Palestine Journal of Mathematics

Vol 13(Special Issue III)(2024) , 105–123

A recent survey of permutation binomials over finite fields

Varsha Jarali, Prasanna Poojary and Vadiraja Bhatta G.R.*

Communicated by Harikrishnan Panackal

Keywords and phrases: Permutation polynomials, Binomial permutations, Trinomial permutations, Niho-type exponents.

Abstract Permutation polynomials over finite fields are an important research area in which significant progress has been made. Some special polynomials with fewer terms serve more effective applications than a general permutation polynomial. We review the recent substantial contributions to the development of permutation binomials over finite fields. Significant results and unique methodologies are emphasized. The paper is divided into two parts: the existence and nonexistence of permutation binomials.

1 Introduction

Let F_{p^n} 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 the associated mapping $x \to f(x)$ form F_q to F_q is a permutation of F_q. The study of permutation polynomials on finite fields began with Hermite [1], Dickson [2], and Carlitz [3] and since then has been carried out by many other researchers Since then many researchers [42, 5, 6, 7, 37, 9, 10, 11]. The study of permutation polynomials over finite fields have attracted people's interest for many years due to their wide applications in cryptography [12, 13, 14, 15, 16], coding theory [17, 18, 19] and combinatorial designs [20].

By the Lagrange interpolation formula, it is not difficult to construct random permutation polynomials for a given finite field. However, it is difficult to find permutation polynomials with simple or nice algebraic appearance. Permutation polynomials with fewer terms are particularly interesting due to their nice algebraic structure over the finite field. As an illustration, the study of almost perfect nonlinear mappings is important because of their applications in encryption. The monomial x^r is a permutation polynomial over F_q if and only if $\gcd(r, q-1) = 1$. To the same extent as it is difficult to determine the conditions on a, b, n, m and q such that binomials $ax^n + bx^m$ are permutations on F_q. And so are the cases for trinomials and quadrinomials. So far, only a few classes of permutation binomials and trinomials are known in the literature. In 2015 Hou [21] briefly surveyed the known classes of permutation binomials but very few classes of permutation binomials were known at that time. Lately, one can observe increasing interest in the permutation binomials in the last ten years. We follow this development, and survey recent results on these classes of permutation binomials.

The purpose of the present paper is to review some of the recent contributions to the area with more details and background. Our primary focus is on the results of permutation binomials that have appeared in the last ten years. We will also present to the reader a selection process of new approaches and novel methods that have emerged recently. There have been some recent publications on quadrinomials, although there are few classes of permutation quadrinomials that are well-known in the literature. For more information on quadrinomials one can refer [22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34].

A very important class of polynomials whose permutation behavior is well understood in the class of Dickson polynomials, which is defined as let k be a positive integer such that $0 \le k \le p-1$ and $a \in F_{p^n}$. The Dickson polynomial of $(k+1)^{th}$ kind is,

$$D_{n,k}(x,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-a)^k x^{n-2k}. \tag{1.1}$$

The Dickson polynomial $D_n(x, a) \in F_q[x]$ is a permutation polynomial over F_q if and only if either $a = 0$ and $(n, q-1) = 1$ or $a \neq 0$ and $(n, q^2-1) = 1$. The reversed Dickson polynomials $D_n(a, x)$ are reversing the parameter a and variable n in the Dickson polynomial $D_n(x, a)$. In the case of reversed Dickson polynomials $D_n(a, x)(a \neq 0)$ are permutation polynomials over F_q if and only if $D_n(1, x)$ does. But the big open problem with reversed Dickson polynomial $D_n(a, x)(a \neq 0)$ is finding (q, n) such that $D_n(1, x)$ is a permutation over F_q. The following results provide some basic ideas commonly used to prove that a given polynomial is a permutation polynomial.

Hermite-Dickson criteria [1] is one of the familiar methods to construct any kind of permutation polynomials. Hermite first introduced this criterion for a prime field and it was later improved to a general finite field by Dickson.

Lemma 1.1. *(Hermite-Dickson criterion)[1] 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:*

(i) $f(x)$ has exactly one root in F_q,

(ii) for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod p$, the reduction of $f(x^t) \pmod{x^q - x}$ has degree $\leq q-2$.

Reduction to a given binomial $f(x) = x^m + ax^n \in F_q[x]$, where $0 \leq n \leq m \leq q$ and $a \in F_q^*$ using the Hermite's criterion is there exist integers $r, t, d > 0$ with $\gcd(t, q-1) = 1$ and $d|q-1$ such that $f(x^t) \equiv x^r(x^{q-1/d} + a) \pmod{x^q - x}$.

The permutation polynomials of the form $x^r h(x^{(q-1)/d})$ over F_q are interesting and have a connection between permutation polynomials of this type with permutations of the subgroup of order d of F_q^*. The following lemma was first stated by Wan and Lidl [35] and later modified by Wang [36] and Zieve [37].

Lemma 1.2. *[35, 36, 37] 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*

(i) $\gcd(r, (q-1)/d) = 1$ and,

(ii) $x^r h(x)^{(q-1)/d}$ permutes μ_d.

While applying Hermite-Dickson criteria one should deal with the binomial coefficients in the expression of a given polynomial. The following famous theorem was first described by Lucas in his Theorie des Nombreis is very useful to solve binomial coefficients of the polynomials during the expansion.

Theorem 1.3. *[38] Let p be a prime and $n, r_1, r_2, \ldots, r_t$ be non-negative integers such that*

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

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 $\binom{n}{r_1, r_2, \ldots, r_t} \neq 0 \pmod p$ if and only if $\sum_{i=1}^{t} d_{ij} = d_j$, $\forall\, 0 \leq j \leq s$.

Definition 1.4. [71] Two permutation polynomials $f(x)$ and $g(x)$ in $F_q[x]$ are called multiplicative equivalent if there exists an integer $1 \leq d < q-1$ such that $\gcd(d, q-1) = 1$ and $f(x) = g(x^d)$.

To prove any given polynomial is a permutation binomial or trinomial there are several methods. A commonly know method is Hermite-Dickson criteria [1] this is one of the familiar methods to construct any kind of permutation polynomials and while applying this criterion one can make use of Lucas sequence [38] to compute binomial coefficients in the expressions of the polynomial. However, in this method computing the $\sum_{x \in F_q} f(x)^s$ goes a little lengthy and toughest one. To overcome this difficulty recent discoveries include Lemma (1.2). The next method is an elementary approach which involves, letting $f(x) = d$ and $u = cx + d$ then computing u and x and plugging in $f(x) = d$ leads to an equation of u with a lower degree. This method is used often as it would be easy to find solutions to lower-degree equations. Recently, two more methods came into existence to compute permutation binomials and trinomials which are computing fractional polynomial and multivariate methods. Computation of fractional polynomial was initiated in [39] and the multivariate method was introduced by Dobbertin [40]. AGW Criterion is another significant technique to determine a polynomial's permutation property (Akbary, Ghioca, Wang)[see, [42]]. By using a subfield of the finite field and a known polynomial that permutes the subfield, it is possible to test the permutation property of any given polynomial over the finite field.

In addition to the above methods, there is one more method based on the algebraic curves. To investigate the solution of a system of polynomial equations one can use the resultant of two polynomials. To identify the common factor of two polynomials we typically utilize the gcd approach, but in higher-order fields, this may be difficult to find a common divisor for all degree polynomials. Hence, the resultant of those two polynomials can be used for this purpose. From the linear algebra, we know that there is a non-zero solution if and only if the coefficient matrix has zero determinant, for more information one can refer [83]. Concerning the connection between the resultant of two polynomials and deciding whether a polynomial is a permutation polynomial over any field is based on the investigation of the plane algebraic curve $C_f = \frac{f(x)-f(y)}{x-y} = 0$ has no F_{q^2}- rational point (a, b) with $a \neq b$. So, by first factorizing the plane curve in terms of two polynomials $F(x, y)$ and $G(x, y)$ and then finding its resultant $Res(F, G, y)$ we can prove those points do not belong to the curve using the resultant.

The paper is organized as follows, After the introduction, in Section 2 we list all the permutation binomials followed by non-existing results of permutation binomials in Section 3. A review of recent conjectures and open problems is included in Section 2 and Section 3.

2 Existence of permutation binomials and criteria

In this section, we survey all the types of permutation binomial existence results together with some of the proposed conjectures in the recent articles and the methods employed.

Carlitz and Wells [43] studied permutation binomials of the form $x^c(x^{(q-1)/e} + a)$ using the bound on Weil sum of a multiplicative character of F_q. In the following theorem, they let $d = e/q - 1$ and specified sufficiency condition on permutation binomial existence for a large q.

Theorem 2.1. *[43] Let e be a fixed divisor of $q - 1$, $e > 1$. Then for sufficiently large q there exists $a \in F_q$ for which $x(x^d + a)$ is a permutation polynomial.*

Lidl and Niederreiter [44] determined an explicit proof for the construction of permutation binomials using the fact that, for the odd prime and positive integers m and k such that $\frac{m}{\gcd(m,k)}$ is odd, then $x^{p^k} + x$ is a permutation polynomial over F_{p^m}. Using this tool Wan and Lidl [35] constructed permutation polynomial of the form $x^r f(x^{(q-1)/d})$ which is stated in the following lemma.

Lemma 2.2. *[35] If $n \geq 2$ is an integer such that $q \equiv 1 \pmod{n}$, then $x^{(q+n-1)/n} + bx \in F_q[x]$ is a permutation polynomial of F_q if and only if following hold:*

(i) $(-b)^n \neq 1$,

(ii) $\psi_n((b + \omega^i)(b + \omega^j)^{-1}) \neq \omega^{j-i}$ *for all $0 \leq i < j < n$, where ω is fixed primitive n^{th} root of unity in F_q.*

From the following corollary, one can extract permutation binomials and trinomials for $k = 1$ and $k = 2$ respectively.

