Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 9409130, 13 pages
https://doi.org/10.1155/2021/9409130

Research Article

Constructions and Necessities of Some Permutation Polynomials over Finite Fields

Xiaogang Liu

Department of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, Jiangsu, China

Correspondence should be addressed to Xiaogang Liu; liuxg0201@163.com

Received 3 November 2021; Accepted 9 December 2021; Published 31 December 2021

Academic Editor: Li Haitao

Let $\mathbb{F}_q$ denote the finite field with q elements. Permutation polynomials over finite fields have important applications in many areas of science and engineering such as coding theory, cryptography, and combinatorial design. The study of permutation polynomials has a long history, and many results are obtained in recent years. In this paper, we obtain some further results about the permutation properties of permutation polynomials. Some new classes of permutation polynomials are constructed, and the necessities of some permutation polynomials are studied.

1. Introduction

For a prime power q, let $\mathbb{F}_q$ denote the finite field of order q, and $\mathbb{F}_q^*$ the multiplicative group. A polynomial $f(x) \in \mathbb{F}_q$ is called a permutation polynomial (PP) over $\mathbb{F}_q$, if the associated polynomial mapping $f: c \longrightarrow f(c)$ is a permutation of $\mathbb{F}_q$. They have applications in coding theory, cryptography, and combinatorial design theory [1, 2]. Thus, in both theoretical and applied aspects, finding new PPs is of great interest. Permutation polynomials with few terms attract many authors' attention for their simple algebraic structures. In particular, there are many results about permutation binomials and trinomials [3–5].

Permutation polynomials attract peoples' interest for their extraordinary properties and algebraic forms. Complete permutation polynomial (CPP) is a permutation polynomial such that $f(x) + x$ is also a permutation polynomial. Mann introduced CPPs in the construction of orthogonal Latin squares [6]. Orthomorphisms map each maximal subgroup of the additive group of $\mathbb{F}_q$ half into itself and half into its complement, and they have a single fixed point and are the same as CPPs in even characteristic. Nonlinear orthomorphisms (or CPPs) are of cryptographic interest, and Mittenthal used them for the design of a nonlinear dynamic substitution device [7, 8]. PPs have been applied in the Lay–Massey scheme, the block cipher SMS4, the stream cipher Loiss [1, 9, 10], the design of Hash functions, quasigroups, and also in the constructions of some cryptographically strong functions [2, 11–14]. In [15–17], the authors investigated the set stability of switched delayed logical networks (SDLNs), the optimal state estimation of finite-field networks (FFNs), and containment problem of finite-field networks (FFNs).

A monomial x^n permutes $\mathbb{F}_q$ if $\gcd(n, q-1) = 1$, and they are the simplest kind of permutation polynomials. For binomials and trinomials, the permutation properties are not so easy to determine. Carlitz studied permutation binomials in 1962 [3]. In [18], Carlitz and Wells found that for q large enough than d, the polynomial $f(x) = x(x^{q-1/d} + a)$ might be a permutation polynomial over $\mathbb{F}_q$. Hou and Lappano studied permutation binomials of the forms $ax + x^{3q-2}$ and $ax + x^{5q-4}$ [19]. However, only a limited number of constructions are known for PPs. More recent constructions of PPs can be found in [4, 20–31], and the references therein.

For two positive integers m and n with $m|n$, $\mathrm{Tr}_m^n(\cdot)$ denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, that is,

$$\mathrm{Tr}_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(n/m-1)m}}. \tag{1}$$

Permutation polynomials of the form $x + \gamma \mathrm{Tr}_m^n(x^k)$ have been studied for special $\gamma \in \mathbb{F}_{q^n}$, with even characteristic [32, 33], and for the case $n = 2$, i.e., permutation trinomials

[4, 34]. Later, Zheng, Yuan, and Yu investigated permutation polynomials with the form

$$cx - x^s + x^{qs}, \tag{2}$$

over $\mathbb{F}_{q^n}$, where s is a positive integer, and $c \in \mathbb{F}_q$ [35]. For this, they used the AGW criterion to prove three classes of permutation trinomials. For the fourth class of permutation trinomials, a symbolic computation method related with resultants was used. And, they found a new relation with a class of PPs of the form

$$\left(x^{q^k} - x + \delta\right)^s + cx. \tag{3}$$

over $\mathbb{F}_{q^n}$, where δ is arbitrary and $c \in \mathbb{F}_q$. This class of permutation polynomials are related to δ. Based on their relationship, the aforementioned class of permutation trinomials without restriction on δ is derived.

In the study of CPPs, Li et al., found that certain polynomials over $\mathbb{F}_{2^n}$ can have the same permutation properties as $ax^k + bx$ over $\mathbb{F}_{2^m}$ for positive divisor m of n such that n/m is odd [36]. They constructed some permutation binomials, and thus more permutation polynomials of the form $a[Tr_m^n(x)]^k + u(c + x)(Tr_m^n(x) + x) + bx$ can be obtained, and here $a, b, c, u \in \mathbb{F}_{2^m}^*$ are constants. They also studied permutation polynomials over $\mathbb{F}_{p^{2m}}$ of the form $ax^{p^m} + bx + h(x^{p^m} \pm x)$, and Niho-type permutation trinomials over $\mathbb{F}_{p^{2m}}$ were constructed.

In this paper, some preliminaries are presented first in Section 2. In Sections 3 and 4, we construct some new classes of PPs including the following:

(a) In [35], permutation polynomials of the kind $x + x^s + x^{qs}$ are proposed, but with all coefficients 1, here we add a variable to the coefficient to investigate more general situations. In Proposition 1, PPs of the kind $cx + x^s + c^q x^{qs}$ are studied.

(b) In [36], permutation behavior of $x^{2^{2m}-1/3+1} + bx$ is studied for odd value m, and here in Proposition 10, all positive values of m will be investigated.

(c) In [37], Xu et al. proposed a class of permutation polynomials of the form $(x^{2^m} + x + \delta)^{-s} + bx$ for s, m satisfying $(2^m + 1)(-s) \equiv 2^m - 1 \pmod{2^{2m} - 1}$. In Proposition 11, the case of $(2^m + 2)(-s) \equiv 2^m - 1 \pmod{2^{2m} - 1}$ is studied.

(d) In Proposition 13, a totally new class of PPs $x^{2^{m+1}} + b'x^2 + bx$ is proposed.

(e) And the PPs in the other propositions are presented in these two sections.

In [37], Xu et al. proposed two classes of permutation polynomials of the form $(x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}} + bx$ and $(x^2 + x + \delta)^{2^{2k-1}-2^{k-1}} + bx$ over $\mathbb{F}_{2^{2m}}$ and $\mathbb{F}_{2^{2k}}$, respectively, and sufficient conditions were given. In this work, we investigate the necessities of the above two classes of permutation polynomials, and the necessary conditions are given in Section 5.

2. Preliminaries

Let $\mathbb{F}_{q^n}$ be the finite field which is an extension of $\mathbb{F}_q$ of degree n and $\mathbb{F}_{q^n}^*$ denotes its multiplicative group. Use N to denote the norm function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, i.e., for $x \in \mathbb{F}_{q^n}$, $N(x) = x^{1+q+q^2+\cdots+q^{n-1}}$. Let $L(x) = ax + bx^q + x^{q^2}$ be a linearized polynomial, with $a, b \in \mathbb{F}_{q^n}^*$. Define

$$u = \frac{a^q}{b^{q+1}}. \tag{4}$$

There is the following result about the number of solutions of $L(x)$ over $\mathbb{F}_{q^3}$.

Lemma 1 (see [38]). *Let $L(x) = ax + bx^q + x^{q^2}$ with $a, b \in \mathbb{F}_{q^3}^*$. Then $L(x)$ has 1 root in $\mathbb{F}_{q^3}$ if and only if $1 + N(b)(u^{q^2} + u^q + u + 1) + N(a) \neq 0$.*

Lemma 2 (see [39]). *Let $q = 2^k$, where k is a positive integer. The quadratic equation $x^2 + ux + v = 0$, where $u, v \in \mathbb{F}_q$ and $u \neq 0$, has roots in $\mathbb{F}_q$ if and only if $Tr_q(v/u^2) = 0$.*

Lemma 3 (see [40]). *For a positive integer m, $a, b \in \mathbb{F}_{2^{2m}}^*$ satisfying $Tr_1^n(b/a^2) = 0$. Then the quadratic equation $x^2 + ax + b = 0$ has*

(i) both solutions in the unit circle if and only if $b = a/a^{2^m}$ and $Tr_1^m(b/a^2) = Tr_1^m(1/a^{2^m+1}) = 1$,

(ii) exactly one solution in the unit circle if and only if $b \neq a/a^{2^m}$ and $(1 + b^{2^m+1})(1 + a^{2^m+1} + b^{2^m+1}) + a^2b^{2^m} + a^{2^m+1}b = 0$.

Lemma 4 (see [35]). *Let m, k be integers with $0 < k < m$ and $l = gcd(k, m)$. Let $c \in \mathbb{F}_{q^l}^*$ and $g(x) \in \mathbb{F}_{q^m}[x]$. Then $g(x^{q^k} - x + \delta) + cx$ permutes $\mathbb{F}_{q^m}$ for each $\delta \in \mathbb{F}_{q^m}$ if and only if $h(x) = g(x)^{q^k} - g(x) + cx$ permutes $\mathbb{F}_{q^m}$.*

Lemma 5 (see [41]). *Let $d, r > 0$ with $d|q - 1$, and let $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if the following two conditions hold:*

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

(ii) $x^r h(x)^{(q-1)/d}$ permutes μ_d, where μ_d denotes the d-th root of unity in $\mathbb{F}_q$.

