Hindawi
Journal of Mathematics
Volume 2021, Article ID 5872429, 7 pages
https://doi.org/10.1155/2021/5872429

Research Article

A Class of New Permutation Polynomials over $\mathbb{F}_{2^n}$

Qian Liu,[1,2] **Ximeng Liu**,[1,2] **and Jian Zou**[1,2]

[1]*College of Computer and Data Science, Fuzhou University, Fuzhou 350116, China*
[2]*Key Laboratory of Information Security of Network Systems, Fuzhou University, Fuzhou 350116, China*

Correspondence should be addressed to Qian Liu; lqmova@foxmail.com

Received 14 August 2021; Accepted 15 October 2021; Published 15 November 2021

Academic Editor: Li Guo

In this paper, according to the known results of some normalized permutation polynomials with degree 5 over $\mathbb{F}_{2^n}$, we determine sufficient and necessary conditions on the coefficients $(b_1, b_2) \in \mathbb{F}_{2^n}^2$ such that $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ permutes $\mathbb{F}_{2^n}$. Meanwhile, we obtain a class of complete permutation binomials over $\mathbb{F}_{2^n}$.

1. Introduction

Denote $\mathbb{F}_q$ as a finite field with q elements, where q is a prime power; then, $\mathbb{F}_q^*$ is its multiplicative group. The bijectivity of the associated polynomial mapping(s) $f: x \longmapsto f(x)$ from $\mathbb{F}_q$ into itself (and $f(x) + x$) makes a polynomial $f(x) \in \mathbb{F}_q[x]$ as a (complete) permutation polynomial [1]. Research interests in (complete) permutation polynomials over finite fields have been aroused due to their widespread applications in cryptography [2, 3], combinatorial designs [4], design theory [1, 5], coding theory [6], and other areas of mathematics and engineering [1, 7]. Readers could refer to [1, 8] for a comprehensive survey about (complete) permutation polynomials. So, it is important to realize that there is significance in discovering new methods to construct permutation polynomials. Readers can find recent progress in [9, 10].

Few-term permutation polynomials, especially binomials and trinomials, have not only simple algebraic form but excellent properties. The following form over $\mathbb{F}_{2^n}$ from Niho exponents has drawn much attention:

$$f(x) = x^r\left(1 + b_1x^{s(2^m-1)} + b_2x^{t(2^m-1)}\right), \tag{1}$$

where $n = 2m$, $r, s, t \in \mathbb{Z}$, $b_1, b_2 \in \mathbb{F}_{2^n}$. Note that (s, t) can be viewed as modulo $2^m + 1$. It is a hard problem to find necessary and sufficient conditions on (b_1, b_2) for (1) being a permutation polynomial over $\mathbb{F}_{2^n}$ with given (r, s, t). In most known cases, the coefficients are assumed to be trivial, such as $(b_1, b_2) = (1, 1)$; some pairs (r, s, t) in (1) were made in [10–15]. For $(r, s, t) = (1, 1, 2)$, Hou [16] completely characterized all non-trivial (b_1, b_2) over $\mathbb{F}_{q^2}$ through the Hermite criterion. After that, Tu et al. [17] studied the case over $\mathbb{F}_{q^2}$ where $(r, s, t) = (1, 2^m, 2)$ by solving low-degree equations with variable in the unit circle. The latter only obtained the sufficient conditions but conjectured their necessity based on numerical experiments, which were then proved by Bartoli [18] and Hou [19], respectively, using algebraic curves over finite fields and the Hasse–Weil bound. In 2018, Tu and Zeng [20] determined all (b_1, b_2) with $(r, s, t) = (1, 2^{m-1}, 2^{n-1})$ and gave sufficient conditions for $(r, s, t) = (1, 3 \cdot 2^{2m-2}, 2^{2m-2})$ over $\mathbb{F}_{2^n}$, the necessity of which was later proved by Hou [21], using a similar method described in [19]. Recently, Zheng et al. [22] claimed sufficient conditions for both $(r, s, t) = (1, 1, (2^k(2^{mk} - 1)/((2^k - 1)(2^m - 1))))$ and $(r, s, t) = (1, (2^k/(2^k - 1)), (-1/(2^k - 1)))$ over $\mathbb{F}_{2^n}$. Furthermore, they conjectured the necessity of the former based on numerical experiments. Very recently, by making use of the similar approach in [18], Bartoli and Timpanella [23] provided necessary conditions for $(r, s, t) = (n + m, m, n)$ over finite fields with characteristic 2.

To our knowledge, only above seven different pairs (r, s, t) had been characterized completely. However, the exponents of $f(x)$ in (1) are also Niho exponents. This motivates us to explore new permutation polynomials with general coefficients (b_1, b_2) from non-Niho exponents with even characteristics. By transforming the problem into studying some normalized permutation polynomials with

degree 5 over even characteristics, we determine the coefficients (b_1, b_2) for $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ being a permutation over $\mathbb{F}_{2^n}$.

