)$, but we are separately listing this form for the benefit of future research so that it will be easier to obtain new classes by referring to this article.

Using the multivariate method introduced by Dobbertin [21], Wang et al. [71] constructed six new classes of permutation trinomials over F_{2^n}. In the following theorem, all five classes of permutation trinomials over F_{2^n} when $n \equiv 0, 1, 2 \pmod 3$ are listed.

Theorem 4.1. *[71] Let k be a positive integer. Then, $f(x) = x^a + x^b + x$ is a permutation polynomial over F_{2^n} if, for the case that $n \equiv 0 \pmod 3$,*

(1) $k \not\equiv 2 \pmod 3$ *for* $a = 2^{2k} + 2^k - 1$, $b = 2^{2k}$,
(2) $k \not\equiv 2 \pmod 3$ *for* $a = 2^{2k} + 2^k - 1$, $b = 2^{2k} + 2^k - 1$;

for the case that $n \equiv 1 \pmod 3$,

$$a = 2^{2k+1} + 2^{k+1} + 1,\ b = 2^{k+1} + 1;$$

for the case that $n \equiv 2 \pmod 3$ *and* $n = 3k - 1$,

(1) $a = 2^{3k-1} - 2^{2k} + 2^k$, $b = 2^k - 1$,
(2) $a = 2^{2k} + 2^k + 1$, $b = 2^{2k} + 1$.

In the following theorem, the last class of a permutation trinomial over F_{2^n} with $n \equiv 0 \pmod 4$ is stated.

Theorem 4.2. *[71] Let k be an odd integer, and let m, n, d be positive integers satisfying*

$$n = 4m,\ \ 1 \le k \le n-1,\ \ \gcd(m,k) = 1 \ \ and \ \ d = \sum_{i=0}^{2m} 2^{ik}.$$

Then, $f(x) = x^d + x^{2^{2m}} + x$ *is a permutation polynomial over* F_{2^n}.

Yuan and Ding [80, 81] determined many classes of permutation trinomials of the form $cx - x^s + x^{qs}$ by using the AGW criterion. The obtained permutation polynomials were derived from a linear bijection between subsets S and $\bar{S}$ of a finite field, as well as their permutation behavior, which was related to δ. Using this construction as their reference, Zheng et al. [83] looked into the relationship between permutation trinomials of the form $cx - x^s + x^{qs}$ and permutation polynomials of the form $(x^q - x + \delta)^s + cx$, restricting them on δ over F_{q^2} (see [83, Proposition 3]). There is no inclusion of subsets or their bijections in the proposed relationship between these two varieties of permutation polynomials. Furthermore, they stated that a variety of classes of permutation polynomials of the form $(x^q - x + \delta)^s + cx$ without a restriction on δ can be constructed on the basis of this relation. In addition, they constructed the four classes of permutation trinomials of the form $cx - x^s + x^{qs}$ over F_{q^2} that are listed below.

Theorem 4.3. *[83] Let* $c \in F_{q^2}^*$. *The polynomial* $cx - x^s + x^{qs}$ *permutes* F_{q^2} *in each of the following cases:*

(1) $s = \frac{3q^2+2q-1}{4}$,

(a) $q \equiv 1 \pmod 8$ *and* $\left(-\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$,

(b) $q \equiv 5 \pmod 8$ *and* $\left(\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$.

(2) $s = \frac{(q+1)^2}{4}$,

(a) $q \equiv 5 \pmod 8$ *and* $\left(-\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$,

(b) $q \equiv 1 \pmod 8$ *and* $\left(\frac{2}{c}\right)^{\frac{q+1}{2}} = 1$.

(3) $s = \frac{q^2+q+1}{3}$, $c = 1$ *and* $q \equiv 1 \pmod 3$.

Theorem 4.4. *[83] Let q be power of an odd prime and $s = q^3 + q^2 - q$. Then, the polynomial $f(x) = x - x^s + x^{q^2 s}$ permutes F_{q^4}.*

Li et al. [44] proposed several classes of complete permutation binomials over a finite field based on certain polynomials over its subfields or subsets. In addition, a class of complete permutation trinomials with Niho exponents was studied, and the number of these complete permutation trinomials was also determined. They found that certain polynomials over F_{2^n} can have the same properties those of $ax^k + bx$ over F_{2^m} for a positive divisor m of n such that $\frac{n}{m}$ is odd. Later, they presented complete permutation trinomials of the form $ax^{p^{2m}-p^m+1}+a^{p^m}x^{p^m}+(a^{p^m+1}+1)x$ with Niho-type exponents. Liu [48] modified the conditions and generalized the results based on the results presented in [44]; they also showed that the relationship exists between two permutation polynomials proposed by Zheng et al. [83].

The following corollary is a generalization of the result stated in [83].

Corollary 4.1. *[48] For a positive integer m and $c \in F_{2^m}^*$, the polynomial*

$$g(x) = x^{2^m(2^{2m}+1)} + x^{2^{2m}+1} + cx$$

is a permutation over $F_{2^{3m}}$.

In the next proposition, Liu [48] considers an arbitrary value for c and generalizes the result, which was constructed with the coefficient 1 in Theorem 4.3 case 3 by Zheng et al. [83].

Proposition 4.1. *[48] Let $q = 2^m$ be even with $s = \frac{q^2+q+1}{3}$, and let $q \equiv 1 \pmod 3$. Then, the polynomial $cx + x^s + c^q x^{qs}$ permutes F_{q^2} for $c \in F_{q^2}^*$ satisfying $Tr_1^m(c^{q+1}) = 0$.*

The binomial $ax^k + bx$ over F_{2^m}, which was proved for the case of an odd value of m in [44], Liu considered the same binomial and proved it to be a permutation trinomial for all positive values of m by using different methods.

When we go through the permutation polynomials' application part, involve the concept of differential uniformity, which is crucial to the S-box. On the way to determining the permutation polynomial's differential uniformity, Peng et al. [56] constructed permutation trinomials of the form $x^{2^{k+1}+3} + ax^{2^k+2} + bx$ over $F_{2^{2k}}$ and established its differential uniformity by using **MAGMA**. They observed that $x^{2^{k+1}+3} + ax^{2^k+2} + bx \in F_{2^{2k}}$ permutes $F_{2^{2k}}$ if and only if

$$g(x) = x^5 + (b + \bar{b} + a\bar{a})x^3 + [(b + \bar{b} + a\bar{a})(a + \bar{a}) + a\bar{b} + b\bar{a}]x^2 + [(a + \bar{a})^4 + (b + \bar{b} + a\bar{a})(a + \bar{a})^2 + b\bar{b}]x$$

permutes F_{2^k}. Furthermore, $g(x)$ permutes F_{2^k} if and only if $g(x) = x^5$ for $k \equiv 2 \pmod 4$ or $g(x) = x^5 + ax^3 + a^2x$, $a \in F_{2^k}$ for odd values of k. Later, Peng et al. [56] conjectured that the differential uniformity of the permutation trinomials is 12 and 10 for both cases when $k \geq 5$.

Sharma and Gupta [60] constructed permutation trinomials of the form $ax + bx^{q+2} + x^{2q+3}$ and $ax^2 + bx^{q+3} + x^{2q+4}$. The polynomial

$$f(x) = ax + bx^{q+2} + x^{2q+3}$$

can be written as $xh(x^{q+1})$, where $h(x) = x^2 + bx + a$. For any $\alpha \in F_q$,

$$g(\alpha) = \alpha^5 + (b^q + b)\alpha^4 + (a + a^q + b^{q+})\alpha^3 + (ab^q + a^q b)\alpha^2 + a^{q+1}\alpha,$$

it can be further simplified as

$$G(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x.$$

Using this simplification, they proved that $f(x)$ permutes F_{q^2} if and only if $g(x)$ permutes μ_{q+1} if and only if $g(x)$ permutes F_q, which is subject to the condition of if and only if $G(x)$ permutes F_q. Following certain assumptions on coefficients a and b, they proved the following theorems.

Theorem 4.5. *[60] Let $q = 2^m$. The polynomial $f(x) = ax + bx^{q+2} + x^{2q+3}$ permutes F_{q^2} if and only if one of the following conditions is satisfied:*

(1) $m = 1$, $a \neq b + 1$, $a_2 = 0$ and either $a_3 = 1$ or $a_1 = a_4$,
(2) $m \geq 3$, $m \not\equiv 0 \pmod 4$, $a_2 = a_3 = 0$ and $a_1^4 = a_4$,
(3) $m \geq 3$ is odd, $a_1a_2 + a_3 = 0$ and $a_2^2 = a_1^4 + a_1^2a_2 + a_4$.

In the above theorem, under the condition that $a \in F_q^*$, $f(x)$ permutes F_{q^2} if and only if either (1) $m = 1$ and $a \neq b+1$ or (2) $m \geq 3$ is odd, either $b^{q-1} = 1$ and $a = b^2$, or $a = b^{q+1}$ and $b^{2(q-1)} + b^{q-1} + 1 = 0$. Similarly, under the condition that $b \in F_q^*$, $f(x)$ permutes F_{q^2} if and only if either (1) $m = 1$ and $a \neq b + 1$; (2) $m = 1$, $a \neq b + 1$ and $a + a^4 = b^2$ or (3) $m \geq 3$ is odd, $a^{q-1} = 1$ and $a = b^2$.