Corollary 2.3. *[35] Let d be a positive integer to satisfy that $d/q - 1$. Let $f(x) \in F_q[x]$ be a polynomial. For sufficiently large q, there is an element $a \in F_q$ such that the polynomial $g(x) = x^r(f(x^{(q-1)/d}) + a)^k$ is a permutation polynomial of F_q for all $k \geq 1$ and $\gcd(r, q - 1) = 1$.*

As of now, we have read that having exactly one root in F_q is a necessary but not sufficient condition for permutation polynomials. We can take example of cyclotomic polynomials $\phi_3 = x^2 + x + 1$ over F_3 to contradict this thought. Mollin and Small [81] characterized one particular class of permutation binomial i.e., cyclotomic polynomial $\phi_m(x)$ over F_q which is permutation polynomial over F_q if and only if either $m = 2$ or both q and m are power of 2. They defined permutation binomials in terms of their coefficients in the subsequent theorem.

Theorem 2.4. *[81] Suppose k and j are positive integers such that $q > k > j \geq 1$ and $\gcd(k-j, q-1) = 1$. Then $ax^k + bx^j + c$ with $a \neq 0$ is a permutation of F_q if and only if $\gcd(k, q-1) = 1$ and $b = 0$.*

This theorem was proved using the fact that $ax^k + bx^j + c$ is a permutation polynomial if and only if $x^k + a^{-1}bx^j$ is a permutation polynomial. They have considered two cases $\alpha = 0$ and $\alpha \neq 0$ for $\alpha = -a^{-1}b$. Consequently, this leads to the fact that $ax^2 + bx + c(a \neq 0)$ is a permutation polynomial over F_q if and only if $b = 0$ and the characteristic of F_q is 2.

Followed by the element $o \neq \alpha = -a^{-1}b \in F_q$ chosen in [81], Small [82] considered binomial $f(x) = x^i - \alpha x^j, i > j > 1$ and proved that polynomial $f(x) = x^i - \alpha x^j$ of the degree i, where $1 < i|q-1$ doesn't permute F_q. Based on the results proved in his paper he made observations that polynomials of the form $f(x) = ax^i + bx^j + c$ is a permutation polynomial in the following cases,

(i) f permutes F_q if and only if $x^i - \alpha x^j$ does, where $\alpha = -a^{-1}b \neq 0$, $i > j > 1$ with assumption that $i < q-1$ and α is not an $(i-j)^{th}$ power.

(ii) If $\gcd(i, j) = 1$ and $i \not| q-1$.

(iii) For $k = i - j$ with assumptions that $d = \gcd(k, q-1) > 1$ and $\alpha^{(q-1)/d} \neq 1$ and either $i \not| q-1+k$ or $p| \gcd(k-1, (q-1+k)/i)$.

By using the Lucas sequence to calculate the sum of the coefficients of the polynomials and the following criteria, Akbary and Wang [45] considered the binomials of the type $x^r + x^u$ and demonstrated that they are permutation binomials over F_q. Let p be an odd prime, $q = p^m$ and l is a odd positive integer with $p \equiv -1 \pmod 1$ or $p \equiv 1 \pmod l$ and $l|m$,

$$(*)\ (r, s) = 1, (e, l) = 1, l \text{ odd}.$$

Theorem 2.5. *[45] Let p be an odd prime and $q = p^m$. Let l be an odd positive integer. Let $p \equiv -1 \pmod 1$ or $p \equiv 1 \pmod 1$ and $l|m$. Under the conditions (*) on r, e, l and s the binomial $P(x) = x^r(1 + x^{es})$ is a permutation binomial of F_q if and only if $(2r + es, l) = 1$.*

They established the existence of $\frac{\phi(l)\phi(q-1)}{2}$ number of permutation binomials of the form $P(x) = x^r(1 + x^{es})$ over F_q under the same assumptions as Theorem (2.5) on q and l .

Charpin and Kyureghyan [46] constructed permutation binomials of the form $x^{2^k+2} + \nu x$ over F_{2^t} and determined all the parameters $0 \leq k \leq n-1$ and $\nu \neq 0$ in the following theorem.

Theorem 2.6. *[46] Let $0 \leq k \leq n-1$ and $\nu \neq 0$. Then $f(x) = x^{2^k+2} + \nu x$ in $F_{2^t}[x]$ is a permutation polynomial of F_{2^t} if and only if t is even and*

(i) either $k = 1$ and ν is not a third power in F_{2^t}, or

(ii) $t = 2r$, $r \geq 3$ with r odd, $k = r$, and $\nu \in \omega F_{2^r}$, where $\omega \in F_{2^2} \backslash F_2$.

In the following lemma, they considered t to be even, $\frac{t}{\gcd(t,k)}$ is even and k is odd.

Lemma 2.7. *[46] Let $\nu \in F_{2^t}$, $2 \leq k \leq t-1$ and $f(x) = x^{2^k+2} + \nu x$ be the given polynomial in $F_{2^t}[x]$. Take $c = \gcd(t, k-1)$. Then $f(x)$ is a permutation polynomial of F_{2^t} if and only if $\frac{t}{c}$ is odd and $T_c^t(\gamma^{2^k}\nu) \neq 1$ for every γ in F_{2^t}.*

Lemma (1.2) has been used to generate the majority of permutation polynomials; it enhances the construction of permutation polynomials over extension fields by well-known permutation polynomials over sub-fields like F_p or $\mu_{(q+1)}$. Zieves [47] created various binomials and trinomials based on this idea, and he also provided an answer to a conjecture put out by Wu and Lin [48]. In the subsequent corollary, he constructed a $(q+2)$ degree permutation polynomial over F_{q^2} using a degree 3 permutation polynomial over F_q.

Corollary 2.8. *[47] Pick $\alpha \in F_{q^2}^*$ and write $f_\alpha(x) = x^{q+2} + \alpha x$. Then $f_\alpha(x)$ permutes F_{q^2} if and only if one of the following occurs:*

(i) $q \equiv 5 \pmod 6$ and α^{q-1} has order 6,

(ii) $q \equiv 2 \pmod 6$ *and* α^{q-1} *has order* 3, *or*

(iii) $q \equiv 0 \pmod 3$ *and* $\alpha^{q-1} = -1$.

He provided $(q^2 + q + 2)$ degree permutation polynomials over F_{q^3} by using a degree 4 permutation polynomial over F_q in the next corollary.

Corollary 2.9. *[47] Let q be a prime power. For $\alpha \in F_{q^3}^*$, the $f(x) = x^{q^2+q+2} + \alpha x$ permutes F_{q^3} if and only if one of the following occurs:*

(i) q *is even and* $\alpha^{q^2} + \alpha^q + \alpha = 0$,

(ii) $q = 7$ *and* $\alpha^{18} + 4\alpha^{12} + 2 = 0$,

(iii) $q = 3$ *and* $\alpha^{12} + \alpha^{10} + \alpha^4 + 1 = 0$,

(iv) $q = 2$ *and* $\alpha \neq 1$.

By Lemma (1.2), $f(x) = x^{q^2+q+2} + \alpha x$ permutes F_{q^3} if and only if $g_\alpha(x) = x(x+\alpha)(x+\alpha^q)(x+\alpha^{q^2})$ permutes F_q, remaining conditions never occurs if q is odd except 3 and 7. In the following corollary, he considered binomial $f(x) = x^{2q+3} + \alpha x$ over F_{q^2} and determined its permutation behavior for all the possible values of q. Sharma and Gupta [49] came up with the same set of conditions on q and α but with different techniques to prove the binomial $f(x) = x^{2q+3} + \alpha x$ is a permutation binomial over F_{q^2}.

Corollary 2.10. *[47] Pick $\alpha \in F_{q^2}^*$ and write $f(x) = x^{2q+3} + \alpha x$. Then $f(x)$ permutes F_{q^2} if and only if one of the following holds:*

(i) $q = \pm 2 \pmod 5$ *and* $\alpha^{2q-2} - 3\alpha^{q-1} + 1 = 0$,

(ii) $q = 5^n$ *and either* $\alpha^{q-1} = -1$ *or* $\alpha^{(q-1)/2} = -1$,

(iii) $q = 13$ *and* $\alpha^{12} - 3\alpha^6 + 1 = 0$,

(iv) $q = 5$ *and* $\alpha^4 - \alpha^2 + 1 = 0$, *or*

(v) $q = 3$ *and either* $\alpha = 1$ *or* $\alpha^2 = -1$.

Remark 2.11. Using the Lemma (2.2) Bassalygo and Zinoviev [50] came out with different conditions for the permutation binomials of the form $x^{q+2} + \alpha x$ over F_{q^2} and polynomial of the form $x^{q^2+q+2} + \alpha x$ over F_{q^3} which were constructed by Zieve [47]. Using Lemma (2.2) they have proved $x^{q+2} + \alpha x$ permutes F_{q^2} and $f(x) = x^{q^2+q+2} + \alpha x$ permutes F_{q^3} for all values of q when $\alpha \in F_{q^2} \backslash F_q$.

Further, they have obtained another proof of the results mentioned in[46, 51] and strengthened the results obtained in [52, 53]. In the Lemma (2.2) by replacing $x = \omega^i$, $y = \omega^j$ for the $n = q - 1$ the condition $(-\alpha)^n \neq 1$ implies $\alpha \in F_{q^2} \backslash F_q$. Substituting these assumptions in (2) case of Lemma (2.2) they have obtained $x(\alpha^q + x)(\alpha + x) - y(\alpha^q + y)(\alpha + y) = 0$, so by showing that this equation does not have any solution in F_q for all $x, y \in F_q$ such that $x \neq 0$, $y \neq 0$, $x \neq y$ they have constructed permutation binomials of the form $x^{q+2} + \alpha x$ over F_{q^2}. Similarly, in the case of F_{q^3} for the polynomial $x^{q^2+q+2} + \alpha x$ in the Lemma (2.2) if we replace $x = \omega^i$, $y = \omega^j$ for the $n = q - 1$ the condition $(-\alpha)^n \neq 1$ implies $\alpha \in F_{q^2} \backslash F_q$. Then $x(\alpha^{q^2} + x)(\alpha^q + x)(\alpha + x) - y(\alpha^{q^2} + y)(\alpha^q + y)(\alpha + y) = 0$ has no solution in F_q for all $x, y \in F_q$ such that $x \neq 0$, $y \neq 0$, $x \neq y$.

