Finite Fields and Their Applications 59 (2019) 57–85

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A revisit to a class of permutation quadrinomials

Ziran Tu [a], Xianping Liu [b], Xiangyong Zeng [b,*]

[a] *School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471003, China*
[b] *Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan 430062, China*

ARTICLE INFO

Article history:
Received 10 September 2018
Received in revised form 2 February 2019
Accepted 9 April 2019
Available online xxxx
Communicated by D. Panario

MSC:
05A05
11T06
11T55

Keywords:
Permutation quadrinomial
Permutation trinomial
Finite field

ABSTRACT

This paper revisits the quadrinomials $x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ over $\mathbb{F}_{q^2}$, where q is a power of 2. We propose a more comprehensive characterization of the coefficients that give rise to new permutation quadrinomials. The new characterization not only contains those coefficients given in [20], but also seems to completely cover all the coefficients that yield permutation quadrinomials, which is evidenced by exhaustive searches on small finite fields.

* Corresponding author.
E-mail addresses: tuziran@yahoo.com (Z. Tu), liuxianpingadela@126.com (X. Liu), xiangyongzeng@aliyun.com (X. Zeng).

https://doi.org/10.1016/j.ffa.2019.04.008
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements and $\mathbb{F}_q^*$ its multiplicative group, where q is a prime power. A polynomial $f \in \mathbb{F}_q[x]$ is called *a permutation polynomial* (PP) if the induced mapping $f\colon c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is bijective. Permutation polynomials over finite fields have various applications in cryptography, coding theory and combinatorial design theory [16], and the study in this area has a long history. However, an exhaustive classification of PPs is still elusive and looks hopeless. Recently, PPs with special forms have attracted great attention of many researchers.

Permutations over $\mathbb{F}_q$ having the form $x^r f(x^{\frac{q-1}{d}})$ are a class of important PPs and they were first investigated in [21], where $d \,|\, q-1$ and $1 < r < \frac{q-1}{d}$. There is a close connection between the PPs of this type and certain permutations of the subgroup of order d of $\mathbb{F}_q^*$. Some classes of permutation polynomials have been found by choosing special parameters r, q, d [4,5,17]. A criterion in terms of primitive d-th roots was proposed in [21], and Akbary, Wang [1], Zieve [23] also subsequently investigated such kind of PPs and proposed their criteria, respectively.

Permutation polynomials that have a simple algebraic appearance or possess additional properties are of significant interest. In recent years, permutation trinomials with Niho exponents [18] over $\mathbb{F}_{q^2}$, i.e. permutation trinomials having the form $x+a_1x^{s_1(q-1)+1}+a_2x^{s_2(q-1)+1}$, have received a lot of attentions [6,8–10,12–14,22]. Under the criteria in [1,21,23] the problem of finding such permutation trinomials can be transformed to determining whether some rational functions are bijective on the *unit circle*. However, due to difficulties in this procedure, known works in the literature mostly assumed the coefficients to be 1 when Niho exponents are fixed, which might only capture a small portion of the permutation trinomials for those specific Niho exponents. In fact, the complete characterization of permutation polynomials in certain forms, even in carefully chosen forms, are generally nontrivial. Until recently some progress was made in this direction. Hou first in [9,10] determines all possible coefficients when $(s_1, s_2) = (1, 2)$; in [19] the authors propose a characterization of the coefficients a_1, a_2 when $(s_1, s_2) = (-1, 2)$, which is later proved to be complete in [3,11] by the curve theory and Hasse-Weil bound. To the best of our knowledge, these are the only two instances of which the coefficients are completely determined.

Permutation quadrinomials have not been well explored so far. Very recently a class of permutation quadrinomials of the form

$$f(x) = x^3\left(x^{3(q-1)} + a_1x^{2(q-1)} + a_2x^{q-1} + a_3\right) \tag{1}$$

over $\mathbb{F}_{q^2}$ was investigated in [20], where $q = 2^m$ for an odd integer m. By the additive character criterion [15, Th. 7.7], the permutation problem was transformed into the determination of solutions in the *unit circle* of some cubic equations. As a result, three subclasses of permutation quadrinomials were found. However, as the coefficients in the cubic equations are rather complex and involve a free variable stemming from the additive

character criterion, the characterized coefficients [20] are incomplete and it doesn't seem to be a feasible approach to characterizing all the coefficients.

The purpose of this paper is to revisit the quadrinomials and to characterize the coefficients of those permutation quadrinomials more comprehensively. Due to the fact that the quadrinomials under discussion are quadratic, we consider the permutation behavior of these quadrinomials in a direct manner, namely, we directly investigate the solution to the affine equation $f(x+a)+f(x)=0$ for all nonzero a in $\mathbb{F}_{q^2}$. Thanks to an observation by Hou [11] and a manipulation of the element a, we manage to thoroughly analyze the solutions to the resulting low-degree affine equations. Consequently we obtain a more comprehensive characterization of the coefficient triples (a_1, a_2, a_3) such that the quadrinomials in (1) are permutations. Interestingly, the new characterization not only covers the results established in [20], but also seems to produce all permutation quadrinomials of the form in (1) according to our exhaustive searches on small fields. Nevertheless, the technique in this paper and the ones in [3,11] seem to be insufficient to prove this observation.

The remainder of this paper is organized as follows. In Section 2, we introduce some basic concepts and related results. Section 3 gives the new sufficient condition on the coefficients of the permutation quadrinomials in (1) and Section 4 concludes the study.

2. Preliminaries

For two positive integers m and n with $m \mid n$, we use $\mathrm{Tr}_m^n(\cdot)$ to denote the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ [15], i.e.

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

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 defined as the set

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

Lemma 1. ([15]) *For a positive integer n, the quadratic equation $x^2 + ax + b = 0$, $a, b \in \mathbb{F}_{2^n}, a \neq 0$, has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$.*

Furthermore, when n is an even integer and $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$, the solutions of $x^2+ax+b = 0$ in U were characterized in [2,7,19].

Lemma 2. ([19]) *Let $n = 2m$ be an even positive integer and $a, b \in \mathbb{F}_{2^n}^*$ satisfying $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$. Then the quadratic equation $x^2 + ax + b = 0$ has*

(1) *both solutions in the unit circle if and only if*

$$b = \frac{a}{\overline{a}} \text{ and } \mathrm{Tr}_1^m\left(\frac{b}{a^2}\right) = \mathrm{Tr}_1^m\left(\frac{1}{a\overline{a}}\right) = 1;$$

(2) *exactly one solution in the unit circle if and only if*

$$b \neq \frac{a}{\overline{a}} \text{ and } (1+b\overline{b})(1+a\overline{a}+b\overline{b})+a^2\overline{b}+\overline{a}^2 b=0.$$

The following result provides a necessary and sufficient condition for a special affine equation to have no solution in $\mathbb{F}_{2^n}$, which will be heavily used in the proof of the main result.

Proposition 1. *For an integer $n=2m$ with odd m, suppose that $A_1, A_2, A_3 \in \mathbb{F}_{2^n}$ satisfy $A_1A_2 \neq 0$ and $A_1+A_2+A_3=0$. Then the equation*

$$A_1x^2+A_2\overline{x}+A_3x+A_1=0 \tag{3}$$

has no solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^m\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)=1$.

Proof. By taking power 2^m on both sides of (3), we have

$$\overline{A}_1\overline{x}^2+\overline{A}_2x+\overline{A}_3\overline{x}+\overline{A}_1=0. \tag{4}$$

Since $A_2 \neq 0$, substituting $A_2\overline{x}=A_1x^2+A_3x+A_1$ from (3) into (4) gives

$$B_1x^4+B_2x^2+B_3x+B_4=0, \tag{5}$$

where

$$\begin{cases} B_1 = A_1^2\overline{A}_1, \\ B_2 = A_3^2\overline{A}_1+A_1A_2\overline{A}_3, \\ B_3 = A_2(A_2\overline{A}_2+A_3\overline{A}_3), \\ B_4 = (A_1^2+A_2^2)\overline{A}_1+A_1A_2\overline{A}_3. \end{cases}$$

Due to the equality $A_1+A_2+A_3=0$, it can be easily verified that $B_2=B_4=B_1+B_3$. Then (5) can be rewritten as

$$x^4+\tfrac{B_1+B_3}{B_1}x^2+\tfrac{B_3}{B_1}x+\tfrac{B_1+B_3}{B_1}=(x^2+x+1)(x^2+x+1+\tfrac{B_3}{B_1})=0.$$

Letting $u=\frac{B_3}{B_1}$, by $A_3=A_1+A_2$ we have

$$u=\frac{A_2(A_2\overline{A}_2+A_3\overline{A}_3)}{A_1^2\overline{A}_1}=\frac{A_2}{A_1}+\frac{A_2^2}{A_1^2}+\frac{A_2\overline{A}_2}{A_1\overline{A}_1}. \tag{6}$$

By Lemma 1, $\mathrm{Tr}_1^n(1+u)=0$ means that $x^2+x+1+u=0$ has two solutions in $\mathbb{F}_{2^n}$. Hence (5) has four solutions in $\mathbb{F}_{2^n}$ since $x^2+x+1=0$ has two solutions in $\mathbb{F}_{2^n}$ due to $\mathrm{Tr}_1^n(1)=0$.

In the sequel, we will prove that none of these four solutions satisfies (3) if and only if $\mathrm{Tr}_1^m\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)=1$. Suppose that $\lambda\in\mathbb{F}_{2^n}$ satisfies $\lambda^2+\lambda+1=0$. Therefore, for odd m, we have

$$\overline{\lambda}=\left(\lambda^{2^m}+\lambda^{2^{m-1}}\right)+\left(\lambda^{2^{m-1}}+\lambda^{2^{m-2}}\right)+\cdots+\left(\lambda^2+\lambda\right)+\lambda=1+\lambda$$

Hence

$$A_1\lambda^2+A_2\overline{\lambda}+A_3\lambda+A_1=(A_1+A_2+A_3)\lambda+A_2=A_2\neq 0,$$

i.e., λ is not a solution to (3). Suppose that $\xi\in\mathbb{F}_{2^n}$ satisfies $\xi^2+\xi+1+u=0$.

Then one has

$$\begin{cases}\xi^{2^2} &= \xi+(1+u)+(1+u)^2,\\ \xi^{2^3} &= \xi+(1+u)+(1+u)^2+(1+u)^{2^2},\\ &\cdots\\ \xi^{2^m} &= \xi+(1+u)+(1+u)^2+\cdots+(1+u)^{2^{m-1}},\\ &= \xi+1+\sum_{i=0}^{m-1}u^{2^i},\end{cases}$$

where the last equality holds due to odd m. Moreover, by (6), we have

$$\begin{cases} u &= \frac{A_2}{A_1}+\left(\frac{A_2}{A_1}\right)^2+\frac{A_2\overline{A}_2}{A_1\overline{A}_1},\\ u^2 &= \left(\frac{A_2}{A_1}\right)^2+\left(\frac{A_2}{A_1}\right)^4+\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)^2,\\ &\cdots\\ u^{2^{m-1}} &= \left(\frac{A_2}{A_1}\right)^{2^{m-1}}+\left(\frac{A_2}{A_1}\right)^{2^m}+\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)^{2^{m-1}}\end{cases}$$

and then

$$\sum_{i=0}^{m-1}u^{2^i}=\frac{A_2}{A_1}+\frac{\overline{A}_2}{\overline{A}_1}+\mathrm{Tr}_1^m\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right).$$

It can be verified that

$$\begin{aligned}&A_1\xi^2+A_2\overline{\xi}+A_3\xi+A_1\\ &=(A_1+A_2+A_3)\xi+A_2\left(\tfrac{A_1}{A_2}u+\sum_{i=0}^{m-1}u^{2^i}+1\right)\\ &=A_2\left(\tfrac{A_1}{A_2}\left(\tfrac{A_2}{A_1}+\left(\tfrac{A_2}{A_1}\right)^2+\tfrac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)+\tfrac{A_2}{A_1}+\tfrac{\overline{A}_2}{\overline{A}_1}+\mathrm{Tr}_1^m\left(\tfrac{A_2\overline{A}_2}{A_1\overline{A}_1}\right)+1\right)\\ &=A_2\cdot\mathrm{Tr}_1^m\left(\tfrac{A_2\overline{A}_2}{A_1\overline{A}_1}\right).\end{aligned}$$

Thus, $\xi \in \mathbb{F}_{2^n}$ is not a solution to (3) if and only if $\mathrm{Tr}_1^m\left(\frac{A_2\overline{A}_2}{A_1\overline{A}_1}\right) = 1$. The proof is finished. □

3. Main results

In this section, we shall discuss the permutation behavior of the quadrinomials in (1). As pointed out by Hou [11], the coefficient a_1 can be assumed to be in $\mathbb{F}_{2^m}$ since

$$\begin{aligned} f(\beta x) &= (\overline{\beta}\overline{x})^3 + a_1(\overline{\beta}\overline{x})^2\beta x + a_2\beta^2x^2\overline{\beta}\overline{x} + a_3(\beta x)^3 \\ &= \overline{\beta}^3\left(\overline{x}^3 + a_1(\beta/\overline{\beta})\overline{x}^2x + a_2(\beta/\overline{\beta})^2x^2\overline{x} + a_3(\beta/\overline{\beta})^3x^3\right), \end{aligned}$$

where $\beta \in \mathbb{F}_{2^{2m}}^*$ satisfies $\beta^2a_1 = 1$, and $a_1(\beta/\overline{\beta}) = \beta^{-1-2^m} \in \mathbb{F}_{2^m}$.