Similarly, Sharma and Gupta [60] determined the necessary and sufficient conditions for the coefficients when $q = 3^m$, $q = 5^m$ and $q = p^m$, $p > 5$ for the permutation polynomial of the form $f(x) = ax + bx^{q+2} + x^{2q+3}$ over F_{q^2}. And, they determined conditions on q and coefficients $a, b \in F_q$ for the polynomial of the form $ax^2 + bx^{q+3} + x^{2q+4}$ over F_{q^2}. The polynomial

$$f(x) = ax + bx^{q+2} + x^{2q+3}$$

can be written as

$$f(x) = x^2h(x^{q+1}),$$

where

$$h(x) = x^2 + bx + a \in F_{q^2}[x].$$

By Lemma 1.2, $f(x)$ permutes F_{q^2} if and only if

$$\gcd(2, q + 1) = 1 \text{ and } g(x) = x^2(x^2 + bx + a)^{q+1}$$

permutes $\mu_{q-1} = F_q^*$. Here, $g(x)$ permutes F_q^* if and only if $g(x)$ permutes F_q, which is subject to the condition of if and only if

$$G(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_4x^2$$

permutes F_q; so, by taking different conditions on q and coefficients $a, b \in F_q$ over F_{q^2}, this can be achieved.

A permutation polynomial $f(x) \in F_q[x]$ of degree n is said to be normalized if $f(x)$ is monic and $f(0) = 0$, and the coefficient of x^{n-1} equals 0 if $p \nmid n$, where p is a characteristic of F_q. By knowing some of the normalized permutation polynomials of degree 5 over F_{2^n}, Liu et al. [50] determined some necessary and sufficient conditions for the coefficients $(b_1, b_2) \in F_{2^n}^2$ such that

$$f(x) = x^3\bar{x}^2 + b_1x^2\bar{x} + b_2x$$

is a permutation polynomial, where $\bar{x}$ is a conjugation of any $x \in F_{2^{2m}}$, which is denoted as $\bar{x} = x^{2^m}$. Permutation polynomials that have been determined are presented in the next theorem.

Theorem 4.6. *[50] For the two positive integers m, n with $n = 2m$, let $(b_1, b_2) \in F_{2^n}$, which are not both zero. Then, the polynomial*

$$f(x) = x^3\bar{x}^2 + b_1x^2\bar{x} + b_2x$$

is a permutation polynomial over F_{2^m} under the following condition:

(1) if and only if m is even with $m \equiv 2 \pmod 4$, $b_1 = \theta b_2$ and b_2 as a root of $x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0$, where $\theta \in F^*_{2^m}$ and $\omega \in F^*_{2^m}$ is a primitive third root of unity.

It is also true if condition (1) is not satisfied but one of the following two conditions are satisfied when m is odd:

(2) $b_1 = 0$, $b_2 = \theta\omega$ or $b_2 = \theta\omega^2$, where $\theta \in F^*_{2^m}$ and $\omega \in F_{2^n}$ is a primitive third root of unity.
(3) $b_1 = \theta\omega$ or $b_1 = \theta\omega^2$ and $b_2 = \theta^2 + \theta\eta\omega^2$ or $b_2 = \theta^2 + \theta\eta\omega$, where $\theta \in F^*_{2^m}$, $\eta \in F^*_{2^m}$ and $\omega \in F_{2^n}$ is a primitive third root of unity.

Guo et al. [25] observed that, by reversing the method introduced by Tu et al. [64], so many new classes of permutation trinomials with a coefficient of 1 can be determined. On that note, they determined the permutation polynomial $x^{d_1} + x^{d_2} + x^{d_3}$ and its compositional inverse for $i = j + m - 1$, which is listed below.

Theorem 4.7. *[25] Let $n = 2m$, $m > 0$, $i, j \in N^+$, $I \neq j$, $u \in Z$, $J = 2^j$ and $I = 2^i$. Suppose that* $\gcd(d_1, 2^{2m} - 1) = 1$, $\gcd(2^i - 2^j, 2^m + 1) = 1$ *and*

$$\begin{cases} d_1 = 2^{i-1} - 2^{j-1} + u \times (2^m + 1), \\ d_2 = 2^{i-1} + 2^{j-1} + (u - 2^{j-1})(2^m + 1), \\ d_3 = -(2^{i-1} + 2^{j-1}) + (u + 2^{i-1})(2^m + 1), \end{cases}$$

where $\frac{1}{J-I} \pmod{2^m + 1} \equiv t$, $0 \leq t \leq 2^m + 1$. Then, $x^{d_1} + x^{d_2} + x^{d_3}$ is a permutation polynomial over F_{2^n}.

Considering the work of Guo et al. [25], Zieve [89] made remarkable observations and provided another and simpler proof, which demonstrates the general method for producing the permutation polynomials that were introduced in [88]. Moreover, Zieve observed that the newly constructed permutation trinomials [25] are multiplicatively equivalent to many previous results.

Recently, Xie et al. [76] proposed two classes of permutation trinomials over F_{q^3} for an arbitrary odd characteristic based on the multivariate method and some suitable manipulation; this was done to solve equations with low degrees over finite fields. In the following theorem, two classes of permutation polynomials are listed. They stated that sufficient conditions in both classes are also necessary, but they were kept as an open problem.

Theorem 4.8. *[76] Let q be an odd prime power and $a, b \in F^*_{q^3}$. Then,*

(1) $f(x) = ax^{q(q^2-q+1)} + bx^{q^2-q+1} + 2x$ is a permutation polynomial of F_{q^3} if one of the following conditions is satisfied:
  (a) $ab = 1$ and $a^{q^2+q+1} \neq -1$,
  (b) $ab \in F^*_q \backslash \{1\}$ and $a^{q^2+q+1} + 2ab + b^{q^2+q+1} = 0$.

(2) $f(x) = x^{q^2-q+1} + ax^{q^2} + bx$ *is a permutation polynomial of* F_{q^3} *if one of the following conditions is satisfied:*

(a) $a^q b = 1$ *and* $a^{q^2+q+1} \neq -1$,
(b) $a^q b \in F_q^* \backslash \{1\}$ *and* $a^{q^2+q+1} - 2a^q b + b^{q^2+q+1} = 0$.

Inspired by the work of Wang et al. [71], Zheng et al. [84] investigated infinite classes of permutation polynomials with the form $f(x) = x + ax^{2^m} + bx^d$, defined on F_{2^n}, under the condition that m is any positive integer, $d = \sum_{i=0}^{\frac{n}{2}} 2^{ik}$, with k being an odd positive integer satisfying $\gcd(k, m) = 1$, and $a, b \in F_{2^m}^*$. And, following the case considered in [45],

$$(s, t) = \left(\frac{2^k}{2^k - 1}, \frac{-1}{2^k - 1}\right),$$

where k is a positive integer satisfying $1 \leq k \leq m - 1$ and $\gcd(2^k - 1, 2^m + 1) = 1$; also, assuming that $a, b \in F_{2^m}^*$, they obtained some sufficient conditions for a and b such that

$$f(x) = x + ax^{s(q-1)+1} + bx^{t(q-1)+1}$$

is a permutation polynomial of F_{2^n}. Also, they observed that

$$f(x) = x + ax^{s(q-1)+1} + bx^{t(q-1)+1}$$

is a permutation polynomial of F_{q^2}, where $ab \neq 0$; then, $a + b + 1 \neq 0$. In the following theorem, they proved that $f(x) = x + ax^{2^m} + bx^d$ permutes F_{2^n} when m is any positive integer, $d = \sum_{i=0}^{\frac{n}{2}} 2^{ik}$, with k being an odd positive integer satisfying $\gcd(k, m) = 1$, and $a, b \in F_{2^m}^*$.

Theorem 4.9. *[84] Let k be an odd positive integer and m, n and d be positive integers such that*

$$n = 2m, \;\; 1 \leq k \leq n - 1, \;\; \gcd(k, m) = 1 \;\; \textit{and} \;\; d = \sum_{i=0}^{\frac{n}{2}} 2^{ik}.$$

Let $a, b \in F_{2^m}^*$, with $a + b + 1 \neq 0$. Then, $f(x) = x + ax^{2^m} + bx^d$ permutes F_{2^n} if one of the following items is satisfied, where $B \in F_{2^n}$ such that $B^{2^k-1} = a$:

(1) $b = B^{2^k}\left(\frac{1}{B} + \frac{1}{B^2} + \cdots + \frac{1}{B^{2^{k-1}}}\right)^2$ *and* $Tr_1^m\left(\frac{b}{a+b+1}\right) = 0$,
(2) $b = B^{2^k}\left(\frac{1}{B} + \frac{1}{B^2} + \cdots + \frac{1}{B^{2^{k-1}}}\right)^2 + B^{2^k}$ *and* $Tr_1^m\left(\frac{b}{a+b+1}\right) = 0$.

Later, they mentioned an open problem based on the above theorem with the same conditions as mentioned above; as with $a \in F_{2^m}^*$ and $b \in F_{2^n}^*$, $f(x)$ will be a permutation polynomial for any $B \in F_{2^m}$. Recently, Ding and Zieve [20] analyzed these open problems by using geometric techniques. In the following theorem, another class of permutation trinomial is described.