Proposition 2.12. *[50] The polynomial $x^{q+2} + \alpha x$ is a permutation over F_{q^2} if and only if $\alpha \in F_{q^2} \backslash F_q$ and the equation $(x+y)^2 + (x+y)(\alpha + \alpha^q) + \alpha^{q+1} - xy = 0$ has no solution in F_q for all $x, y \in F_q$ such that $x \neq 0$, $y \neq 0$, $x \neq y$.*

Also, the author described the same field with even and odd scenarios and offered a different strategy for the results found in [46, 51].

Using the computation of permutation polynomials of the form $x^l g(x^{\frac{p^n-1}{p^k-1}+1})$ proposed in [47](Theorem 1.1) Wu et al. [54] stated the following lemma to determine permutation binomial $x^d + ax$ over F_{p^n}.

Lemma 2.13. *[54] Let n, r, k be integers such that $n = rk$, $d = \frac{p^{rk}-1}{p^k-1} + 1$ and $a \in F_{p^n}$. Then $x^d + ax \in F_{p^n}[x]$ is a permutation polynomial over F_{p^n} if and only if $h_\alpha(x) = x\sum_{i=0}^{r}(x + a^{p^{ik}}) \in F_{p^k}$ is a permutation over F_{p^k}.*

Following the work of Akbhary and Wang [45] on the generalized Lucas sequence, Wang [36] characterized a class of permutation binomials in terms of the generalized Lucas sequence and established a strong relationship between permutation binomials and the generalized Lucas sequence.

In the following theorem Wang [36] proved binomials of the form $x^r(x^{es}+1)$ are permutation polynomials over F_q.

Theorem 2.14. *[36] Let p be an odd prime and $q = p^m$. Assume that l, s, r, e are positive integers such that l is odd, $q - 1 = ls$ and $(e, l) = 1$. Then $p(x) = x^r(x^{es} + 1)$ is a permutation polynomial over F_q if and only if*

(i) $(r, s) = 1$,

(ii) $2^s \equiv 1 \pmod p$,

(iii) $2r + es \not\equiv 0 \pmod 1$,

(iv) $\sum_{k=0}^{cj/2} \frac{cj}{cj-k}\binom{cj-k}{k}(-1)^k a_{cs+cj-2k} = -1 \in F_p$ *for all* $c = 1, \ldots, l-1$, *where* $\{a_n\}_{n=0}^{\infty}$ *is the generalized Lucas sequence of order* $(l-1)/2$ *and* $2e^{\phi(l)-1}r + s \equiv j \pmod{21}$.

Later, Zieve [37] came up with a fresh approach to the Lucas sequence a_n, but he didn't change any of the prerequisites; rather, he demonstrated that when Akbary and Wang's [45] requirements for a_n were met, Zieve's general assumptions were also met. In the consecutive theorem, he provided adequate conditions for permutation binomials.

Theorem 2.15. *[37] Pick $u > r > 0$ and $a \in F_q^*$. Write $s = \gcd(u - r, q - 1)$ and $d = (q - 1)/s$. Suppose that $(\eta + a/\eta) \in \mu_s$ for every $\eta \in \mu_{2d}$. Then $x^u + ax^r$ permutes F_q if and only if $-a \notin \mu_d$, $\gcd(r, s) = 1$ and $\gcd(2d, u + r) \le 2$.*

Masuda and Zieve [56] considered binomials of the form $x^m + ax^n$ over F_p, where $m > n > 0$, $a \in F_p^*$ and characterized bound on p based on Carlitz–Well's existence result (with $k = 1$).

Theorem 2.16. *[56] $f(x) = x^m + ax^n$ over F_p, where $m > n > 0$, $a \in F_p^*$ is a permutation binomial over F_p then*

(i) *either* $q \le (m-2)^4 + 4m - 4$ *or* $m = np^i$,

(ii) $p - 1 \le (m-1) \cdot max(n, \gcd(m-n, p-1))$,

(iii) $\gcd(m-n, p-1) \ge \sqrt{p - (\frac{3}{4})} - (\frac{1}{2}) > \sqrt{p} - 1$.

For the 3^{rd} condition of the above theorem was improvised and verified through the computer for $p < 10^5$ it gives $gcd(m-n, p-1) \ge p/(2\log p)$.

But there doesn't exist any permutation binomial $f(x) = x^m + ax^n$ over F_q, where $m > n > 0$, $a \in F_q^*$ such that $gcd(m-n, p-1) \le q/(2\log q)$ for at least sufficiently large q. Later author found number T is a values of $a \in F_q$ for which $f(x) = x^m + ax^n$ is a permutation binomial as follows,

$$\frac{q - 2\sqrt{q} + 1}{r^{r-1}} - (r-3)\sqrt{q} - 2 \le \frac{T}{(r-1)!} \le \frac{q + 2\sqrt{q} + 1}{r^{r-1}} + (r-3)\sqrt{q}$$

Ayad et al. [55] considered permutation binomials of the form $f(x) = ax^n + x^m$ and computed the bound on p by taking condition $\gcd(n-m, p-1)$, which was improved case of Zieve's theorems [56]

Theorem 2.17. *[55] If $f(x) = ax^n + x^m$ permutes F_p, where $n > m > 0$ and $a \in F_p^*$. Let $d = \gcd(n-m, q-1)$ then $(p-1) \le (d-1) \cdot d$*

When $m = 1$ and $n-1|p-1$ implies $p-1 \leq (n-1)(n-3)$ which improves 2^{nd} case of Theorem (2.16). The author obtained the following corollary to generate permutation binomials, similar to that of Hermite's criterion for prime fields and Dickson's for general cases were used to obtain permutation polynomials.

Corollary 2.18. *[55] Let $f(x) = ax^n + x^m \in F_q[x]$ such that $a \neq 0$ and $\gcd(m,n) = 1$. Let $d = \gcd(n-m, q-1)$. Suppose that $d \geq 2$. Then $f(x)$ is a permutation polynomial of F_q if and only if*

(i) $f(x) = 0$ has a unique solution in F_q,

(ii) for every $l \in \{1,\ldots,q-2\}$ such that $d|l$, where $deg f^l\bar{(}x) \leq (q-2)$.

Based on the criterion stated by Wan and Lidl [35] for the construction of permutation polynomials of the form $x^r h(x^{q-1/n})$, Sarkar et al. [51] determined the existence of permutation binomials and the number of permutation binomials. Meanwhile, he also extended the work of Carlitz [57]. In the following proposition, they characterized permutation polynomials of the form $x^{\frac{2^n-1}{3}+1} + ax$ over the field of characteristic 2. Moreover, they concluded that for every integer $n = 2^i t$, where $t > 2$ odd and integer $n = 2^i$ where $i > 2$, binomial of the form $f(x) = x(x^{\frac{2^n-1}{3}} + a)$ always exists.

Proposition 2.19. *[51] Let $n = 2k$, $k > 2$ be any integer. Then $f(x) = x(x^{\frac{2^n-1}{3}} + a)$ is a permutation polynomial over F_{2^n} if and only if the elements $(1+a)^{\frac{2^n-1}{3}}, \omega(\omega+a)^{\frac{2^n-1}{3}}, \omega^2(\omega^2 + a)^{\frac{2^n-1}{3}}$ are all distinct.*

Applying the criteria for construction permutation polynomials in terms of the additive characteristics of the underlining finite field as described in [38], as well as based the computations on the Walsh spectrum of any Boolean function on F_{2^n}, binomial permutation polynomials were created by Tu et al. [58]. They made use of the lemma in [see Lemma, [38]] which explains how additive exponent sum and permutation polynomials are related. The author made various assumptions, such as that for an even integer n, an integer $t \geq 2$, the polynomials of the form $f(x) = \sum_{i=1}^{t} u_i x^{d_i}$ for each i, $1 \leq i \leq t$, $u_i \in F_{2^n}$ and $d_i \equiv e \pmod{2^{\frac{n}{2}} - 1}$ for a positive integer e. With this assumption $\sum_{x \in F_{2^n}} (-1)^{Tr_i^n(\gamma f(x))}$ reduces to $\sum_{x \in F_{2^n}} (-1)^{Tr_i^n(x^{d_1} + \sum_{i=2}^{t} u_i \delta^{d_1 - d_i} x^{d_i})}$ for any non-zero $\gamma \in F_{2^n}$ can be represented on δ^{d_i} for a unique non-zero $\delta \in F_{2^n}$.

Now we recall unit circle of $F_{2^{2m}}$, basically, it is a set

$$U = \{\lambda \in F_{2^{2m}} : \lambda^{2^m+1} = 1\}. \tag{2.1}$$

Let $N(w_2, w_3, \ldots, w_t)$ is a number of λ's in U such that $\lambda^{d_1} + \sum_{i=2}^{t} w_i \lambda^{d_i} + (\lambda^{d_1} + \sum_{i=2}^{t} w_i \lambda^{d_i})^{2^m} = 0$, for $w_2, w_3, \ldots, w_t \in F_{2^n}$ and remaining conditions on d_i and i are same as defined above. In the next theorem, they proved binomial of the form $x^{d_1} + ux^{d_2}$ is a permutation polynomial.

Theorem 2.20. *[58] Let positive integers n, m, e, s, l, d_1 and d_2 satisfy $n = 2m$, $d_1 = s(2^m - 1) + e$, $d_2 = (s-l)(2^m-1) + e$ and $\gcd(d_1, 2^n - 1) = 1$ then the polynomial $x^{d_1} + ux^{d_2}$ is a permutation polynomial over F_{2^n} if the following conditions are satisfied:*

(i) $r = \gcd(l, 2^m + 1) > 1$,

(ii) $\gcd(e + l - 2s, 2^m + 1) = 1$,

(iii) $u \in U \backslash U^r$, where $U^r = \{v^r : v \in U\}$.