Theorem 1. *Let $n = 2m$ for odd m and define*

$$\Gamma = \left\{(a_1, a_2, a_3) : \theta_2^2 = \theta_1\overline{\theta}_3, \theta_1 \neq 0, \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1, a_1 \in \mathbb{F}_{2^m}, a_2, a_3 \in \mathbb{F}_{2^n}\right\},$$

where

$$\theta_1 = 1 + a_1^2 + a_2\overline{a}_2 + a_3\overline{a}_3, \quad \theta_2 = a_1 + \overline{a}_2a_3, \quad \theta_3 = \overline{a}_2 + a_1\overline{a}_3, \quad \theta_4 = a_1^2 + a_2\overline{a}_2. \quad (7)$$

Then for any $(a_1, a_2, a_3) \in \Gamma$, the quadrinomial

$$f(x) = \overline{x}^3 + a_1\overline{x}^2x + a_2x^2\overline{x} + a_3x^3$$

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

Before proceeding the proof of this main result, we first discuss the properties of a_i's and θ_i's given in Theorem 1.

Lemma 3. *For $(a_1, a_2, a_3) \in \Gamma$, we have*
(i) $\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 = \theta_4(\theta_1 + \theta_4)$;
(ii) $\theta_1\theta_2\theta_3\theta_4 \neq 0$ *and* $\theta_2^2\theta_3 = \overline{\theta}_2^2\overline{\theta}_3$;
(iii) $\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 = \frac{\theta_2\overline{\theta}_2(\theta_2+\overline{\theta}_2)}{\theta_1}$ *and* $\theta_2\overline{\theta}_3 + \overline{\theta}_2\theta_3 = \frac{\theta_2^3+\overline{\theta}_2^3}{\theta_1}$;
(iv) $\theta_2\overline{\theta}_2 = \theta_1\theta_4$, *or* $\theta_2\overline{\theta}_2 = \theta_1\theta_4 + \theta_1^2$. *Accordingly, we have* $\theta_3\overline{\theta}_3 = \theta_4^2$, *or* $\theta_3\overline{\theta}_3 = \theta_1^2 + \theta_4^2$.

Proof. (i) It can be verified that

$$\begin{aligned} \theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 &= (a_1 + \overline{a}_2a_3)(a_1 + a_2\overline{a}_3) + (\overline{a}_2 + a_1\overline{a}_3)(a_2 + a_1a_3) \\ &= (a_1^2 + a_2\overline{a}_2)(1 + a_3\overline{a}_3) \\ &= \theta_4(\theta_1 + \theta_4). \end{aligned}$$

In fact, the above equality always holds just from the definitions of θ_i, without the assumption $(a_1, a_2, a_3) \in \Gamma$.

(ii) It follows from the definition of Γ that $\theta_1\theta_4 \neq 0$. Suppose $\theta_2 = a_1 + \overline{a}_2 a_3 = 0$. Then $\theta_3 = 0$ due to $\theta_2^2 = \theta_1\overline{\theta}_3$ by the definition of Γ. By (i), we have $\theta_1 = \theta_4$. Therefore, by $a_1 = \overline{a}_2 a_3$, we have

$$\theta_1 = 1 + a_2\overline{a}_2 a_3\overline{a}_3 + a_2\overline{a}_2 + a_3\overline{a}_3 = (1 + a_2\overline{a}_2)(1 + a_3\overline{a}_3)$$

and

$$\theta_4 = a_2\overline{a}_2 a_3\overline{a}_3 + a_2\overline{a}_2 = a_2\overline{a}_2(1 + a_3\overline{a}_3).$$

Thus, the equality $\theta_1 = \theta_4$ yields $1 + a_2\overline{a}_2 = a_2\overline{a}_2$, which is impossible. This shows $\theta_2 \neq 0$ and then $\theta_3 \neq 0$.

The assumption $\theta_2^2 = \theta_1\overline{\theta}_3$ gives $\theta_2^2\theta_3 = \theta_1\theta_3\overline{\theta}_3$. This together with $\theta_1 = \overline{\theta}_1$ shows $\theta_2^2\theta_3 = \overline{\theta}_2^2\overline{\theta}_3$.

(iii) Since $\theta_2^2 = \theta_1\overline{\theta}_3$ from the definition of Γ and $\theta_1 = \overline{\theta}_1$ from the expression of θ_1, it can be verified that

$$\begin{cases} \theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 = \theta_2\frac{\overline{\theta}_2^2}{\theta_1} + \overline{\theta}_2\frac{\theta_2^2}{\theta_1} = \frac{\theta_2\overline{\theta}_2(\theta_2+\overline{\theta}_2)}{\theta_1}, \\ \theta_2\overline{\theta}_3 + \overline{\theta}_2\theta_3 = \frac{\theta_2^3+\overline{\theta}_2^3}{\theta_1}. \end{cases}$$

(iv) Suppose $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4 + c$ for some $c \in \mathbb{F}_{2^m}$. By $\theta_2^2 = \theta_1\overline{\theta}_3$, we have $\overline{\theta}_2^2 = \theta_1\theta_3$ and then

$$(\theta_2\overline{\theta}_2)^2 = \theta_1^2\theta_3\overline{\theta}_3. \tag{8}$$

Multiplying both sides of the equality in (i) by θ_1^2 gives

$$\begin{aligned} &\theta_1^2\theta_2\overline{\theta}_2 + \theta_1^2\theta_3\overline{\theta}_3 + \theta_1^2\theta_4(\theta_1 + \theta_4) = 0 \\ \Leftrightarrow\ &\theta_1^2\theta_2\overline{\theta}_2 + (\theta_2\overline{\theta}_2)^2 + \theta_1^2\theta_4(\theta_1 + \theta_4) = 0 \\ \Leftrightarrow\ &\theta_1^2(\theta_1^2 + \theta_1\theta_4 + c) + (\theta_1^2 + \theta_1\theta_4 + c)^2 + \theta_1^2\theta_4(\theta_1 + \theta_4) = 0 \\ \Leftrightarrow\ &c^2 + \theta_1^2 c = 0. \end{aligned}$$

That is to say, $c = 0$ or $c = \theta_1^2$. When $\theta_2\overline{\theta}_2 = \theta_1\theta_4$, by (8), we have $\theta_3\overline{\theta}_3 = \theta_4^2$, and $\theta_3\overline{\theta}_3 = \theta_1^2 + \theta_4^2$ can be similarly proved for $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$. The proof is finished. □

In the following, we will express a_2 and a_3 in terms of a_1 and θ_i's. Observe that

$$\begin{cases} a_1\overline{\theta}_2 + a_2\theta_3 = a_1(a_1 + a_2\overline{a}_3) + a_2(\overline{a}_2 + a_1\overline{a}_3) = \theta_4, \\ a_3\theta_3 + \theta_2 = a_3(\overline{a}_2 + a_1\overline{a}_3) + a_1 + \overline{a}_2 a_3 = a_1(\theta_1 + \theta_4). \end{cases}$$

Then we have

$$a_2 = \frac{a_1\overline{\theta}_2 + \theta_4}{\theta_3} \quad \text{and} \quad a_3 = \frac{a_1(\theta_1+\theta_4)+\theta_2}{\theta_3}. \tag{9}$$

Let

$$u = \theta_2 + \overline{\theta}_2. \tag{10}$$

Then (9) gives

$$a_2 + \overline{a}_2 = \frac{a_1(\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3) + \theta_4(\theta_3+\overline{\theta}_3)}{\theta_3\overline{\theta}_3} = \frac{a_1\theta_2\overline{\theta}_2 u + \theta_4 u^2}{\theta_1\theta_3\overline{\theta}_3}, \tag{11}$$

$$a_3 + \overline{a}_3 = \frac{a_1(\theta_1+\theta_4)(\theta_3+\overline{\theta}_3) + \theta_2\overline{\theta}_3 + \overline{\theta}_2\theta_3}{\theta_3\overline{\theta}_3} = \frac{a_1(\theta_1+\theta_4)u^2 + u^3 + \theta_2\overline{\theta}_2 u}{\theta_1\theta_3\overline{\theta}_3}, \tag{12}$$

and

$$\begin{aligned} a_2^2\overline{a}_3 + \overline{a}_2^2 a_3 &= a_2(\theta_2 + \overline{\theta}_2 + \overline{a}_2 a_3) + \overline{a}_2(\theta_2 + \overline{\theta}_2 + a_2\overline{a}_3) \\ &= \frac{a_1\theta_2\overline{\theta}_2 u^2 + \theta_4 u^3 + (\theta_4 + a_1^2)(a_1(\theta_1+\theta_4)u^2 + u^3 + \theta_2\overline{\theta}_2 u)}{\theta_1\theta_3\overline{\theta}_3}. \end{aligned} \tag{13}$$

Lemma 4. *For $(a_1, a_2, a_3) \in \Gamma$ and $a_1 = 1$, we have*

$$\mathrm{Tr}_1^m\left(\frac{(1+a_2)(1+\overline{a}_2)}{(\overline{a}_2+\overline{a}_3)(a_2+a_3)}\right) = 1.$$

Proof. By (9) and $a_1 = 1$, we have

$$\begin{cases} \theta_1 = a_2\overline{a}_2 + a_3\overline{a}_3, \\ \theta_2 = 1 + \overline{a}_2 a_3, \\ \theta_3 = \overline{a}_2 + \overline{a}_3, \\ \theta_4 = 1 + a_2\overline{a}_2, \\ a_2 = \frac{\overline{\theta}_2+\theta_4}{\theta_3}, \\ a_2 + \overline{a}_2 = \frac{\theta_2\overline{\theta}_2 u + \theta_4 u^2}{\theta_1\theta_3\overline{\theta}_3}. \end{cases}$$

Then $\theta_3\overline{\theta}_3 = (\overline{a}_2+\overline{a}_3)(a_2+a_3) = \theta_1 + \theta_2 + \overline{\theta}_2$. Since $\theta_3\overline{\theta}_3 = \frac{(\theta_2\overline{\theta}_2)^2}{\theta_1^2}$ due to $\theta_2^2 = \theta_1\overline{\theta}_3$ by the definition of Γ, we have $\theta_2 + \overline{\theta}_2 = \theta_1 + \frac{(\theta_2\overline{\theta}_2)^2}{\theta_1^2}$, i.e. $\theta_1^2 u = \theta_1^3 + (\theta_2\overline{\theta}_2)^2$. Let $\Omega_1 = \frac{(1+a_2)(1+\overline{a}_2)}{(\overline{a}_2+\overline{a}_3)(a_2+a_3)}$. Then

$$\begin{aligned}\Omega_1 &= \frac{\theta_4}{\theta_3\overline{\theta}_3} + \frac{\theta_2\overline{\theta}_2 u + \theta_4 u^2}{\theta_1(\theta_3\overline{\theta}_3)^2} = \frac{\theta_1^2\theta_4}{(\theta_2\overline{\theta}_2)^2} + \frac{\theta_2\overline{\theta}_2\theta_1^3 u + \theta_4\theta_1^3 u^2}{\theta_1^4(\theta_3\overline{\theta}_3)^2} \\ &= \frac{\theta_1^2\theta_4}{(\theta_2\overline{\theta}_2)^2} + \frac{\theta_2\overline{\theta}_2\theta_1\left(\theta_1^3 + (\theta_2\overline{\theta}_2)^2\right) + \frac{\theta_4}{\theta_1}\left(\theta_1^6 + (\theta_2\overline{\theta}_2)^4\right)}{(\theta_2\overline{\theta}_2)^4} \\ &= \frac{\theta_1^2\theta_4}{(\theta_2\overline{\theta}_2)^2} + \frac{\theta_1^4}{(\theta_2\overline{\theta}_2)^3} + \frac{\theta_1}{\theta_2\overline{\theta}_2} + \frac{\theta_1^5\theta_4}{(\theta_2\overline{\theta}_2)^4} + \frac{\theta_4}{\theta_1}.\end{aligned}$$