The rest of this paper is arranged as follows. Some notations and useful results are presented in Section 2. In Section 3, the sufficient and necessary conditions are shown to determine the coefficients of a class of permutation polynomials over $\mathbb{F}_{2^n}$. Finally, Section 4 provides some concluding remarks.

2. Preliminaries

Let m and n be two positive integers with $m|n$ and $\mathbb{F}_{2^n}$ be a finite field with 2^n elements; the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is denoted by $\mathrm{Tr}_m^n(\cdot)$, where

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

If the usual complex conjugation of any $x \in \mathbb{F}_{2^{2m}}$ is defined as $\overline{x} = x^{2^m}$, the following relations hold.

(i) For all $x \in \mathbb{F}_{2^{2m}}$, $x + \overline{x} \in \mathbb{F}_{2^m}$, $x\overline{x} \in \mathbb{F}_{2^m}$.

(ii) For all $x, y \in \mathbb{F}_{2^{2m}}$, $\overline{x+y} = \overline{x} + \overline{y}, \overline{xy} = \overline{x}\,\overline{y}$.

U_{2^m+1} denotes the unit circle of $\mathbb{F}_{2^{2m}}$ as

$$U_{2^m+1} = \left\{x \in \mathbb{F}_{2^{2m}} : x^{2^m+1} = x\overline{x} = 1\right\}. \tag{3}$$

Lemma 1 (see [24]). *$f(x) \in \mathbb{F}_q[x]$ with $f(0) = 0$ is a permutation polynomial over $\mathbb{F}_q$ iff $f: x \longmapsto f(x)$ from $\mathbb{F}_q^*$ into itself is a bijection.*

Hereinafter, we claim that $f(x)$ is a permutation polynomial over $\mathbb{F}_q^*$ upon the bijectivity of $f(x)$ from $\mathbb{F}_q^*$ to $\mathbb{F}_q^*$, which is the only case we consider.

Lemma 2 (see [1]). *The irreducibility of $f(x) \in \mathbb{F}_q[x]$ with degree n remains over $\mathbb{F}_{p^m}$ iff* $\gcd(m, n) = 1$.

Definition 1 (see [25]). A permutation polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is said to be normalized if the following properties hold:

(i) $f(x)$ is monic and the value of $f(x)$ at 0 is equal to 0.

(ii) The coefficient of x^{n-1} equals 0 if $p \nmid n$, where p is the characteristic of $\mathbb{F}_q$.

Remark 1. Let $b, c \in \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$; for any permutation polynomial $f(x) \in \mathbb{F}_q[x]$, there exists a unique normalized form provided by $g(x) = af(x + b) + c$.

Theorem 1 (Hermite's criterion) (see [1]). *Let p be the characteristic of $\mathbb{F}_q$. Thus, $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial over $\mathbb{F}_q$ iff*

(i) $f(x)$ has exactly one solution over $\mathbb{F}_q$.

(ii) $\forall t \in \mathbb{Z}$, where $1 \le t \le q-2$, $t \neq 0 \pmod p$, the degree of the reduction of $f(x)^t \pmod{x^q - x}$ is no greater than $q-2$.

From Hermite's criterion, the characterization of all normalized permutation polynomials with degree no greater than 5 in $\mathbb{F}_q$ is due to ([1], Section 7.2), and they are listed in Table 1.

3. A Class of Permutation Polynomials over $\mathbb{F}_{2^n}$

In this section, we consider the coefficients $b_1, b_2 \in \mathbb{F}_{2^n}$ such that the polynomial $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ permutes over $\mathbb{F}_{2^n}$.

The main results in this paper are given in the following theorems.

Theorem 2. *For two positive integers m and n with $n = 2m$, let $b_1, b_2 \in \mathbb{F}_{2^n}$. Define $g(z) = z^5 + z^3(b_1\overline{b_1} + b_2 + \overline{b_2}) + z^2[(b_1 + \overline{b_1})(b_1\overline{b_1} + b_2 + \overline{b_2}) + \overline{b_1}b_2 + b_1\overline{b_2}] + z[(b_1 + \overline{b_1})^4 + (b_1 + \overline{b_1})^2(b_1\overline{b_1} + b_2 + \overline{b_2}) + b_2\overline{b_2}] \in \mathbb{F}_{2^m}[z]$. Then, the polynomial*

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{4}$$

permutes $\mathbb{F}_{2^n}$ iff one of the following two cases holds:

(1) If $m \equiv 2 \pmod 4$, $g(x) = x^5$ permutes $\mathbb{F}_{2^m}$.

(2) If m is odd, $g(x) = x^5 + ax^3 + 5^{-1}a^2x$ permutes $\mathbb{F}_{2^m}$.