Theorem 4.10. *[84] Let $n = 2m$ and $\gcd(2^k - 1, 2^m + 1) = 1$, where m, k are positive integers with $k < m$. Let $d = ord_2(\gcd(k, m))$ and $a, b \in F_{2^m}^*$, with $a + b + 1 \neq 0$. If*

$$\left(\frac{b}{a^2 + b^2 + 1}\right)^{2^k} = \frac{a}{a^2 + b^2 + 1},$$

$$Tr_{2^d}^m\left(\frac{a^2+b^2}{a^2+b^2+1}\right)=0$$

and

$$(a+b)Tr_1^m\left(\frac{b}{a^2+b^2+1}\right)=0,$$

then the trinomial

$$f(x)=x+ax^{s(2^m-1)+1}+bx^{t(2^m-1)+1}$$

permutes F_{2^n}*, where*

$$(s,t)=\left(\frac{2^k}{2^k-1},\frac{-1}{2^k-1}\right).$$

In the above theorem, when $k=1$ and $a\in F_{2^m}^*$ sufficient conditions are also necessary when m is even, but it is not true when m is odd.

By transforming the permutation problem into a root distribution problem in the unit circle of certain quadratic and cubic equations, Liu [51] investigated the permutation behavior of the trinomials over $F_{2^{4m}}$ and quadrinomials over $F_{2^{2m}}$. In the following theorem, he investigated the permutation trinomial of the form

$$f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$$

over $F_{2^{4m}}$.

Theorem 4.11. *[51] Let m be a positive integer; then,*

$$f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$$

is a permutation trinomial over $F_{2^{4m}}$.

Together with trinomials, he investigated permutation quadrinomials of the form

$$f(x)=x+x^{2^m}+x^{2^{m+1}-1}+ax^{2^{2m}-2^m+1}$$

over $F_{2^{2m}}$, which is mentioned below.

Theorem 4.12. *[51] Let* $n=2m$ *be an even integer, with m being even and* $m>2$*. Assume that* $a,\mu\in F_{2^m}$ *satisfy*

$$1+a\neq 0,\ \ 1+a+\mu\neq 0,\ \ Tr_1^m\left(\frac{1}{1+a}\right)=0$$

and

$$Tr_1^m\left(1+\frac{\mu}{(1+a+\mu)^2}\right)=0.$$

Then, the quadrinomial

$$f(x)=x+x^{2^m}+x^{2^{m+1}-1}+ax^{2^{2m}-2^m+1}$$

is a permutation polynomial over F_{2^n}.

Meanwhile, Zheng et al. [86] constructed permutation quadrinomials of the form

$$f(x)=x+a_1x^{s_1(2^m-1)+1}+a_2x^{s_2(2^m-1)+1}+a_3x^{s_3(2^m-1)+1}$$

over $F_{2^{2m}}$ for the cases of

$$(s_1,s_2,s_3)=\left(\frac{-1}{2^k-1},1,\frac{2^k}{2^k-1}\right),\ \ \left(\frac{1}{2^k+1},1,\frac{2^k}{2^k+1}\right)\ \text{ and }\ \left(\frac{1}{4},1,\frac{3}{4}\right).$$

5. Polynomials of the form $f(x) = x + x^{s(q^m-1)+1} + x^{t(q^m-1)+1}$ with Niho exponents

The Niho exponents were introduced by Niho [54] for the case $n = 2m$; $q = 2$ and $1 \leq s, t \leq 2^m$; a positive integer d is called a Niho exponent with respect to the finite field F_{2^n} if $d \equiv 2^j \pmod{2^m - 1}$ for some non-negative integer j. When $j = 0$, the integer d is called a normalized Niho exponent. The inverse of the normalized Niho exponent is also the normalized Niho exponent if it exists. The product of two normalized Niho exponents is also a normalized Niho exponent. So far, the permutation trinomials of the form

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

have drawn a lot of interest. The primary objective for this type of polynomial is to identify a pair (s, t) such that

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation polynomial over any given finite field with Niho exponents. For a complete source of information, Li and Zeng [46] surveyed some recent advances in the field of Niho exponents.

Li and Helleseth [42, 45] determined several new classes of permutation trinomials over F_{2^n} by finding the pair (s, t) of the polynomial $f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$. In the following theorem, they listed a pair (s, t) such that the trinomial $f(x)$ is a permutation over $F_{2^{2m}}$.

Theorem 5.1. *[42] The known pairs (s, t) that exist such that the trinomials*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

are permutations over $F_{2^{2m}}$ are as follows:

(1) $(s, t) = (k, -k)$*, where k is a positive integer, either m is even or m is odd and* $exp_3(x) \geq exp_3(2^m + 1)$*,*
(2) $(s, t) = (2, 2^m) = (2, -1)$ *for every positive integer m,*
(3) $(s, t) = (1, 2^{m-1}) = (1, -1/2)$*, where* $m \not\equiv 0 \pmod 3$.

Using Lemma 1.2 and Theorem 5.1, they noticed some of the pairs to be

$$(s, t) = \left(\frac{k}{2k-1}, \frac{k}{2k-1}\right)$$

if $\gcd(2^k - 1, 2^m + 1) = 1$, and

$$(s, t) = \left(\frac{k}{2k+1}, \frac{k}{2k+1}\right)$$

if $\gcd(2^k + 1, 2^m + 1) = 1$, for which

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation trinomial. For both pairs, the first condition of Theorem 5.1 is met. Similarly, they verified Theorem 5.1 for $(s, t) = (1, 1/3)$ and $(1, 2/3)$ when $\gcd(3, 2^m + 1) = 1$, and $(s, t) = (1, 3/2)$ and $(1/4, 3/4)$ when $m \not\equiv 0 \pmod 3$. Furthermore, they constructed some more permutation trinomials over F_{2^n} by using Lemma 1.2 and some techniques for solving equations with lower degrees over a finite field.

Theorem 5.2. *[42] Let $n = 2m$ for even integers m. The trinomial*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation of $F_{2^{2m}}$ for the following (s, t) pairs:

(1) $(-1/3, 4/3) = \left(\frac{2^{m+1}+1}{3}, \frac{2^m+5}{3}\right)$,

(2) $(3, -1) = (3, 2^m)$,

(3) $(-2/3, 5/3) = \left(\frac{2^m-1}{3}, \frac{2^{m+1}+7}{3}\right)$,

(4) $(1/5, 4/5)$, *where $n = 2m$ satisfies that* $\gcd(5, 2^m + 1) = 1$.

In particular, Theorems 5.1 and 5.2 produce many more permutation trinomials over F_{2^n}, which are described in the following corollary.

Corollary 5.1. *[42] Let $n = 2m$, $q = 2^m$ and k be a positive integer with* $\gcd(2k + 1, q - 1) = 1$. *Then, the following trinomials are permutations over F_{2^n}:*

(1) $x^{(q+1)k+1} + x^{(q+1)k+(2q^2-q+2)/3} + x^{(q+1)k+(q^2+4q-2)/3}$ *if m is even,*

(2) $x^{(q+1)k+1} + x^{(q+1)k+3q-2} + x^{(q+1)k-q+2}$ *if m is even,*

(3) $x^{(q+1)k+1} + x^{(q+1)k+1+(q-1)^2/3} + x^{(q+1)k+(2q^2+5q-4)/3}$ *if m is even,*

(4) $x^{(q+1)k+1} + x^{(q+1)k+1+l(q-1)} + x^{(q+1)k+1+4l(q-1)}$, *where* $5l \equiv 1 \pmod{q+1}$.

By observing the above pairs, they stated the following two conjectures for the pairs (s, t).

Conjecture 5.1. *[42] Determine the conditions on s such that*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation polynomial over $F_{2^{2m}}$ for $s + t = 1$.

Conjecture 5.2. *[42] Determine the conditions on the integer k such that*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation polynomial over $F_{2^{2m}}$ for $(s, t) = (2k, -k)$.

Remark 5.1. *Conjectures 5.1 and 5.2 are not settled yet; one can try to resolve these two conjectures.*

In [45], the authors identified even more pairs of (s, t) such that

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation trinomial over $F_{2^{2m}}$. We list those new pairs of (s, t) in the following theorem. For the proof, the authors used the fractional polynomial method and Lemma 1.2.

Theorem 5.3. *[45] Let $n = 2m$, and m, k be positive integers; then, the trinomial*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation over $F_{2^{2m}}$ if the following holds:

(1) $(s,t) = \left(\frac{2^k}{2^k-1}, \frac{-1}{2^k-1}\right)$, *where* $\gcd(2^k-1, 2^m+1) = 1$ *and* $k < m$,

(2) $(s,t) = \left(\frac{1}{2^k+1}, \frac{2^k}{2^k+1}\right)$, *where* $\gcd(2^k+1, 2^m+1) = 1$.

If $k = 1$, then Theorem 5.3 case 1 generalizes Theorem 3.2 (see [19]). If $k = 2$, then Theorem 5.3 case 1 generalizes Theorem 5.2 case 1. Similarly, if $k = 2$, then Theorem 5.3 case 2 generalizes Theorem 5.2 case 4.