By Lemma 3 (iv), either $\theta_2\overline{\theta}_2 = \theta_1\theta_4$ or $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$ holds. When $\theta_2\overline{\theta}_2 = \theta_1\theta_4$, we have $\Omega_1 = \frac{\theta_4}{\theta_1}$. When $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$, observe that $\theta_1 \neq \theta_4$ due to $\theta_2 \neq 0$. Then

$$\begin{aligned}\Omega_1 &= \frac{\theta_4}{(\theta_1+\theta_4)^2} + \frac{\theta_1}{(\theta_1+\theta_4)^3} + \frac{1}{\theta_1+\theta_4} + \frac{\theta_1\theta_4}{(\theta_1+\theta_4)^4} + \frac{\theta_4}{\theta_1} \\ &= \frac{\theta_1^2}{(\theta_1+\theta_4)^4} + \frac{\theta_1}{(\theta_1+\theta_4)^2} + \frac{\theta_4}{\theta_1}.\end{aligned}$$

Thus, the equality $\mathrm{Tr}_1^m(\Omega_1) = \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1$ always holds in both cases. □

Lemma 5. *For $(a_1, a_2, a_3) \in \Gamma$ with $a_2\overline{a}_2 = a_3\overline{a}_3$, we have*

$$\mathrm{Tr}_1^m\left(\frac{(a_2^2 + a_1a_3)(\overline{a}_2^2 + a_1\overline{a}_3)}{(a_3 + a_1a_2)(\overline{a}_3 + a_1\overline{a}_2)}\right) = 1.$$

Proof. Since $a_2\overline{a}_2 = a_3\overline{a}_3$, θ_i's can be rewritten as

$$\begin{cases}\theta_1 = 1 + a_1^2, \\ \theta_2 = a_1 + \overline{a}_2 a_3, \\ \theta_3 = \overline{a}_2 + a_1\overline{a}_3, \\ \theta_4 = a_1^2 + a_2\overline{a}_2.\end{cases}$$

Denote $\Omega_2 = \frac{(a_2^2+a_1a_3)(\overline{a}_2^2+a_1\overline{a}_3)}{(a_3+a_1a_2)(\overline{a}_3+a_1\overline{a}_2)}$ and it can be expressed in terms of θ_i's. Recall that $\theta_2^2 = \theta_1\overline{\theta}_3$ from the definition of Γ and $u = \theta_2 + \overline{\theta}_2$, then $\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 = \frac{\theta_2\overline{\theta}_2 u}{\theta_1}$ and $\theta_2\overline{\theta}_3 + \overline{\theta}_2\theta_3 = \frac{u^3+\theta_2\overline{\theta}_2 u}{\theta_1}$ by Lemma 3 (iii). Since

$$\begin{aligned}\theta_2\overline{\theta}_2 &= (a_1 + \overline{a}_2 a_3)(a_1 + a_2\overline{a}_3) \\ &= a_1^2 + a_1(\theta_2 + \overline{\theta}_2) + a_2\overline{a}_2 a_3\overline{a}_3 \\ &= a_1^2 + a_1 u + \theta_4^2 + a_1^4,\end{aligned}$$

we have

$$a_1 u = \theta_2\overline{\theta}_2 + \theta_4^2 + a_1^2\theta_1 \tag{14}$$

due to $\theta_1 = a_1^2 + 1$. The denominator of Ω_2 is

$$\begin{aligned}&(a_3 + a_1a_2)(\overline{a}_3 + a_1\overline{a}_2) = a_3\overline{a}_3 + a_1^2a_2\overline{a}_2 + a_1(\theta_2 + \overline{\theta}_2)\\ &= a_2\overline{a}_2(1 + a_1^2) + a_1u = (\theta_4 + \theta_1 + 1)\theta_1 + \theta_2\overline{\theta}_2 + \theta_4^2 + (1 + \theta_1)\theta_1\\ &= \theta_2\overline{\theta}_2 + \theta_4^2 + \theta_1\theta_4 \end{aligned} \tag{15}$$

and the numerator of Ω_2 is

$$\begin{aligned}(a_2^2 + a_1a_3)(\overline{a}_2^2 + a_1\overline{a}_3) &= (a_2\overline{a}_2)^2 + a_1^2a_3\overline{a}_3 + a_1(a_2^2\overline{a}_3 + \overline{a}_2^2a_3)\\ &= (\theta_1 + \theta_4 + 1)\theta_4 + \frac{a_1u\left(\theta_4^3 + (1 + \theta_1)(\theta_2\overline{\theta}_2 + \theta_1\theta_4)\right)}{\theta_1\theta_3\overline{\theta}_3}. \end{aligned} \tag{16}$$

The equality (16) holds due to the numerator of (13) and

$$\begin{aligned}&a_1\theta_2\overline{\theta}_2u^2 + \theta_4u^3 + a_1u^2(\theta_1 + \theta_4)\theta_4 + u^3\theta_4 + \theta_2\overline{\theta}_2\theta_4u\\ &\quad + a_1^3u^2(\theta_1 + \theta_4) + a_1^2u^3 + a_1^2u\theta_2\overline{\theta}_2\\ &= a_1u^2(\theta_2\overline{\theta}_2 + \theta_1\theta_4 + \theta_4^2 + a_1^2(\theta_1 + \theta_4) + a_1u) + u\theta_2\overline{\theta}_2(\theta_4 + a_1^2)\\ &= a_1u^2\theta_4 + u\theta_2\overline{\theta}_2(\theta_1 + \theta_4 + 1)\\ &= u\left((\theta_2\overline{\theta}_2 + \theta_4^2 + a_1^2\theta_1)\theta_4 + \theta_2\overline{\theta}_2(\theta_1 + \theta_4 + 1)\right)\\ &= u(\theta_4^3 + \theta_1\theta_4(1 + \theta_1) + \theta_2\overline{\theta}_2(1 + \theta_1))\\ &= u\left(\theta_4^3 + (1 + \theta_1)(\theta_2\overline{\theta}_2 + \theta_1\theta_4)\right), \end{aligned}$$

where the equality (14) and the fact $a_1^2 = 1 + \theta_1$ are used.

By Lemma 3 (iv), either $\theta_2\overline{\theta}_2 = \theta_1\theta_4$ or $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$ holds. When $\theta_2\overline{\theta}_2 = \theta_1\theta_4$, together with the fact $\theta_3\overline{\theta}_3 = \theta_4^2$ and (14), we have $\Omega_2 = \frac{\theta_4}{\theta_1}$ by (15) and (16). When $\theta_2\overline{\theta}_2 = \theta_1\theta_4 + \theta_1^2$, we have $\theta_3\overline{\theta}_3 = \theta_1^2 + \theta_4^2$ and $a_1u = \theta_1\theta_4 + \theta_4^2 + \theta_1$. Thus, the denominator of Ω_2 becomes $\theta_1^2 + \theta_4^2$ and the numerator equals

$$\begin{aligned}&(1 + \theta_1 + \theta_4)\theta_4 + \tfrac{(\theta_1\theta_4 + \theta_4^2 + \theta_1)(\theta_4^3 + \theta_1^2 + \theta_1^3)}{\theta_1(\theta_1 + \theta_4)^2}\\ &= \theta_4 + \theta_4(\theta_1 + \theta_4) + \tfrac{\theta_4(\theta_1 + \theta_4)^4 + \theta_1(\theta_1 + \theta_4)^3 + \theta_1\theta_4^2(\theta_1 + \theta_4)^2 + \theta_1^3}{\theta_1(\theta_1 + \theta_4)^2}\\ &= \theta_4(\theta_1 + \theta_4) + \tfrac{\theta_4(\theta_1 + \theta_4)^2}{\theta_1} + \theta_1 + \theta_4^2 + \tfrac{\theta_1^2}{(\theta_1 + \theta_4)^2}. \end{aligned}$$

Therefore,

$$\Omega_2 = \frac{\theta_4}{\theta_1 + \theta_4} + \frac{\theta_4}{\theta_1} + \frac{\theta_1}{(\theta_1 + \theta_4)^2} + \frac{\theta_4^2}{(\theta_1 + \theta_4)^2} + \frac{\theta_1^2}{(\theta_1 + \theta_4)^4}.$$

That is to say, $\mathrm{Tr}_1^m(\Omega_2) = 1$ holds in both cases. The proof is finished. □

Lemma 6. *For $(a_1, a_2, a_3) \in \Gamma$, if there exists an element $\lambda \in U$ such that $\theta_1 + \theta_2\overline{\lambda} + \overline{\theta}_2\lambda = 0$, then*

$$\theta_2\overline{\theta}_2 = \theta_1\theta_4,\ \theta_3\overline{\theta}_3 = \theta_4^2 \text{ and } \theta_2^2\theta_3 = \theta_1\theta_4^2.$$

Proof. By Lemma 3 (iv), either $\theta_2\overline{\theta}_2 = \theta_1\theta_4$ or $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$ holds. The equation $\theta_1 + \theta_2\overline{\lambda} + \overline{\theta}_2\lambda = 0$ is equivalent to

$$\lambda^2 + \frac{\theta_1}{\overline{\theta}_2}\lambda + \frac{\theta_2}{\overline{\theta}_2} = 0,$$

which has solutions in U if and only if

$$\mathrm{Tr}_1^m\left(\frac{\theta_2\overline{\theta}_2}{\theta_1^2}\right) = 1$$

by Lemma 2. The case $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$ means that $\mathrm{Tr}_1^m\left(\frac{\theta_2\overline{\theta}_2}{\theta_1^2}\right) = \mathrm{Tr}_1^m\left(1 + \frac{\theta_4}{\theta_1}\right) = 0$ due to odd m. Thus, by Lemma 3(iv), we have $\theta_2\overline{\theta}_2 = \theta_1\theta_4$, $\theta_3\overline{\theta}_3 = \theta_4^2$, and then $\theta_2^2\theta_3 = \theta_1\overline{\theta}_3\theta_3 = \theta_1\theta_4^2$ due to $\theta_2^2 = \theta_1\overline{\theta}_3$ by the definition of Γ. □

Lemma 7. *For $(a_1, a_2, a_3) \in \Gamma$ and $\lambda \in U$, we have*

$$\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 \neq 0.$$

Proof. We will finish the proof by contradiction. Assume there exists some $\lambda \in U$ such that $\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 = 0$, i.e.

$$\lambda^2(\lambda + a_1) = a_2\lambda + a_3. \tag{17}$$

If $\lambda = a_1$, we have $a_1 = 1$ by $1 = \lambda\overline{\lambda} = a_1\overline{a}_1 = a_1^2$, and then $a_3 = a_2$, a contradiction to the assumption $\theta_1 \neq 0$. Thus, $\lambda \neq a_1$. By (17), we have

$$\begin{aligned} &\lambda^2(\lambda + a_1) \cdot \overline{\lambda^2(\lambda + a_1)} = (a_2\lambda + a_3) \cdot \overline{(a_2\lambda + a_3)} && (18)\\ \Leftrightarrow\ &1 + a_1^2 + a_1\overline{\lambda} + a_1\lambda = a_2\overline{a}_2 + a_3\overline{a}_3 + a_2\overline{a}_3\lambda + \overline{a}_2a_3\overline{\lambda} \\ \Leftrightarrow\ &\theta_1 + \overline{\theta}_2\lambda + \theta_2\overline{\lambda} = 0. && (19)\end{aligned}$$

By Lemma 6, (19) holds only if $\theta_2\overline{\theta}_2 = \theta_1\theta_4$. By plugging $\lambda^2 = \frac{\theta_1\lambda + \theta_2}{\overline{\theta}_2}$ into (17), we get

$$\begin{aligned} &\frac{\theta_1\lambda + \theta_2}{\overline{\theta}_2}(\lambda + a_1) = a_2\lambda + a_3 \\ \Leftrightarrow\ &\frac{\theta_1}{\overline{\theta}_2}\lambda^2 + \left(\frac{\theta_2 + a_1\theta_1}{\overline{\theta}_2} + a_2\right)\lambda + \frac{a_1\theta_2}{\overline{\theta}_2} + a_3 = 0 \\ \Leftrightarrow\ &\left(\frac{\theta_1^2}{\overline{\theta}_2^2} + \frac{\theta_2 + a_1\theta_1}{\overline{\theta}_2} + a_2\right)\lambda + \frac{\theta_1\theta_2}{\overline{\theta}_2^2} + \frac{a_1\theta_2}{\overline{\theta}_2} + a_3 = 0.\end{aligned}$$

The last equality gives

$$\begin{aligned}\lambda &= \frac{\theta_1\theta_2 + a_1\theta_2\overline{\theta}_2 + a_3\overline{\theta}_2^2}{\theta_1^2 + \theta_2\overline{\theta}_2 + a_1\theta_1\overline{\theta}_2 + a_2\overline{\theta}_2^2} = \frac{\theta_1\theta_2 + a_1\theta_1\theta_4 + a_3\theta_1\theta_3}{\theta_1^2 + \theta_1\theta_4 + a_1\theta_1\overline{\theta}_2 + a_2\theta_1\theta_3} \\ &= \frac{a_1\theta_4 + a_3\theta_3 + \theta_2}{\theta_1 + \theta_4 + a_1\overline{\theta}_2 + a_2\theta_3} = \frac{a_1\theta_4 + a_3(\overline{a}_2 + a_1\overline{a}_3) + \theta_2}{\theta_1 + \theta_4 + a_1(a_1 + a_2\overline{a}_3) + a_2(\overline{a}_2 + a_1\overline{a}_3)} \\ &= \frac{a_1\theta_1}{\theta_1} = a_1.\end{aligned}$$

As mentioned above, $\lambda = a_1$ is impossible. The proof is finished. □

With the proceeding preparation, we now give the proof of the main result Theorem 1.