Proof. Based on Lemma 1, in order to prove that $f(x)$ is a permutation polynomial in $\mathbb{F}_{2^n}^*$, we only consider that for any $c \in \mathbb{F}_{2^n}^*$, the equation

$$x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x = c \tag{5}$$

has exactly one root in $\mathbb{F}_{2^n}^*$.

Let $x = \lambda y$, where $\lambda \in U_{2^m+1}$ and $y \in \mathbb{F}_{2^m}$. Then, equation (5) becomes

$$\lambda y^5 + b_1\lambda y^3 + b_2\lambda y = c. \tag{6}$$

Raising both sides of equation (6) to the power 2^m leads to

$$y^5 + \overline{b_1}y^3 + \overline{b_2}y = \lambda\overline{c}. \tag{7}$$

Since $c \in \mathbb{F}_{2^n}^*$, we can let $c = de$, where $d \in \mathbb{F}_{2^m}^*$ and $e \in U_{2^m+1}$. Then, equation (7) can be rewritten as

$$y^5 + \overline{b_1}y^3 + \overline{b_2}y = \lambda\, de^{-1}. \tag{8}$$

Raising both sides of equation (8) to the power 2^m yields

$$y^5 + b_1y^3 + b_2y = \lambda^{-1}de\,. \tag{9}$$

Multiplying equations (8) and (9), we can obtain

$$\begin{aligned} y^{10} + y^8\left(b_1 + \overline{b_1}\right) + y^6\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) \\ + y^4\left(\overline{b_1}b_2 + b_1\overline{b_2}\right) + y^2b_2\overline{b_2} = d^2. \end{aligned} \tag{10}$$

The substitution of y^2 with y in equation (10) leads to

$$\begin{aligned} y^5 + y^4\left(b_1 + \overline{b_1}\right) + y^3\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) \\ + y^2\left(\overline{b_1}b_2 + b_1\overline{b_2}\right) + yb_2\overline{b_2} = d^2. \end{aligned} \tag{11}$$

Let $y = z + (b_1 + \overline{b_1})$, and we can get

Table 1: Normalized permutation polynomials with degree no greater than 5 in $\mathbb{F}_q$.

Normalized permutation polynomial	q
x	All q
x^2	Even q
x^3	$q \not\equiv 1 \pmod 3$
$x^3 - ax$ (a is not a square of $\mathbb{F}_q$)	$3 \mid q$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$ (0 is a unique solution in $\mathbb{F}_q$)	Even q
x^5	$q \not\equiv 1 \pmod 5$
$x^5 - ax$ (a is not a fourth power of $\mathbb{F}_q$)	$5 \mid q$
$x^5 + ax$ ($a^2 = 2$)	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a is not a square of $\mathbb{F}_q$)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$ (all a)	$q \equiv \pm 2 \pmod 5$
$x^5 + ax^3 + 3a^2x$ (a is not a square of $\mathbb{F}_q$)	$q = 13$
$x^5 - 2ax^3 + a^2x$ (a is not a square of $\mathbb{F}_q$)	$5 \mid q$

$$\begin{aligned} & z^5 + z^3\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) \\ & \quad + z^2\left[\left(b_1 + \overline{b_1}\right)\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + \overline{b_1}b_2 + b_1\overline{b_2}\right] \\ & \quad + z\left[\left(b_1 + \overline{b_1}\right)^4 + \left(b_1 + \overline{b_1}\right)^2\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + b_2\overline{b_2}\right] \\ & \quad = \text{constant}, \end{aligned} \tag{12}$$

where constant $= b_1\overline{b_1}\,(b_1^3 + \overline{b_1}^3) + (b_1 + \overline{b_1})^2(b_1b_2 + \overline{b_1b_2}) + (b_1 + \overline{b_1})(b_2\overline{b_2} + b_1^2\overline{b_1}^2) + d^2$ and constant $\in \mathbb{F}_{2^m}$.

From the above discussion, we can deduce $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ permutes $\mathbb{F}_{2^n}$ iff $g(z) = z^5 + z^3(b_1\overline{b_1} + b_2 + \overline{b_2}) + z^2[(b_1 + \overline{b_1})(b_1\overline{b_1} + b_2 + \overline{b_2}) + \overline{b_1}b_2 + b_1\overline{b_2}] + z[(b_1 + \overline{b_1})^4 + (b_1 + \overline{b_1})^2(b_1\overline{b_1} + b_2 + \overline{b_2}) + b_2\overline{b_2}]$ permutes $\mathbb{F}_{2^m}$.

Based on Table 1, we know that if $g(z)$ is a normalized permutation polynomial of degree 5 over $\mathbb{F}_q$ ($q = 2^m$), then it must have the following forms:

(1) z^5, $q \not\equiv 1 \pmod 5$.

(2) $z^5 + az^3 + 5^{-1}a^2z$ (a arbitrary), $q \equiv \pm 2 \pmod 5$.