The same binomials are permutation polynomials over F_{2^n} even if $d_2 = 1$.

Similarly, author proved binomial $x^{d_1} + ux^{d_2}$ for $n = 2m$, $d_1 = s(2^m-1) + e$, $d_2 = (s-l)(2^m-1) + e$ and $\gcd(d_1, 2^n-1) = 1$ is a permutation polynomial over F_{2^n} with three non-negative integers k_1, k_2, k_3 with certain conditions on e, s, l in [see proposition 1, [58]]. Further, the author put forward the following conjecture regarding two classes of trinomials. For the case of $q = 2^{2m+1}$ it was later answered by Zieve [59].

Conjecture 2.21. [58] For an odd integer m, $n = 2m$,

$$f(x) = x^{2^m+4} + x^{2^{m+1}+3} + x^{2^{m+2}+1}, \tag{2.2}$$

$$g(x) = x^{2^m} + x^{2^{m+1}-1} + x^{2^{2m}-2^m+1}, \tag{2.3}$$

are permutation polynomials over F_{2^n}.

For a positive integer d and $a \in F_q^*$, a monomial function ax^d is a complete permutation polynomial over F_q if and only if $\gcd(d, q-1) = 1$ and $ax^d + x$ is a permutation polynomial over F_q and such d is called as complete permutation polynomial exponent. Wu et al. [53] studied four classes of complete permutation polynomials for four different complete permutation polynomial exponents. Together with that they constructed binomial permutations over F_{2^n} of the form $x^d + ax$ for $a \notin F_{2^k}^*$ and the exponents $d = \frac{2^{rk}-1}{2^k-1} + 1$, where $\gcd(d-1, 2^k-1) = \gcd(r, 2^k-1) = 1$. Later Bhattacharya and Sarkar [60] observed that for $a \in F_{2^{2t}}^*$, $x^{\frac{2^{4t}-1}{2^t-1}+1} + ax$ is a permutation binomial over $F_{2^{4t}}$, but there is no such $a \in F_{2^{2t}}^*$ such that $x^{\frac{2^{8t}-1}{2^t-1}+1} + ax$ is a permutation binomial over $F_{2^{8t}}$. Later independently, Bassalygo and Zinoviev [61] proved that when $t \geq 4$ and even $x^{\frac{2^{4t}-1}{2^t-1}+1} + ax$ is not a permutation binomial over $F_{2^{4t}}$ but it is when $t \geq 3$ and odd.

After some time Bhattacharya and Sarkar [60] computed permutation binomials of the form $x^{\frac{2^n-1}{2^t-1}+1} + ax \in F_{2^n}[x]$, $n = 2^s t$, $a \in F_{2^{2t}}^*$ which is generalization of the forms discussed in [48, 61] as well they computed permutation trinomials of the form $x^{2^s+1} + x^{2^{s-1}+1} + \alpha x \in F_{2^t}[x]$, where s, t are positive integers.

Theorem 2.22. *[60] Let s, t be positive integers and $n = 2^s t$. Then the polynomial $x^{\frac{2^n-1}{2^t-1}+1} + ax \in F_{2^n}[x]$, where $a \in F_{2^{2t}}^*$ is a permutation polynomial of F_{2^n} if and only if*

(i) t is odd,

(ii) $s \in \{1, 2\}$ and

(iii) $a \in \omega F_{2^t}^* \cup \omega^2 F_{2^t}^*$, where $\omega \in F_{2^2}$ is a root of the equation $\omega^2 + \omega + 1 = 0$.

In addition to the aforementioned theorem, they discovered that there are $2(2^t - 1)$ a's in $F_{2^{2t}}$ for odd t such that $x^{\frac{2^n-1}{2^t-1}+1} + ax \in F_{2^n}[x]$ is a permutation binomial.

Using the concept of reversed Dickson polynomials of $(k+1)^{th}$ kind, Fernando [62] extracted permutation binomials and trinomials when $n = p^l + 2$, where $l \in N$. In the following theorem, we state their permutation binomial of the form $x^n + x$.

Theorem 2.23. *[62] Let $p = 3$ and $q = 3^e$, where e is a non-negative integer. Let $f(x) = x^{\frac{p^l-1}{2}} + x$. Then $f(x)$ is a permutation polynomial of F_q if and only if*

(i) $l = 0$, or

(ii) $l = me + 1$, where m is a non-negative even integer.

It is typically challenging to consider any binomials and trinomials of the form $x^r h(x^{q+1})$ without making any additional assumptions about the coefficients. Sharma and Gupta [49] established the requirements for the coefficients that are both necessary and sufficient for such polynomials to be permutation polynomials. They have considered permutation binomials of the form $x^r h(x^{q+1})$, where $h(x) = x + a$ for $r = 1, 2, 3, 4$ and $h(x) = x^2 + a$ for $r = 1, 2$ and trinomials with $h(x) = x^2 + bx + a$ for $r = 1, 2$. The trinomials with $h(x) = x^2 + bx + a$ for $r = 1, 2$. By Lemma (1.2) $f(x) = x^r(x^{k(q+1)+a})$ permutes F_{q^2} if and only if $\gcd(r, q+1) = 1$ and $g(x) = x^r(x^k + a)^{q+1}$ permutes $\mu_{q+1} = F_q^*$ if and only if $g(x)$ permutes F_q. $g(x)$ can be further simply as, for $\alpha \in F_q$ we have $\alpha^q = \alpha$, therefore $g(\alpha) = \alpha^r(\alpha^{2k} + (a^q + a)\alpha^k + a^{q+1})$. If $a_1 = a^q + a$, and $a_2 = a^{q+1}$ then $G(x) = x^r(x^{2k} + a_1 x^k + a_2)$. Using all these techniques Sharma and Gupta stated the following theorems. In the following theorem they have considered $f(x) = x^r h(x^{q+1})$, where $h(x) = x + a$ for $r = 1, 2, 3, 4$.

Theorem 2.24. *[49] The polynomial $f(x) = x^r h(x^{q+1})$, where $h(x) = x + a$ permutes F_{q^2} if and only if*

(i) $r = 2$, $q = 2$ *and* $a \neq 1$,

(ii) $r = 3$, *either* $q = 2$ *and* $a \neq 1$ *or* $q = 3$ *and* $a^2 = -1$,

(iii) $r = 4$, $q = 2$ *and* $a \neq 1$.

In the next theorem, they have taken $h(x) = a + x^2$ and $r = 2$.

Theorem 2.25. *[49] The polynomial $f(x) = ax^2 + x^{2q+4}$ permutes F_q if and only if q is even, $q \equiv 2 \pmod 3$ and $a^{2(q-1)} + a^{q-1} + 1 = 0$.*

Very recently, some of the results were listed on the permutation binomials of the form $f_{q,r,t,a} = x^r(a + x^{t(q-1)})$ over F_{q^2}, where $1 \leq r \leq q^2 - 2$, $1 \leq t \leq q$ and $a \in F^*_{q^2}$. A necessary condition for $f_{q,r,t,a}$ to be a permutation polynomial of F_{q^2} is that $\gcd(r, q-1) = 1$. If $p = charF_q$ divides t then $f_{q,r,t,a}(x) = f_{q,r',t,a}(x^p) \pmod{x^p - x}$, where $1 \leq r' \leq q^2 - 2$ is such that $r'p \equiv r \pmod{q^2 - 1}$, which implies $f_{q,r,t,a}(x) = f_{q,r',t,a}(x^d)$, where $d = \gcd(r, t)$ and another necessary condition for $f_{q,r,t,a}$ to be a permutation polynomial of F_{q^2} is that $(-a)^{(q+1)/\gcd(q+1,t)} \neq 1$. Concerned with permutation binomials of the form $f = ax^r + x^{t(q-1)+r}$, the necessary and sufficient conditions on (q, r, t, a) for f to be a permutation polynomial are not known completely. Many studies on permutation binomials [59, 63, 64, 65, 66] have been conducted under these circumstances. More specifically, Hou [**?**] considered $e = 2$, Liu [67] took $e = 3$ and odd q and both of them proved that $f(x) = x^r(x^{q-1} + a)$ is a permutation polynomial over F_{q^e}. In addition, Masuda et al. [68] described similar permutation binomials over F_{q^e} for $e \in \{2, 3, 4\}$ and also over F_{p^e} when $e \in \{5, 6\}$. Hou [64]confirmed that when $r = 1$ and $t > 2$ there are only finitely many (q, a) with conditions $a^{q+1} \neq 1$ and $\gcd(rp, t(q-1)) = 1$ such that $f_{q,r,t,a}$ is a permutation polynomial of F_{q^2} . Firstly, Hou [63] studied binomials of the form $ax + x^{2q-1}$ its equivalent form was conjectured, that originated from certain permutation polynomials over finite fields defined by functional equations. Moreover, Hou [**?**] determined an infinite family of permutation binomials for $r = 1, 3$ and $t = 2$ over F_{q^2}. Together with that, he proved, that if $r > 3$ and q is not too small relative to r then f is not a permutation of F_{q^2}. In the following table, we list all the possible conditions on (q, r, t, a) for which the binomial $f = ax^r + x^{t(q-1)+r}$ is a permutation polynomial over F_{q^2}.