Proof of Theorem 1. It suffices to prove that for any $a \in \mathbb{F}_{2^n}^*$, the differential equation $f(x+a)+f(x)=0$ has no solution in $\mathbb{F}_{2^n}$. Let $x = ay$. It is equivalent to showing that $f(a(y+1))+f(ay)=0$ has no solution in $\mathbb{F}_{2^n}$. With the expression of $f(x)$, the equation becomes

$$\overline{a}^3(\overline{y}^2 + \overline{y} + 1) + a_1\overline{a}^2 a(\overline{y}^2 + y + 1) + a_2 a^2\overline{a}(y^2 + \overline{y} + 1) + a_3 a^3(y^2 + y + 1) = 0.$$

By letting $\lambda = \frac{\overline{a}}{a} \in U$ and rearranging the terms, we can rewrite the above equation as

$$\epsilon_1\overline{y}^2 + \epsilon_2 y^2 + \epsilon_3\overline{y} + \epsilon_4 y + \epsilon_5 = 0, \tag{20}$$

where the coefficients

$$\begin{aligned}&\epsilon_1 = \lambda^3 + a_1\lambda^2,\ \epsilon_2 = a_2\lambda + a_3, \\ &\epsilon_3 = \lambda^3 + a_2\lambda,\quad \epsilon_4 = a_1\lambda^2 + a_3,\quad \epsilon_5 = \epsilon_1 + \epsilon_2 = \epsilon_3 + \epsilon_4.\end{aligned} \tag{21}$$

Hence it suffices to prove that for any $\lambda \in U$, (20) has no solution in $\mathbb{F}_{2^n}$. From Lemma 7 it follows that $\epsilon_5 = \lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 \neq 0$. Based on Proposition 1, we shall investigate the solution to (20) in three cases: $\epsilon_1 = 0$; $\epsilon_2 = 0$; and $\epsilon_1\epsilon_2 \neq 0$.

Case 1: $\epsilon_1 = 0$. In this case we have $\lambda = a_1 = 1$ since $a_1 \in \mathbb{F}_q$ and $\epsilon_2 = \epsilon_5 \neq 0$, and (20) becomes

$$\epsilon_2 y^2 + \epsilon_3\overline{y} + \epsilon_4 y + \epsilon_5 = 0.$$

We also have $\epsilon_3 \neq 0$, otherwise $a_2 = 1$ and then $\theta_4 = a_1^2 + a_2\overline{a}_2 = 0$. This is impossible by Lemma 3 (ii). Since $\epsilon_2 + \epsilon_3 + \epsilon_4 = 0$ and $\epsilon_5 = \epsilon_2$, by Lemma 4 we have

$$\mathrm{Tr}_1^m\left(\frac{\epsilon_3\overline{\epsilon}_3}{\epsilon_2\overline{\epsilon}_2}\right) = \mathrm{Tr}_1^m\left(\frac{(1+a_2)(1+\overline{a}_2)}{(a_2+a_3)(\overline{a}_2+\overline{a}_3)}\right) = 1.$$

By Proposition 1, (20) has no solution in $\mathbb{F}_{2^n}$.

Case 2: $\epsilon_2 = 0$. In this case we have $\lambda = \frac{a_3}{a_2}$ and $\epsilon_1 = \epsilon_5 \neq 0$, and (20) is equivalent to

$$\overline{\epsilon}_1 y^2 + \overline{\epsilon}_4 \overline{y} + \overline{\epsilon}_3 y + \overline{\epsilon}_5 = 0.$$

We claim $\epsilon_4 \neq 0$. Otherwise $a_3 = a_1\lambda^2$ and then $a_3\overline{a}_3 = a_1\lambda^2 \cdot \overline{a_1\lambda^2} = a_1^2$. Further, $\epsilon_2 = a_3 + a_2\lambda = 0$ implies that $a_3\overline{a}_3 = a_2\overline{a}_2$. Thus, $a_1^2 = a_2\overline{a}_2$ which contradicts with $\theta_4 \neq 0$. By $\epsilon_2 = 0$, i.e., $a_2\lambda = a_3$, we have $\epsilon_4 = a_3 + a_1\lambda^2 = a_3 + a_1\frac{a_3^2}{a_2^2} = \frac{a_2^2 a_3 + a_1 a_3^2}{a_2^2}$ and $\epsilon_1 = \lambda^3 + a_1\lambda^2 = \frac{a_3^3}{a_2^3} + a_1\frac{a_3^2}{a_2^2} = \frac{a_3^3 + a_1 a_2 a_3^2}{a_2^3}$. Again by $a_3\overline{a}_3 = a_2\overline{a}_2$, we have

$$\frac{\epsilon_4\overline{\epsilon}_4}{\epsilon_1\overline{\epsilon}_1} = \frac{a_2\overline{a}_2 a_3\overline{a}_3(a_2^2 + a_1a_3)(\overline{a}_2^2 + a_1\overline{a}_3)}{a_3^2\overline{a}_3^2(a_3 + a_1a_2)(\overline{a}_3 + a_1\overline{a}_2)} = \frac{(a_2^2 + a_1a_3)(\overline{a}_2^2 + a_1\overline{a}_3)}{(a_3 + a_1a_2)(\overline{a}_3 + a_1\overline{a}_2)}.$$

Lemma 5 implies $\mathrm{Tr}_1^m\left(\frac{\epsilon_4\overline{\epsilon}_4}{\epsilon_1\overline{\epsilon}_1}\right) = 1$. Then by Proposition 1, (20) has no solution in $\mathbb{F}_{2^n}$.

Case 3: $\epsilon_1\epsilon_2 \neq 0$. By taking power 2^m on both sides of (20), we have

$$\overline{\epsilon}_1 y^2 + \overline{\epsilon}_2 \overline{y}^2 + \overline{\epsilon}_3 y + \overline{\epsilon}_4 \overline{y} + \overline{\epsilon}_5 = 0. \tag{22}$$

By multiplying both sides of (20) by $\overline{\epsilon}_2$ and (22) by ϵ_1, and then adding these two equalities, we have

$$\tau_1 y^2 + \tau_2 \overline{y} + \tau_3 y + \tau_4 = 0, \tag{23}$$

where

$$\begin{cases} \tau_1 = \epsilon_1\overline{\epsilon}_1 + \epsilon_2\overline{\epsilon}_2, \\ \tau_2 = \epsilon_1\overline{\epsilon}_4 + \overline{\epsilon}_2\epsilon_3, \\ \tau_3 = \epsilon_1\overline{\epsilon}_3 + \overline{\epsilon}_2\epsilon_4, \\ \tau_4 = \epsilon_1\overline{\epsilon}_5 + \overline{\epsilon}_2\epsilon_5. \end{cases}$$

It can be verified that

$$\tau_1 + \tau_2 + \tau_3 = \epsilon_1(\overline{\epsilon}_1 + \overline{\epsilon}_4 + \overline{\epsilon}_3) + \overline{\epsilon}_2(\epsilon_2 + \epsilon_3 + \epsilon_4) = \epsilon_1\overline{\epsilon}_2 + \overline{\epsilon}_2\epsilon_1 = 0 \tag{24}$$

and

$$\tau_1 + \tau_4 = \epsilon_1\overline{\epsilon}_1 + \epsilon_2\overline{\epsilon}_2 + \epsilon_1\overline{\epsilon}_5 + \overline{\epsilon}_2\epsilon_5 = \epsilon_1\overline{\epsilon}_1 + \epsilon_2\overline{\epsilon}_2 + \epsilon_1(\overline{\epsilon}_1 + \overline{\epsilon}_2) + \overline{\epsilon}_2(\epsilon_1 + \epsilon_2) = 0, \tag{25}$$

due to $\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 = 0$ and $\epsilon_5 = \epsilon_1 + \epsilon_2$. The proof proceeds in two subcases $\tau_2 = 0$ and $\tau_2 \neq 0$.

Subcase 1. $\tau_2 = 0$. The equalities

$$\begin{cases} \epsilon_1\overline{\epsilon}_4 = (\lambda^3 + a_1\lambda^2)(a_1\overline{\lambda}^2 + \overline{a}_3) = a_1\lambda + a_1^2 + \overline{a}_3\lambda^3 + a_1\overline{a}_3\lambda^2, \\ \overline{\epsilon}_2\epsilon_3 = (\overline{a}_2\overline{\lambda} + \overline{a}_3)(\lambda^3 + a_2\lambda) = a_2\overline{a}_3\lambda + a_2\overline{a}_2 + \overline{a}_3\lambda^3 + \overline{a}_2\lambda^2, \end{cases}$$

give

$$\begin{aligned} \tau_2 &= (a_1 + a_2\overline{a}_3)\lambda + a_1^2 + a_2\overline{a}_2 + (\overline{a}_2 + a_1\overline{a}_3)\lambda^2 \\ &= \lambda(\overline{\theta}_2 + \theta_3\lambda + \theta_4\overline{\lambda}). \end{aligned}$$

Similarly, we have

$$\begin{aligned} \tau_1 &= (\lambda^3 + a_1\lambda^2)(\overline{\lambda}^3 + a_1\overline{\lambda}^2) + (a_2\lambda + a_3)(\overline{a}_2\overline{\lambda} + \overline{a}_3) \\ &= \theta_1 + \theta_2\overline{\lambda} + \overline{\theta}_2\lambda. \end{aligned}$$

In the sequel, we will prove that $\tau_2 = 0$ if and only if $\tau_1 = 0$. When $\tau_2 = 0$, i.e. $\overline{\theta}_2 = \theta_3\lambda + \theta_4\overline{\lambda}$, we have

$$\theta_2\overline{\theta}_2 = (\theta_3\lambda + \theta_4\overline{\lambda})(\overline{\theta}_3\overline{\lambda} + \theta_4\lambda) = \theta_3\overline{\theta}_3 + \theta_4^2 + \theta_3\theta_4\lambda^2 + \overline{\theta}_3\theta_4\overline{\lambda}^2.$$

By Lemma 3 (i), we have $\theta_1\theta_4 = \theta_3\theta_4\lambda^2 + \overline{\theta}_3\theta_4\overline{\lambda}^2$, which indicates

$$\theta_1^2 + \theta_1\theta_3\lambda^2 + \theta_1\overline{\theta}_3\overline{\lambda^2} = (\theta_1 + \overline{\theta}_2\lambda + \theta_2\overline{\lambda})^2 = 0.$$

Then $\tau_1 = 0$. Conversely, suppose $\tau_1 = 0$. From Lemma 6, we have $\theta_2\overline{\theta}_2 = \theta_1\theta_4$. By $\theta_1 + \theta_2\overline{\lambda} + \overline{\theta}_2\lambda = 0$, we have

$$\overline{\theta}_2(\theta_1 + \theta_2\overline{\lambda} + \overline{\theta}_2\lambda) = \theta_1(\overline{\theta}_2 + \theta_4\overline{\lambda} + \theta_3\lambda),$$

which means $\tau_2 = 0$. This together with (24) and (25) gives $\tau_1 = \tau_2 = \tau_3 = \tau_4 = 0$, which is equivalent to

$$\frac{\epsilon_1}{\overline{\epsilon}_2} = \frac{\epsilon_2}{\overline{\epsilon}_1} = \frac{\epsilon_3}{\overline{\epsilon}_4} = \frac{\epsilon_4}{\overline{\epsilon}_3} = \frac{\epsilon_5}{\overline{\epsilon}_5},$$

where $\epsilon_5 \neq 0$ by Lemma 7, and $\epsilon_3\epsilon_4 \neq 0$ by $0 = \tau_2 = \epsilon_1\overline{\epsilon}_4 + \overline{\epsilon}_2\epsilon_3$, $0 = \tau_3 = \epsilon_1\overline{\epsilon}_3 + \overline{\epsilon}_2\epsilon_4$, $\epsilon_5 = \epsilon_3 + \epsilon_4$.