As we have seen, there are numerous classes of permutation trinomials over F_{q^k} for any k that can be computed from Niho exponents. Wu and Li [75] also obtained permutation trinomials over F_{5^n} by using Niho exponents.

Particularly, they considered polynomials of the form

$$f(x) = x + c_1 x^{s(5^k-1)+1} + c_2 x^{t(5^k-1)+1},$$

where $n = 2k$, $1 \leq s,t \leq 5^k$ and $c_1, c_2 \in \{1,-1\}$. Their construction of permutation trinomials is conditional on taking the fractional polynomial that permutes $(5^k+1)^{th}$ roots of unity in $F_{5^{2k}}$, which was the utilization of Lemma 1.2. In the following theorem, they listed all of the trinomials for k, both even and odd cases.

Theorem 5.4. *[75] Let* $q = 5^k$ *and* k *be a positive integer such that, for the following pairs of* (s,t),

$$f(x) = x + c_1 x^{s(5^k-1)+1} + c_2 x^{t(5^k-1)+1}$$

is a permutation trinomial over F_{q^2}*:*

(1) $(c_1,c_2) = (1,-1)$ *and* $(s,t) = \left(\frac{q+3}{4}, \frac{q+3}{2}\right)$,
(2) k *is odd,* $(c_1,c_2) = (1,-1)$ *and* $(s,t) = \left(\frac{q-1}{2}, \frac{q+3}{2}\right)$,
(3) when k *is odd,* $(c_1,c_2) = (-1,1)$ *and* $(s,t) = \left(\frac{q+3}{2}, q\right), \left(\frac{q+1}{2}, 2\right), \left(\frac{q+3}{2}, \frac{q+5}{2}\right), \left(\frac{q+1}{2}, \frac{q-1}{2}\right)$,
(4) when k *is even,* $(c_1,c_2) = (-1,1)$, $(s,t) = \left(2, \frac{q+3}{2}\right), \left(1, \frac{q+5}{2}\right)$,
(5) when k *is even,* $(c_1,c_2) = (1,-1)$, $(s,t) = \left(1, \frac{q-1}{2}\right), \left(\frac{q+3}{2}, \frac{q+5}{2}\right), \left(\frac{q+3}{2}, q\right)$.

In addition, Wu and Li [75] defined two sets $\lambda_- = \{x^2 | x \in \mu_{q+1}\}$ and $\lambda_+ = \{-x^2 | x \in \mu_{q+1}\}$ treating the squares and non-squares separately to construct another kind of fractional permutation polynomial over μ_{q+1}.

Lemma 5.1. *[75] Let* $q = 5^k$*, where* k *is a positive integer. Let*

$$g_1(x) = -x^{\frac{q+1}{2}} \left(\frac{x^s - 2}{x^s + 2}\right)^2,$$

where $s = \frac{q+3}{4}$*. Then,* $g_1(x)$ *permutes* μ_{q+1}.

Before publishing this article, Wu and Li [75] proposed the following two conjectures in the online preprint, and those conjectures were addressed by Ma and Ge [53]. Later, Bartoli and Giulietti [5] provided alternative and shorter proofs for these two conjectures, which are presented in [53] and proposed in [75].

Conjecture 5.3. *[75] The polynomial* $f(x) = x\left(\frac{x^2-x+2}{x^2+x+2}\right)^2$ *is a permutation polynomial over* F_{5^k} *for odd values of k.*

Conjecture 5.4. *[75] Let* $q = 5^k$ *and k be an even integer. Then,*

$$g(x) = -x\left(\frac{x^2-2}{x^2+2}\right)^2$$

permutes μ_{q+1}.

The permutation trinomials of the form $x + a_1x^{s_1(q-1)+1} + a_2x^{s_2(q-1)+1}$, for a_1, a_2 equal to one, have been the subject of extensive research to date. However, choosing general coefficients other than one will be a challenging task. On this note, Tu et al. [66] defined permutation trinomials of the form $x + a_1x^{s_1(q-1)+1} + a_2x^{s_2(q-1)+1}$ for the general coefficients a_1, a_2 by defining two subsets Γ_1 and Γ_2 of $F_{2^n}^* \times F_{2^n}^*$ as follows:

$$\Gamma_1 = \left\{(a_1, a_2)|a_2 = \frac{\bar{a_1}}{a_1} \text{ and } Tr_1^m\left(1 + \frac{1}{a_1\bar{a_1}}\right) = 0\right\} \tag{5.1}$$

and

$$\Gamma_2 = \left\{(a_1, a_2)|a_2(1 + a_1\bar{a_1} + a_2\bar{a_2}) + \bar{a_1}^2 = 0, a_2\bar{a_2} \neq 1 \text{ and } Tr_1^m\left(\frac{a_2\bar{a_2}}{a_1\bar{a_1}}\right) = 0\right\}. \tag{5.2}$$

By analysis of the solutions of the equation $f(x) = b$ for any $b \in F_{2^n}$, for all coefficients (a_1, a_2) in the set $\Gamma_1 \cup \Gamma_2$, they proved that $f(x)$ is a permutation trinomial over F_{2^n}. This can be easily achieved by determining the number of solutions of some low-degree equations in the unit circle of F_{q^2}. In the following theorem, they assumed that $n = 2m$ and $(s_1, s_2) = (q, 2)$, with $q = 2^m$.

Theorem 5.5. *[66] For any* (a_1, a_2) *in the set* $\Gamma_1 \cup \Gamma_2$*, the trinomial* $f(x) = x + a_1x^{q(q-1)+1} + a_2x^{2(q-1)+1}$ *permutes* F_{2^n}.

Tu et al. [66] confirms that, via numerical experiments with $n = 6, 8, 10, 12, 14$, the above Theorem 5.5 covers permutation trinomials of the form

$$f(x) = x + a_1x^{q(q-1)+1} + a_2x^{2(q-1)+1}$$

for all possible coefficients $a_1, a_2 \in F_{2^n}^*$. Nonetheless, they suggested the following open problem in order to use effective approaches to demonstrate this truth.

Open problem 1. *[66] The trinomial*

$$f(x) = x + a_1x^{q(q-1)+1} + a_2x^{2(q-1)+1} \in F_{q^2},$$

where $q = 2^m$ *and* $a_1a_2 \neq 0$*, is a permutation of* F_{q^2} *if and only if the coefficients* a_1, a_2 *satisfy one of the following two conditions:*

(1) $Tr_1^m\left(1 + \frac{1}{a_1\bar{a_1}}\right) = 0$ *if* $a_2 = \frac{\bar{a_1}}{a_1}$,
(2) $a_2(1 + a_1\bar{a_1} + a_2\bar{a_2}) + \bar{a_1}^2 = 0$ *and* $Tr_1^m\left(\frac{a_2\bar{a_2}}{a_1\bar{a_1}}\right) = 0$ *if* $a_2\bar{a_2} \neq 1$.

Dealing with technique involves the connection between the permutation polynomial and algebraic curve C_f, which does not have F_q-rational points $(a, b), a \neq b \in F_q$, is actually a hard problem. If the degree d of C is small with respect to size q of F_q, i.e., $d < \sqrt[4]{q}$, then there exists an absolutely irreducible F_q-rational component in C that is distinct from $x = y$, i.e., the existence of F_q-rational points off the line $x = y$. By the Hasse-Weil theorem [63] if the curve C_f has absolutely irreducible components defined over F_q, then it contains at least $q - 2\sqrt{q} - 7$ affine F_q-rational points off the line $x = y$. So, if $q \geq 16$ and $f(x)$ is a permutation polynomial of F_{q^2}, then C_f has no affine rational points off the line $x = y$; therefore, C_f splits completely into absolutely irreducible components that are not defined over F_q. Utilizing this approach, Bartoli [4] provided a solution to Open problem 1.

Based on the sufficient conditions for (a_1, a_2) that would result in the polynomial $x + a_1x^{s_1(q-1)+1} + a_2x^{s_2(q-1)+1}$ being a permutation over $F_{2^{2m}}$ that were proposed in [66], Tu and Zeng [68] generalized those results by using the same techniques for odd characteristics. As with Γ_1 and Γ_2 in [66] here, the Tu and Zeng [68] defined new sets Γ_1 and Γ_2 for $p \geq 3$. Tu and Zeng [68] considered $p \geq 3$ as an odd prime, $n = 2m$ for a positive integer m and $(a_1, a_2) \in F^*_{p^n} \times F^*_{p^n}$; they later considered $v_1 = a_1\bar{a}_1$ and $v_2 = a_2\bar{a}_2$ and defined following sets:

$$\Gamma_1 = \left\{(a_1, a_2) : \bar{a}_1\bar{a}_2 = a_1(a_2\bar{a}_2 - a_1\bar{a}_1) \text{ and } \frac{v_1 - 4v_2}{v_1} \text{ is a square of } F^*_{p^m}\right\} \tag{5.3}$$

and

$$\Gamma_2 = \left\{(a_1, a_2) : 3a_2 + \frac{\bar{a}_1}{a_2} = 0 \text{ and } (-3)v_1(9v_1 - 4) \text{ is a square of } F^*_{p^m}\right\}. \tag{5.4}$$

Observe that $\Gamma_2 = \emptyset$ for $p = 3$ and $\Gamma_1 = \emptyset$, when $p = 3$ and $m = 1$. So, Tu and Zeng [68] considered $m \geq 2$, when $p = 3$ and defined the following trinomial for $(s_1, s_2) = (p^m, 2)$ and odd primes p.