Table 1. conditions on (q, r, t, a) for which the $f = ax^r + x^{t(q-1)+r}$ is a permutation polynomial over F_{q^2}.

q	r	t	a	$f_{q,r,t,a}$	**ref**
$q+1 \equiv 0 \pmod{t}$ q odd	1 1	$t > 2$ fixed prime $t = 2$	$a^{q+1} \neq 1$ $-a^{q+1} \neq -1$ or 3	$f_{q,1,t,a}$ $f_{q,1,2,a}$	[64] [64]
q power of a prime $q \equiv \pm 1 \pmod{12}$ $q \equiv 1 \pmod{4}$ $q \equiv -1 \pmod{6}$	1	2	$a = -3$ $a = 1$ $a = 3$	$f_{q,1,2,a}$ over F_q	[63]
q is odd	1	2	$(-a)^{(q+1)/2} = -1$ or 3	$f_{q,1,2,a}$	[69]
	1	2	$(-a)^{(q+1)/2} = 3$	$f_{q,1,2,a}$	[?]
$q = 2^e$, e odd	1	3	$a^{\frac{q+1}{3}}$ primitive 3rd root of unity and $a^{q+1} = 1$	$f_{q,1,3,a}$	[66]
$q \geq 5$, $q = 2^{4k+2}$ $q \geq 7$	1	5 7	$a^{(q+1)/5} \neq 1$	$f_{q,1,5,a}$ Theorem(2.26), $f_{q,1,7,a}$ Theorem(2.27)	[65]
q odd, $q \not\equiv 1 \pmod{3}$	3	2	$(-a)^{(q+1)/2} = -1$ or $1/3$	$f_{q,3,2,a}$	
	3	2	$(-a)^{(q+1)/2} = 1/3$	$f_{q,3,2,a}$	[?]
$q+1 \mid r-1$	$r \geq 1$ and $\gcd(r, q-1) = 1$	1	$a^{q+1} \neq 1$	$f_{q,r,1,a}$	[?]
$q = 2^m$, $m \geq 4$ even	$\gcd(r, q-1) = 1$ and $r \equiv 3 \pmod{q+1}$	3	$a^{q+1} \neq 1$	$f_{q,r,3,a}$ Theorem(2.38)	[70]
$q = 2^m$, $m \geq 5$ odd	$\gcd(r, 3(q-1)) = \gcd(r-3, q+1) = 1$	3	$a^{(q+1)/3}$ primitive 3rd root of unity	$f_{q,r,3,a}$ Theorem(2.39)	[70]
	$\gcd(r, q-1) = 1$	$\gcd(r-t, q+1) = 1$	$(-a)^{(q+1)\gcd(q+1,t)} \neq 1$	$f_{q,r,t,a}$	[59]
		$\gcd(r-t, q+1) = 1$	$a^{q+1} = 1$	$f_{q,r,t,a}$	[?]

Lappano [65] presented permutation binomials of the form $ax + x^{5q-4}$ and $ax + x^{7q-6}$ over F_{q^2} and mentioned a conjecture regarding permutation behaviour of $f(x) = ax + x^{r(q-1)+1}$ for odd primes r.

Theorem 2.26. *[65] Assume $q \geq 5$. Let $f(x) = ax + x^{5q-4} \in F_{q^2}[x]$. Then $f(x)$ is a permutation polynomial of F_{q^2} if and only if one of the following occurs;*

(i) $q = 2^{4k+2}$ and $a^{\frac{q+1}{5}} \neq 1$ is a fifth root of unity,

(ii) $q = 3^2$ and a^2 is a root of $(1+x)(1+x^2)(2+x+x^2)(1+x+x^2+x^4)(1+x^2+x^3+x^4)(1+2x+x^2+2x^3+x^4)$,

(iii) $q = 19$ *and* a^4 *is a root of* $(1+x)(2+x)(3+x)(4+x)(5+x)(9+x)(10+x)(13+x)(17+x)(16+3x+x^2)(1+4x+x^2)(6+18x+x^2)$,

(iv) $q = 29$ *and* $a^6 \in \{15, 18, 22, 23\}$,

(v) $q = 7^2$ *and* a^{10} *is a root of* $(1+4x+x^2)$,

(vi) $q = 59$ *and* a^{12} *is a root of* $(4+x)(55+x)(x^2+36)$,

(vii) $q = 2^6$ *and* a^{13} *is a root of* $(1+x+x^2)(1+x+x^3)$.

Theorem 2.27. *[65] Assume* $q \geq 7$. *Let* $f(x) = ax + x^{7q-6} \in F_{q^2}[x]$. *Then* $f(x)$ *is a permutation polynomial of* F_{q^2} *if and only if one of the following occurs;*

(i) $q = 13$ *and* a^2 *is a root of* $(1+x)(2+x)(3+x)(4+x)(5+x)(6+x)(7+x)(8+x)(9+x)(10+x)(11+x)(12+x+x^2)(9+2x+x^2)(10+3x+x^2)(9+4x+x^2)(12+4x+x^2)(10x+5x+x^2)(3+6x+x^2)(1+7x+x^2)(4+7x+x^2)(1+8x+x^2)(12+9x+x^2)(1+10x+x^2)(3+12x+x^2)(4+12x+x^2)(12+12x+x^2)$,

(ii) $q = 3^3$ *and* a^4 *is a root of* $(2+x+x^2+x^3)(1+2x+x^2+x^3)(1+x+2x^2+x^3)(2+2x+2x^2+x^3)(1+2x+x^2+2x^3+x^4+2x^5+x^6)$,

(iii) $q = 41$ *and* a^6 *is a root of* $(9+x)(10+x)(26+x)(30+x)(32+x)(34+x)(35+x)(37+x)(39+2x+x^2)(1+14x+x^2)(20+40x+x^2)$.

Using the above theorem author proposed the following conjecture.

Conjecture 2.28. [65] Let $t > 2$ be a fixed prime. If both $(q+1) \equiv 0 \pmod{t}$ and $a^{(q+1)/t}$ are not $t-$th roots of unity, then there are only finitely many values (q, a), where $a \in F_{q^2}^*$, for which $f = ax + x^{t(q-1)+1} \in F_{q^2}[x]$ is a permutation polynomial of F_{q^2}.

The same conjecture was individually proposed by Hou [69] and Lappano [65] when $t > 2$ be a fixed prime, under the assumption that $a^{q+1} \neq 1 (a \in F_{q^2}^*)$ there are only finitely many (q, a) for which f is a permutation polynomial of F_{q^2}. Recently, Hou [64] answered this conjecture by using the following theorem.

Theorem 2.29. *[64] Assume that* f *is a permutation polynomial of* F_{q^2}. *Then* $\gcd(t, q+1) > 1$ *and* $(-a)^{(q+1)/\gcd(t,q+1)} \neq 1$. *In particular, if* t *is a prime, then* $q+1 \equiv 0 \pmod{t}$ *and* $(-a)^{(q+1)/t} \neq 1$.

Together with this he also proved that when $r \geq 3$ and $p = \{2, 3, 5\}$ with certain conditions on power τ of p then f is not a permutation polynomial of F_{q^2}.

After the determination of permutation binomials [63] of the form $ax + x^{2q-1} (a \in F_{q^2}^*)$ Hou and Lappano [66] presented another permutation binomial of the form $ax + x^{3q-2}$ over F_{q^2}. In the following theorem, they mentioned certain conditions on q and $a \in F_{q^2}^*$.

Theorem 2.30. *[66] Let* $f(x) = ax + x^{3q-2} \in F_{q^2}[x]$, *where* $a \in F_{q^2}^*$. *Then* $f(x)$ *is a permutation polynomial of* F_{q^2} *if and only if one of the following occurs;*

(i) $q = 2^{2k+1}$ *and* $a^{q+1/3}$ *is a primitive* 3^{rd} *root of unity,*

(ii) $q = 5$ *and* a^2 *is a root of* $(x+1)(x+2)(x-2)(x^2-x+1)$,

(iii) $q = 2^3$ *and* a^3 *is a root of* $x^3 + x + 1$,

(iv) $q = 11$ *and* a^4 *is a root* $(x-5)(x+2)(x^2-x+1)$,

(v) $q = 17$ *and* $a^6 = 4, 5$,

(vi) $q = 23$ *and* $a^8 = -1$,

(vii) $q = 29$ *and* $a^{10} = -3$.

Moreover, Hou [**?**] determined an infinite family of permutation binomials for $r = 1, 3$ and $t = 2$ over F_{q^2}. Together with that, he proved, that if $r > 3$ and q is not too small relative to r then f is not a permutation of F_{q^2}. In the following theorem, he determined the necessary and sufficient conditions on (q, r, a) for $f_{q,r,1,a}$ to be a permutation polynomial of F_{q^2}.

Theorem 2.31. *[?] For $r \geq 1$ and $a \in F_{q^2}^*$, $f_{q,r,1,a}$ is a permutation polynomial of F_{q^2} if and only if* $\gcd(r, q-1) = 1$, $q+1|r-1$, *and* $a^{q+1} \neq 1$.

Using the Hermite criterion, Li et al. [71] determined permutation binomials over F_{q^2}. They used well know the concept that, $f(x) = g(h(x))$ is a permutation polynomial over F_q if and only if both $g(x)$ and $h(x)$ permutes F_q. If $h(x) = x^d$, then $f(x) = ag(x^d)$ permutes F_q if and only if $\gcd(d, q-1) = 1$ and $g(x)$ does for any $a \in F_q^*$ and $1 \leq d \leq q-1$. Later author defined that if any such polynomials $f(x)$ and $g(x)$ satisfy these properties then they are multiplicatively equivalent. So far, we are familiar with the fact that any two polynomials $f(x)$ and $g(x)$ equivalent if $f(x) = cg(ax+b)+d$, where $a, c \in F_q^*$ and $b, d \in F_q$. They proved the binomial $f(x) = x^r(x^{q-1}+a)$ permutes F_{q^2} if and only if $r = 1$ and $a^{q+1} \neq 1$, where $1 \leq r \leq q+1$.

Later Masuda et al. [68] characterized permutation binomials of the form $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ over F_{q^e} for $e \in \{2, 3, 4\}$ and over F_{p^e} where $e \in \{5, 6\}$ for odd prime p. The existing results are listed below.

Theorem 2.32. *[68] Let $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ with $2 \leq e \leq 6$ and $a \neq 0$ and let $l = q^{e-1} + \cdots + q + 1$,*

(i) when $e = 2, 3, 4$, $f(x)$ permutes F_{q^e} if and only if $(-a)^l \neq 1$, $\gcd(r, q-1) = 1$ *and* $r \pmod 1 \in \{1, l-q\}$.