By multiplying both sides of (22) by ϵ_5, we have

$$\overline{\epsilon}_1\epsilon_5 y^2 + \overline{\epsilon}_2\epsilon_5\overline{y}^2 + \overline{\epsilon}_3\epsilon_5 y + \overline{\epsilon}_4\epsilon_5\overline{y} + \overline{\epsilon}_5\epsilon_5 = 0.$$

Let $z = \overline{\epsilon}_1\epsilon_5 y^2 + \overline{\epsilon}_3\epsilon_5 y$, and the above equation becomes $z + \overline{z} + \epsilon_5\overline{\epsilon}_5 = 0$. If

$$\mathrm{Tr}_1^n\left(\frac{\overline{\epsilon}_1\epsilon_5 z}{\overline{\epsilon}_3^2\epsilon_5^2}\right)=\mathrm{Tr}_1^n\left(\frac{\overline{\epsilon}_1 z}{\overline{\epsilon}_3^2\epsilon_5}\right)=1$$

holds for any z satisfying $z+\overline{z}+\epsilon_5\overline{\epsilon}_5=0$, by Lemma 1 the equation $z=\overline{\epsilon}_1\epsilon_5 y^2+\overline{\epsilon}_3\epsilon_5 y$ about the variable y has no solution in $\mathbb{F}_{2^n}$ and then (22) has no solution in $\mathbb{F}_{2^n}$. Note that

$$\mathrm{Tr}_1^n\left(\frac{\overline{\epsilon}_1 z}{\overline{\epsilon}_3^2\epsilon_5}\right)=\mathrm{Tr}_1^m\left(\frac{\overline{\epsilon}_1 z}{\overline{\epsilon}_3^2\epsilon_5}+\frac{\epsilon_1\overline{z}}{\epsilon_3^2\overline{\epsilon}_5}\right)=\mathrm{Tr}_1^m\left(\left(\frac{\overline{\epsilon}_1}{\overline{\epsilon}_3^2\epsilon_5}+\frac{\epsilon_1}{\epsilon_3^2\overline{\epsilon}_5}\right)z+\frac{\epsilon_1\epsilon_5}{\epsilon_3^2}\right).$$

Thus, to prove $\mathrm{Tr}_1^n\left(\frac{\overline{\epsilon}_1 z}{\overline{\epsilon}_3^2\epsilon_5}\right)=1$, it suffices to prove the following claim:

Claim:

- $\frac{\overline{\epsilon}_1}{\overline{\epsilon}_3^2\epsilon_5}+\frac{\epsilon_1}{\epsilon_3^2\overline{\epsilon}_5}=0$, which is equivalent to $\frac{\epsilon_1\epsilon_5}{\epsilon_3^2}\in\mathbb{F}_{2^m}$;
- $\mathrm{Tr}_1^m\left(\frac{\epsilon_1\epsilon_5}{\epsilon_3^2}\right)=1$.

The proof of the claim involves heavy calculation and is rather lengthy. So it is provided in Appendix.

Subcase 2. $\tau_2\neq 0$. From the above discussion, we have $\tau_1\neq 0$ since $\tau_2=0$ if and only if $\tau_1=0$. By Proposition 1, to prove that (23) has no solution in $\mathbb{F}_{2^n}$, it suffices to verify

$$\mathrm{Tr}_1^m\left(\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1}\right)=1.$$

It can be verified that

$$\begin{aligned}\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1}&=\frac{\theta_2\overline{\theta}_2+\theta_3\overline{\theta}_3+\theta_4^2+(\theta_2\theta_3+\overline{\theta}_2\theta_4)\lambda+(\overline{\theta}_2\overline{\theta}_3+\theta_2\theta_4)\overline{\lambda}+\overline{\theta}_3\theta_4\overline{\lambda}^2+\theta_3\theta_4\lambda^2}{\theta_1^2+\theta_2^2\overline{\lambda}^2+\overline{\theta}_2^2\lambda^2}\\&=\frac{\theta_1\theta_4+(\theta_2\theta_3+\overline{\theta}_2\theta_4)\lambda+(\overline{\theta}_2\overline{\theta}_3+\theta_2\theta_4)\overline{\lambda}+\overline{\theta}_3\theta_4\overline{\lambda}^2+\theta_3\theta_4\lambda^2}{\theta_1^2+\theta_2^2\overline{\lambda}^2+\overline{\theta}_2^2\lambda^2},\end{aligned}$$

where the second equality holds due to Lemma 3 (i).

In the case $\theta_2\overline{\theta}_2=\theta_1\theta_4$, combining with $\theta_2^2=\theta_1\overline{\theta}_3$, we have $\frac{\overline{\theta}_2}{\theta_2}=\frac{\theta_4}{\theta_3}$, i.e. $\overline{\theta}_2\overline{\theta}_3+\theta_2\theta_4=0$. By Lemma 3 (i),

$$\mathrm{Tr}_1^m\left(\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1}\right)=\mathrm{Tr}_1^m\left(\frac{\theta_1\theta_4+\overline{\theta}_3\theta_4\overline{\lambda}^2+\theta_3\theta_4\lambda^2}{\theta_1^2+\theta_1\overline{\theta}_3\overline{\lambda}^2+\theta_1\theta_3\lambda^2}\right)=\mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right)=1.$$

In the case $\theta_2\overline{\theta}_2 = \theta_1\theta_4 + \theta_1^2$, we have

$$\begin{aligned}
\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1} &= \frac{(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)\theta_4+\theta_2\theta_3\lambda+\overline{\theta}_2\overline{\theta}_3\overline{\lambda}+\overline{\theta}_3\theta_4\overline{\lambda}^2+\theta_3\theta_4\lambda^2}{(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2} \\
&= \frac{\theta_4}{\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda} + \frac{\theta_1(\theta_2\theta_3\lambda+\overline{\theta}_2\overline{\theta}_3\overline{\lambda}+\overline{\theta}_3\theta_4\overline{\lambda}^2+\theta_3\theta_4\lambda^2)}{\theta_1(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2} \\
&= \frac{\theta_4}{\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda} + \frac{\theta_2\overline{\theta}_2^2\lambda+\overline{\theta}_2\theta_2^2\overline{\lambda}+\theta_2^2\theta_4\overline{\lambda}^2+\overline{\theta}_2^2\theta_4\lambda^2}{\theta_1(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2} \\
&= \frac{\overline{\theta}_2\theta_2(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)+\theta_4(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2+\theta_1\theta_2\overline{\theta}_2+\theta_1^2\theta_4}{\theta_1(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2} + \frac{\theta_4}{\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda} \\
&= \frac{\theta_4}{\theta_1} + \frac{(\theta_1\theta_4+\theta_1^2)}{\theta_1(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)} + \frac{\theta_1^2}{(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2} + \frac{\theta_4}{\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda} \\
&= \frac{\theta_4}{\theta_1} + \frac{\theta_1}{\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda} + \frac{\theta_1^2}{(\theta_1+\theta_2\overline{\lambda}+\overline{\theta}_2\lambda)^2},
\end{aligned}$$

and then

$$\mathrm{Tr}_1^m\left(\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1}\right) = \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1.$$

By Lemma 3 (iv), either $\theta_2\overline{\theta}_2 = \theta_1\theta_4$ or $\theta_2\overline{\theta}_2 = \theta_1^2 + \theta_1\theta_4$ holds. Thus, $\mathrm{Tr}_1^m\left(\frac{\tau_2\overline{\tau}_2}{\tau_1\overline{\tau}_1}\right) = 1$ holds in both cases. The proof is finished. □

The following is the main result of [20].

Theorem 2. ([20]) *Let m be an odd positive integer and $n = 2m$, $a, b, c \in \mathbb{F}_{2^n}$. Then*

$$g(x) = \overline{x}^3 + a\overline{x}^2x + b\overline{x}x^2 + cx^3$$

permutes $\mathbb{F}_{2^n}$ if one of the following three conditions is satisfied:

1. *$c = 1$, a satisfies $\overline{\lambda}\overline{a} + a + \lambda \neq 0$ and $b = \lambda(a+1)+1$ where $\lambda \in \mathbb{F}_{2^n}$ satisfying $\lambda^2 + \lambda + 1 = 0$;*
2. *$c = 1$, $b = a + 1$ and $a + \overline{a} + 1 \neq 0$;*
3. *$a, b, c \in \mathbb{F}_{2^m}$, $A = ab + c$, $B = 1 + a + b + c \neq 0$ and $C = a^2 + b^2 + ac + b$ satisfy: if $C = 0$, then $\mathrm{Tr}_1^m\left(\frac{A}{B^2}\right) = 1$; if $C = B^2$, then $\mathrm{Tr}_1^m\left(\frac{A}{B^2}\right) = 0$.*

In the following we will describe the relations between Theorems 1 and 2. Since there are no assumptions $a \in \mathbb{F}_{2^m}$ in Theorem 2 (1) and (2), by the analysis before Theorem 1, if $a \neq 0$, we choose $\beta \in \mathbb{F}_{2^{2m}}^*$ that satisfies $\beta^2 a = 1$ and let $(a_1, a_2, a_3) = \left(a\beta/\overline{\beta}, b(\beta/\overline{\beta})^2, c(\beta/\overline{\beta})^3\right)$. Note that if $a \in \mathbb{F}_{2^m}^*$, then $\beta \in \mathbb{F}_{2^m}^*$ and $(a_1, a_2, a_3) = (a, b, c)$. When $a = 0$, the coefficient triples (a_1, a_2, a_3) coming from Theorem 2 (1) and (2) are $\{(0, \lambda+1, 1), (0, 1, 1)\}$. Then we have the following proposition.

Proposition 2. *Let (a_1, a_2, a_3) be defined as above, then $(a_1, a_2, a_3) \in \Gamma$.*

Proof. It is obvious to see that $\{(0, \lambda+1, 1), (0, 1, 1)\} \subset \Gamma$. We need to consider (a_1, a_2, a_3) from $a \neq 0$. For Cases 1 and 2, by $c = 1$, it can be verified that $a_3\overline{a}_3 = 1$ and

$$\begin{aligned}
\theta_1 &= 1 + a_1^2 + a_2\overline{a}_2 + a_3\overline{a}_3 = a\overline{a} + b\overline{b},\\
\theta_2 &= a_1 + \overline{a}_2 a_3 = (a+\overline{b})\beta/\overline{\beta},\\
\theta_3 &= \overline{a}_2 + a_1\overline{a}_3 = (a+\overline{b})(\overline{\beta}/\beta)^2,\\
\theta_4 &= a_1^2 + a_2\overline{a}_2 = \theta_1.
\end{aligned}$$

Then $\mathrm{Tr}_1^m(\frac{\theta_4}{\theta_1}) = 1$ is obvious, and it suffices to verify that $\overline{\theta}_2^2 = \theta_1\theta_3$, which is equivalent to

$$(b+\overline{a})^2 = (\overline{b}+a)(a\overline{a} + b\overline{b}). \tag{26}$$

(1) $b = \lambda(a+1)+1$ where $\lambda^2+\lambda+1=0$. The left-hand side of (26) is

$$1 + \lambda^2(a^2+1) + \overline{a}^2 = \lambda(a^2+1) + a^2 + \overline{a}^2,$$

and the right-hand side equals

$$\begin{aligned}
&\left(\overline{\lambda}(\overline{a}+1) + 1 + a\right)(\lambda a + \overline{\lambda}\overline{a} + a + \overline{a} + 1)\\
&= a(\overline{a}+1) + \lambda a(a+1) + \overline{\lambda}^2\overline{a}(\overline{a}+1)\\
&\quad + \overline{\lambda}\overline{a}(a+1) + \overline{\lambda}(\overline{a}+1)(a+\overline{a}+1) + (a+1)(a+\overline{a}+1)\\
&= \lambda(a(a+1) + \overline{a}(\overline{a}+1) + \overline{a}(a+1) + (\overline{a}+1)(a+\overline{a}+1))\\
&\quad + a(\overline{a}+1) + \overline{a}(a+1) + (a+1)(a+\overline{a}+1) + (\overline{a}+1)(a+\overline{a}+1)\\
&= \lambda(1+a^2) + a^2 + \overline{a}^2.
\end{aligned}$$

Thus, the equality (26) holds.