Theorem 5.6. *[68] Let $n = 2m$ for a positive integer m and p be an odd prime. Then, the polynomial*

$$f(x) = x + a_1x^{p^m(q-1)+1} + a_2x^{2(q-1)+1}$$

permutes $F_{p^{2m}}$ if $(a_1, a_2) \in \Gamma_1 \cup \Gamma_2$.

The condition mentioned in [66, 68] to construct permutation trinomials of the form

$$f(x) = x + a_1x^{q(q-1)+1} + a_2x^{2(q-1)+1}$$

for $p = 2$ and $p = 3$, respectively, was just a sufficient condition. On this note, Bartoli [4] proved that the condition mentioned in [66] for $p = 2$ was also a necessary condition. And, Hou et al. [33] proved that the conditions mentioned in [68] for $p = 3$ is necessary for $f(x)$ to be a permutation polynomial over F_{q^2}. The conclusion of the proof was that $f(x) = xh(x^{q-1})$ permutes F_{q^2} if and only if

$$g(x) = x(1 + ax^q + bx^2)^{q-1}$$

permutes μ_{q+1}, which is subject to the condition of if and only if $bx^3 + x + a$ has no root in μ_{q+1} and

$$H(x) = \frac{a^qx^3 + x^2 + b^q}{bx^3 + x + a}$$

permutes μ_{q+1}.

Later, Tu and Zeng [67] constructed two classes of permutation trinomials of the form

$$f(x) = x + a_1 x^{s_1(q-1)+1} + a_2 x^{s_2(q-1)+1} \in F_{q^2},$$

for the pair $(s_1, s_2) = (-1/2, 1/2), (3/4, 1/4)$, with general coefficients a_1, a_2. In the following theorem, they mentioned both classes of permutation trinomials over F_{q^2} when $q = 2^m$.

Theorem 5.7. *[67]*

(1) Let $n = 2m$ be a positive integer with $m \geq 3$ and $a_1, a_2 \in F_{2^n}^*$. Then, the trinomial

$$f(x) = x + a_1 x^{2^{m-1}(2^m-1)+1} + a_2 x^{2^{n-1}(2^m-1)+1}$$

permutes F_{2^n} if and only if $a_1 = \bar{a_2}$ and $Tr_1^m(a_1\bar{a_1}) = 0$.

(2) Let $n = 2m$ be a positive integer. Assume that $(a_1, a_2) \in F_{2^n}^* \times F_{2^n}^*$ satisfying that $a_1 = \frac{a_2^2}{a_2}$ and $x^3 + x + \frac{1}{a_2\bar{a_2}} = 0$ has no solution in F_{2^m}. Then,

$$f(x) = x + a_1 x^{\frac{3}{4}(2^m-1)+1} + a_2 x^{\frac{1}{4}(2^m-1)+1}$$

permutes F_{2^n}.

Since the conditions given in Theorem 5.7 case 1 are both sufficient and necessary, the conditions mentioned in Theorem 5.7 case 2 are just sufficient; as a result, Tu and Zeng [67] mentioned it as a conjecture to establish the necessary part.

Hou [34] made the observation that

$$f(x) = x + a_1 x^{\frac{3}{4}(2^m-1)+1} + a_2 x^{\frac{1}{4}(2^m-1)+1} = x^4(1 + ax^{q-1} + bx^{q-1})$$

is a permutation polynomial over F_{q^2} if $a = b$ and $x^3 + x + a^{-1}$ has no root in F_q by applying an appropriate substitution of $x \to ux$ and $a \in F_q^*$, $b \in F_{q^2}^*$ in order to address this conjecture.

Tu and Zeng [68] considered polynomials of the form

$$f_{a,b}(x) = x(1 + ax^{q(q-1)} + bx^{q(q-1)}) \in F_{q^2}[x],$$

where $a, b \in F_{q^2}^*$. This type of polynomial belongs to a more general family of permutation polynomials of F_{q^2}. This family has been investigated in several papers, but only a few have been determined as necessary and sufficient conditions. On this note, Bartoli and Timpanella [8] characterized this general family of permutation trinomials, which was considered in [66–68] for the case of $p > 3$, by using the connections with algebraic curves over finite fields. They proved that the condition mentioned in Theorem 5.6 was not only sufficient, but that it was necessary too.

Following the work on permutation polynomials discussed in [42,45], Deng and Zheng [14] further studied the polynomials of the form

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

by using the technique provided in [30], and they presented new classes of permutation trinomials over $F_{3^{2m}}$. In the following theorem, they discussed permutation trinomials for the pairs $(s, t) = (2/7, 8/7), (-2/7, 8/7)$ over $F_{2^{2m}}$.

Theorem 5.8. *[14] Let $q = 2^m$. The trinomial*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation over F_{q^2} if the following holds:

(1) $\gcd(m, 2) = 1$ *and* $(s, t) = (2/7, 8/7)$,
(2) $m \equiv 2, 4 \pmod 6$ *and* $(s, t) = (-2/7, 8/7)$.

Inspired by the proof of the previous theorem, they presented the following new permutation polynomial for integers n and k_i satisfying that $n \geq 2$, $k_0 = 0$ and $k_i + k_{n-i} = k_n$ for $0 \leq i \leq n$, $q = 2^m$, and that $R(x) = \sum_{i=0}^{n} x^{k_i}$ is a polynomial over F_{q^2}.

Theorem 5.9. *[14] Let r and l be positive integers. Let $h(x)$ be a polynomial over F_{q^2}. Assume that $R(x) \neq 0$ for $x \in \mu_{q+1}$; then, the polynomial*

$$F(x) = x^{r+k_n l} R(x^{q-1})^l h(x^{q-1})$$

permutes F_{q^2} if and only if $\gcd(r + k_n l, q - 1) = 1$ *and the polynomial $g(x) = x^r h(x)^{q-1}$ permutes μ_{q+1}.*

In the following theorem, they constructed permutation trinomials of the form $f(x) = x^{4(q-1)+1} + x^{(q-1)^2+1} - x$ over F_{q^2}, where $q = 3^m$.

Theorem 5.10. *[14] Let m be a positive integer with $m \not\equiv 0 \pmod 6$. Let $q = 3^m$. The polynomial*

$$f(x) = x^{4(q-1)+1} + x^{(q-1)^2+1} - x$$

is a permutation trinomial over F_{q^2}.

During the study, they observed that the polynomial

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation trinomial for the pairs $(s, t) = (4/11, 10/11)$, and m with $\gcd(m, 5) = 1$, over $F_{2^{2m}}$ and proposed as a conjecture.

As it was noted in [75] that their approach cannot be applied to a general characteristic $p > 5$, Cao et al. [11] attempted to extend this inquiry and mentioned another proof of Tu and Zeng's [67] theorem.

They constructed the permutation trinomials of the form

$$f(x) = x + \lambda_1 x^{s(p^k-1)+1} + \lambda_2 x^{t(p^k-1)+1}$$

for the pair (s, t). In the following theorem, they constructed a permutation trinomial $f(x)$ for the pair

$$(s, t) = \left(\frac{q+3}{4}, \frac{q+3}{2}\right).$$

Theorem 5.11. *[11] Let k be a positive odd integer, $q = p^k$, where $p \equiv 5 \pmod 8$ is a prime number. Let*

$$f(x) = x^r + \lambda_1 x^{s(q-1)+r} + \lambda_2 x^{2s(q-1)+r},$$

where $\lambda_1, \lambda_2 \in F_{q^2}$ and r is a positive integer with $\gcd(r, q - 1) = 1$. *Then, $f(x)$ permutes F_{q^2} in the following cases:*

(1) $(\lambda_1, \lambda_2) = (a + b, ab)$, *where* $a, b \in F_{q^2}$, $a \neq b$, $a\bar{b} = 1$ *and* $\gcd(r - 2s, q + 1) = 1$,

(2) $(\lambda_1, \lambda_2) = (a + 1, a)$, *where* $a \in F_q$, $a^2 = -1$ *and* $r = 1$.

The following theorem covers a general proof for the existence of necessary and sufficient conditions for $\lambda_1 = 2a$, with $r = 1$, $t = 2s$ and $\lambda_2 = -1$ required for a polynomial to be a permutation of F_{q^2} with Niho exponents.

Theorem 5.12. *[11] Let* $q = p^k$, *where* $q \equiv 1 \pmod 4$. *Let* $a \in F_q$ *and* $s = \frac{q+3}{4}$. *Then, the trinomial*

$$f(x) = x + 2ax^{s(q-1)+1} - x^{2s(q-1)+1}$$

permutes F_{q^2} *if and only if* $a^4 = 1$.

In the next theorem, they considered

$$(s, t) = \left(\frac{q-1}{2}, \frac{q+3}{2}\right)$$

with $(\lambda_1, \lambda_2) = (a, a)$ and presented two infinite families of permutation trinomials with odd characteristics.