Using the same idea as in [[45], Proposition 3], we can get the following lemma.

Lemma 6 (see [24]). *Let m, k be integers with $0 < k < m$ and $l = gcd(k, m)$. Let $c \in \mathbb{F}_{q^l}^*$ and $g(x) \in \mathbb{F}_{q^m}[x]$. Then $g(x^{q^k} + x + \delta) + cx$ permutes $\mathbb{F}_{q^m}$ for each $\delta \in \mathbb{F}_{q^m}$ if and only if $h(x) = g(x)^{q^k} + g(x) + cx$ permutes $\mathbb{F}_{q^m}$.*

For each element x in the finite field $\mathbb{F}_{2^{2m}}$, define $\overline{x} = x^{2^m}$. The unit circle of $\mathbb{F}_{2^{2m}}$ is the set

$$\mathcal{U} = \left\{\eta \in \mathbb{F}_{2^{2m}} : \eta^{2^m+1} = \eta\overline{\eta} = 1\right\}, \tag{5}$$

which is also denoted by μ_{q+1} occasionally.

The following lemma can be verified without much difficulty.

Lemma 7 (see [24]). *Each nonzero element x in the finite fields x has a unique expression of the following form:*

$$x = u\lambda, \tag{6}$$

with $u \in \mathbb{F}_{2^m}^*$ and $\lambda \in \mathcal{U}$.

Lemma 8 (see [24]). *Let m be a positive integer, and $a, b \in \mathbb{F}_{2^{3m}}^*$. Then the equation the following equation:*

$$x^{2^m} + ax + b = 0, \tag{7}$$

(i) has at most one possible solution $a^{2^{2m}}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}}/a^{2^{2m}+2^m+1} + 1$, when $a^{2^{2m}+2^m+1} + 1 \neq 0$,

(ii) has 2^m solutions, when $a^{2^{2m}+2^m+1} + 1 = 0$ and $a^{2^m}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}} = 0$,

(iii) has no solutions, when $a^{2^{2m}+2^m+1} + 1 = 0$ and $a^{2^m}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}} \neq 0$.

Proof. Let x be a solution, then

$$x^{2^m} = ax + b. \tag{8}$$

Taking the 2^m power on both sides of the above equation,

$$x^{2^{2m}} = a^{2^m}x^{2^m} + b^{2^m}. \tag{9}$$

Substituting equation (8) into the above equation,

$$x^{2^{2m}} = a^{2^m}(ax + b) + b^{2^m}. \tag{10}$$

Taking the 2^m power of the above equation,

$$x^{2^{3m}} = a^{2^{2m}}\left(a^{2^m}x^{2^m} + b^{2^m}\right) + b^{2^{2m}}. \tag{11}$$

Substituting equation (8) into the above equation,

$$x^{2^{3m}} = a^{2^{2m}}\left(a^{2^m}(ax + b) + b^{2^m}\right) + b^{2^{2m}}. \tag{12}$$

Noting that $x^{2^{3m}} = x$, the above equation can be transformed into

$$\left(a^{2^{2m}+2^m+1} + 1\right)x = a^{2^{2m}}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}}. \tag{13}$$

For case (ii), we need to show that there are 2^m solutions. Taking the 2^m power of the right side of equation (13),

$$ab^{2^{2m}} + a^{2^{2m}+1}b^{2^m} + b = 0. \tag{14}$$

Then we can find that $x = a^{2^{2m}}b^{2^m}$ is a solution of equation (8). Let us consider the equation

$$c^{2^m-1} = a. \tag{15}$$

Since $a^{2^{2m}+2^m+1} = 1$ and $2^{3m} - 1 = (2^m - 1)(2^{2m} + 2^m + 1)$, the above equation has $2^m - 1$ solutions. For every such c, we can find that $c + a^{2^{2m}}b^{2^m}$ is a solution of (2).

3. Permutation Polynomials That Can be Transformed to the Case of Monomials

In this section, we study the permutation behavior of six kinds of polynomials. Propositions 1 and 2 have the property that after some operations the complicated terms can be canceled. Propositions 3–6 have the property that exponents can be simplified. Denote $\mu_{q+1} = \{x | x^{q+1} = 1\}$.

Proposition 1. *Let $q = 2^m$ be even with $q \equiv 1 \,(mod 3)$, and $s = q^2 + q + 1/3$. Then*

$$f(x) = cx + x^s + c^q x^{qs}, \tag{16}$$

and it is a permutation polynomial over $\mathbb{F}_{q^2}$ for $c \in \mathbb{F}_{q^2}^*$ satisfying $Tr_1^m(c^{q+1}) = 0$.

Proof. It can be found that $3|(q + 2)$ from the assumption $q \equiv 1 \,(\mathrm{mod} 3)$. Let us rewrite the polynomial $f(x)$ in the following:

$$f(x) = cx + x^{q+2/3(q-1)+1} + c^q x^{(q(q+2)/3+1)(q-1)+1}. \tag{17}$$

Set $u = q + 2/3$, equation (83) becomes

$$f(x) = x\left(c + x^{(q-1)u} + c^q x^{(qu+1)(q-1)}\right). \tag{18}$$

By Lemma 5, $f(x)$ is a permutation polynomial if and only if

$$g(x) = x\left(c + x^u + c^q x^{qu+1}\right)^{q-1} \tag{19}$$

permutes μ_{q+1}. On the set μ_{q+1}, $x^{3u} = x^{q+2} = x$ and $g(x)$ become

$$g(x) = x\left(c + x^u + c^q x^{-u+1}\right)^{q-1}. \tag{20}$$

It is necessary to show that

$$c + x^u + c^q x^{-u+1} = 0 \tag{21}$$

has no zeros on μ_{q+1}. The above equation can be written as

$$c + x^u + c^q x^{2u} = 0. \tag{22}$$

We can find that $\gcd(u, q + 1) = \gcd(q + 2/3, q + 1) = 1$. Set $z = x^u$, then equation (22) becomes

$$z^2 + \frac{1}{c^q}z + \frac{c}{c^q} = 0. \tag{23}$$

For Lemma 3, we have $b/a^2 = c^{q+1}$ which lies in $\mathbb{F}_q$. And equation (23) has no solutions in the unit circle by our assumption.

Let us make the following transformations for $g(x)$ on the unit circle μ_{q+1}:

$$\begin{aligned} g(x) &= x\frac{c^q + x^{-u} + cx^{-1+u}}{c + x^u + c^q x^{-u+1}} \\ &= \frac{c^q x + x^{1-u} + cx^u}{c + x^u + c^q x^{-u+1}} \\ &= \frac{c^q x^{3u} + x^{2u} + cx^u}{c + x^u + c^q x^{2u}} \\ &= x^u \frac{c^q x^{2u} + x^u + c}{c + x^u + c^q x^{2u}} \\ &= x^u. \end{aligned} \tag{24}$$

Thus, $g(x)$ is a permutation of μ_{q+1}.

Example 1. Set $m = 4$. Using Magma, it can be verified that

$$f(x) = cx + x^{91} + c^{16}x^{1456} \tag{25}$$

is a permutation polynomial over $\mathbb{F}_{256}$ for $\mathrm{Tr}_1^4(c^{17}) = 0$.

Proposition 2. *Let r, i, m be positive integers with $gcd(r - i, 2^m + 1) = 1$ and $gcd(r, i(2^m - 1)) = 1$, and $b \in \mathbb{F}_{2^{2m}}^*$ satisfying $b^{2^{2m}-1/gcd(i(2^m-1),2^{2m}-1)} \neq 1, b^{2^m+1} = 1$. Then the polynomial*

$$f(x) = x^{i(2^m-1)+r} + bx^r \tag{26}$$

is a permutation polynomial over $\mathbb{F}_{2^{2m}}^*$.

Proof. Let $g(x) = x^r(x + b)^{i(2^m-1)}$ and $S = \{x^{i(2^m-1)} | x \in \mathbb{F}_{2^{2m}}^*\}$.

It can be verified that the above diagram is commutative. By assumption, we have $x + b \neq 0$ for $x \in S$. So, $g(x)$ maps S to S. We need to check that $g(x)$ is bijective on S. For $x \in S$, it is not difficult to show that

$$x^{2^m+1} = 1, \tag{27}$$

which means that $x^{2^m} = x^{-1}$. Thus

$$g(x) = x^r \frac{\left(x^{2^m} + b^{2^m}\right)^i}{(x + b)^i} = x^r \frac{\left(x^{-1} + b^{-1}\right)^i}{(x + b)^i} = \frac{x^{r-i}}{b^i} \tag{28}$$

permutes S since $\gcd(r - i, 2^m + 1) = 1$.

For $x_1, x_2 \in \mathbb{F}_{2^{2m}}^*$ satisfying $x_1^{i(2^m-1)} = x_2^{i(2^m-1)}$, the following holds

$$\left(\frac{x_1}{x_2}\right)^{i(2^m-1)} = 1. \tag{29}$$

If

$$f(x_1) = f(x_2), \tag{30}$$

then $x_1^r = x_2^r$. Since $\gcd(r, i(2^m - 1)) = 1$, we have $x_1 = x_2$. That is $f(x)$ is injective on the set $\{x | x^{i(2^m-1)} = z\}$ for $z \in S$. Using the AGW criterion [42], $f(x)$ is a permutation over $\mathbb{F}_{2^{2m}}^*$.