When $q \not\equiv 1 \pmod 5$, we have $4 \nmid m$, which includes that $m \equiv 2 \pmod 4$ and m is odd. When m is odd, that is, $q = \pm 2 \pmod 5$, we mainly study the permutation polynomial of $z^5 + az^3 + 5^{-1}a^2z$ (a arbitrary). When $m \equiv 2 \pmod 4$, we consider the permutation polynomial of z^5. Hence, $g(z)$ permutes $\mathbb{F}_{2^m}$ iff one of the following two cases holds:

(1) If $m \equiv 2 \pmod 4$, $g(z) = z^5$ permutes $\mathbb{F}_{2^m}$.

(2) If m is odd, $g(z) = z^5 + az^3 + 5^{-1}a^2z$ permutes $\mathbb{F}_{2^m}$.

In conclusion, we deduce that the polynomial

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{13}$$

permutes $\mathbb{F}_{2^n}$ iff the following two cases are satisfied:

(1) If $m \equiv 2 \pmod 4$, $g(x) = x^5$ permutes $\mathbb{F}_{2^m}$.

(2) If m is odd, $g(x) = x^5 + ax^3 + 5^{-1}a^2x$ permutes $\mathbb{F}_{2^m}$. □

Remark 2. When b_1 and b_2 are both 0, if $4 \nmid m$, then $\gcd(2^{m+1} + 3, 2^n - 1) = 1$, so we achieve that the monomial $f(x) = x^3\overline{x}^2$ permutes $\mathbb{F}_{2^n}$. If $b_1, b_2 \in \mathbb{F}_{2^n}$ are not both 0, then $f(x)$ is binomial or trinomial in $\mathbb{F}_{2^n}$. We will investigate the permutation behavior of those polynomials in the sequel.

Theorem 3. *For two positive integers m and n with $n = 2m$ and m being even, let $b_1, b_2 \in \mathbb{F}_{2^n}$ which are not both 0. Then, the polynomial*

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{14}$$

permutes $\mathbb{F}_{2^n}$ iff $m \equiv 2 \pmod 4$, $b_1 = \theta b_2$, and b_2 is a root of $x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0$, where $\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity.

Proof. Based on Theorem 2, we deduce that $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ permutes $\mathbb{F}_{2^n}$ iff $g(x) = x^5 + x^3(b_1\overline{b_1} + b_2 + \overline{b_2}) + x^2[(b_1 + \overline{b_1})(b_1\overline{b_1} + b_2 + \overline{b_2}) + \overline{b_1}b_2 + b_1\overline{b_2}] + x[(b_1 + \overline{b_1})^4 + (b_1 + \overline{b_1})^2(b_1\overline{b_1} + b_2 + \overline{b_2}) + b_2\overline{b_2}]$ permutes $\mathbb{F}_{2^m}$. When $m \equiv 2 \pmod 4$, we get that $f(x)$ permutes $\mathbb{F}_{2^n}$ iff $g(x) = x^5$ permutes $\mathbb{F}_{2^m}$.

"⇒" Comparing the coefficients of $g(x)$ and x^5, we have

$$b_1\overline{b_1} + b_2 + \overline{b_2} = 0, \tag{15}$$

$$b_1\overline{b_2} + \overline{b_1}b_2 = 0, \tag{16}$$

$$\left(b_1 + \overline{b_1}\right)4 + b_2\overline{b_2} = 0. \tag{17}$$

From equation (16), we can directly obtain that $(b_1/b_2) = (\overline{b_1}/\overline{b_2})$, i.e., $(b_1/b_2) \in \mathbb{F}_{2^m}$. Hence, there exists some element $\theta \in \mathbb{F}_{2^m}^*$ such that $b_1 = \theta b_2$.

Plugging $b_1 = \theta b_2$ into equation (15), we have

$$\theta^2b_2\overline{b_2} + b_2 + \overline{b_2} = 0. \tag{18}$$

By substituting b_1 with θb_2 in equation (17), we obtain

$$\theta^4\left(b_2 + \overline{b_2}\right)^4 + b_2\overline{b_2} = 0. \tag{19}$$

Combining equations (18) and (19), we know that $\theta^{12}(b_2\overline{b_2})^3 = 1$. This means that $b_2\overline{b_2} = \theta^{-4}\omega$ and $b_2 + \overline{b_2} = \theta^{-2}\omega$, where $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity.

Therefore, we conclude that b_2 and $\overline{b_2}$ are exactly two roots of the equation

$$x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0. \tag{20}$$

Hence, the above analysis shows that for $m \equiv 2 \pmod 4$, if $f(x)$ permutes $\mathbb{F}_{2^n}$, then $b_1 = \theta b_2$ and b_2 is a root of $x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0$, where $\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity.

In what follows, we will proceed to prove the necessity.