(ii) when $e = 5$ and q is an odd prime, $f(x)$ permutes F_{q^e} if and only if $(-a)^l \neq 1$, $\gcd(r, q-1) = 1$ *and* $r \pmod 1 \in \{1, l-q, q^3+1, q^4+q^2+1\}$.

(iii) when $e = 5$ and q is an odd prime, $f(x)$ permutes F_{q^e} if and only if $(-a)^l \neq 1$, $\gcd(r, q-1) = 1$ *and* $r \pmod 1 \in \{1, l-q\}$.

In the following theorem, they have characterized the existence of the permutation binomials $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ over F_{q^e} for arbitrary e.

Theorem 2.33. *[68] Let $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ with $e \geq 2$ and $a \neq 0$ and let $l = q^{e-1} + \cdots + q + 1$. Then $f(x)$ permutes F_{q^e} and is the composition of a linearized binomial and a monomial if and only if $(-a)^l \neq 1$ and $r = sl + \sum_{i=0}^{k-1} q^{hi} \pmod{q^e - 1}$, where* $\gcd(h, e) = 1$, *$k \pmod e = h^{-1}$, s is a positive integer and* $\gcd(r, q-1) = 1$.

In addition to these investigations, they also proved that there do not exist permutation binomials of the form $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ over F_{q^e} for $e \geq 2$ and $q \neq 2$. When $q = 2$, the binomial take the form $f(x) = x^r(x + a)$ which does not permutes F_{2^e} if $a \neq 0$. Based on these observations they did a computer run for $q^e < 10^8$ and proposed the following conjecture for a more generalized value of e and $t = 1$.

Conjecture 2.34. [68] Let $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ with $e \geq 2$ and $a \neq 0$ and let $l = q^{e-1} + \cdots + q + 1$. Then $f(x)$ permutes F_{q^e} if and only if $f(x)$ is congruent to the composition of a linearized binomial $L(x) = x^{q^h} + ax$ and a monomial x^r modulo $x^{q^e} - x$, where $(-a)^l \neq 1$ and $\gcd(r, q-1) = 1$.

Using the relationship between the polynomials and the number of rational points on algebraic curves, Oliveira and Martinez [72] determined the exact number of elements $a \in F_q$ for which the binomial $x^n(x^{\frac{q-1}{r}} + a)$ is a permutation polynomial in the cases $r = 2$ and $r = 3$. In the following theorem, they estimated the number of permutation binomials of the form $x^n(x^{\frac{q-1}{2}} + a)$ related to points on an algebraic curve of degree 2.

Theorem 2.35. *[72] Let n be an integer such that* $\gcd(n, \frac{q-1}{2}) = 1$. *The number of elements $a \in F_q$ for which the binomial $x^n(x^{\frac{q-1}{2}} + a)$ permutes F_q is given by the formula $\frac{q-2+(-1)^n}{2}$.*

Using the criteria determined by Wan and Lidl [35] (Theorem 1.2), Oliveira and Martinez [72] stated the following lemma to determine the number of permutation binomials of the form $x^n(x^{\frac{q-1}{3}} + a)$.

Lemma 2.36. *[72] Let n be a positive integer. The polynomial $f(x) = x^n(x^{\frac{q-1}{3}} + a)$ is a permutation polynomial over F_q if and only if the following conditions are satisfied*

(i) $\gcd(n, \frac{q-1}{3}) = 1$,

(ii) $a \notin \{-1, -\zeta, \zeta^2\}$,

(iii) $\eta\left(\frac{\zeta+a}{1+a}\right) \neq \delta^{2n}$,

(iv) $\eta\left(\frac{1+a}{\zeta^2+a}\right) \neq \delta^{2n}$,

(v) $\eta\left(\frac{\zeta^2+a}{\zeta+a}\right) \neq \delta^{2n}$.

In the following theorem, they estimated the number of permutation binomials of the form $f(x) = x^n(x^{\frac{q-1}{3}} + a)$ related to rational points on an elliptic curve.

Theorem 2.37. *[72] Let $q = p^k$. Assume $q \equiv 1 \pmod 3$. Let n be a positive integer such that $\gcd(n, \frac{q-1}{3}) = 1$. The number of elements $a \in F_q$ for which the binomial $f(x) = x^n(x^{\frac{q-1}{3}} + a)$ permutes F_q is given by $\frac{2q-3(\epsilon_1+\epsilon_2)-10-2(\pi_p^k+\bar{\pi_p}^k)}{9}$, where $\pi_p = \frac{-k_p}{2} + i\sqrt{p - \frac{-k_p^2}{4}}$,*

$$\epsilon_1 = \begin{cases} -2, & \text{if } q - 3n \equiv 1 \pmod 9 \\ 1, & \text{if } q - 3n \not\equiv 1 \pmod 9 \end{cases} \quad \text{and} \quad \epsilon_2 = \begin{cases} -2, & \text{if } n \equiv 0 \pmod 3 \\ 1, & \text{if } n \not\equiv 0 \pmod 3 \end{cases}$$

By generalizing the form which was discussed in [66], Tu et at. [70] determined the all the values of r and a such that the binomial $f(x) = x^r(a + x^{3(q-1)})$ is a permutation over F_{q^2} with $q = 2^m$. Characterization was based on the case of even m and odd m with $3|m$, which further shows that the characterization is necessary and sufficient for almost all r values. They defined permutation binomials in the following theorem where m is an even positive integer with $m \geq 4$.

Theorem 2.38. *[70] Let $q = 2^m$ with an even positive integer $m \geq 4$. Then for $a \in F_{q^2}^*$, $f(x) = x^r(x^{3(q-1)} + a)$ permutes F_{q^2} if and only if $\gcd(r, q-1) = 1$, $r \equiv 3 \pmod{q+1}$ and $a^{q+1} \neq 1$.*

In the next theorem, they characterized permutation binomials when m is odd.

Theorem 2.39. *[70] Let $q = 2^m$ with an odd positive integer $m \geq 5$. if $\gcd(r, 3(q-1)) = \gcd(r-3, q+1) = 1$ and $a \in F_{q^2}^*$ such that $a^{\frac{q+1}{3}}$ is a primitive 3rd root of unity, then $f(x) = x^r(x^{3(q-1)} + a)$ permutes F_{q^2}.*

When r is a positive integer they also concluded that the conditions mentioned above are necessary in one of the cases (i) $3 \nmid m$; (ii) $3|m$ and $r \pmod{(q+1)}$ satisfies either $r = k\frac{q+1}{9} + 3, k \in \{0, 1, \ldots, 8\}$ or $r = k\frac{q+1}{9} + r_2 + 3, k \in \{0, 1, \ldots, 8\}, 0 < r_2 < \frac{q+1}{9}$ and $(k, r_2) \notin S_1 \cup S_2$, where S_1 and S_2 are defined in [70].

3 Non-existence of permutation binomials

Several findings demonstrate that permutation polynomials do not exist. Cavior [73] investigated octic form of permutation polynomials of the form $f(x) = x^8 + ax^t$ with $1 \leq t \leq 7$ where t is odd. Chou [74] answered Cavior's [73] questions on existence of permutation binomials of the form $f(x) = x^8 + ax^5 \in F_q$ if $n = 1$ and $a = 3$ or $a = 4$ and $q = 7^n$. In addition to that he proved $f(x) = x^8 + ax^5$ is a permutation polynomial of F_{11^n} if and only if $n = 1$ and $a = 2, 4, 7$ or $a = 9$. Finally he proved that $f(x) = x^8 + ax^5$ is not a permutation polynomial over F_{13^n} for $a \in F_{13^n}$. Later Dickson [2] proved that $x^4 + 3x$ over F_7 is a permutation polynomial but not over F_{7^n} for $n > 1$, this was further generalized by Carlitz [57] as, when $q = 2m+1$ and $a \in F_q^*$ is suitably chosen then $f(x) = x^{m+1} + ax$ is a permutation polynomial over F_q when $q \geq 7$ but not on F_{q^r} with $r > 1$ and he raised the same question for $q = 3m + 1$. The same statement can be generalized as for fixed integer $k \geq 2$ and $q = km + 1$ there exist a constant N_k and $a \in F_q$ such that $f(x) = x^{m+1} + ax$ is a permutation polynomial for F_q provided $q > N_k$. Using the following theorems stated by Niederreiter and Robinson [75] for non-existence of permutation binomials when $q \geq (k^2-4k+6)^2$, Wan [76, 77] answered Carlitz [57] question for the case of $q = 3m+1$ when $p \neq 2$.

Theorem 3.1. *[75] Let $k > 2$. Then*

(i) if k is not a prime power, then for all finite fields F_q with $q \geq (k^2-4k+6)^2$ there is no permutation polynomial of F_q of the form $ax^k + bx \in F_q[x]$ with $ab \neq 0$;

(ii) if k is power of the prime p, then for all finite fields F_q with $q \geq (k^2-4k+6)^2$ and characteristic$\neq p$ there is no permutation polynomial of F_q of the form $ax^k + bx \in F_q[x]$ with $ab \neq 0$.

Remark 3.2. In general for $m \geq 2$ and $a \neq 0$ it is not clear that the polynomial of the form $f(x) = x^{1+\frac{q-1}{m}} + ax$ where $q \equiv 1 \pmod m$, is a permutation polynomial or not over F_q. But when $m = \frac{q-1}{p^i-1}$ where, $F_{p^i} \subset F_q$ then $f(x)$ is a permutation polynomial of F_{q^r} if and only if $(-a)^{(q^r-1)/(p^i-1)} \neq 1$.

Chou [74] considered a specific kind of permutation binomial which was a general form of the polynomial considered in [73] and Chou adopted the same method as considered in [73] to prove the following theorem.