Example 2. Set $m = 3, r = 4, i = 3$. Using Magma, it can be verified that the following polynomial:

$$f(x) = x^{25} + bx^4, \tag{31}$$

is a permutation polynomial over $\mathbb{F}_{64}$ for $b^3 \neq 1, b^9 = 1$.

In the following, Propositions 3 and 4 are concerned with degree two extensions, but with different exponents and coefficients. Propositions 5 and 6 are concerned with degree three extensions.

Proposition 3. *Le r, s, m be positive integers with $s > 1, gcd(r, 2^{2m} - 1) = 1$, and $a, \delta \in \mathbb{F}_{2^{2m}}$ satisfying $Tr_1^m(a^{2^m+1}\delta^{2^m+1}/(a^{2^m+1} + \delta^{2^m+1} + 1)^2) = 0$. Then the polynomial*

$$f(x) = x^r\left(x^{s(2^m-1)} + ax^{2^m-1} + \delta\right)^{2^m+1} \tag{32}$$

is a permutation over $\mathbb{F}_{2^{2m}}$.

Proof. For Lemma 5, we have $d = 2^m + 1$. Since $\gcd(r, 2^{2m} - 1) = 1$, $f(x)$ is a permutation polynomial if and only if

$$g(x) = x^r\left(x^s + ax + \delta\right)^{2^{2m}-1} \tag{33}$$

permutes the unit circle μ_{2^m+1}. We claim that

$$x^s + ax + \delta = 0 \tag{34}$$

has no zeros in the unit circle. Otherwise, take the 2^m power on both sides of the above equation

$$x^{-s} + a^{2^m}x^{-1} + \delta^{2^m} = 0. \tag{35}$$

From the above two equations, we have

$$x^s x^{-s} = \left(a^{2^m}x^{-1} + \delta^{2^m}\right)(ax + \delta) = 1, \tag{36}$$

which is equivalent to

$$\left(a^{2^m} + \delta^{2^m}x\right)(ax + \delta) = x. \tag{37}$$

After simplification, the above equation can be transformed into

$$a\delta^{2^m}x^2 + \left(a^{2^m+1} + \delta^{2^m+1} + 1\right)x + a^{2^m}\delta = 0. \tag{38}$$

Thus

$$x^2 + \frac{\left(a^{2^m+1} + \delta^{2^m+1} + 1\right)}{a\delta^{2^m}}x + \frac{a^{2^m}\delta}{a\delta^{2^m}} = 0. \tag{39}$$

By Lemma 3, the above equation has no zeros in the unit circle since $\mathrm{Tr}_1^m(a^{2^m+1}\delta^{2^m+1}/(a^{2^m+1} + \delta^{2^m+1} + 1)^2) = 0$.

Now, equation (33) becomes

$$g(x) = x^r, \tag{40}$$

which permutes μ_{2^m+1} since $\gcd(r, 2^{2m} - 1) = 1$.

Example 3. Set $r = 4, s = 3, m = 4$. Let ω be a primitive element of $\mathbb{F}_{256}$ and $\delta = \omega$. Then the polynomial

$$f(x) = x^4\left(x^{45} + ax^{15} + \delta\right)^{17} \tag{41}$$

is a permutation polynomial over $\mathbb{F}_{256}$ when $\mathrm{Tr}_1^4(a^{17}\delta^{17}/(a^{17} + \delta^{17} + 1)^2) = 0$.

Proposition 4. *Let r, s, m be positive integers with $gcd(r, 2^{2m} - 1) = 1$, and $a, \delta \in \mathbb{F}_{2^m}^*$ satisfying $Tr_1^m(a\delta) = 1$. Then the polynomial*

$$f(x) = x^r\left(x^{2^{m-1}(2^m+1)} + ax^{2^m+1} + \delta\right)^{s(2^m-1)} \tag{42}$$

is a permutation polynomial over $\mathbb{F}_{2^{2m}}$.

Proof. For Lemma 5, we have $d = 2^m - 1$. Since $\gcd(r, 2^{2m} - 1) = 1$, $f(x)$ is a permutation polynomial if and only if

$$g(x) = x^r\left(x^{2^{m-1}} + ax + \delta\right)^{s\left(2^m-1\right)} \tag{43}$$

permutes $\mathbb{F}_{2^m}^*$, which means that

$$x^{2^{m-1}} + ax + \delta = 0 \tag{44}$$

has no zeros in $\mathbb{F}_{2^m}^*$. Squaring both sides of the above equation

$$x + a^2x^2 + \delta^2 = 0, \tag{45}$$

which is equivalent to

$$x^2 + \frac{1}{a^2}x + \frac{\delta^2}{a^2} = 0. \tag{46}$$

By Lemma 2, the above equation has no solutions in $\mathbb{F}_{2^m}$.

Example 4. Set $m = 4, r = 4, s = 3$. Let ω be a primitive element of $\mathbb{F}_{256}$, and $\delta = w^{85}$. Using Magma, it can be verified that

$$f(x) = x^4\left(x^{136} + ax^{17} + \delta\right)^{45} \tag{47}$$

is a permutation polynomial when $\mathrm{Tr}_1^m(a\delta) = 1$.

Proposition 5. *Let r, m, s be positive integers, and $a, b \in \mathbb{F}_{2^{3m}}^*$. Then the polynomial*

$$f(x) = x^r\left(x^{2^m(2^m-1)} + ax^{2^m-1} + b\right)^{s\left(2^{2m}+2^m+1\right)} \tag{48}$$

is a permutation polynomial for the following two cases:

(i) $a^{2^{2m}+2^m+1} + 1 \neq 0$ *and* $(a^{2^{2m}}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}}/a^{2^{2m}+2^m+1} + 1)^{2^{2m}+2^m+1} \neq 1$,

(ii) $a^{2^{2m}+2^m+1} + 1 = 0$ *and* $a^{2^{2m}}b^{2^m} + a^{2^{2m}+2^m}b + b^{2^{2m}} \neq 0$.

Here $gcd(r, 2^{3m} - 1) = 1$.

Proof. For Lemma 5, we have $d = 2^{2m} + 2^m + 1$. Since $\gcd(r, 2^{3m} - 1) = 1$, then $f(x)$ is a permutation polynomial over if and only if

$$\begin{aligned} g(x) &= x^r\left(x^{2^m} + ax + b\right)^{(2^m-1)\left(2^{2m}+2^m+1\right)} \\ &= x^r\left(x^{2^m} + ax + b\right)^{s\left(2^{3m}-1\right)} \end{aligned} \tag{49}$$

permutes $\mu_{2^{2m}+2^m+1}$. We only need to show that $(x^{2^m} + ax + b)^{2^{3m}-1}$ is nonzero on the set $\mu_{2^{2m}+2^m+1}$, which can be deduced from Lemma 8.

Example 5. Let $r = 4, m = 3, s = 3, b = 1$. Using Magma, it can be verified that the following polynomial

$$f(x) = x^4\left(x^{56} + ax^7 + 1\right)^{219} \tag{50}$$

is a permutation polynomial over $\mathbb{F}_{2^9}$ when $a^{73} \neq 1$ and $(a^{64} + a^{72} + 1/a^{73})^{73} \neq 1$.

Proposition 6. *Let r, s, m be positive integers satisfying $gcd(r, 2^{3m} - 1) = 1, gcd(3, 2^m - 1) = 1$. Then the polynomial*

$$f(x) = x^r\left(x^{2^{2m}(2^m-1)} + bx^{2^m(2^m-1)} + ax^{2^m-1} + \delta\right)^{s\left(2^{2m}+2^m+1\right)} \tag{51}$$

is a permutation polynomial over $\mathbb{F}_{2^{3m}}$, where $a + b + 1 \neq 0, \delta/a + b + 1 \in \mathbb{F}_{2^m}^*$, $a + b + \delta + 1 \neq 0$ and $1 + N(b)(u^{q^2} + u^q + u + 1) + N(a) \neq 0$. Here u is defined as in (1).

Proof. For Lemma 5, we have $d = 2^{2m} + 2^m + 1$. Since $\gcd(r, 2^{3m} - 1) = 1$, $f(x)$ is a permutation polynomial over $\mathbb{F}_{2^{3m}}$ if and only if

$$g(x) = x^r\left(x^{2^{2m}} + bx^{2^m} + ax + \delta\right)^{s\left(2^{3m}-1\right)} \tag{52}$$

permutes $\mu_{2^{2m}+2^m+1}$, which is equivalent to

$$x^{2^{2m}} + bx^{2^m} + ax + \delta = 0, \tag{53}$$

which has no solutions in $\mu_{2^{2m}+2^m+1}$.

Since $a + b + 1 \neq 0, \delta/a + b + 1 \in \mathbb{F}_{2^m}^*$, the above equation has a solution $x_0 = \delta/a + b + 1$ in $\mathbb{F}_{2^m}^*$. But $\gcd(3, 2^m - 1) = 1$, and x_0 lies in $\mu_{2^{2m}+2^m+1}$ if and only $x_0 = 1$. This is contradiction with the assumption that $a + b + \delta + 1 \neq 0$.

By Lemma 1, equation (53) is in fact a permutation polynomial over $\mathbb{F}_{2^{3m}}$. It has only one solution x_0, which does not belong to the set $\mu_{2^{2m}+2^m+1}$.