"⇐" For some $\theta \in \mathbb{F}_{2^m}^*$, let $b_1 = \theta b_2$, and then we know $(b_1/b_2) \in \mathbb{F}_{2^m}^*$, and this is equivalent to $(b_1/b_2) = (\overline{b_1}/\overline{b_2})$, which implies that $b_1\overline{b_2} + \overline{b_1}b_2 = 0$.

Suppose that b_2 and $\overline{b_2}$ are two different roots of equation (20) in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$; then, we have $b_2\overline{b_2} = \theta^{-4}\omega$ and $b_2 + \overline{b_2} = \theta^{-2}\omega$. Recall that $b_1 = \theta b_2$, and we have

$$b_1\overline{b_1} = \theta^2 b_2\overline{b_2} = \theta^{-2}\omega,$$
$$b_1 + \overline{b_1} = \theta\left(b_2 + \overline{b_2}\right) = \theta^{-1}\omega, \tag{21}$$

which implies that

$$b_1\overline{b_1} + b_2 + \overline{b_2} = \theta^{-2}\omega + \theta^{-2}\omega = 0,$$
$$\left(b_1 + \overline{b_1}\right)^4 + b_2\overline{b_2} = \theta^{-4}\omega^4 + \theta^{-4} = 0, \tag{22}$$

where $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity.

Therefore, equations (15)–(17) are satisfied. Furthermore, we know that if $m \equiv 2 \pmod 4$, $b_1 = \theta b_2$ and b_2 is a root of $x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0$, where $\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity, and thus $f(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$.

To summarize, we conclude that the polynomial

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{23}$$

permutes $\mathbb{F}_{2^n}$ iff $m \equiv 2 \pmod 4$, $b_1 = \theta b_2$, and b_2 is a root of $x^2 + \theta^{-2}\omega x + \theta^{-4}\omega = 0$, where $\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^m}^*$ is a primitive third root of unity. □

Theorem 4. *For two positive integers m and n with $n = 2m$ and m being odd, let $b_1, b_2 \in \mathbb{F}_{2^n}$ which are not both 0. Then, the polynomial*

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{24}$$

permutes $\mathbb{F}_{2^n}$ iff one of the following two cases holds:

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

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

Proof. Based on Theorem 2, if m is odd, then $f(x)$ permutes $\mathbb{F}_{2^n}$ iff $g(x) = x^5 + ax^3 + 5^{-1}a^2x$ permutes $\mathbb{F}_{2^m}$, where $g(x) = x^5 + x^3(b_1\overline{b_1} + b_2 + \overline{b_2}) + x^2[(b_1 + \overline{b_1})(b_1\overline{b_1} + b_2 + \overline{b_2}) + \overline{b_1}b_2 + b_1\overline{b_2}] + x[(b_1 + \overline{b_1})^4 + (b_1 + \overline{b_1})^2(b_1\overline{b_1} + b_2 + \overline{b_2}) + b_2\overline{b_2}]$.

Since $\gcd(2, m) = 1$, $x^2 + x + 1$ is a irreducible polynomial in $\mathbb{F}_2$, and we deduce that $x^2 + x + 1$ also remains irreducible over $\mathbb{F}_{2^m}$ by Lemma 2. Let ω be one of the roots of $h(x) = x^2 + x + 1$ in $\mathbb{F}_{2^n}$; then, $\omega^2 + \omega + 1 = 0$ and ω is a primitive third root of unity. Furthermore, we can view 1 and ω as a basis of vector space $\mathbb{F}_{2^n}$ upon $\mathbb{F}_{2^m}$.

"⇒" Comparing the coefficients of $g(x)$ and $x^5 + ax^3 + 5^{-1}a^2x$, we have

$$\left(b_1 + \overline{b_1}\right)\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + \overline{b_1}b_2 + b_1\overline{b_2} = 0, \tag{25}$$

$$5^{-1}\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right)2 = \left(b_1 + \overline{b_1}\right)4 + \left(b_1 + \overline{b_1}\right)2\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + b_2\overline{b_2}. \tag{26}$$

From equation (26), we know that

$$\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right)^2 + \left(b_1 + \overline{b_1}\right)^4 + \left(b_1 + \overline{b_1}\right)^2\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + b_2\overline{b_2} = 0. \tag{27}$$

Then, we can discuss the solutions of $g(x) = 0$. as follows. □

Case 1. $b_1 = 0$. Then, equation (27) turns to

$$\left(b_2 + \overline{b_2}\right)^2 = b_2\overline{b_2}. \tag{28}$$

Since 1 and ω are basis of vector space $\mathbb{F}_{2^n}$ upon $\mathbb{F}_{2^m}$, for any element $b_2 \in \mathbb{F}_{2^n}$, we can set $b_2 = \lambda + \theta\omega$ with $\lambda \in \mathbb{F}_{2^m}, \theta \in \mathbb{F}_{2^m}^*$.