Theorem 3.3. *[74] Let $q = p^n$ with p is an odd prime and n is a positive integer. Let k, j be integers with $1 \leq j < k$ such that $k|(p^2-1)$ and $(k-j)|(p-1)$. Write $(p^2-1)/k = lp + r$ with $1 \leq r \leq p-1$. If $(p-1)/(k-j) \leq l + r + p$ then for all $n \geq 2$, $f(x) = bx^k + ax^j$ is not a permutation polynomial of F_q for any $a, b \in F_q^*$.*

Ayad et al. [78] proved non-existence of permutation binomials of the form $f(x) = ax^n + x^m$ over F_q based on the certain congruence condition on d, where $d = \gcd(n-m, q-1)$ which are mentioned below.

Theorem 3.4. *[78] Let $f(x)$ be a binomial such that $d > 1$. If $p \equiv 1 \pmod{d^2}$ then $f(x)$ is not a permutation polynomial of F_q.*

Theorem 3.5. *[78] Let $f(x)$ be a binomial such that $d > 1$. Suppose that there exists an integer $\delta > \frac{d}{2}$ such that $n \equiv 0 \pmod{2\delta}$ and $q \equiv 1 \pmod{2\delta}$. Then $f(x)$ is not a permutation polynomial of F_q.*

Theorem 3.6. *[78] Let $f(x) = ax^n + x^m$ be a binomial. Suppose that n is even, $p \neq 2$, $n \equiv m \pmod 9$ and $\gcd(n-m, q-1) = 3$. Then the following assertions hold:*

(i) If $p \equiv -1 \pmod 3$ then $f(x)$ is not a permutation polynomial of F_q.

(ii) If $p \equiv 1 \pmod 3$ and for every primitive cube root of $\zeta \in F_p$ the polynomial $g(x) = \zeta a x^{n-m} + 1$ has no root in F_q then $f(x)$ is not a permutation polynomial of F_q.

Theorem 3.7. *[78] Let k and d be positive integers such that $d \geq 2$, $1 \leq k \leq d-1$, $d|q-1$ and $d^2 < q-1$. Then, for any $a \in F_q$, the polynomial $f(x) = ax^{m+d} + x^m$ does not permute F_q if m satisfies one of the following conditions;*

(i) $m = k(q-1)/d$,

(ii) $m = u + k(q-1)/d$ with $\frac{q-1}{d} - d \leq u \leq \frac{q-1}{d} - 1$ and $\binom{d}{\frac{q-1}{d}-u} \neq 0 \pmod p$.

In the next theorem they considered that, $2 \leq d|q+1$, for sufficiently large q and $a^{q+1} \neq 1$. If $n = 1$ then the following theorem covers the result of [79].

Theorem 3.8. *[78] Let $n \geq 1$, $d \geq 2$ and $a \in F_{q^2}^*$ be such that $d|q+1$, $q \geq (2max\{n, 2d-n\})^4$ and $a^{q+1} \neq 1$. Then $f(x) = x^n(a + x^{d(q-1)})$ is not a permutation binomial of F_{q^2} if one of the following conditions is satisfied;*

(i) $d - n > 1$ and $\gcd(d, n+1)$ is a power of 2,

(ii) $d+2 \le n < 2d$ *and* $\gcd(d, n-1)$ *is a power of 2,*

(iii) $n \ge 2d$*,* $\gcd(d, n-1)$ *is a power of 2, and* $\gcd(n-d, q-1) = 1$.

Based on their observations, they also questioned that, when $d - n = \pm 1$ and $e > 2$ are there infinite classes of permutation binomials of the form $f(x) = x^n(a + x^{d(q-1)})$ of F_{q^e}?

Together with construction of permutation binomials of the form $f_{q,r,t,a}$ over F_{q^2} Hou [**?**] investigated that if $r > 3$ and q is not too small relative to r, then f is not a permutation of F_{q^2}. More precisely, the result has been stated in the following theorem.

Theorem 3.9. *[**?**] Let* $f = f_{q,r,2,a} = x^r(a + x^{2(q-1)})$*, where* r *and* q *are both odd,* $r > 3$*, and* $a \in F_{q^2}^*$ *is such that* $a^{q+1} \neq 1$*. Then* f *is not a permutation polynomial of* F_{q^2} *if*

$$q \ge \begin{cases} r^2 - 4r + 5 & \text{if } r \equiv 3 \pmod p, \\ 8r - 15 & \text{if } r \not\equiv 3 \pmod p \text{ and either } p = 3 \text{ or } r \equiv 7/4 \pmod p, \\ 6r - 11 & \text{if } p > 3 \text{ and } r \not\equiv 3, 7/4 \pmod p. \end{cases}$$

The permutation binomials of the form $x^r(x^{q-1} + a)$ over F_{q^2} which was considered by Li et al. [71] was further studied by Liu [67] over F_{q^3} and F_{q^e} where e is a large value using different method. In the following theorem he proved that $f(x) = x^r(x^{q-1} + a)$ is almost always not a permutation polynomial over F_{q^3} except for the case that $r = 1$.

Theorem 3.10. *[67] Let* $f(x) = x^r(x^{q-1} + a) \in F_{q^3}[x]$*,* $1 \le r \le q^2 + q + 1$*. Then* $f(x)$ *is a permutation binomial over* F_{q^3} *if and only if* $r = 1$*, here* $a^{q^2+q+1} \neq -1$ *and* q *is a power of an odd prime.*

Later in the following theorem he proved that $f(x) = x^r(x^{q-1} + a) \in F_{q^e}[x]$ for large value of e is not a permutation binomial over F_{q^e}.

Theorem 3.11. *[67] Let* $1 < r < q^{\frac{e}{4}} - q + 3$ *be an integer, and* $a \in F_{q^e}^*$*,* $q \ge 6$*. Then* $f(x) = x^r(x^{q-1} + a)$ *is not a permutation polynomial over* F_{q^e}*.*

Hou and Lavorante [80] investigated the non-existence of permutation binomials of the form $x^n(a + x^{d(q-1)})$ where n, d are positive integers and $a \in F_{q^2}^*$. In the following theorem, they proved the non-existence of binomials of the form $x^n(a+x^{d(q-1)})$ when q is even and sufficiently large and $a^{q+1} \neq 1$. This theorem partially confirms the conjecture proposed by Tu et al. [70].

Theorem 3.12. *[80] Let* $q = 2^m$*,* $n \ge 1$ *and* $a \in F_{q^2}^*$ *be such that* $q \ge (2max\{n, 6-n\})^4$ *and* $a^{q+1} \neq 1$*. Then* $f(x) = x^n(a + x^{3(q-1)})$ *is not a permutation binomial of* F_{q^2}*.*

Hou [79] investigated the binomials of the form $f(x) = x(x^{r(q-1)} + a)$ for large q and concluded that, these binomials can not permute F_{q^2} when $r > 2$, $q \ge 2^8(r-1)^4$, $a \in F_{q^2}^*$ and $a^{q+1} \neq 1$ using Hasse–Weil bound.

On the bases of observations made in Table 2, we come to know that, the binomials of the form $f_{q,r,t,a} = x^r(a + x^{t(q-1)})$ over F_{q^2}, where $1 \le r \le q^2 - 2$, $1 \le t \le q$, $a \in F_{q^2}^*$ are not know completely. Finding the necessary and sufficient condition on (q, r, t, a) for $f_{q,r,t,a} = x^r(a + x^{t(q-1)})$ to be a permutation polynomial is itself a difficult task. Based on these insights, the following open problem is suggested for the readers' future work.

Open problem 1. Find the necessary and sufficient conditions on (q, r, t, a) such that $f_{q,r,t,a} = x^r(a+x^{t(q-1)})$ is a permutation binomial over F_{q^2}, where $1 \le r \le q^2-2$, $1 \le t \le q$ and $a \in F_{q^2}^*$ when $t > 3$ and $r > 4$ for large q.

4 Conclusion

The richness of finite fields is enhanced due to the ability of polynomials that permute the elements. Over many decades, various classes of permutation polynomials have been investigated. In recent years, the topic of generating these polynomials has taken the limelight. In this paper, we surveyed all existing and nonexisting classes of permutation binomials with all mentioned methodologies. Furthermore, using similar methods, many new permutation binomials can be obtained.

Acknowledgements

The first author extends sincere gratitude to the UGC-CSIR Grant Commission for their generous support via Grant No. 201610069412, and to Manipal Academy of Higher Education for their continuous encouragement and assistance. The corresponding author wishes to express appreciation to the Manipal Institute of Technology, Manipal Academy of Higher Education, India, for their encouragement and support. Additionally, the second author would like to acknowledge the Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, India, for their encouragement and support.

References

[1] C. Hermite, Sur les fonctions de sept lettres, *Académie des sciences* (1863).

[2] L. E. Dickson, The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group. *The Annals of Mathematics JSTOR* 11(1/6) (1896) 65–120.

[3] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc* 4(1) (1953) 538.

[4] A. Akbary, D. Ghoica, Q. Wang, On constructing permutations of finite fields, *Finite Fields and Their Applications, Elsevier* 17 (1) (2011) 51–67.

[5] K. Li, L. Qu, Q. Wang, New constructions of permutation polynomials of the form $x^r h(x^{q-1})$ over F_{q^2} , *Designs, Codes and Cryptography* 86 (10) (2018) 2379–2405.

[6] P. Yuan, C. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields and Their Applications* 17 (6) (2011) 560–574.

[7] X. Zeng, S. Tian, Z. Tu, Permutation polynomials from trace functions over finite fields, *Finite Fields and Their Applications* 35 (2015) 36–51.

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

[9] J. Macros, Specific permutation polynomials over finite fields, *Finite Fields and Their Applications* 17 (2) (2011) 105–112.

[10] G.R.V. Bhatta, B.R. Shankar, A study of permutation polynomials as Latin squares, *Nearrings, Nearfields, and Related Topics, World Scientific* (2017) 270–281.

[11] V. Jarali, P. Poojary, G.R.V. Bhatta, Construction of Permutation Polynomials Using Additive and Multiplicative Characters, *Symmetry, MDPI* 14 (8) (2022) 1539.

[12] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* 21 (1978) 120–126.

[13] R. P. Singh, K. B. Sarma, A. Saikia, Public key cryptography using permutation p-polynomials over finite fields, *Cryptology ePrint Archive* (2009).