(2) $b = a+1$. Then (26) holds due to $\overline{b}+a = a+\overline{a}+1 = b+\overline{a}$ and $\theta_1 = a\overline{a}+b\overline{b} = a+\overline{a}+1$.

(3) We have

$$\begin{aligned}
\theta_1 &= 1 + a_1^2 + a_2\overline{a}_2 + a_3\overline{a}_3 = (1+a+b+c)^2,\\
\theta_2 &= a_1 + \overline{a}_2 a_3 = a + bc,\\
\theta_3 &= \overline{a}_2 + a_1\overline{a}_3 = b + ac,\\
\theta_4 &= a_1^2 + a_2\overline{a}_2 = a^2 + b^2.
\end{aligned}$$

From the definitions of A, B, C and Lemma 6 of [20], we have

$$\mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = \mathrm{Tr}_1^m\left(\frac{a+b}{B}\right) = 1.$$

Furthermore, we have

$$\begin{aligned}\theta_2^2+\theta_1\overline{\theta}_3 &= (a+bc)^2+(1+a+b+c)^2(b+ac)\\ &= a^2+b^2c^2+b+ac+a^2b+a^3c+b^3+ab^2c+bc^2+ac^3\\ &= (ac+b+c^2+1)(a^2+b^2+ac+b) = (B^2+C)C,\end{aligned}$$

which is zero from the assumption. □

From Proposition 2 we see that the three classes of coefficients in Theorem 2 are included in Theorem 1. According to a computer verification, the number pairs of coefficient triples covered by Theorems 1 and 2 are $(442, 100)$ for $n = 6$ and $(31714, 1924)$ for $n = 10$, respectively. This indicates that Theorem 1 indeed covers more coefficients than Theorem 2.

The following example shows that there exist coefficients in Theorem 1 that can not be deduced from Theorem 2.

Example 1. Let $q = 2^3$ and $w \in \mathbb{F}_{2^6}$ with the minimal polynomial $m(x) = x^6 + x^4 + x^3 + x + 1$. It can be verified that

$$f(x) = x^{24} + x^{17} + wx^{10} + w^{38}x^3$$

is a permutation of $\mathbb{F}_{2^6}$ by Theorem 1. Then the triple $(a_1, a_2, a_3) = (1, w, w^{38})$ does not come from Theorem 2. Otherwise, we must have had $a_3\overline{a}_3 = 1$ or $a_3 \in \mathbb{F}_{2^m}$ from the discussions in Proposition 2.

It is worth noting that our magma program indicates that Theorem 1 covers all the coefficients a_i's such that $\overline{x}^3 + a_1\overline{x}^2x + a_2\overline{x}x^2 + a_3x^3$ is a permutation of $\mathbb{F}_{2^{2m}}$ for $m = 3$ and 5. From our investigation of the permutation behavior of these quadrinomials, we believe the characterized set in this paper is complete. Nevertheless, our techniques as well as the ones in [3,11] seem insufficient to address this problem. We cordially invite interested readers to attack it.

4. Conclusion

This paper provides a sufficient condition on the coefficients that make quadrinomials having the form as in (1) permutations. The new characterization gives a more concise description on the coefficients and improves the results of [20]. Further, the numerical experiments on small fields indicate that all the possible coefficients might have been covered. We believe that the sufficient condition is also necessary, however, we cannot prove the necessary direction yet.

Declaration of Competing Interest

The authors declare that there is no conflict of interests regarding the publication of this article.

Acknowledgment

The authors would like to thank the Associate Editor and the two anonymous referees for their valuable comments and suggestions. Research partially supported by National Natural Science Foundation of China under grant No. 61761166010.

Appendix A. The proof of the Claim in Theorem 1

Recall that all the following discussions are under the assumption $\theta_2\overline{\lambda}+\overline{\theta}_2\lambda+\theta_1=0$ for some $\lambda\in U$, which indicates that Lemma 6 holds, i.e.

$$\theta_2\overline{\theta}_2=\theta_1\theta_4,\ \theta_3\overline{\theta}_3=\theta_4^2\ ,\ \theta_2^2\theta_3=\theta_1\theta_4^2.$$

We will use the facts that $\theta_2\theta_3+\overline{\theta}_2\overline{\theta}_3=\theta_4 u,\ a_2\theta_3+\overline{a}_2\overline{\theta}_3=a_1u$, the expressions of a_2,a_3 from (9),

$$a_2+\overline{a}_2=\frac{a_1u\theta_1+u^2}{\theta_1\theta_4},\ a_3+\overline{a}_3=\frac{a_1(\theta_1+\theta_4)u^2+u^3+\theta_1\theta_4u}{\theta_1\theta_4^2}$$

by (11) and (12), and

$$\begin{aligned}\overline{a}_2^2a_3+a_2^2\overline{a}_3&=\frac{a_1u^2\theta_1+u^3}{\theta_1\theta_4}+\frac{a_1(\theta_1+\theta_4)u^2+u^3+\theta_1\theta_4u}{\theta_1\theta_4}\\&\quad+\frac{a_1^3(\theta_1+\theta_4)u^2+a_1^2u^3+a_1^2\theta_1\theta_4u}{\theta_1\theta_4^2}\\&=\frac{a_1u^2\theta_4+\theta_1\theta_4u}{\theta_1\theta_4}+\frac{a_1^3(\theta_1+\theta_4)u^2+a_1^2u^3+a_1^2\theta_1\theta_4u}{\theta_1\theta_4^2}.\end{aligned}\tag{27}$$

(1) To prove $\frac{\overline{\epsilon}_1}{\overline{\epsilon}_3^2\epsilon_5}+\frac{\epsilon_1}{\epsilon_3^2\overline{\epsilon}_5}=0$ is equivalent to proving

$$\epsilon_1\epsilon_5\overline{\epsilon}_3^2=\overline{\epsilon}_1\overline{\epsilon}_5\epsilon_3^2.$$

Since $\epsilon_1\overline{\epsilon}_3^2=(\lambda^3+a_1\lambda^2)(\overline{\lambda}^3+\overline{a}_2\overline{\lambda})^2=(\lambda+a_1)(\overline{\lambda}^4+\overline{a}_2^2)=\overline{\lambda}^3+a_1\overline{\lambda}^4+\overline{a}_2^2\lambda+a_1\overline{a}_2^2$, we have

$$\begin{aligned}\epsilon_1\epsilon_5\overline{\epsilon}_3^2&=(\overline{\lambda}^3+a_1\overline{\lambda}^4+\overline{a}_2^2\lambda+a_1\overline{a}_2^2)(\lambda^3+a_1\lambda^2+a_2\lambda+a_3)\\&=1+(a_1^2+a_2)\overline{\lambda}^2+(a_1a_2+a_3)\overline{\lambda}^3+\overline{a}_2^2(a_1^2+a_2)\lambda^2+\overline{a}_2^2(a_1a_2+a_3)\lambda\\&\quad+a_1a_3\overline{\lambda}^4+a_1\overline{a}_2^2a_3+\overline{a}_2^2\lambda^4.\end{aligned}$$

By taking power 2^m on both sides of the above equality and then adding these two equalities, we have

$$\begin{aligned}\epsilon_1\epsilon_5\overline{\epsilon}_3^2+\overline{\epsilon}_1\overline{\epsilon}_5\epsilon_3^2 = {} & (a_2^2+a_1a_3)\overline{\lambda}^4+(\overline{a}_2^2+a_1\overline{a}_3)\lambda^4+(a_1^2+a_2+a_2^2\overline{a}_2+a_1^2a_2^2)\overline{\lambda}^2\\ & +(a_1^2+\overline{a}_2+\overline{a}_2^2a_2+a_1^2\overline{a}_2^2)\lambda^2+(a_1a_2+a_3)\overline{\lambda}^3+(a_1\overline{a}_2+\overline{a}_3)\lambda^3\\ & +\overline{a}_2^2(a_1a_2+a_3)\lambda+a_2^2(a_1\overline{a}_2+\overline{a}_3)\overline{\lambda}+a_1(\overline{a}_2^2a_3+a_2^2\overline{a}_3).\end{aligned}$$

It suffices to prove that

$$C_1\lambda^4+\overline{C}_1\overline{\lambda}^4+C_2\lambda^2+\overline{C}_2\overline{\lambda}^2+C_3\lambda^3+\overline{C}_3\overline{\lambda}^3+C_4\lambda+\overline{C}_4\overline{\lambda}+C_5=0 \tag{28}$$

under the assumption $\overline{\theta}_2\lambda+\theta_2\overline{\lambda}+\theta_1=0$, where

$$\begin{aligned}C_1 &= \overline{a}_2^2+a_1\overline{a}_3,\\ C_2 &= a_1^2+\overline{a}_2+\overline{a}_2^2a_2+a_1^2\overline{a}_2^2,\\ C_3 &= a_1\overline{a}_2+\overline{a}_3,\\ C_4 &= \overline{a}_2^2(a_1a_2+a_3),\\ C_5 &= a_1(\overline{a}_2^2a_3+a_2^2\overline{a}_3).\end{aligned}$$

By recursively using $\lambda^2=\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2}$, we obtain

$$\begin{cases}\lambda^3 = \lambda\left(\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2}\right)=\lambda\frac{\theta_1^2+\theta_2\overline{\theta}_2}{\overline{\theta}_2^2}+\frac{\theta_1\theta_2}{\overline{\theta}_2^2}=\lambda\frac{\theta_1^2+\theta_1\theta_4}{\overline{\theta}_2^2}+\frac{\theta_1\theta_2}{\overline{\theta}_2^2},\\ \lambda^4 = \frac{\theta_1^2}{\overline{\theta}_2^2}\left(\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2}\right)+\frac{\theta_2^2}{\overline{\theta}_2^2}=\frac{\theta_1^3}{\overline{\theta}_2^3}\lambda+\frac{\theta_2(\theta_1^2+\theta_1\theta_4)}{\overline{\theta}_2^3},\end{cases} \tag{29}$$

which can be used to rewrite (28) as $A\lambda+\overline{A\lambda}+B=0$, where

$$\begin{aligned}A &= C_1\frac{\theta_1^3}{\overline{\theta}_2^3}+C_2\frac{\theta_1}{\overline{\theta}_2}+C_3\frac{\theta_1^2+\theta_1\theta_4}{\overline{\theta}_2^2}+C_4,\\ B &= C_1\frac{\theta_2(\theta_1^2+\theta_1\theta_4)}{\overline{\theta}_2^3}+\overline{C}_1\frac{\overline{\theta}_2(\theta_1^2+\theta_1\theta_4)}{\theta_2^3}+C_2\frac{\theta_2}{\overline{\theta}_2}+\overline{C}_2\frac{\overline{\theta}_2}{\theta_2}\\ &\quad +C_3\frac{\theta_1\theta_2}{\overline{\theta}_2^2}+\overline{C}_3\frac{\theta_1\overline{\theta}_2}{\theta_2^2}+a_1(\overline{a}_2^2a_3+a_2^2\overline{a}_3).\end{aligned}$$

In the sequel, we will show that $A=B=0$. From (9), we have

$$\theta_4+a_1^2=a_2\overline{a}_2=\frac{(a_1\overline{\theta}_2+\theta_4)(a_1\theta_2+\theta_4)}{\theta_3\overline{\theta}_3}=\frac{a_1^2\theta_1\theta_4+a_1\theta_4(\theta_2+\overline{\theta}_2)+\theta_4^2}{\theta_4^2},$$

which gives

$$a_1^2(\theta_1+\theta_4)+a_1u+\theta_4+\theta_4^2=0, \tag{30}$$

where $u = \theta_2 + \overline{\theta}_2$. Note that

$$\begin{aligned} A\overline{\theta}_2^3 &= \theta_1^3 C_1 + \theta_1 \overline{\theta}_2^2 C_2 + \theta_1(\theta_1+\theta_4)\overline{\theta}_2 C_3 + \overline{\theta}_2^3 C_4 \\ &= \theta_1(\theta_1^2 C_1 + \overline{\theta}_2^2 C_2 + (\theta_1+\theta_4)\overline{\theta}_2 C_3 + \overline{\theta}_2\theta_3 C_4). \end{aligned}$$