By plugging $b_2 = \lambda + \theta\omega$ into equation (28), we obtain

$$\theta^2(\omega + \overline{\omega})^2 = (\lambda + \theta\omega)(\lambda + \theta\overline{\omega}). \tag{29}$$

Since m is odd, we know that $\overline{\omega} = \omega^{2^m} = \omega^2$. Then, equation (29) can be written as

$$\lambda^2 + \lambda\theta = 0, \tag{30}$$

which implies that $\lambda = 0$ or $\lambda = \theta$. Consequently, we conclude that $b_2 = \theta\omega$ or $b_2 = \theta\omega^2$.

The above analysis indicates that if $f(x)$ permutes $\mathbb{F}_{2^n}$ and m is odd, then $b_1 = 0$, $b_2 = \theta\omega$ or $b_2 = \theta\omega^2$, where $\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^n}$ is a primitive third root of unity.

Case 2. $b_1 \neq 0$. Thus, equation (25) becomes

$$b_1b_2 + \overline{b_1b_2} = b_1\overline{b_1}\left(b_1 + \overline{b_1}\right), \tag{31}$$

and this is equivalent to

$$b_1 + \frac{b_2}{\overline{b_1}} = \overline{b_1} + \frac{\overline{b_2}}{b_1}. \tag{32}$$

From equation (32), we can directly obtain that $b_1 + (b_2/b_1) \in \mathbb{F}_{2^m}$. Hence, there exists some element $\eta \in \mathbb{F}_{2^m}$ such that $b_1 + (b_2/\overline{b_1}) = \eta$, i.e., $b_2 = \overline{b_1}(b_1 + \eta)$.

Plugging $b_2 = \overline{b_1}(b_1 + \eta)$ into equation (27) gives

$$\left(b_1 + \overline{b_1}\right)^2\eta^2 + b_1\overline{b_1}\left(b_1 + \overline{b_1}\right)\eta + \left(b_1 + \overline{b_1}\right)^4 = b_1\overline{b_1}\eta^2 + \left(b_1 + \overline{b_1}\right)^3\eta + b_1\overline{b_1}\left(b_1 + \overline{b_1}\right)^2. \tag{33}$$

Comparing the coefficients on both sides of equation (33), we have

$$\left(b_1 + \overline{b_1}\right)^2 = b_1\overline{b_1}. \tag{34}$$

Discussion similar to that in Case 1 shows that $b_1 = \theta\omega$ or $b_1 = \theta\omega^2$. Meanwhile, we obtain $b_2 = \theta^2 + \theta\eta\omega^2$ or $b_2 = \theta^2 + \theta\eta\omega$, which follows from $b_2 = \overline{b_1}(b_1 + \eta)$.

Therefore, the above analysis demonstrates that if $f(x)$ permutes $\mathbb{F}_{2^n}$ and m is odd, then $b_1 = \theta\omega$ or $b_1 = \theta\omega^2$, $b_2 = \theta^2 + \theta\eta\omega^2$ or $b_2 = \theta^2 + \theta\eta\omega$, where $\theta \in \mathbb{F}_{2^m}^*$, $\eta \in \mathbb{F}_{2^m}$, and $\omega \in \mathbb{F}_{2^n}$ is a primitive third root of unity.

All in all, when m is odd, if the polynomial $f(x)$ permutes $\mathbb{F}_{2^n}$, then one of the following two cases is satisfied:

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

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

Next, we will continue to prove the necessity.

"$\Leftarrow$" If $b_1 = 0$, $b_2 = \theta\omega$ or $b_2 = \theta\omega^2$, then $(b_1\overline{b_1} + b_2 + \overline{b_2})(b_1 + \overline{b_1}) + \overline{b_1}b_2 + b_1\overline{b_2} = 0$, which means that equation (25) is satisfied. Since $\omega \in \mathbb{F}_{2^n}$ is a primitive third root of unity and $\omega^2 + \omega + 1 = 0$, we can calculate that $b_2 + \overline{b_2} = \theta$ and $b_2\overline{b_2} = \theta^2$, and thus the left-hand side of equation (27) turns to $(b_2 + \overline{b_2})^2 + b_2\overline{b_2} = \theta^2 + \theta^2 = 0$, which implies that equation (27) is satisfied. Therefore, when m is odd, we conclude that if $b_1 = 0$, $b_2 = \theta\omega$, or $b_2 = \theta\omega^2$, ($\theta \in \mathbb{F}_{2^m}^*$ and $\omega \in \mathbb{F}_{2^n}$ is a primitive third root of unity), the polynomial $f(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$.