Theorem 5.13. *[11] Let* $q = p^k$, *where* p *is odd prime. Assume that* $a \in F_q$ *is such that* $1 - 4a^2$ *is square in* F_q. *Then,*

$$f(x) = x + ax^{s(q-1)+1} + ax^{t(q-1)+1}$$

permutes F_{q^2} *if and only if one of the following conditions is satisfied:*

(1) $a \neq -1/2$ *when* $q \equiv 1 \pmod 4$,
(2) $a \neq \pm 1/2$ *when* $q \equiv 3 \pmod 4$.

For the same pair

$$(s, t) = \left(\frac{q-1}{2}, \frac{q+3}{2}\right),$$

they presented another class of permutation trinomial of the form

$$f(x) = 2ax + x^{s(q-1)+1} - x^{t(q-1)+1}$$

for the case when $p = 5$, $e \geq 4$ is even and $a = 2$. They also conjectured that this polynomial is not always a permutation polynomial if $a = 1$. For

$$(s, t) = \left(2, \frac{q+3}{2}\right),$$

they presented another class of permutation trinomial of the form

$$f(x) = x^r(1 + x^{s(q-1)} + cx^{t(q-1)})$$

for the case $\gcd(x^2 \pm cx + 1, x^{q+1} - 1) = 1$. Furthermore, they constructed four classes of permutation trinomials:

$$f(x) = x + \lambda_1 x^{s(q-1)+1} + \lambda_2 x^{t(q-1)+1}$$

for some values of λ_1, λ_2, (s, t) and $q = 5^k$. All four classes of these permutation trinomials are listed below.

Theorem 5.14. *[11] Let $q = 5^k$. Then,*

$$f(x) = x + \lambda_1 x^{s(q-1)+1} + \lambda_2 x^{t(q-1)+1}$$

permutes F_{q^2} if one of the following conditions is satisfied:

(1) $(s,t) = \left(\frac{q+3}{2}, q\right)$, $(s,t) = \left(\frac{q+3}{2}, \frac{q+5}{2}\right)$,
  (a) $(\lambda_1, \lambda_2) = (-1,-1)$, *k odd,*
  (b) $(\lambda_1, \lambda_2) = (1,1), (1,-1)$ *k even;*

(2) $(s,t) = \left(2, \frac{q+3}{2}\right)$,
  (a) $(\lambda_1, \lambda_2) = (-1,-1)$, *k odd,*
  (b) $(\lambda_1, \lambda_2) = (1,1), (1,-1)$, *k even,*
  (c) $(\lambda_1, \lambda_2) = (1,2)$.

Transforming the problem into an investigation into some quartic equations over the subfield F_{2^m} and showing that these equations have no solutions in F_{2^m}, Zheng et al. [85] determined two classes of permutation trinomials over F_{2^m}. The following theorem is the first class considered by Zheng et al. when m is odd or $m \equiv 2 \pmod 4$ and $(s,t) = (2/7, 8/7)$.

Theorem 5.15. *[85] Let $n = 2m$ be a positive integer and U be a unit circle of $F_{2^{2m}}$. Then,*

$$f(x) = x + ax^{s(2^m-1)+1} + bx^{t(2^m-1)+1}$$

is a permutation of $F_{2^{2m}}$, if a, b and m satisfy the following conditions:

(1) m is odd, $b \in U$ and $a = b^{\frac{1}{4}}\xi$, where $\xi \in F_{2^m}$ satisfies that $Tr_1^m(1/\xi^{\frac{1}{3}}) = 1$,
(2) $m \equiv 2 \pmod 4$, $b \in U$ and $a = b^{\frac{1}{4}}\xi$, where $\xi \in F_{2^e}$ satisfies that $Tr_1^e(1/\xi^{\frac{1}{3}}) = 1$, and $e = \frac{m}{2}$.

The following class was constructed when m and k are two positive integers satisfying that $k < m$, $\gcd(2^k + 1, 2^m + 1) = 1$ and $(s,t) = \left(\frac{1}{2^k+1}, \frac{2^k}{2^k+1}\right)$.

Theorem 5.16. *[85] Let $n = 2m$ and $d = ord_2(\gcd(m,k))$. Let $a, b \in F_{2^{2m}}^*$. Then,*

$$f(x) = x + ax^{s(2^m-1)+1} + bx^{t(2^m-1)+1}$$

is a permutation of $F_{2^{2m}}$ if a and b satisfy

$$a^{2^m+1} + b^{2^m+1} + 1 \neq 0, \quad \frac{b}{a^{2^m+1} + b^{2^m+1} + 1} = \left(\frac{a}{a^{2^m+1} + b^{2^m+1} + 1}\right)^{2^k}$$

and

$$Tr_{2^d}^m\left(\frac{1}{a^{2^m+1} + b^{2^m+1} + 1}\right) = \frac{m}{2^d}.$$

They have expressed the open problem based on Lemma 1.2 as, under the identical conditions as listed above,

$$f(x) = x(1 + ax^{s(2^m-1)} + bx^{t(2^m-1)})$$

is a permutation of $F_{2^{2m}}$.

Inspired by the idea proposed in [21], Wang et al. [72] constructed six classes of permutation trinomials of the form

$$f(x) = \lambda_1 x + \lambda_2 x^{q(q+1)-1} + \lambda_3 x^{s_1(q-1)+s_2}$$

for $\lambda_1, \lambda_2, \lambda_3 \in \{1, -1\}$ and $s_1, s_2 \in \{0, 1, q, q^2\}$ over F_{q^3}, where $q = 3^k$. Wang et al. [72] used a multivariate method and resultant elimination method to prove that $f(x)$ is a permutation polynomial over F_{q^3}. They characterized three classes of permutation polynomials for the case when $k \not\equiv 1 \pmod 3$, and three classes for the case when $k \not\equiv 2 \pmod 3$. The following theorem included all six classes of the permutation trinomials for all values of $\lambda_1, \lambda_2, \lambda_3$ and s_1, s_2.

Theorem 5.17. *[72] Let $q = 3^k$, where k is a positive integer. Then, $f(x)$ is a permutation trinomial over F_{q^3} for the following cases when $k \not\equiv 1 \pmod 3$:*

(1) $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, -1)$, $(s_1, s_2) = (q, 1)$,
(2) $(\lambda_1, \lambda_2, \lambda_3) = (1, -1, 1)$, $(s_1, s_2) = (q, q)$,
(3) $(\lambda_1, \lambda_2, \lambda_3) = (-1, 1, 1)$, $(s_1, s_2) = (0, q)$,

and the following cases when $k \not\equiv 2 \pmod 3$:

(1) $(\lambda_1, \lambda_2, \lambda_3) = (1, 1, -1)$, $(s_1, s_2) = (q, 1)$,
(2) $(\lambda_1, \lambda_2, \lambda_3) = (1, -1, 1)$, $(s_1, s_2) = (0, q)$,
(3) $(\lambda_1, \lambda_2, \lambda_3) = (-1, 1, 1)$, $(s_1, s_2) = (q, q)$.

In the above theorem, Wang et al. [72] stated all six classes of permutation trinomials for $q = p^k$, where $p = 3$. Later, Bartoli [6] considered the same form for more general values of q, such as $q = p^h$ and $p > 3$. He mentioned sufficient conditions for the pairs (λ_1, λ_2) for which these polynomials permute F_{q^3}. He also determined the lower bound on the number of these pairs by using the techniques based on function field theory, which provides exact estimates of the number of F_q-rational solutions of a particular system of equations. The following theorems contained all four classes of the permutation polynomials and lower bounds on the number of pairs (λ_1, λ_2) for which these polynomials permute F_{q^3}.

Theorem 5.18. *[6] Let $\lambda_1, \lambda_2 \in F_q$ be such that $\lambda_1^3 + \lambda_2^2 - \lambda_2 + 1 = 0$, $\lambda_2 \neq 0, 1$. Suppose that*

$$T^3 + \lambda_1^2 T^2 + (\lambda_1\lambda_2 + \lambda_1)T - 1 \in F_q[T]$$

has no roots in μ_{q^2+q+1}. Then, the following two polynomials are permutation polynomials over F_{q^3}:

(1) $f(x) = x^{q(q+1)-1} + \lambda_1 x^{q(q-1)+1} + \lambda_2 x$,
(2) $f(x) = x^{q(q+1)-1} + \lambda_1 x^{q^2(q-1)+q} + \lambda_2 x$.

There are at least $\frac{q-72\sqrt{q}-95}{6}$ pairs of (λ_1, λ_2) that satisfy the condition that $f(x)$ are permutation trinomials in both of the above cases.

Theorem 5.19. *[6] Let $q \equiv 1 \pmod 3$. If $\lambda_1, \lambda_2 \in F_q$, $\lambda_2^2 + \lambda_2 + 1 = 0$, $h_1(\lambda_1) \neq 0$ and $\lambda_1^3 \neq -1$, then the polynomial*

$$f(x) = x^{q(q+1)-1} + \lambda_1 x^{q^2} - \lambda_2 x$$

is a permutation polynomial over F_{q^3}.