Example 6. Set $m = 3, b = 1, r = 4, s = 2, \delta = 1$. Then for all values $a \neq 0, 1$ in $\mathbb{F}_{2^3}$, using Magma, it can be verified that

$$f(x) = x^4\left(x^{448} + x^{56} + ax^7 + 1\right)^{146} \tag{54}$$

is a permutation polynomial over $\mathbb{F}_{2^9}$.

4. Construction of Permutation Polynomials with Two or More terms

4.1. Three Classes of Permutation Polynomials of Degree Three or Four Extensions over $\mathbb{F}_q$. In the following, Propositions 7–9 are concerned with PPs over field extensions of degrees 3 and 4.

Proposition 7. *Let $c \in \mathbb{F}_q^*$, $\delta \in \mathbb{F}_{q^3}$. Then $f(x) = g(x^q - x + \delta) + cx$ is a class of permutation polynomials of $\mathbb{F}_{q^3}$ if one of the following conditions holds:*

(i) $g(x) = u(x)^{q^2} + u(x)^q + u(x)$, and $u(x)$ is a polynomial over $\mathbb{F}_{q^3}$,

(ii) $g(x) = x^{i(q^2+q+1)}$, and i is a positive integer.

Proof. We only prove case (ii), and case (i) can be proved similarly.

Due to Lemma 4, $f(x)$ is a permutation polynomial if and only if

$$h(x) = g(x)^q - g(x) + cx \tag{55}$$

is a permutation of $\mathbb{F}_{q^3}$. But

$$g(x)^q - g(x) = \left(x^{i(q^2+q+1)}\right)^q - x^{i(q^2+q+1)} = 0. \tag{56}$$

That is $h(x) = cx$, which is a permutation of $\mathbb{F}_{q^3}$ for $c \in \mathbb{F}_q^*$.

Remark 1. For $f(x) = g(x^q - x + \delta) + cx$ to be a permutation polynomial over $\mathbb{F}_{q^3}$, $g(x)$ satisfies $g(x)^q = g(x)$. Here we give two explicit expressions of $g(x)$.

Proposition 8. *Let $c \in \mathbb{F}_q^*$, $\delta \in \mathbb{F}_{q^4}$. Then $f(x) = g(x^q + x + \delta) + cx$ is a permutation polynomial if one of the following conditions holds:*

(i) $g(x) = c_0(u(x)^{q^3} + u(x)^{q^2} + u(x)^q + u(x))$, where $u(x)$ is a polynomial over $\mathbb{F}_{q^4}$ and $c_0 \in \mathbb{F}_{q^4}^*$ satisfying $c_0^q + c_0 = 0$,

(ii) $g(x) = c_0 x^{i(q^3+q^2+q+1)}$, where i is a positive integer and $c_0 \in \mathbb{F}_{q^4}^*$ satisfying $c_0^q + c_0 = 0$.

Proof. We only consider case (i), and case (ii) can be proved in a similar way.

Due to Lemma 6, $f(x)$ is a permutation polynomial if and only if

$$h(x) = g(x)^q + g(x) + cx \tag{57}$$

is a permutation of $\mathbb{F}_{q^4}$. But

$$\begin{aligned} g(x)^q + g(x) &= \left(c_0 x^{i(q^3+q^2+q+1)}\right)^q + c_0 x^{i(q^3+q^2+q+1)} \\ &= (c_0 + c_0^q) x^{i(q^3+q^2+q+1)} = 0. \end{aligned} \tag{58}$$

That is $h(x) = cx$, which is a permutation of $\mathbb{F}_{q^4}$ for $c \in \mathbb{F}_q^*$.

Remark 2. Note that in the above proposition $c_0 \notin \mathbb{F}_q^*$ for odd characteristic.

Proposition 9. *For a positive integer m, a fixed $\delta \in \mathbb{F}_{2^{3m}}$, and $c \in \mathbb{F}_{2^m}^*$, the polynomial*

$$f(x) = \left(x^{2^m} + x + \delta\right)^{2^{2m}+1} + cx \tag{59}$$

is a permutation of $\mathbb{F}_{2^{3m}}$.

Proof. [[43], Proposition 4] says that

$$g(x) = \left(x^{2^m} + x + \delta\right)^{2^{2m}+1} + x \tag{60}$$

is a permutation of $\mathbb{F}_{q^{3m}}$. Set $x = c_0 y$, with $c_0 \in \mathbb{F}_{2^m}^*$. Then we have

$$\begin{aligned} g(x) = g(c_0 y) &= \left((c_0 y)^{2^m} + c_0 y + \delta\right)^{2^{2m}+1} + c_0 y \\ &= c_0^2 \left(y^{2^m} + y + \frac{1}{c_0}\delta\right)^{2^{2m}+1} + c_0 y \\ &= c_0^2 \left(\left(y^{2^m} + y + \frac{1}{c_0}\delta\right)^{2^{2m}+1} + \frac{1}{c_0} y\right). \end{aligned} \tag{61}$$

Since $g(x)$ is a permutation for every $\delta \in \mathbb{F}_{q^{3m}}$, setting $\delta_0 = 1/c_0\delta$,

$$f_0(y) = \left(y^{2^m} + y + \delta_0\right)^{2^{2m}+1} + \frac{1}{c_0} y \tag{62}$$

is a permutation of $\mathbb{F}_{q^{3m}}$ for every $\delta_0 \in \mathbb{F}_{q^{3m}}$. Let $c_0 = 1/c$.

$$f(y) = \left(y^{2^m} + y + \delta_0\right)^{2^{2m}+1} + cy \tag{63}$$

is a permutation of $\mathbb{F}_{q^{3m}}$ for every $\delta_0 \in \mathbb{F}_{q^{3m}}$.

Note that, in Proposition 9, c is unconnected with δ. Combining with Lemma 4, the following result is obtained.

Corollary 1For a positive integer m and $c \in \mathbb{F}_{2^m}^*$, the polynomial

$$g(x) = x^{2^m(2^{2m}+1)} + x^{2^{2m}+1} + cx \tag{64}$$

is a permutation of $\mathbb{F}_{2^{3m}}$.

Example 7. Set $m = 3$. Using Magma, it can be verified that the following polynomial:

$$g(x) = x^{520} + x^{65} + cx, \tag{65}$$

is a permutation over $\mathbb{F}_{512}$ for $c \in \mathbb{F}_8^*$.

4.2. PPs of Type $x^{2^{2m}-1/3+1} + bx$ over $\mathbb{F}_{2^{2m}}$. The following proposition is concerned with PPs of both odd and even positive values of m.

Proposition 10. *Let m be a positive integer, $b \in \mathbb{F}_{2^{2m}}$, and γ is a primitive element of $\mathbb{F}_{2^{2m}}$. Then $g(x) = x^{2^{2m}-1/3+1} + bx$ is a permutation polynomial of $\mathbb{F}_{2^{2m}}$ if and only if*

$$b \neq \frac{\gamma^{2^{2m}-1/3i'}}{\gamma^{3(k-k')+i-i'} + 1}\left(\gamma^{3(k-k')+2^{2m}+2/3(i-i')} + 1\right) \text{and } b \neq \gamma^{2^{2m}-1/3s}, \tag{66}$$

where $0 \le i \neq i' \le 2, 0 \le s \le 2$ and $1 \le k, k' \le 2^{2m} - 1/3$.

Proof. We can find that

$$g(x) = x\left(x^{2^{2m}-1/3} + b\right), \tag{67}$$

and $g(0) = 0$. Let us consider the nonzero elements in $\mathbb{F}^*_{2^{2m}}$.

It is not difficult to check that

$$\mathbb{F}^*_{2^{2m}} = U_0 \cup U_1 \cup U_2, \tag{68}$$

with

$$U_i = \left\{ \gamma^{3k+i} | 1 \le k \le \frac{2^{2m}-1}{3} \right\}, \tag{69}$$

for $i = 0, 1, 2$. And we have

$$U_i \cap U_j = \varnothing, \tag{70}$$

for $i \neq j$. Then $g(x)$ maps U_i to the set

$$V_i = \left\{ \gamma^{3k+i} \left(\gamma^{2^{2m}-1/3i} + b \right) | 1 \le k \le \frac{2^{2m}-1}{3} \right\}, \tag{71}$$

for $i = 0, 1, 2$. For fixed i, the elements in V_i are different. Then $g(x)$ is a permutation polynomial if and only if

$$V_i \cap V_j = \varnothing \text{ and } 0 \notin V_s, \tag{72}$$

for $i \neq j$, which is equivalent to that

$$\gamma^{3k+i} \left(\gamma^{2^{2m}-1/3i} + b \right) \neq \gamma^{3k'+i'} \left(\gamma^{2^{2m}-1/3i'} + b \right) \text{and } b \neq \gamma^{2^{2m}-1/3s}, \tag{73}$$

for $i \neq i'$ and $1 \le k, k' \le 2^{2m} - 1/3$. After simplification, we get the result.

Example 8. Let $m = 4$, and γ be a primitive element of $\mathbb{F}_{256}$. For $i = 2, i' = 1$, the polynomial

$$g(x) = x^{86} + bx \tag{74}$$

is not a permutation polynomial when $b = \gamma^{85}/\gamma^{3(k-k')+1} + 1\,(\gamma^{3(k-k')+86} + 1)$, and here $1 \le k, k' \le 85$.

4.3. PPs of Type $(bx + \delta)^{2^m+1} + x^{2^m} + cx$ over $\mathbb{F}_{2^{km}}$. In the following proposition, we study PPs of type $(bx + \delta)^{2^m+1} + x^{2^m} + cx$ over $\mathbb{F}_{2^{km}}$ with constant c.