If $b_1 \neq 0$, recall that $b_1 = \theta\omega$ or $b_1 = \theta\omega^2$, $b_2 = \theta^2 + \theta\eta\omega^2$ or $b_2 = \theta^2 + \theta\eta\omega$, and we have

$$\begin{aligned}
b_1\overline{b_1} &= \theta\omega(\theta\overline{\omega}) = \theta^2\omega^3 = \theta^2,\\
b_1 + \overline{b_1} &= \theta\omega + \theta\omega^2 = \theta,\\
b_2 + \overline{b_2} &= \theta^2 + \theta\eta\omega^2 + \theta^2 + \theta\eta\overline{\omega}^2 = \theta\eta\omega^2 + \theta\eta\omega = \theta\eta,\\
b_2\overline{b_2} &= \left(\theta^2 + \theta\eta\omega^2\right)\left(\theta^2 + \theta\eta\overline{\omega}\right) = \theta^4 + \theta^3\eta\omega + \theta^3\eta\omega^2 = \theta^2\eta^2,\\
\overline{b_1}b_2 &= \theta\overline{\omega}\left(\theta^2 + \theta\eta\omega^2\right) = \theta\omega^2\left(\theta^2 + \theta\eta\omega^2\right) = \theta^3\omega^2 + \theta^2\eta\omega,\\
b_1\overline{b_2} &= \theta\omega\left(\theta^2 + \theta\eta\overline{\omega}^2\right) = \theta\omega\left(\theta^2 + \theta\eta\omega\right) = \theta^3\omega + \theta^2\eta\omega^2,
\end{aligned} \tag{35}$$

which implies that

$$\begin{aligned}
&\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right)\left(b_1 + \overline{b_1}\right) + \overline{b_1}b_2 + b_1\overline{b_2}\\
&\quad= \left(\theta^2 + \theta\eta\right)\theta + \theta^3\omega^2 + \theta^2\eta\omega + \theta^3\omega + \theta^2\eta\omega^2\\
&\quad= \theta^3 + \theta^2\eta\left(1 + \omega + \omega^2\right) + \theta^3\left(\omega + \omega^2\right)\\
&\quad= \theta^3 + \theta^3\\
&\quad= 0,
\end{aligned} \tag{36}$$

where the third equation holds only if $\omega^2 + \omega + 1 = 0$. Consequently, we conclude that equation (25) is satisfied.

Next we consider

$$\begin{aligned}
&\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right)^2 + \left(b_1 + \overline{b_1}\right)^4 + \left(b_1 + \overline{b_1}\right)^2\left(b_1\overline{b_1} + b_2 + \overline{b_2}\right) + b_2\overline{b_2}\\
&\quad= \left(\theta^2 + \theta\eta\right)^2 + \theta^4 + \left(\theta^2 + \theta\eta\right)\theta^2 + \theta^4 + \theta^3\eta\omega + \theta^3\eta\omega^2 + \theta^2\eta^2\\
&\quad= \theta^3\eta\left(1 + \omega + \omega^2\right)\\
&\quad= 0,
\end{aligned} \tag{37}$$

where the second equation holds only if $\omega^2 + \omega + 1 = 0$. Hence, we can get that equation (27) is satisfied.

Therefore, the above analysis shows that for m is odd, if $b_1 = \theta\omega$ or $b_1 = \theta\omega^2$, $b_2 = \theta^2 + \theta\eta\omega^2$ or $b_2 = \theta^2 + \theta\eta\omega$, where $\theta \in \mathbb{F}_{2^m}^*$, $\eta \in \mathbb{F}_{2^m}$, and $\omega \in \mathbb{F}_{2^n}$ is a primitive third root of unity, then the polynomial $f(x)$ permutes $\mathbb{F}_{2^n}$.

All in all, for m is odd, we know that $f(x)$ permutes $\mathbb{F}_{2^n}$ if one of the following two cases is satisfied:

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

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

In conclusion, we deduce that the polynomial

$$f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x \tag{38}$$

permutes $\mathbb{F}_{2^n}$ iff one of the following two cases is met:

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

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

Applying Theorem 4 to $b_1 = 0$ and $\theta = 1$, we have the following.

Corollary 1. *For two positive integers m and n satisfying $n = 2m$ and m is odd, the binomial $f(x) = x^3\overline{x}^2 + \omega x$ is a complete permutation polynomial over $\mathbb{F}_{2^n}$.*

Remark 3. Observe that a complete permutation binomial $f(x)$ proposed in Corollary 1 is obtained by Zieve [26]. However, the approach we used to prove the permutation property is different from that in [26].