Thus,

$$A = 0 \Leftrightarrow \theta_1^2 C_1 + \overline{\theta}_2^2 C_2 + (\theta_1+\theta_4)\overline{\theta}_2 C_3 + \overline{\theta}_2\theta_3 C_4 = 0. \tag{31}$$

From

$$\begin{aligned} C_1 &= \overline{a}_2^2 + a_1\overline{a}_3 = \left(\frac{a_1\theta_2+\theta_4}{\overline{\theta}_3}\right)^2 + a_1\frac{a_1(\theta_1+\theta_4)+\overline{\theta}_2}{\overline{\theta}_3} \\ &= \frac{a_1^2\theta_2^2 + \theta_4^2 + a_1^2(\theta_1+\theta_4)\overline{\theta}_3 + a_1\overline{\theta}_2\overline{\theta}_3}{\overline{\theta}_3^2} = \frac{\theta_4^2 + a_1^2\theta_4\overline{\theta}_3 + a_1\overline{\theta}_2\overline{\theta}_3}{\overline{\theta}_3^2}, \\ C_2 &= a_1^2 + \overline{a}_2(1 + a_2\overline{a}_2 + a_1^2\overline{a}_2) = a_1^2 + \frac{a_1\theta_2+\theta_4}{\overline{\theta}_3^2}\left(\overline{\theta}_3(1+\theta_4+a_1^2) + a_1^2(a_1\theta_2+\theta_4)\right) \\ &= a_1^2 + \frac{(a_1\theta_2+\theta_4)(1+\theta_4+a_1^2)}{\overline{\theta}_3} + \frac{a_1^4\theta_1 + a_1^2\theta_3}{\overline{\theta}_3}, \end{aligned}$$

and

$$\begin{aligned} C_3 &= a_1\overline{a}_2 + \overline{a}_3 = a_1\frac{a_1\theta_2+\theta_4}{\overline{\theta}_3} + \frac{a_1(\theta_1+\theta_4)+\overline{\theta}_2}{\overline{\theta}_3} = \frac{a_1^2\theta_2 + a_1\theta_1 + \overline{\theta}_2}{\overline{\theta}_3}, \\ C_4 &= \overline{a}_2^2(a_1a_2 + a_3) = \left(\frac{a_1\theta_2+\theta_4}{\overline{\theta}_3}\right)^2 \frac{a_1^2\overline{\theta}_2 + a_1\theta_1 + \theta_2}{\theta_3} \\ &= \frac{a_1^4\theta_2^2\overline{\theta}_2 + a_1^2\theta_4^2\overline{\theta}_2 + a_1^3\theta_1\theta_2^2 + a_1\theta_1\theta_4^2 + a_1^2\theta_2^3 + \theta_2\theta_4^2}{\theta_3\overline{\theta}_3^2}, \end{aligned}$$

we have

$$\overline{\theta}_3^2\theta_1^2 C_1 = \theta_1^2(\theta_4^2 + a_1^2\theta_4\overline{\theta}_3 + a_1\overline{\theta}_2\overline{\theta}_3) = \theta_1^2\theta_4^2 + a_1^2\theta_1\theta_4\theta_2^2 + a_1\theta_1^2\theta_4\theta_2,$$

where the second equality holds due to $\theta_2\overline{\theta}_2 = \theta_1\theta_4$ and $\theta_1\overline{\theta}_3 = \theta_2^2$. Similarly, other three terms related to (31) are

$$\begin{aligned} \overline{\theta}_3^2\overline{\theta}_2^2 C_2 &= a_1^2\overline{\theta}_3^2\overline{\theta}_2^2 + \overline{\theta}_2^2\overline{\theta}_3(a_1\theta_2+\theta_4)(1+\theta_4+a_1^2) + \overline{\theta}_2^2\overline{\theta}_3(a_1^4\theta_1 + a_1^2\theta_3) \\ &= a_1^2\theta_4^2(\theta_2^2 + \overline{\theta}_2^2) + a_1^4\theta_1^2\theta_4^2 + a_1\theta_1\theta_4^2\overline{\theta}_2 + a_1^2\theta_1^2\theta_4^2 + a_1\theta_1\theta_4^3\theta_2 + a_1^3\theta_1\theta_4^2\theta_2, \\ \overline{\theta}_3^2(\theta_1+\theta_4)\overline{\theta}_2 C_3 &= (\theta_1+\theta_4)\overline{\theta}_2\overline{\theta}_3(a_1^2\theta_2 + a_1\theta_1 + \overline{\theta}_2) \\ &= a_1^2\theta_1\theta_4\theta_2^2 + a_1^2\theta_4^2\theta_2^2 + a_1\theta_1^2\theta_4\theta_2 + a_1\theta_1\theta_4^2\theta_2 + \theta_1^2\theta_4^2 + \theta_1\theta_4^3 \end{aligned}$$

and

$$\begin{aligned}\overline{\theta}_3^2\overline{\theta}_2\theta_3C_4 &= \overline{\theta}_2(a_1^4\theta_2^2\overline{\theta}_2 + a_1^2\theta_4^2\overline{\theta}_2 + a_1^3\theta_1\theta_2^2 + a_1\theta_1\theta_4^2 + a_1^2\theta_2^3 + \theta_2\theta_4^2)\\ &= a_1^4\theta_1^2\theta_4^2 + a_1^2\theta_4^2\overline{\theta}_2^2 + a_1^3\theta_1^2\theta_4\theta_2 + a_1\theta_1\theta_4^2\overline{\theta}_2 + a_1^2\theta_1\theta_4\theta_2^2 + \theta_1\theta_4^3.\end{aligned}$$

Then adding these four equalities together gives

$$\begin{aligned}&\overline{\theta}_3^2(\theta_1^2C_1 + \overline{\theta}_2^2C_2 + (\theta_1+\theta_4)\overline{\theta}_2C_3 + \overline{\theta}_2\theta_3C_4)\\ &= a_1^2\theta_1^2\theta_4^2 + a_1\theta_1\theta_4^3\theta_2 + a_1^3\theta_1\theta_4^2\theta_2 + a_1^2\theta_1\theta_4\theta_2^2 + a_1\theta_1\theta_4^2\theta_2 + a_1^3\theta_1^2\theta_4\theta_2\\ &= a_1^2\theta_1^2\theta_4^2 + a_1\theta_1\theta_4\theta_2(\theta_4^2 + a_1^2\theta_4 + a_1\theta_2 + \theta_4 + a_1^2\theta_1)\\ &= a_1^2\theta_1^2\theta_4^2 + a_1\theta_1\theta_4\theta_2a_1\overline{\theta}_2 = 0,\end{aligned}$$

which means $A = 0$.

From the expression of B, we have

$$\begin{aligned}B\theta_2^3\overline{\theta}_2^3 &= \theta_1^3(\theta_1+\theta_4)(\overline{\theta}_3^2C_1 + \theta_3^2\overline{C}_1) + \theta_1^3\theta_4^2(\overline{\theta}_3C_2 + \theta_3\overline{C}_2)\\ &\quad + \theta_1^3\theta_4(\theta_2\overline{\theta}_3C_3 + \overline{\theta}_2\theta_3\overline{C}_3) + \theta_1^3\theta_4^3a_1(\overline{a}_2^2a_3 + a_2^2\overline{a}_3).\end{aligned}$$

Then, to prove $B = 0$ is equivalent to showing that

$$\begin{aligned}&\theta_1(\theta_1+\theta_4)(\overline{\theta}_3^2C_1 + \theta_3^2\overline{C}_1) + \theta_1\theta_4^2(\overline{\theta}_3C_2 + \theta_3\overline{C}_2)\\ &+ \theta_1\theta_4(\theta_2\overline{\theta}_3C_3 + \overline{\theta}_2\theta_3\overline{C}_3) + a_1\theta_1\theta_4^3(\overline{a}_2^2a_3 + a_2^2\overline{a}_3) = 0.\end{aligned} \tag{32}$$

Combining the expressions of C_i's, we have

$$\begin{aligned}\theta_1(\theta_1+\theta_4)(C_1\overline{\theta}_3^2 + \overline{C}_1\theta_3^2) &= (\theta_1+\theta_4)\left(\theta_1\left(a_1^2\theta_4(\theta_3+\overline{\theta}_3) + a_1(\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3)\right)\right)\\ &= a_1^2u^2\theta_1\theta_4 + a_1^2u^2\theta_4^2 + a_1u\theta_1^2\theta_4 + a_1u\theta_1\theta_4^2,\\ \theta_1\theta_4^2(\overline{\theta}_3C_2 + \theta_3\overline{C}_2) &= a_1u\theta_1\theta_4^2 + a_1^3u\theta_1\theta_4^2 + a_1u\theta_1\theta_4^3,\\ \theta_1\theta_4(\theta_2\overline{\theta}_3C_3 + \overline{\theta}_2\theta_3\overline{C}_3) &= a_1^2u^2\theta_1\theta_4 + a_1u\theta_1^2\theta_4,\end{aligned}$$

and

$$\begin{aligned}\theta_1a_1\theta_4^3(\overline{a}_2^2a_3 + a_2^2\overline{a}_3) &= a_1\theta_4^2(a_1\theta_4u^2 + \theta_1\theta_4u) + a_1\theta_4(a_1^3\theta_1u^2 + a_1^3\theta_4u^2 + a_1^2u^3 + a_1^2\theta_1\theta_4u)\\ &= a_1^2u^2\theta_4^3 + a_1u\theta_1\theta_4^3 + a_1^4u^2\theta_1\theta_4 + a_1^4u^2\theta_4^2 + a_1^3u^3\theta_4 + a_1^3u\theta_1\theta_4^2.\end{aligned}$$

The left-hand side of (32) becomes

$$a_1^2u^2\theta_4^2 + a_1^2u^2\theta_4^3 + a_1^4u^2\theta_1\theta_4 + a_1^4u^2\theta_4^2 + a_1^3u^3\theta_4 = a_1^2u^2\theta_4(\theta_4 + \theta_4^2 + a_1^2\theta_1 + a_1^2\theta_4 + a_1u),$$

which is zero by (30). This proves $B = 0$.

(2) It remains to prove that $\mathrm{Tr}_1^m\left(\frac{\epsilon_1\epsilon_5}{\epsilon_3^2}\right) = \mathrm{Tr}_1^m\left(\frac{\epsilon_1\overline{\epsilon}_1\epsilon_5\overline{\epsilon}_5}{(\epsilon_3\overline{\epsilon}_3)^2}\right) = 1$. Let $\Omega_3 = \frac{\epsilon_1\overline{\epsilon}_1\epsilon_5\overline{\epsilon}_5}{(\epsilon_3\overline{\epsilon}_3)^2}$. Since $\epsilon_5 = \epsilon_1 + \epsilon_2$ and $\epsilon_1\overline{\epsilon}_1 + \epsilon_2\overline{\epsilon}_2 = 0$, we have $\Omega_3 = \frac{\epsilon_1\overline{\epsilon}_1(\epsilon_1\overline{\epsilon}_2+\overline{\epsilon}_1\epsilon_2)}{(\epsilon_3\overline{\epsilon}_3)^2}$. Note that

$$\begin{cases} \epsilon_1\overline{\epsilon}_1 = (\lambda+a_1)(\overline{\lambda}+a_1) = 1+a_1^2+a_1\lambda+a_1\overline{\lambda}, \\ \epsilon_1\overline{\epsilon}_2 = \lambda^2(\lambda+a_1)(\overline{a}_2\overline{\lambda}+\overline{a}_3) = \lambda^2(\overline{a}_2+a_1\overline{a}_2\overline{\lambda}+\overline{a}_3\lambda+a_1\overline{a}_3), \\ \epsilon_3\overline{\epsilon}_3 = (\lambda^2+a_2)(\overline{\lambda}^2+\overline{a}_2) = 1+a_2\overline{a}_2+a_2\overline{\lambda}^2+\overline{a}_2\lambda^2, \end{cases}$$

we have

$$\begin{aligned} \epsilon_1\overline{\epsilon}_2+\overline{\epsilon}_1\epsilon_2 &= \lambda^2(\theta_3+a_1\overline{a}_2\overline{\lambda}+\overline{a}_3\lambda)+\overline{\lambda}^2(\overline{\theta}_3+a_1a_2\lambda+a_3\overline{\lambda}) \\ &= \overline{a}_3\lambda^3+a_3\overline{\lambda}^3+\theta_3\lambda^2+\overline{\theta}_3\overline{\lambda}^2+a_1\overline{a}_2\lambda+a_1a_2\overline{\lambda} \end{aligned}$$

and then

$$\Omega_3 = \frac{(1+a_1^2+a_1\lambda+a_1\overline{\lambda})(\overline{a}_3\lambda^3+a_3\overline{\lambda}^3+\theta_3\lambda^2+\overline{\theta}_3\overline{\lambda}^2+a_1\overline{a}_2\lambda+a_1a_2\overline{\lambda})}{(1+a_2\overline{a}_2+a_2\overline{\lambda}^2+\overline{a}_2\lambda^2)^2}.$$