Proposition 11. *For positive integers m, n, k with $n = km, 2|k$. For any $\delta \in \mathbb{F}_{2^n}$, the polynomial*

$$g(x) = (bx + \delta)^{2^m+1} + x^{2^m} + cx \tag{75}$$

is a permutation of $\mathbb{F}_{2^n}$, where $b, c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ satisfying $c = b/b^{2^m}$.

Proof. We prove that $g(x) = d$ has at most one solution for any $d \in \mathbb{F}_{2^n}$, which is equivalent to

$$x^{2^m} + cx + d = (bx + \delta)^{2^m+1}, \tag{76}$$

which has a unique solution.

It can be verified that $\gcd(2^m + 1, 2^n - 1) = 1$ for $n = km$ when $2 \nmid k$. Let $y = bx + \delta$, then $x = y/b + \delta/b$. Equation (76) can be rewritten as

$$\left(\frac{y}{b} + \frac{\delta}{b} \right)^{2^m} + c\left(\frac{y}{b} + \frac{\delta}{b} \right) + d = y^{2^m+1}, \tag{77}$$

which is equivalent to

$$y^{2^m+1} + \frac{1}{b^{2^m}} y^{2^m} + \frac{c}{b} y + \frac{\delta^{2^m}}{b^{2^m}} + \frac{c\delta}{b} + d = 0. \tag{78}$$

That is,

$$\left(y^{2^m} + \frac{c}{b} \right) \left(y + \frac{1}{b^{2^m}} \right) + \frac{c}{b^{2^m+1}} + \frac{\delta^{2^m}}{b^{2^m}} + \frac{c\delta}{b} + d = 0. \tag{79}$$

So,

$$\left(y + \frac{1}{b^{2^m}} \right)^{2^m+1} = \frac{c}{b^{2^m+1}} + \frac{\delta^{2^m}}{b^{2^m}} + \frac{c\delta}{b} + d, \tag{80}$$

by the assumption. Now, $\gcd(2^m + 1, 2^n - 1) = 1$ means that y^{2^m+1} is a permutation of $\mathbb{F}_{2^n}$. Therefore there is a unique y satisfying equation (80).

Example 9. Let $m = 2, k = 3$, then $n = 6$. Let $\delta \in \mathbb{F}_{2^6}$ be any element, $b, c \in \mathbb{F}_{2^6}/\mathbb{F}_2$, satisfying $c = b^{48}$. Using Magma, it can be verified that

$$g(x) = (bx + \delta)^5 + x^4 + cx \tag{81}$$

is a permutation polynomial over $\mathbb{F}_{2^6}$.

4.4. PPs of Type $(x^{2^m} + x + \delta)^{-s} + bx$ over $\mathbb{F}_{2^{2m}}$. In the following proposition, we consider PPs of type $(x^{2^m} + x + \delta)^{-s} + bx$ over $\mathbb{F}_{2^{2m}}$.

Proposition 12. *Let s, m be positive integers satisfying $(2^m + 2)(-s) \equiv 2^m - 1 \ (mod 2^{2m} - 1)$, where m is an odd integer. Let $\delta \in \mathbb{F}_{2^m}$, then the polynomial*

$$g(x) = \left(x^{2^m} + x + \delta \right)^{-s} + bx \tag{82}$$

is a permutation of $\mathbb{F}_{2^{2m}}$, with $b \in \mathbb{F}_{2^m} \backslash \mathbb{F}_2$.

Proof. Since $\gcd(2^m + 2, 2^m + 1) = 1$, and $\gcd(2^m + 2, 2^m - 1) = \gcd(3, 2^m - 1) = 1$ for m odd,

$$\gcd\left(2^m + 2, 2^{2m} - 1 \right) = 1. \tag{83}$$

To prove that $g(x)$ is a permutation polynomial, it is enough to prove that for any $d \in \mathbb{F}_{2^{2m}}$, $g(x) = d$ has a unique solution. That is

$$\left(x^{2^m} + x + \delta \right)^{-s} = bx + d \tag{84}$$

is satisfied by at most one x. By (83), taking the $(2^m + 2)^{th}$ power on both sides of the above equation gives the equivalent equation:

$$\left(x^{2^m} + x + \delta \right)^{2^m-1} = (bx + d)^{2^m+2}. \tag{85}$$

First, if there exists a solution x such that

$$x^{2^m} + x + \delta = 0, \tag{86}$$

then $x = d/b$, for the right side of equation (85) is also zero. In this case, the above equation becomes

$$\frac{d^{2^m}}{b^{2^m}} + \frac{d}{b} + \delta = 0. \tag{87}$$

Second, let us assume that $x^{2^m} + x + \delta \neq 0$. Since taking the $(2^m + 1)^{\text{th}}$ power, the left side of equation (85) is 1, and the right side is in the unit circle $\mathcal{U}$, that is,

$$(bx + d)^{2^m+2} = \lambda_0, \tag{88}$$

for some $\lambda_0 \in \mathcal{U}$. But since $\gcd(2^m + 2, 2^m + 1) = 1$,

$$bx + d = \lambda, \tag{89}$$

for some $\lambda \in \mathcal{U}$. Thus

$$(bx + d)^{2^m+2} = \lambda^{2^m+2} = \lambda = bx + d. \tag{90}$$

And equation (85) can be rewritten as

$$\left(x^{2^m} + x + \delta\right)^{2^m-1} = bx + d. \tag{91}$$

Since $\delta^{2^m} = \delta$, the left side of the above equation becomes

$$\frac{x^{2^m} + x + \delta^{2^m}}{x^{2^m} + x + \delta} = 1. \tag{92}$$

So, we have $x = d + 1/b$.

Now, the above two situations can be summarized. For every element $d \in \mathbb{F}_{2^{2m}}$, if d satisfies equation (87), there are two possibilities for the values of x as considered above. But $x = d + 1/b$ is not the solution. For substituting it into equation (85), the left side becomes

$$\left(\frac{d^{2^m}}{b^{2^m}} + \frac{d}{b} + \delta + \frac{1}{b^{2^m}} + \frac{1}{b}\right)^{2^m-1} = \left(\frac{1}{b^{2^m}} + \frac{1}{b}\right)^{2^m-1} = 0. \tag{93}$$

It is not equal to the right side which now becomes 1. If d does not satisfy equation (87), and if x is a solution of equation (85), then $x^{2^m} + x + \delta \neq 0$. The second situation tells us that the only solution is $x = d + 1/b$.

Example 10. Set $m = 3, s = 6$. Let $\delta \in \mathbb{F}_{2^3}$ be any element, and $b \in \mathbb{F}_{2^3} \backslash \mathbb{F}_2$. Using Magma, it can be verified that

$$g(x) = \left(x^8 + x + \delta\right)^{57} + bx \tag{94}$$

is a permutation polynomial over $\mathbb{F}_{2^6}$.

4.5. PPs of Type $x^{2^{m+1}} + b'x^2 + bx$ over $\mathbb{F}_{2^{2m}}$. In the following proposition, we consider PPs of type $x^{2^{m+1}} + b'x^2 + bx$ over $\mathbb{F}_{2^{2m}}$.

Proposition 13. *For the finite field $\mathbb{F}_{2^{2m}}$, let $b' \in \mathcal{U}$ be in the unit circle, and $b \notin \mathbb{F}_{2^m}$ satisfying $b^{2(2^m-1)}b'^3 = 1$. Then the linearized polynomial*

$$g(x) = x^{2^{m+1}} + b'x^2 + bx \tag{95}$$

is a permutation polynomial of $\mathbb{F}_{2^{2m}}$.

Proof. By the assumption, it can be checked that

$$b' \neq b^{1-2^m}. \tag{96}$$

Otherwise from $b^{2(2^m-1)}b'^3 = 1$, we have $b^{2^m-1} = 1$, contradiction with the condition that $b \notin \mathbb{F}_{2^m}$.

Since $g(x)$ is a linearized polynomial; to verify that it is a permutation polynomial, it is necessary to check that

$$g(x) = x^{2^{m+1}} + b'x^2 + bx = 0 \tag{97}$$

has only the zero solution. There are two situations to be considered.

First assume that $x \in \mathbb{F}_{2^m}^*$ is a solution of (97), and then

$$g(x) = x^{2^{m+1}} + b'x^2 + bx = x^2 + b'x^2 + bx = 0. \tag{98}$$

That is,

$$(1 + b')x + b = 0. \tag{99}$$

If $b' = 1$, the above equation becomes $b = 0$, contradiction. So, let us assume that $b' \neq 1$, then

$$x = \frac{b}{1 + b'}. \tag{100}$$

But we have $x \in \mathbb{F}_{2^m}^*$, that is, $x^{2^m} = x$, and thus

$$\frac{b^{2^m}}{1 + b'^{2^m}} = \frac{b}{1 + b'}. \tag{101}$$

So,

$$\frac{b^{2^m}b'}{1 + b'} = \frac{b}{1 + b'}, \tag{102}$$

which implies that

$$b' = b^{1-2^m}, \tag{103}$$

contradiction with equation (96).