[14] R. P. Singh, K. B. Sarma, A. Saikia, A public key cryptosystem using a group of permutation polynomials, *Tatra Mountains Mathematical Publications* 77(1) (2020) 139–162.

[15] R. P. Singh, K. B. Sarma, A. Saikia, Poly-dragon: an efficient multivariate public key cryptosystem, *Journal of Mathematical Cryptology* 4(4) (2011) 349–364.

[16] G. Khachatrian, M. Kyureghyan, Permutation polynomials and a new public-key encryption, *Discrete Applied Mathematics* 216 (2017) 622–626.

[17] C. Ding, Z. Zhou, Binary cyclic codes from explicit polynomials over $GF(2m)$, *Discrete Mathematics* 321 (2014) 76–89.

[18] C. Ding, Cyclic codes from some monomials and trinomials, *SIAM Journal on Discrete Mathematics* 27 (4) (2013) 1977–1994.

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

[20] C. Ding, J. Yuan, A family of skew Hadamard difference sets, *Journal of Combinatorial Theory, Series A* 113 (7) (2006) 1526–1535.

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

[22] Q. Liu, Two classes of permutation polynomials with niho exponents over finite fields with even characteristic, *Turkish Journal of Mathematics* 46 (3) (2022) 919–928.

[23] Z. Tu, X. Zeng, T. Helleseth, New permutation quadrinomials over $F_{2^{2m}}$, *Finite Fields and Their Applications* 50 (2018) 304–318.

[24] Z. Ding, M. Zieve, Determination of a class of permutation quadrinomials, *arXiv preprint arXiv:2203.04216* (2022).

[25] K. H. Kim, S. Mesnager, C. H. Kim, M. C. Jo, Completely characterizing a class of permutation quadrinomials, *Finite Fields and Their Applications* 87 (2023) 102155.

[26] F. Ozbudak, B. G. Tem¨ur, Classification of some quadrinomials over finite fields of odd characteristic, *Finite Fields and Their Applications* 87 (2023) 102158.

[27] K. H. Kim, S. Mesnager, J. H. Choe, D. N. Lee, S. Lee, M. C. Jo, On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity, *Designs, Codes and Cryptography* 90 (6) (2022) 1437–1461.

[28] Z. Tu, X. Liu, X. Zeng, A revisit to a class of permutation quadrinomials, *Finite Fields and Their Applications* 59 (2019) 57–85.

[29] Z. Tu, N. Li, X. Zeng, J. Zhou, A class of quadrinomial permutations with boomerang uniformity four, *IEEE Transactions on Information Theory* 66 (6) (2020) 3753–3765.

[30] Z. Tu, X. Zeng, T. Helleseth, A class of permutation quadrinomials, Discrete Mathematics 341 (11) (2018) 3010–3020.

[31] L. Zheng, B. Liu, H. Kan, J. Peng, D. Tang, More classes of permutation quadrinomials from niho exponents in characteristic two, *Finite Fields and Their Applications* 78 (2022) 101962.

[32] V. P. Lavorante, On permutation quadrinomials from niho exponents in characteristic two, *arXiv preprint arXiv:2112.07006* (2021).

[33] R. Gupta, Several new permutation quadrinomials over finite fields of odd characteristic, *Designs, Codes and Cryptography* 88 (1) (2020) 223–239.

[34] R. Gupta, More results about a class of quadrinomials over finite fields of odd characteristic, *Communications in Algebra* 50 (1) (2022) 324–333.

[35] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{(q-1)}{d}})$ and their group structure, *Monatshefte f¨ur Mathematik* 112 (2) (1991) 149–163.

[36] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, *Sequences, Subsequences, and Consequences, Springer* (2007) 119–128.

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

[38] R. Lidl, H. Niederreiter, Finite fields, *Cambridge university press* 20 (1997).

[39] K. Li, L. Qu, C. Li, S. Fu, New permutation trinomials constructed from fractional polynomials, *arXiv preprint arXiv:1605.06216* (2016).

[40] H. Dobbertin, Uniformly representable permutation polynomials, *Sequences and their Applications, Springer* (2002) 1–22.

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

[42] D. Cox, J. Little, D. O'Shea, M. Sweedler, Ideals, varieties, and algorithms, American Mathematical Monthly 101 (6) (1994) 582–586.

[43] L. Carlitz, C. Wells, The number of solutions of a special system of equations in a finite field, *Acta Arithmetica* 12 (1) (1966) 77–84.

[44] R. Lidl, H. Niederreiter, Finite fields, *Encyclopedia of Mathematics and its Applications* 20 (1983).

[45] A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, *Proceedings of the American Mathematical Society* 134 (1) (2006) 15–22.

[46] P. Charpin, G. M. Kyureghyan, Cubic monomial bent functions: A subclass of m, *SIAM Journal on Discrete Mathematics* 22 (2) (2008) 650–665.

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

[48] B. Wu, D. Lin, On constructing complete permutation polynomials over finite fields of even characteristic, *Discrete Applied Mathematics* 184 (2015) 213–222.

[49] R. K. Sharma, R. Gupta, Determination of a type of permutation binomials and trinomials, *Applicable Algebra in Engineering, Communication and Computing* 31 (1) (2020) 65–86.

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

[51] S. Sarkar, S. Bhattacharya, A. C¸ esmelioglu,On Some Permutation Binomials of the Form $x^{\frac{2^n-1}{k}+1}+ax$ over F_{2^n} : Existence and Count, *International Workshop on the Arithmetic of Finite Fields WAIFI* (2012) 236–246.

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

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

[54] G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of complete permutation polynomials over F_q, *Science China Mathematics* 58 (10) (2015) 1–14.

[55] M. Ayad, K. Belghaba, O. Kihel, On permutation binomials over finite fields, *Bulletin of the Australian Mathematical Society* 89 (1) (2014) 112–124.

[56] A. Masuda, M. Zieve, Permutation binomials over finite fields, *Transactions of the American Mathematical Society* 361 (8) (2009) 4169–4180.

[57] L. Carlitz, Some theorems on permutation polynomials, *Bulletin of the American Mathematical Society* 68 (2) (1962) 120–122.

[58] Z. Tu, X. Zeng, L. Hu, C. Li, A class of binomial permutation polynomials, *arXiv preprint arXiv:1310.0337* (2013).

[59] M. Zieve, Permutation polynomials on F_q induced form R´edei function bijections on subgroups of F_q^* (2013).

[60] S. Bhattacharya, S. Sarkar, On some permutation binomials and trinomials over F_{2^n} , *Designs, Codes and Cryptography* 82 (1) (2017) 149–160.

[61] L. A. Bassalygo, V. A. Zinoviev, On one class of permutation polynomials over finite fields of characteristic two, *WCC2015-9th International Workshop on Coding and Cryptography* (2015).

[62] N. Fernando, A note on permutation binomials and trinomials over finite fields, *arXiv preprint arXiv:1609.07162* (2016).

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

[64] X. Hou, Permutation polynomials of F_{q^2} of the form $ax+x^{r(q-1)+1}$, *Contemporary developments in finite fields and applications, World Scientific* (2016) 74–101.

[65] S. D. Lappano, A note regarding permutation binomials over F_{q^2}, *Finite Fields and Their Applications* 34 (2015) 153–160.

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

[67] X. Liu, Some results about permutation properties of a kind of binomials over finite fields, *arXiv preprint arXiv:1906.09168* (2019).

[68] A. Masuda, I. Rubio, J. Santiago, Permutation binomials of the form $x^r(x^{q-1}+a)$ over F_{q^e}, *Finite Fields and Their Applications* 79 (2022) 102003.

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

[70] Z. Tu, X. Zeng, Y. Jiang, Y. Li, Binomial permutations over finite fields with even characteristic, *Designs, Codes and Cryptography* 89 (12) (2021) 2869–2888.

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

[72] J. A. Oliveira, F. E. B. Mart´ınez, Permutation binomials over finite fields, *Discrete Mathematics* 345 (3) (2022) 112732.

[73] S. R. Cavior, A note on octic permutation polynomials, *Mathematics of Computation* 17 (1963) 450–452.

[74] W. Chou, Binomial permutations of finite fields, *Bulletin of the Australian Mathematical Society* 38 (3) (1988) 325–327.

[75] H. Niederreiter, K. H. Robinson, Complete mappings of finite fields, *Journal of the Australian Mathematical Society* 33 (2) (1982) 197–212.

[76] D. Q. Wan, Permutation polynomials over finite fields, *Acta Math. Sinica(N.S.)* 3 (1) (1987) 1–5. doi:10.

[77] D. Q. Wan, Permutation binomials over finite fields, *Acta Math. Sinica(N.S.)* 10 (1994) Special Issue 30–35.

[78] M. Ayad, K. Belghaba, O. Kihel, On permutation binomials, *Rocky Mountain Journal of Mathematics* 45 (2) (2015) 389–399.

[79] X. Hou, Applications of the hasse–weil bound to permutation polynomials, *Finite Fields and Their Applications* 54 (2018) 113–132.

[80] X. Hou, V. P. Lavorante, New results on permutation binomials of finite fields, *arXiv preprint arXiv:2111.06533* (2021).

[81] R. A Mollin, C. Small, On permutation polynomials over finite fields, *International Journal of Mathematics and Mathematical Sciences* 10 (3) (1987) 535–543.

[82] C. Small, Permutation binomials, *International Journal of Mathematics and Mathematical Sciences* 13 (2) (1990) 337–342.

[83] D. Cox, J. Little, D. O'Shea, Ideals, varieties, and algorithms, *American Mathematical Monthly* 101 (6) (1994) 582–586

Author information

Varsha Jarali, Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
E-mail: varshapjarali@gmail.com

Prasanna Poojary, Department of Mathematics, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India.
E-mail: poojaryprasanna34@gmail.com, poojary.prasanna@manipal.edu

Vadiraja Bhatta G.R.*, Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.
E-mail: vadiraja.bhatta@manipal.edu, grvbhatta@gmail.com