4. Concluding Remarks

In this paper, by transforming the problem into studying some normalized permutation polynomials of degree five with even characteristics, we investigate the coefficient pairs (b_1, b_2) making $f(x) = x^3\overline{x}^2 + b_1x^2\overline{x} + b_2x$ to be a permutation polynomial over $\mathbb{F}_{2^n}$. The sufficient and necessary conditions are shown in Theorems 3 and 4. Furthermore, a class of complete permutation binomials with the form $f(x) = x^3\overline{x}^2 + \omega x$ over $\mathbb{F}_{2^n}$ is obtained.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported in part by the Educational Research Project of Young and Middle-Aged Teachers of Fujian Province under grant no. JAT200033, the Talent Fund Project of Fuzhou University under grant no. GXRC-20002, and the National Natural Science Foundation of China under grant nos. 61902073, 62072109, and U1804263.

References

[1] R. Lidl and H. Niederreiter, "Finite fields," *Encyclopedia Math. Appl.*Vol. 20, Cambridge University Press, Cambridge, UK, 2nd edition, 1997.

[2] C. Ding and Z. Zhou, "Binary cyclic codes from explicit polynomials overGF (2 ^{m})," *Discrete Mathematics*, vol. 321, pp. 76–89, 2014.

[3] J. Schwenk and K. Huber, "Public key encryption and digital signatures based on permutation polynomials," *Electronics Letters*, vol. 34, no. 8, pp. 759-760, 1998.

[4] C. Ding and J. Yuan, "A family of skew hadamard difference sets," *Journal of Combinatorial Theory - Series A*, vol. 113, no. 7, pp. 1526–1535, 2006.

[5] H. Niederreiter and K. H. Robinson, "Complete mappings of finite fields," *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics*, vol. 33, no. 2, pp. 197–212, 1982.

[6] Y. Laigle-Chapuy, "Permutation polynomials and applications to coding theory," *Finite Fields and Their Applications*, vol. 13, no. 1, pp. 58–70, 2007.

[7] G. L. Mullen, "Permutation polynomials over finite fields," in *Finite Fields, Coding Theory, and Advances in Communications and Computing, Lect. Notes Pure Appl. Math*, vol. 141, pp. 131–151, Marcel Dekker, New York, NY, USA, 1993.

[8] G. L. Mullen and D. Pannario, *Handbook of Finite Fields*, Taylor & Francis, Boca Raton, FL, USA, 2013.

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

[10] N. Li and X. Zeng, "A Survey on the applications of Niho exponents," *Cryptography and Communications*, vol. 11, no. 3, pp. 509–548, 2019.

[11] C. Ding, L. Qu, Q. Wang, J. Yuan, and P. Yuan, "Permutation trinomials over finite fields with even characteristic," *SIAM Journal on Discrete Mathematics*, vol. 29, no. 1, pp. 79–92, 2015.

[12] R. Gupta and R. K. Sharma, "Some new classes of permutation trinomials over finite fields with even characteristic," *Finite Fields and Their Applications*, vol. 41, pp. 89–96, 2016.

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

[14] 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.

[15] 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.

[16] X.-D. Hou, "Determination of a type of permutation trinomials over finite fields, II," *Finite Fields and Their Applications*, vol. 35, pp. 16–35, 2015.

[17] Z. Tu, X. Zeng, C. Li, and T. Helleseth, "A class of new permutation trinomials," *Finite Fields and Their Applications*, vol. 50, pp. 178–195, 2018.

[18] D. Bartoli, "On a conjecture about a class of permutation trinomials," *Finite Fields and Their Applications*, vol. 52, pp. 30–50, 2018.

[19] X.-D. Hou, "On a class of permutation trinomials in characteristic 2," *Cryptography and Communications*, vol. 11, no. 6, pp. 1199–1210, 2019.

[20] Z. Tu and X. Zeng, "Two classes of permutation trinomials with Niho exponents," *Finite Fields and Their Applications*, vol. 53, pp. 99–112, 2018.

[21] X.-D. Hou, "On the Tu-Zeng permutation trinomial of type (1/4, 3/4)," *Discrete Mathematics*, vol. 344, no. 3, Article ID 112241, 2021.

[22] L. Zheng, H. Kan, and J. Peng, "Two classes of permutation trinomials with Niho exponents over finite fields with even characteristic," *Finite Fields and Their Applications*, vol. 68, Article ID 101754, 2020.

[23] D. Bartoli and M. Timpanella, "On trinomials of type $x^{n+m}(1 + Ax^{m(q-1)} + Bx^{n(q-1)})$, n, m odd, over F_{q^2}, $q = 2^{2s+1}$," *Finite Fields and Their Applications*, vol. 72, Article ID 101816, 2021.

[24] D. Wu, P. Yuan, C. Ding, and Y. Ma, "Permutation trinomials over F_2^m," *Finite Fields and Their Applications*, vol. 46, pp. 38–56, 2017.

[25] C. Malvenuto and F. Pappalardi, "Enumerating permutation polynomials II: k-cycles with minimal degree," *Finite Fields and Their Applications*, vol. 10, no. 1, pp. 72–96, 2004.

[26] M. E. Zieve, "Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal Latin squares," 2013, https://arxiv.org/abs/1312.1325.