Second let us assume that $x \in \mathbb{F}_{2^{2m}}\mathbb{F}_{2^m}$; by Lemma 7, we can write

$$x = u\lambda. \tag{104}$$

with $u \in \mathbb{F}_{2^m}^*$ and $\lambda \in \mathcal{U}$. Substituting the above x into equation (97),

$$g(x) = x^{2^{m+1}} + b'x^2 + bx = u^2\frac{1}{\lambda^2} + b'u^2\lambda^2 + bu\lambda = 0. \tag{105}$$

That is,

$$u\frac{1}{\lambda^2} + b'u\lambda^2 + b\lambda = u\left(\frac{1}{\lambda^2} + b'\lambda^2\right) + b\lambda = 0. \tag{106}$$

If $\lambda^4 = 1/b' = b'^{2^m}$. The above equation becomes $b\lambda = 0$, contradiction. So, $\lambda^4 \neq 1/b\prime$; that is,

$$\frac{1}{\lambda^2} + b'\lambda^2 \neq 0. \tag{107}$$

Then from equation (106),

$$u = \frac{b\lambda}{b'\lambda^2 + 1/\lambda^2}. \tag{108}$$

Since $u \in \mathbb{F}_{2^m}^*$, we have that $u^{2^m} = u$. The above equation becomes

$$\begin{aligned} \frac{b\lambda}{b'\lambda^2 + 1/\lambda^2} &= \frac{b^{2^m}\lambda^{2^m}}{b'^{2^m}\lambda^{2^{m+1}} + 1/\lambda^{2^{m+1}}} \\ &= \frac{b^{2^m} 1/\lambda}{b'^{2^m} 1/\lambda^2 + \lambda^2}. \end{aligned} \tag{109}$$

That is,

$$\frac{b\lambda^3}{b'\lambda^4 + 1} = \frac{b^{2^m}\lambda}{b'^{2^m} + \lambda^4} \Longleftrightarrow \frac{b\lambda^2}{b'\lambda^4 + 1} = \frac{b^{2^m}}{b'^{2^m} + \lambda^4}, \tag{110}$$

which can be rewritten as

$$\begin{aligned} b\lambda^6 + bb'^{2^m}\lambda^2 = b'b^{2^m}\lambda^4 + b^{2^m} \Longleftrightarrow \lambda^6 + b'b^{2^m-1}\lambda^4 \\ + b'^{2^m}\lambda^2 + b^{2^m-1} = 0. \end{aligned} \tag{111}$$

Let $\lambda_0 = \lambda^2$; equation (111) can be transformed into

$$\lambda_0^3 + b'b^{2^m-1}\lambda_0^2 + b'^{2^m}\lambda_0 + b^{2^m-1} = 0. \tag{112}$$

Take derivative of the above equation;

$$\lambda_0^2 + b'^{2^m} = 0. \tag{113}$$

Substituting $\lambda_0^2 = b'^{2^m}$ into equation (112),

$$b'^{2^m}\lambda_0 + b'^{2^m+1}b^{2^m-1} + b'^{2^m}\lambda_0 + b^{2^m-1} = b^{2^m-1} + b^{2^m-1} = 0. \tag{114}$$

That is, $\lambda_0 = b'^{2^{m-1}}$ is a double root of (21), which has three roots at most counting multiplicity. But,

$$\lambda^4 = \lambda_0^2 = b'^{2^m}, \tag{115}$$

contradiction with equation (107).

The third root of (112) is

$$\lambda_1 = \frac{b^{2^m-1}}{b'^{2^m}} = b^{2^m-1}b'. \tag{116}$$

So

$$\lambda^2 = \lambda_1 = b^{2^m-1}b' \Longleftrightarrow \lambda^4 = b^{2(2^m-1)}b'^2. \tag{117}$$

And equation (106) becomes

$$u\left(\frac{1 + b'\lambda^4}{\lambda^2}\right) + b\lambda = u\left(\frac{1 + b^{2(2^m-1)}b'^3}{\lambda^2}\right) + b\lambda = b\lambda = 0, \tag{118}$$

by assumption, contradiction.

Example 11. Set $m = 4$. Let $b' \in \mathcal{U}$ be any element of the unit circle in $\mathbb{F}_{2^8}\backslash\mathbb{F}_{2^4}$, $b \in \mathbb{F}_{2^8}\backslash\mathbb{F}_{2^4}$ satisfying $b^{30}b'^3 = 1$. Using Magma, it can be verified that

$$g(x) = x^{32} + b'x^2 + bx \tag{119}$$

is a permutation polynomial over $\mathbb{F}_{2^8}$.

4.6. PPs of Type $x^r(x^{q-1} + a)$ over $\mathbb{F}_{q^e}$. In the following proposition, we study PPs of type $x^r(x^{q-1} + a)$ over $\mathbb{F}_{q^e}$.

Proposition 14. *Let $\mathbb{F}_q$ be the finite field with q elements, then*

$$g(x) = x^r\left(x^{q-1} + a\right) \tag{120}$$

is a permutation polynomial over $\mathbb{F}_{q^e}$ for $r = 1, q^{e-1} + q^{e-2} + \cdots + q^2 + 1$. Here $a \in \mathbb{F}_{q^e}^*$ satisfying $a^{q^{e-1}+q^{e-2}+\cdots+q+1} \neq (-1)^e$, and gcd (e-1, q-1) = 1.

Proof. This can be obtained using Lemma 5.

Example 12. Let $q = 5, e = 4$, and ω be a primitive root of the finite field $\mathbb{F}_{5^4}$, then $r = 1, q^3 + q^2 + 1 = 151$. Using Magma, it can be verified that for $a = w^i$, with $1 \leq i \leq 623, i \neq 0 \bmod 4$,

$$g(x) = x^r\left(x^4 + a\right) \tag{121}$$

is a permutation polynomial over $\mathbb{F}_{5^4}$.

5. Necessities of Two Kinds of Permutation Polynomials

In this section, we investigate the necessities of two classes of permutation polynomials studied in [37], where the sufficient conditions are given.

5.1. PPs of Type $(x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}} + bx$ over $\mathbb{F}_{2^{2m}}$. In [[42], Proposition 10], X. Xu et al. proposed a class of permutation polynomials of the form $(x^{2^m} + x + \delta)^{2^{2m-1}+2^{m-1}} + bx$ over $\mathbb{F}_{2^{2m}}$, and sufficient conditions were given. In the following proposition, we consider its necessary conditions.

Proposition 15. *For a positive integer m and a fixed $\delta \in \mathbb{F}_{2^{2m}}$ with $Tr_m^{2m}(\delta) \neq 0$, let*

$$g(x) = \left(x^{2^m} + x + \delta\right)^{2^{2m-1}+2^{m-1}} + bx, \tag{122}$$

where $b \in \mathbb{F}_{2^{2m}}$. When $b \notin \mathbb{F}_{2^m}$, $g(x)$ is permutation polynomial if and only if $b + b^m = b^{2^m+1}$.

Proof. As pointed out at the beginning of this subsection, ([42], Proposition 10) gives the sufficiency verification. Now let us consider the necessity.

Assume that $g(x)$ is a permutation polynomial. Then for every $d \in \mathbb{F}_{2^{2m}}$, $g(x) = d$ has a unique solution. That is,

$$\left(x^{2^m} + x + \delta\right)^{2^{2m-1}+2^{m-1}} + bx = d \tag{123}$$

has at most one possible root in $\mathbb{F}_{2^{2m}}$. Squaring both sides of the above equation, we get the following equivalent equation

$$\left(x^{2m}+x+\delta\right)^{2^{2m}+2^m}+b^2x^2=d^2. \tag{124}$$

That is,

$$\left(x^{2^m}+x+\delta\right)\left(x^{2^m}+x+\delta^{2^m}\right)=b^2x^2+d^2, \tag{125}$$

which can be transformed into

$$\left(x^{2^m}+x\right)^2+\left(\delta+\delta^{2^m}\right)\left(x^{2^m}+x\right)+\delta^{2^m+1}=b^2x^2+d^2, \tag{126}$$

which implies that

$$x^{2^{m+1}}+\left(\delta+\delta^{2^m}\right)x^{2^m}+\left(b^2+1\right)x^2+\left(\delta+\delta^{2^m}\right)x+\delta^{2^m+1}+d^2=0 \tag{127}$$

has a unique solution in $\mathbb{F}_{2^{2m}}$.

Then for $x_1\neq x_2\in\mathbb{F}_{2^{2m}}$ with x_1 a solution of equation (127), the following equation:

$$x_2^{2^{m+1}}+\left(\delta+\delta^{2^m}\right)x_2^{2^m}+\left(b^2+1\right)x_2^2+\left(\delta+\delta^{2^m}\right)x_2+\delta^{2^m+1}+d^2=0, \tag{128}$$

cannot hold. Adding the above two equations,

$$\begin{aligned}&\left(x_1+x_2\right)^{2^{m+1}}+\left(\delta+\delta^{2^m}\right)\left(x_1+x_2\right)^{2^m}\\&+\left(b^2+1\right)\left(x_1+x_2\right)^2+\left(\delta+\delta^{2^m}\right)\left(x_1+x_2\right)=0\end{aligned} \tag{129}$$

does not hold for any x_2 different from x_1. Now let $y=x_1+x_2$. With x_1 fixed and x_2 varying, y can be any nonzero element of the finite field $\mathbb{F}_{2^{2m}}$. So,

$$y^{2^{m+1}}+\left(\delta+\delta^{2^m}\right)y^{2^m}+\left(b^2+1\right)y^2+\left(\delta+\delta^{2^m}\right)y=0 \tag{130}$$

has only the solution zero in $\mathbb{F}_{2^{2m}}$, and this is from the assumption that $g(x)$ is a permutation polynomial.