Theorem 5.20. *[6] If $\lambda_1, \lambda_2 \in F_q$, $\lambda_2^2 + \lambda_2 + 1 = 0$ and $\lambda_1^3 \neq -1$ are such that $\lambda_2 T^3 + \lambda_1^2 T^2 + (-\lambda_1\lambda_2 + \lambda_1)T - \lambda_2$ has no roots in μ_{q^2+q+1}, then the polynomial*

$$f(x) = x^{q(q+1)-1} + \lambda_1 x^q - \lambda_2 x$$

is a permutation polynomial over F_{q^3}. Also, there are at least $\frac{q-8\sqrt{q}-50}{3}$ values of λ_1 such that $f(x)$ is a permutation trinomial.

One can find pairs of (s, t) such that

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation polynomial in literature. Nevertheless, a complete value of (s, t) is not known in the literature.

Open problem 2. *Find (s, t) such that*

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}$$

is a permutation polynomial over any given finite field with Niho exponents.

6. Conclusions

In this paper, we surveyed all existing classes of permutation trinomials with all mentioned methodologies. Furthermore, similar methods can be used to generate many new permutation trinomials. We have concluded with remarks and open problems based on recent results on permutation trinomials.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors would like to thank the editor and referees for their valuable comments and suggestions, which improved the quality of this article. The corresponding author acknowledges the Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India for their kind encouragement. The first author is grateful to the UGC-CSIR Grant Commission for their support through grant(No. 201610069412), as well as Manipal Academy of Higher Education for their kind encouragement and support.

Conflict of interest

All authors declare no conflicts of interest that could influence the publication of this paper.

References

1. A. Akbary, D. Ghoica, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.*, **17** (2011), 51–67. https://doi.org/10.1016/j.ffa.2010.10.002
2. T. Bai, Y. Xia, A new class of permutation trinomials constructed from Niho exponents, *Cryptography Commun.*, **10** (2018), 1023–1036. https://doi.org/10.1007/s12095-017-0263-4
3. D. Bartoli, L. Quoos, Permutation polynomials of the type $x^r g(x^s)$ over $F_{q^{2n}}$, *Design Codes Cryptography*, **86** (2018), 1589–1599. https://doi.org/10.1007/s10623-017-0415-8
4. D. Bartoli, On a conjecture about a class of permutation trinomials, *Finite Fields Appl.*, **52** (2018), 30–50. https://doi.org/10.1016/j.ffa.2018.03.003
5. D. Bartoli, M. Giulietti, Permutation polynomials, fractional polynomials, and algebraic curves, *Finite Fields Appl.*, **51** (2018), 1–16. https://doi.org/10.1016/j.ffa.2018.01.001
6. D. Bartoli, Permutation trinomials over F_{q^3}, *Finite Fields Appl.*, **61** (2020), 101597. https://doi.org/10.1016/j.ffa.2019.101597
7. D. Bartoli, M. Timpanella, On trinomials of type $x^{n+m}(1 + AX^{m(q-1)} + BX^{n(q-1)})$, n, m odd, over F_{q^2}, $q = 2^{2s+1}$, *Finite Fields Appl.*, **72** (2021), 101816. https://doi.org/10.1016/j.ffa.2021.101816
8. D. Bartoli, M. Timpanella, A family of permutation trinomials over F_{q^2}, *Finite Fields Appl.*, **70** (2021), 101781. https://doi.org/10.1016/j.ffa.2020.101781
9. G. R. V. Bhatta, B. R. Shankar, A study of permutation polynomials as Latin squares, *Nearrings Nearfields Related Topics*, **2017** (2017), 270–281. https://doi.org/10.1142/9789813207363-0025
10. S. Bhattacharya, S. Sarkar, On some permutation binomials and trinomials over F_{2^n}, *Designs Codes Cryptography*, **82** (2017), 149–160. https://doi.org/10.1007/s10623-016-0229-0
11. X. Cao, X. Hou, J. Mi, S. Xu, More permutation polynomials with Niho exponents which permute F_{q^2}, *Finite Fields Appl.*, **62** (2020), 101626. https://doi.org/10.1016/j.ffa.2019.101626
12. L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.*, **4** (1953), 538. https://doi.org/10.1090/S0002-9939-1953-0055965-8
13. W. Cherowitzo, α-flocks and hyperovals, *Geometriae Dedicata*, **72** (1998), 221–245. https://doi.org/10.1023/A:1005022808718
14. H. Deng, D. Zheng, More classes of permutation trinomials with Niho exponents, *Cryptography Commun.*, **11** (2019), 227–236. https://doi.org/10.1007/s12095-018-0284-7
15. L. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. Math.*, **11** (1896), 65–120. https://doi.org/10.2307/1967217
16. C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Comb. Theory*, **113** (2006), 1526–1535. https://doi.org/10.1016/j.jcta.2005.10.006
17. C. Ding, Cyclic codes from some monomials and trinomials, *SIAM J. Discrete Math.*, **27** (2013), 1977–1994. https://doi.org/10.1137/120882275
18. C. Ding, Z. Zhou, Binary cyclic codes from explicit polynomials over $GF(2m)$, *Discrete Math.*, **321** (2014), 76–89. https://doi.org/10.1016/j.disc.2013.12.020
19. C. Ding, L. Qu, Q. Wang, J. Yuan, P. Yuan, Permutation trinomials over finite fields with even characteristic, *SIAM J. Discrete Math.*, **29** (2015), 79–92. https://doi.org/10.1137/140960153

20. Z. Ding, M. Zieve, Determination of a class of permutation quadrinomials, *Proc. London Math. Soc.*, **127** (2023), 221–260. https://doi.org/10.1112/plms.12540

21. H. Dobbertin, *Uniformly representable permutation polynomials*, Springer, 2022.

22. N. Fernando, X. Hou, S. Lappano, A new approach to permutation polynomials over finite fields, II, *Finite Fields Appl.*, **22** (2013), 122–158. https://doi.org/10.1016/j.ffa.2013.01.001

23. N. Fernando, A note on permutation binomials and trinomials over finite fields, *ArXiv*, 2016. https://doi.org/10.48550/arXiv.1609.07162

24. W. Fulton, *Algebraic curves*, University of Michigan, 1989.

25. H. Guo, S. Wang, H. Song, X. Zhang, J. Liu, A new method of construction of permutation trinomials with coefficients 1, *ArXiv*, 2021. https://doi.org/10.48550/arXiv.2112.14547

26. R. Gupta, R. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.*, **41** (2016), 89–96. https://doi.org/10.1016/j.ffa.2016.05.004

27. C. Hermite, *Sur les fonctions de sept lettres*, Académie Sciences, 1863.

28. X. Hou, A class of permutation binomials over finite fields, *J. Number Theory*, **133** (2013), 3549–3558. https://doi.org/10.1016/j.jnt.2013.04.011

29. X. Hou, A class of permutation trinomials over finite fields, *ArXiv*, 2013. https://doi.org/10.48550/arXiv.1303.0568

30. X. Hou, Determination of a type of permutation trinomials over finite fields, *Acta Arith.*, **3** (2014), 253–278. https://doi.org/10.4064/aa166-3-3

31. X. Hou, Determination of a type of permutation trinomials over finite fields, *II*, *Finite Fields Appl.*, **35** (2015), 16–35. https://doi.org/10.1016/j.ffa.2015.03.002

32. X. Hou, A survey of permutation binomials and trinomials over finite fields, *Contemp. Math.*, **632** (2015), 177–191. https://doi.org/10.1090/conm/632/12628

33. X. Hou, Z. Tu, X. Zeng, Determination of a class of permutation trinomials in characteristic three, *Finite Fields Appl.*, **61** (2020), 101596. https://doi.org/10.1016/j.ffa.2019.101596

34. X. Hou, On the Tu-Zeng permutation trinomial of type $(1/4, 3/4)$, *Discrete Math.*, **344** (2021), 112241. https://doi.org/10.1016/j.disc.2020.112241

35. V. Jarali, P. Poojary, G. R. V. Bhatta, Construction of permutation polynomials using additive and multiplicative characters, *Symmetry*, **14** (2022), 1539. https://doi.org/10.3390/sym14081539

36. G. Khachatrian, M. Kyureghyan, Permutation polynomials and a new public-key encryption, *Discrete Appl. Math.*, **216** (2017), 622–626. https://doi.org/10.1016/j.dam.2015.09.001

37. G. Kyureghyan, M. Zieve, Permutation polynomials of the form $x + \gamma Tr(x^k)$, *ArXiv*, 2016. https://doi.org/10.48550/arXiv.1603.01175

38. J. Lee, Y. Park, Some permuting trinomials over finite fields, *Acta Math. Sci.*, **17** (1997), 250–254. https://doi.org/10.1016/S0252-9602(17)30842-1

39. K. Li, L. Qu, C. Li, S. Fu, New permutation trinomials constructed from fractional polynomials, *Acta Arith.*, **183** (2018), 101–116. https://doi.org/10.4064/aa8461-11-2017

40. K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Appl.*, **43** (2017), 69–85. https://doi.org/10.1016/j.ffa.2016.09.002

41. N. Li, On two conjectures about permutation trinomials over $F_{3^{2k}}$, *Finite Fields Appl.*, **47** (2017), 1–10. https://doi.org/10.1016/j.ffa.2017.05.003

42. N. Li, T. Helleseth, Several classes of permutation trinomials from Niho exponents, *Cryptography Commun.*, **9** (2017), 693–705. https://doi.org/10.1007/s12095-016-0210-9