If a nonzero solution $y\in\mathbb{F}_{2^{2m}}$ of equation (130) exists. Taking the 2^mth power,

$$y^2+\left(\delta+\delta^{2^m}\right)y+\left(b^{2^{m+1}}+1\right)y^{2^{m+1}}+\left(\delta+\delta^{2^m}\right)y^{2^m}=0. \tag{131}$$

Adding equations (130) and (131),

$$b^{2^{m+1}}y^{2^{m+1}}+b^2y^2=\left(b^2y^2\right)^{2^m}+\left(b^2y^2\right)=0. \tag{132}$$

Thus,

$$(by)^{2^m}+(by)=0, \tag{133}$$

that is, by lies in the field $\mathbb{F}_{2^m}$. By Lemma 7, we can write

$$b=\frac{c_0}{\lambda_0}, \tag{134}$$

for some fixed $c_0\in\mathbb{F}_{2^m}\backslash\{0\}$, and $\lambda_0\in\mathscr{U}$ the unit circle. If y is written in the following form:

$$y=c\lambda, \tag{135}$$

for $c\in\mathbb{F}_{2^m}$ and $\lambda\in\mathscr{U}$. Since $by\in\mathbb{F}_{2^m}$, we must have $\lambda=\lambda_0$. That is,

$$y=c\lambda_0, \tag{136}$$

for some $c\in\mathbb{F}_{2^m}\backslash\{0\}$.

Substituting (134) and (136) into equation (130),

$$\frac{c^2}{\lambda_0^2}+\left(\delta+\delta^{2^m}\right)\frac{c}{\lambda_0}+\left(\frac{c_0^2}{\lambda_0^2}+1\right)c^2\lambda_0^2+\left(\delta+\delta^{2^m}\right)c\lambda_0=0. \tag{137}$$

Dividing c on both sides of the above equation,

$$\frac{c}{\lambda_0^2}+\left(\delta+\delta^{2^m}\right)\frac{1}{\lambda_0}+\left(\frac{c_0^2}{\lambda_0^2}+1\right)c\lambda_0^2+\left(\delta+\delta^{2^m}\right)\lambda_0=0, \tag{138}$$

which can be transformed into

$$\left(c_0^2+\lambda_0^2+\frac{1}{\lambda_0^2}\right)c=\left(\delta+\delta^{2^m}\right)\frac{1}{\lambda_0}+\left(\delta+\delta^{2^m}\right)\lambda_0. \tag{139}$$

By our assumption, equation (130) has no nonzero solution; then

$$c_0^2+\lambda_0^2+\frac{1}{\lambda_0^2}=0, \tag{140}$$

which is equivalent to

$$c_0=\lambda_0+\frac{1}{\lambda_0}, \tag{141}$$

for some $\lambda_0\neq1$ in $\mathscr{U}$, because $b\notin\mathbb{F}_{2^m}$. By equation (134),

$$b=1+\frac{1}{\lambda_0^2}, \tag{142}$$

That is,

$$b=1+\frac{1}{\lambda}, \tag{143}$$

for some $\lambda\in\mathscr{U}\backslash\{1\}$. So, we have

$$b^{2^m+1}=\left(1+\frac{1}{\lambda}\right)(1+\lambda)=\frac{1}{\lambda}+\lambda. \tag{144}$$

And

$$b^{2^m}+b=(1+\lambda)+\left(1+\frac{1}{\lambda}\right)=\frac{1}{\lambda}+\lambda, \tag{145}$$

which implies that

$$b^{2^m}+b=b^{2^m+1}, \tag{146}$$

that is, the necessity of our proposition.

Example 13. Let $m=4$, $\delta\in\mathbb{F}_{2^8}$ with $\mathrm{Tr}_m^{2m}(\delta)\neq0$. Using Magma, it can be verified that for $b\in\mathbb{F}_{2^8}\backslash\mathbb{F}_{2^4}$,

$$g(x)=\left(x^{16}+x+\delta\right)^{136}+bx \tag{147}$$

is not a permutation polynomial over $\mathbb{F}_{2^8}$ when $b^{16}+b\neq b^{17}$.

5.2. PPs of Type $(x^2+x+\delta)^{2^{2k-1}-2^{k-1}}+bx$ *over* $\mathbb{F}_{2^{2k}}$. In [[42], Proposition 6], Xu et al. proposed a class of permutation polynomials of the form $(x^2+x+\delta)^{2^{2k-1}-2^{k-1}}+bx$ over $\mathbb{F}_{2^{2k}}$, and sufficient conditions are given. In the following proposition, we consider its necessary conditions.

Proposition 16. *For nonnegative integers* n,k *with* $n=2k, k>1$, *let* $\delta\in\mathbb{F}_{2^n}$ *with* $Tr_1^n(\delta)=1$. *Then the polynomial*

$$g(x)=\left(x^2+x+\delta\right)^{2^{2k-1}-2^{k-1}}+bx \tag{148}$$

is a permutation of $\mathbb{F}_{2^n}$ *if and only if* $b\in\mathbb{F}_{2^k}\backslash\{0\}$.

Proof. The sufficiency is given in [[42], Proposition 6]. In the following, we only consider the necessity.

Assume that $b\notin\mathbb{F}_{2^k}$ and $g(x)$ is a PP.

Since $\mathrm{Tr}_1^n(\delta)=1$, $x^2+x+\delta$ is always nonzero by Lemma 2. For any $d\in\mathbb{F}_{2^n}$, the following equation:

$$\left(x^2+x+\delta\right)^{2^{2k-1}-2^{k-1}}+bx=d, \tag{149}$$

has only one solution, which can be transformed into

$$\left(x^2+x+\delta\right)^{2^{2k-1}-2^{k-1}}=bx+d. \tag{150}$$

Taking the $(2^k+1)^{\text{th}}$ power on both sides of the above equation,

$$1=(bx+d)^{2^k+1}. \tag{151}$$

So, $bx+d=\lambda$; that is,

$$x=\frac{\lambda+d}{b}, \tag{152}$$

for some element λ in the unit circle $\mathcal{U}$. Squaring both sides of equation (150)

$$\left(x^2+x+\delta\right)^{1-2^k}=(bx+d)^2, \tag{153}$$

that is,

$$\frac{x^2+x+\delta}{x^{2^{k+1}}+x^{2^k}+\delta^{2^k}}=\lambda^2, \tag{154}$$

which is equivalent to

$$x^2+x+\delta=\lambda^2\left(x^{2^{k+1}}+x^{2^k}+\delta^{2^k}\right). \tag{155}$$

Substituting (152) into the above equation,

$$\left(\frac{1}{b^2}+\frac{d^{2^{k+1}}}{b^{2^{k+1}}}+\frac{d^{2^k}}{b^{2^k}}+\delta^{2^k}\right)\lambda^2+\left(\frac{1}{b}+\frac{1}{b^{2^k}}\right)\lambda+\frac{d^2}{b^2}+\frac{d}{b}+\frac{1}{b^{2^{k+1}}}+\delta=0. \tag{156}$$

We can choose d such that

$$\frac{1}{b^2}+\frac{d^{2^{k+1}}}{b^{2^{k+1}}}+\frac{d^{2^k}}{b^{2^k}}+\delta^{2^k}\neq 0. \tag{157}$$

Since $g(x)$ is a permutation polynomial, there must exists λ_1 in the unit circle $\mathcal{U}$, satisfying equation (156). Then

$$x_1=\frac{\lambda_1+d}{b} \tag{158}$$

satisfies equation (153), and in fact $g(x)=d$, since they are equivalent. Equation (156) can be transformed into

$$\lambda^2+\frac{1/b+1/b^{2^k}}{1/b^2+d^{2^{k+1}}/b^{2^{k+1}}+d^{2^k}/b^{2^k}+\delta^{2^k}}\lambda+\frac{\left(1/b^2+d^{2^{k+1}}/b^{2^{k+1}}+d^{2^k}/b^{2^k}+\delta^{2^k}\right)^{2^k}}{1/b^2+d^{2^{k+1}}/b^{2^{k+1}}+d^{2^k}/b^{2^k}+\delta^{2^k}}=0. \tag{159}$$

Since $(1/b^2+d^{2^{k+1}}/b^{2^{k+1}}+d^{2^k}/b^{2^k}+\delta^{2^k})^{2^k}/1/b^2+d^{2^{k+1}}/b^{2^{k+1}}+d^{2^k}/b^{2^k}+\delta^{2^k}$ is in the unit circle, the other root of equation (156), which we denote λ_2, is also in the unit circle $\mathcal{U}$. And

$$\lambda_1\neq\lambda_2, \tag{160}$$

since $\lambda_1+\lambda_2=1/b+1/b^{2^k}\neq 0$ for $b\notin\mathbb{F}_{2^k}$.

Now, for equation (152), set

$$x_2=\frac{\lambda_2+d}{b}. \tag{161}$$

Then x_2 satisfies equation (153) also, that is, $g(x)=d$ has two solutions x_1,x_2 for such d, contradiction.

Example 14. Set $k=4$; then $n=8$. Let $\delta\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta)=1$. Using Magma, it can be verified that, for $b\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^k}$,

$$g(x)=\left(x^2+x+\delta\right)^{120}+bx \tag{162}$$

is not a permutation polynomial over $\mathbb{F}_{2^8}$.

6. Conclusion

In this paper, based on the results obtained recently about permutation polynomials, we get some further PPs. Also, with suitable modifications on the conditions, some new classes of PPs are proposed. To do this, some coefficients of the original permutation polynomials are made to be variable, or the exponents are unfixed, or the field extensions are different from their work. We also investigate the necessities of permutation properties of the polynomials studied in [37], where the sufficient conditions are given. For future work, Lie et al. [44] combine network aggregation and algebraic state space representation (ASSR) to solve the state feedback stabilization problem of large-scale logical control networks

(LCNs), stability analysis of nonlinear systems on time scales is further investigated in [45], the H_∞ problem of nonlinear descriptor systems (NDSs) is investigated in [46], and the containment problem of finite-field networks (FFNs) with fixed topology (FT-FFNs) and switching topology (ST-FFNs) is studied in [17]. In these works, the authors utilized algebraic properties of some state space representations, and containment problem of finite-field networks (FFNs) is studied using semitensor product (STP) of matrices. By considering their permutation properties, some further results might be obtained.

Data Availability

The data used to support the theoretical findings were generated using Magma.

Disclosure

Reference [24] is just an incomplete draft of this work.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by Research Foundation for Advanced Talents of Nanjing Tech University.

References

[1] D. Feng, X. Feng, W. Zhang, X. Fan, and C. Wu, "Loiss: a byte-oriented stream cipher," in *Proceedings of the IWCC'11 Proceedings of the Third International Conference on Coding and Cryptology*, pp. 109–125, Qingdao, China, June 2011.

[2] C. P. Schnorr and S. Vaudenay, "Black box cryptanalysis of hash networks based on multipermutations," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–57, Perugia, Italy, May 1995.

[3] L. Carlitz, "Some theorems on permutation polynomials," *Bulletin of the American Mathematical Society*, vol. 68, no. 2, pp. 120–122, 1962.

[4] K. Li, L. Qu, X. Chen, and C. Li, "Permutation polynomials of the form cx + $\mathrm{Tr}_q^{q^l}(x_a)$ and permutation trinomials over finite fields with even characteristic," *Cryptography and Communications*, vol. 10, no. 3, pp. 531–554, 2018.

[5] Y. H. Park and J. B. Lee, "Permutation polynomials and group permutation polynomials," *Bulletin of the Australian Mathematical Society*, vol. 63, no. 1, pp. 67–74, 2001.

[6] H. B. Mann, "The construction of orthogonal Latin squares," *The Annals of Mathematical Statistics*, vol. 13, no. 4, pp. 418–423, 1942.

[7] L. Mittenthal, "Block substitutions using orthomorphic mappings," *Advances in Applied Mathematics*, vol. 16, no. 10, pp. 59–71, 1995.

[8] L. Mittenthal, "Nonlinear dynamic substitution devices and methods for block substitutions employing coset decompositions and direct geometric generation," European Patent Office, Munich, Germany, US Patent 5647001, 1997.

[9] W. Diffie and G. Ledin, "SMS4 encryption algorithm for wireless networks," 2008, https://eprint.iacr.org/2008/329.pdf.

[10] S. Vaudenay, "On the Lai-Massey scheme," *Advances in Cryptology-ASIACRYPT'99*, vol. 1716, pp. 8–19, 1999.

[11] S. Markovski and A. Mileva, "Generating huge quasigroups from small non-linear bijections via extended Feistel function," *Quasigroups And Related Systems*, vol. 17, no. 1, pp. 91–106, 2009.

[12] M. Matsui, "New block encryption algorithm MISTY," in *Proceedings of the Fast Software Encryption*, pp. 54–68, Haifa, Israel, January 1997.

[13] A. Mileva and S. Markovski, "Quasigroup representation of some Feistel and generalized Feistel ciphers," in *ICT Innovations 2012. Advances in Intelligent Systems and Computing*, pp. 161–171, Springer, Heidelberg, Germany, 2012.

[14] S. Vaudenay, "On the need for multipermutations: cryptanalysis of MD4 and SAFER," *Fast Software Encryption*, vol. 1008, pp. 286–297, 1994.

[15] Y. Li, H. Li, and X. Ding, "Set stability of switched delayed logical networks with application to finite-field consensus," *Automatica*, vol. 113, Article ID 108768, 2020.

[16] Y. Li, H. Li, and G. Zhao, "Optimal state estimation for finite-field networks with stochastic disturbances," *Neurocomputing*, vol. 414, pp. 238–244, 2020.

[17] Y. Liu, M. Song, H. Li, Y. Li, and W. Hou, "Containment problem of finite-field networks with fixed and switching topology," *Applied Mathematics and Computation*, vol. 411, no. C, 2021.

[18] L. Carlitz and C. Wells, "The number of solutions of a special system of equations in a finite field," *Acta Arithmetica*, vol. 12, no. 1, pp. 77–84, 1966.

[19] X.-D. Hou and S. D. Lappano, "Determination of a type of permutation binomials over finite fields," *Journal of Number Theory*, vol. 147, pp. 14–23, 2015.

[20] X.-D. Hou, "Permutation polynomials over finite fields-a survey of recent advances," *Finite Fields and Their Applications*, vol. 32, pp. 82–119, 2015.

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

[22] N. Li and T. Helleseth, "Several classes of permutation trinomials from Niho exponents," *Cryptography and Communications*, vol. 9, no. 6, pp. 693–705, 2017.

[23] X. Liu, "Necessary and sufficient conditions of two classes of permutation polynomials," *Finite Fields and Their Applications*, vol. 77, Article ID 101949, 2022.

[24] X. Liu, "Constructions and necessities of some permutation polynomials," 2019, https://arxiv.org/abs/1906.06453.

[25] J. Ma and G. Ge, "A note on permutation polynomials over finite fields," *Finite Fields and Their Applications*, vol. 48, pp. 261–270, 2017.

[26] B. Wu and D. Lin, "On constructing complete permutation polynomials over finite fields of even characteristic," *Discrete Applied Mathematics*, vol. 184, pp. 213–222, 2015.

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

[28] G. Wu, N. Li, T. Helleseth, and Y. Zhang, "Some classes of complete permutation polynomials over F_q," *Science China Mathematics*, vol. 58, no. 10, pp. 1–14, 2015.

[29] G. Xu and X. Cao, "Complete permutation polynomials over finite fields of odd characteristic," *Finite Fields and Their Applications*, vol. 31, pp. 228–240, 2015.
[30] Y. Yuan, Y. Tong, and H. Zhang, "Complete mapping polynomials over finite field F_{16}," *Lecture Notes in Computer Science*, vol. 4547, pp. 147–158, 2007.
[31] Z. Zha, L. Hu, and S. Fan, "Further results on permutation trinomials over finite fields with even characteristic," *Finite Fields and Their Applications*, vol. 45, pp. 43–52, 2017.
[32] P. Charpin and G. M. Kyureghyan, "On a class of permutation polynomials over $\mathbb{F}_2$," in *Sequence and Their Application-SETA 2008*, pp. 368–376, Springer, Heidelberg, Germany, 2008.
[33] P. Charpin and G. M. Kyureghyan, "Monomial functions with linear structure and permutation polynomials," *Finite Fields and Their Applications*, vol. 518, no. 16, pp. 99–111, 2010.
[34] G. Kyureghyan and M. E. Zieve, "Permutation polynomials of the form $x + \gamma\,\mathrm{Tr}(x^k)$ over Fqn," *Finite Fields and Applications*, World Scientific, vol. 76, , pp. 178–194, 2021.
[35] D. Zheng, M. Yuan, and L. Yu, "Two types of permutation polynomials with special forms," *Finite Fields and Their Applications*, vol. 56, pp. 1–16, 2019.
[36] L. Li, C. Li, C. Li, and X. Zeng, "New classes of complete permutation polynomials," *Finite Fields and Their Applications*, vol. 55, pp. 177–201, 2019.
[37] X. Xu, X. Feng, and X. Zeng, "Complete permutation polynomials with the form $(x^{p^m}-x+\delta)^s+axp^m+bx$ over $\mathbb{F}p^n$," *Finite Fields and Their Applications*, vol. 57, pp. 309–343, 2019.
[38] G. McGuire and J. Sheekey, "A characterization of the number of roots of linearized and projective polynomials in the field of coefficients," *Finite Fields and Their Applications*, vol. 57, pp. 68–91, 2019.
[39] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.
[40] Z. Tu, X. Zeng, and L. Hu, "Several classes of complete permutation polynomials," *Finite Fields and Their Applications*, vol. 25, pp. 182–193, 2014.
[41] M. E. Zieve, "On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q?1)=d})$," *Proceedings of the American Mathematical Society*, vol. 137, no. 7, pp. 2209–2216, 2009.
[42] A. Akbary, D. Ghioca, and Q. Wang, "On constructing permutations of finite fields," *Finite Fields and Their Applications*, vol. 17, no. 1, pp. 51–67, 2011.
[43] L. Li, S. Wang, C. Li, and X. Zeng, "Permutation polynomials $(x^{p^m}-x+\delta)^{s1}+(x^{p^m}-x+\delta)^{s2}+x$ over $\mathbb{F}^{pn}$," *Finite Fields and Their Applications*, vol. 51, pp. 31–61, 2018.
[44] H. Li, Y. Liu, S. Wang, and B. Niu, "State feedback stabilization of large-scale logical control networks via network aggregation," *IEEE Transactions on Automatic Control*, vol. 66, 2021.
[45] X. Lu and H. Li, "An improved stability theorem for nonlinear systems on time scales with application to multi-agent systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 12, pp. 3277–3281, 2020.
[46] X. Lu and H. Li, "A hybrid control approach to H_∞ problem of nonlinear descriptor systems with actuator saturation," *IEEE Transactions on Automatic Control*, vol. 66, no. 10, pp. 4960–4966, 2021.