43. K. Li, L. Qu, X. Chen, C. Li, Permutation polynomials of the form $cx + Tr_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic, *Cryptography Commun.*, **10** (2018), 531–554. https://doi.org/10.1007/s12095-017-0236-7

44. L. Li, C. Li, C. Li, X. Zeng, New classes of complete permutation polynomials, *Finite Fields Appl.*, **55** (2019), 177–201. https://doi.org/10.1016/j.ffa.2018.10.001

45. N. Li, T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *Cryptography Commun.*, **11** (2019), 129–136. https://doi.org/10.1007/s12095-018-0321-6

46. N. Li, X. Zeng, A survey on the applications of Niho exponents, *Cryptography Commun.*, **11** (2019), 509–548. https://doi.org/10.1007/s12095-018-0305-6

47. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, 1997. https://doi.org/10.1017/CBO9781139172769

48. X. Liu, Further results on some classes of permutation polynomials over finite fields, *ArXiv*, 2019. https://doi.org/10.48550/arXiv.1907.03386

49. Q. Liu, Y. Sun, Several classes of permutation trinomials from Niho exponents over finite fields of characteristic 3, *J. Algebra Appl.*, **18** (2019), 1950069. https://doi.org/10.1142/S0219498819500695

50. Q. Liu, X. Liu, J. Zou, A class of new permutation polynomials over F_{2^n}, *J. Math.*, **2021** (2021), 5872429. https://doi.org/10.1155/2021/5872429

51. Q. Liu, Two classes of permutation polynomials with niho exponents over finite fields with even characteristic, *Turk. J. Math.*, **46** (2022), 919–928. https://doi.org/10.55730/1300-0098.3132

52. J. Ma, T. Zhang, T. Feng, G. Ge, Some new results on permutation polynomials over finite fields, *Designs Codes Cryptography*, **83** (2017), 425–443. https://doi.org/10.1007/s10623-016-0236-1

53. J. Ma, G. Ge, A note on permutation polynomials over finite fields, *Finite Fields Appl.*, **48** (2017), 261–270. https://doi.org/10.1016/j.ffa.2017.08.003

54. Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, University of Southern California, 1972.

55. T. Niu, K. Li, L. Qu, Q. Wang, Finding compositional inverses of permutations from the AGW criterion, *IEEE Trans. Inf. Theory*, **67** (2021), 4975–4985. https://doi.org/10.1109/TIT.2021.3089145

56. J. Peng, L. Zheng, C. Wu, H. Kan, Permutation polynomials $x^{2^{k+1}+3} + ax^{2^k+2} + bx$ over $F_{2^{2k}}$ and their differential uniformity, *Sci. China Inf. Sci.*, **63** (2020), 209101. https://doi.org/10.1007/s11432-018-9741-6

57. H. Peter, G. Korchmáros, F. Torres, F. Orihuela, *Algebraic curves over a finite field*, Princeton University Press, 2008.

58. X. Qin, L. Yan, Constructing permutation trinomials via monomials on the subsets of μ_{q+1}, *Appl. Algebra Eng. Commun. Comput.*, **34** (2023), 321–334. https://doi.org/10.1007/s00200-021-00505-8

59. R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, **21** (1978), 120–126. https://doi.org/10.1145/359340.359342

60. R. K. Sharma, R. Gupta, Determination of a type of permutation binomials and trinomials, *Appl. Algebra Eng. Commun. Comput.*, **31** (2020), 65–86. https://doi.org/10.1007/s00200-019-00394-y

61. R. Singh, K. Sarma, A. Saikia, Poly-dragon: an efficient multivariate public key cryptosystem, *J. Math. Cryptology*, **4** (2011), 349–364. https://doi.org/10.1515/jmc.2011.002

62. R. Singh, K. Sarma, A. Saikia, A public key cryptosystem using a group of permutation polynomials, *Tatra Mt. Math. Publ.*, **77** (2020), 139–162. http://doi.org/10.2478/tmmp-2020-0013

63. H. Stichtenoth, *Algebraic function fields and codes*, Springer Science & Business Media, 2009. http://doi.org/10.1007/978-3-540-76878-4

64. Z. Tu, X. Zeng, L. Hu, C. Li, A class of binomial permutation polynomials, *ArXiv*, 2013. https://doi.org/10.48550/arXiv.1310.0337

65. Z. Tu, X. Zeng, L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.*, **25** (2014), 182–193. https://doi.org/10.1016/j.ffa.2013.09.007

66. Z. Tu, X. Zeng, C. Li, T. Helleseth, A class of new permutation trinomials, *Finite Fields Appl.*, **50** (2018), 178–195. https://doi.org/10.1016/j.ffa.2017.11.009

67. Z. Tu, X. Zeng, Two classes of permutation trinomials with Niho exponents, *Finite Fields Appl.*, **53** (2018), 99–112. https://doi.org/10.1016/j.ffa.2018.05.007

68. Z. Tu, X. Zeng, A class of permutation trinomials over finite fields of odd characteristic, *Cryptography Commun.*, **11** (2019), 563–583. https://doi.org/10.1007/s12095-018-0307-4

69. D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{(q-1)}{d}})$ and their group structure, *Monatsh. Math.*, **112** (1991), 149–163. https://doi.org/10.1007/BF01525801

70. Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Springer, 2007.

71. Y. Wang, Z. Zha, W. Zhang, Six new classes of permutation trinomials over $F_{3^{3k}}$, *Appl. Algebra Eng. Commun. Comput.*, **29** (2018), 479–499. https://doi.org/10.1007/s00200-018-0353-3

72. Y. Wang, W. Zhang, Z. Zha, Six new classes of permutation trinomials over $F_{2^n}^*$, *SIAM J. Discrete Math.*, **32** (2018), 1946–1961. https://doi.org/10.1137/17M1156666

73. B. Wu, D. Lin, On constructing complete permutation polynomials over finite fields of even characteristic, *Discrete Appl. Math.*, **184** (2015), 213–222. https://doi.org/10.1016/j.dam.2014.11.008

74. D. Wu, P. Yuan, C. Ding, Y. Ma, Permutation trinomials over F_{2^m}, *Finite Fields Appl.*, **46** (2017), 38–56. https://doi.org/10.1016/j.ffa.2017.03.002

75. G. Wu, N. Li, Several classes of permutation trinomials over F_{5^n} from Niho exponents, *Cryptography Commun.*,**11** (2019), 313–324. https://doi.org/10.1007/s12095-018-0291-8

76. X. Xie, N. Li, L. Xu, X. Zeng, X. Tang, Two new classes of permutation trinomials over F_{q^3} with odd characteristic, *Discrete Math.*, **346** (2023), 113607. https://doi.org/10.1016/j.disc.2023.113607

77. P. Yuan, Compositional inverses of AGW-PPs-dedicated to professor cunsheng ding for his 60th birthday, *Adv. Math. Commun.*, **16** (2022), 1185–1195. https://doi.org/10.3934/amc.2022045

78. P. Yuan, Permutation polynomials and their compositional inverses, *ArXiv*, 2022, https://doi.org/10.48550/arXiv.2206.04252

79. P. Yuan, Local method for compositional inverses of permutational polynomials, *ArXiv*, 2022. https://doi.org/10.48550/arXiv.2211.10083

80. P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.*, **17** (2011), 560–574. https://doi.org/10.1016/j.ffa.2011.04.001

81. P. Yuan, C. Ding, Further results on permutation polynomials over finite fields, *Finite Fields Appl.*, **27** (2014), 88–103. https://doi.org/10.1016/j.ffa.2014.01.006

82. Z. Zha, L. Hu, S. Fan, Further results on permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.*, **45** (2017), 43–52. https://doi.org/10.1016/j.ffa.2016.11.011

83. D. Zheng, M. Yuan, L. Yu, Two types of permutation polynomials with special forms, *Finite Fields Appl.*, **56** (2019), 1–16. https://doi.org/10.1016/j.ffa.2018.10.008

84. L. Zheng, H. Kan, J. Peng, Two classes of permutation trinomials with Niho exponents over finite fields with even characteristic, *Finite Fields Appl.*, **68** (2020), 101754. https://doi.org/10.1016/j.ffa.2020.101754

85. L. Zheng, H. Kan, J. Peng, D. Tang, Two classes of permutation trinomials with Niho exponents, *Finite Fields Appl.*, **70** (2021), 101790. https://doi.org/10.1016/j.ffa.2020.101790

86. L. Zheng, B. Liu, H. Kan, J. Peng, D. Tang, More classes of permutation quadrinomials from niho exponents in characteristic two, *Finite Fields Appl.*, **78** (2022), 101962. https://doi.org/10.1016/j.ffa.2021.101962

87. M. Zieve, On some permutation polynomials over of the form $x^r h(x^{\frac{q-1}{d}})$, *Proc. Amer. Math. Soc.*, **137** (2009), 2209–2216.

88. M. Zieve, Permutation polynomials on F_q induced form R´edei function bijections on subgroups of F_q^*, *ArXiv*, 2013. https://doi.org/10.48550/arXiv.1310.0776

89. M. Zieve, A note on the paper arXiv: 2112.14547, *ArXiv*, 2022. https://doi.org/10.48550/arXiv.2201.01106

AIMS Press

© 2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)