By using $\theta_2\overline{\lambda}+\overline{\theta}_2\lambda+\theta_1 = 0$, i.e. $\lambda^2+\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2} = 0$, we can rewrite Ω_3 as a linear fraction of λ and $\overline{\lambda}$. Note that

$$\overline{a}_3\lambda^3+a_3\overline{\lambda}^3 = \frac{\overline{a}_3(\theta_1^2+\theta_2\overline{\theta}_2)}{\overline{\theta}_2^2}\lambda+\frac{a_3(\theta_1^2+\theta_2\overline{\theta}_2)}{\theta_2^2}\overline{\lambda}+\frac{\overline{a}_3\theta_1\theta_2}{\overline{\theta}_2^2}+\frac{a_3\theta_1\overline{\theta}_2}{\theta_2^2}$$

due to (29) and

$$\theta_3\lambda^2+\overline{\theta}_3\overline{\lambda}^2 = \overline{\theta}_2\lambda+\theta_2\overline{\lambda}+\frac{\theta_2^2\theta_3+\overline{\theta}_2^2\overline{\theta}_3}{\theta_2\overline{\theta}_2} = \theta_1.$$

Then

$$\overline{a}_3\lambda^3+a_3\overline{\lambda}^3+\theta_3\lambda^2+\overline{\theta}_3\overline{\lambda}^2+a_1\overline{a}_2\lambda+a_1a_2\overline{\lambda} \triangleq M\lambda+\overline{M\lambda}+N,$$

where

$$M = \frac{\overline{a}_3(\theta_1^2+\theta_2\overline{\theta}_2)}{\overline{\theta}_2^2}+a_1\overline{a}_2 = \frac{(\theta_1+\theta_4)(a_1(\theta_1+\theta_4)+\overline{\theta}_2)+a_1^2\theta_2\theta_3+a_1\theta_4\theta_3}{\theta_3\overline{\theta}_3},$$

and $N = \frac{a_1u(\theta_1+\theta_4)}{\theta_4^2}+\theta_1$ since

$$\begin{aligned} &\frac{\overline{a}_3\theta_1\theta_2}{\overline{\theta}_2^2}+\frac{a_3\theta_1\overline{\theta}_2}{\theta_2^2} = \frac{\overline{a}_3\theta_2}{\theta_3}+\frac{a_3\overline{\theta}_2}{\overline{\theta}_3} = \frac{\overline{a}_3\theta_2\overline{\theta}_3+a_3\overline{\theta}_2\theta_3}{\theta_3\overline{\theta}_3} \\ &= \frac{\theta_2(a_1(\theta_1+\theta_4)+\overline{\theta}_2)+\overline{\theta}_2(a_1(\theta_1+\theta_4)+\theta_2)}{\theta_4^2} = \frac{a_1u(\theta_1+\theta_4)}{\theta_4^2}. \end{aligned}$$

The numerator $(1+a_1^2+a_1\lambda+a_1\overline{\lambda})(M\lambda+\overline{M\lambda}+N)$ equals

$$\begin{aligned}&(1+a_1^2)N+a_1(M+\overline{M})+a_1N(\lambda+\overline{\lambda})+(1+a_1^2)(M\lambda+\overline{M\lambda})\\&+a_1M\left(\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2}\right)+a_1\overline{M}\left(\frac{\theta_1}{\theta_2}\overline{\lambda}+\frac{\overline{\theta}_2}{\theta_2}\right)\triangleq I_1\lambda+\overline{I}_1\overline{\lambda}+J_1,\end{aligned}$$

where $I_1=a_1N+(1+a_1^2)M+\frac{a_1M\theta_1}{\overline{\theta}_2}$ and

$$\begin{aligned}J_1&=(1+a_1^2)N+a_1(M+\overline{M})+\tfrac{a_1M\theta_2}{\overline{\theta}_2}+\tfrac{a_1\overline{M\theta}_2}{\theta_2}\\&=(1+a_1^2)\left(\theta_1+\tfrac{a_1u(\theta_1+\theta_4)}{\theta_4^2}\right)+\tfrac{a_1}{\theta_4^2}\left((\theta_1+\theta_4)u+a_1^2(\theta_2\theta_3+\overline{\theta}_2\overline{\theta}_3)+a_1\theta_4(\theta_3+\overline{\theta}_3)\right)\\&\quad+a_1\tfrac{M\theta_2^2+\overline{M\theta}_2^2}{\theta_2\overline{\theta}_2}\\&=(1+a_1^2)\left(\theta_1+\tfrac{a_1u(\theta_1+\theta_4)}{\theta_4^2}\right)+\tfrac{a_1u(\theta_1+\theta_4)}{\theta_4^2}+\tfrac{a_1^3\theta_1\theta_4u+a_1^2\theta_4u^2}{\theta_1\theta_4^2}+a_1\tfrac{M\overline{\theta}_3+\overline{M}\theta_3}{\theta_4}\\&=(1+a_1^2)\theta_1+\tfrac{a_1^3u(\theta_1+\theta_4)}{\theta_4^2}+\tfrac{a_1^2u^2\theta_1+a_1u(\theta_1+\theta_4)\theta_4}{\theta_4^3}\end{aligned}$$

by

$$\begin{aligned}\overline{M}\theta_3+M\overline{\theta}_3&=\frac{(\theta_1+\theta_4)\left((a_1(\theta_1+\theta_4)+\overline{\theta}_2)\overline{\theta}_3+(a_1(\theta_1+\theta_4)+\theta_2)\theta_3\right)}{\theta_3\overline{\theta}_3}+a_1^2(\theta_2+\overline{\theta}_2)\\&=a_1^2u+\frac{(\theta_1+\theta_4)(a_1(\theta_1+\theta_4)u^2+\theta_1\theta_4u)}{\theta_1\theta_4^2}.\end{aligned}$$

From

$$\overline{a}_2\lambda^2+a_2\overline{\lambda}^2=\frac{\overline{a}_2\theta_2\lambda+a_2\overline{\theta}_2\overline{\lambda}}{\theta_4}+\frac{a_1u}{\theta_4},$$

we have the denominator of Ω_3 as

$$\begin{aligned}&\left(1+a_2\overline{a}_2+\frac{\overline{a}_2\theta_2\lambda+a_2\overline{\theta}_2\overline{\lambda}}{\theta_4}+\frac{a_1u}{\theta_4}\right)^2\\&=1+(\theta_4+a_1^2)^2+\frac{a_1^2u^2}{\theta_4^2}+\frac{1}{\theta_4^2}\left(\overline{a}_2^2\theta_2^2\left(\frac{\theta_1}{\overline{\theta}_2}\lambda+\frac{\theta_2}{\overline{\theta}_2}\right)+a_2^2\overline{\theta}_2^2\left(\frac{\theta_1}{\theta_2}\overline{\lambda}+\frac{\overline{\theta}_2}{\theta_2}\right)\right)\\&\triangleq I_2\lambda+\overline{I}_2\overline{\lambda}+J_2,\end{aligned}$$

where

$$\begin{aligned}I_2&=\tfrac{\theta_1\overline{a}_2^2\theta_2^2}{\theta_4^2\overline{\theta}_2}=\tfrac{\overline{a}_2^2\theta_2^3}{\theta_4^3},\\J_2&=1+\theta_4^2+a_1^4+\tfrac{a_1^2u^2}{\theta_4^2}+\tfrac{(\overline{a}_2\theta_2^2+a_2\overline{\theta}_2^2)^2}{\theta_2\overline{\theta}_2\theta_4^2}\\&=1+\theta_4^2+a_1^4+\tfrac{a_1^2u^2(\theta_1+\theta_4)}{\theta_4^3}\end{aligned}$$

due to the fact $\overline{a}_2\theta_2^2+a_2\overline{\theta}_2^2=\theta_1(\overline{a}_2\overline{\theta}_3+a_2\theta_3)=a_1u\theta_1$. Therefore,

$$\begin{aligned}\Omega_3 &= \frac{I_1\lambda + \overline{I}_1\overline{\lambda} + J_1}{I_2\lambda + \overline{I}_2\overline{\lambda} + J_2} = \frac{I_1\theta_2\lambda + \overline{I}_1\theta_2\overline{\lambda} + J_1\theta_2}{I_2\theta_2\lambda + \overline{I}_2\theta_2\overline{\lambda} + J_2\theta_2} \\ &= \frac{I_1\theta_2\lambda + \overline{I}_1(\overline{\theta}_2\lambda + \theta_1) + J_1\theta_2}{I_2\theta_2\lambda + \overline{I}_2(\overline{\theta}_2\lambda + \theta_1) + J_2\theta_2} \\ &= \frac{(I_1\theta_2 + \overline{I}_1\overline{\theta}_2)\lambda + \overline{I}_1\theta_1 + J_1\theta_2}{(I_2\theta_2 + \overline{I}_2\overline{\theta}_2)\lambda + \overline{I}_2\theta_1 + J_2\theta_2}.\end{aligned}$$

To finish the proof, it suffices to prove that

$$\frac{\overline{I}_1\theta_1 + J_1\theta_2}{\overline{I}_2\theta_1 + J_2\theta_2} = \frac{I_1\theta_2 + \overline{I}_1\overline{\theta}_2}{I_2\theta_2 + \overline{I}_2\overline{\theta}_2} \tag{33}$$

and

$$\mathrm{Tr}_1^m\left(\frac{I_1\theta_2 + \overline{I}_1\overline{\theta}_2}{I_2\theta_2 + \overline{I}_2\overline{\theta}_2}\right) = 1. \tag{34}$$

The equation (33) is equivalent to

$$\begin{aligned}&(\overline{I}_1\theta_1 + J_1\theta_2)(I_2\theta_2 + \overline{I}_2\overline{\theta}_2) + (\overline{I}_2\theta_1 + J_2\theta_2)(I_1\theta_2 + \overline{I}_1\overline{\theta}_2) \\ &= \theta_2(\overline{I}_1I_2\theta_1 + I_1\overline{I}_2\theta_1 + I_2J_1\theta_2 + I_1J_2\theta_2 + \overline{I}_2J_1\overline{\theta}_2 + \overline{I}_1J_2\overline{\theta}_2) = 0 \\ &\Leftrightarrow J_2(I_1\theta_2 + \overline{I}_1\overline{\theta}_2) + J_1(I_2\theta_2 + \overline{I}_2\overline{\theta}_2) + \theta_1(I_1\overline{I}_2 + \overline{I}_1I_2) = 0.\end{aligned} \tag{35}$$

Since

$$\begin{aligned}I_1\overline{\theta}_2\theta_4^2 &= \theta_4^2M\left((1+a_1^2)\overline{\theta}_2 + a_1\theta_1\right) + a_1N\overline{\theta}_2\theta_4^2 \\ &= \left(a_1^2\theta_2\theta_3 + a_1\theta_3\theta_4 + a_1(\theta_1+\theta_4)^2 + \overline{\theta}_2(\theta_1+\theta_4)\right)\left((1+a_1^2)\overline{\theta}_2 + a_1\theta_1\right) \\ &\quad + a_1\theta_1\theta_4^2\overline{\theta}_2 + a_1^2u(\theta_1+\theta_4)\overline{\theta}_2,\end{aligned}$$

by multiplying both sides of the above equality by θ_2^2, we have

$$\begin{aligned}I_1\overline{\theta}_2\theta_4^2\theta_2^2 &= \left(a_1^2\theta_2^2\theta_3 + a_1\theta_2\theta_3\theta_4 + a_1(\theta_1+\theta_4)^2\theta_2 + \theta_2\overline{\theta}_2(\theta_1+\theta_4)\right)\left((1+a_1^2)\overline{\theta}_2\theta_2 + a_1\theta_1\theta_2\right) \\ &\quad + a_1\theta_1\theta_4^2\overline{\theta}_2\theta_2^2 + a_1^2u(\theta_1+\theta_4)\overline{\theta}_2\theta_2^2 \\ &= (a_1^2\theta_1\theta_4^2 + a_1\theta_2\theta_3\theta_4 + a_1(\theta_1+\theta_4)^2\theta_2 + \theta_1\theta_4(\theta_1+\theta_4))((1+a_1^2)\theta_1\theta_4 + a_1\theta_1\theta_2) \\ &\quad + a_1\theta_1^2\theta_4^3\theta_2 + a_1^2u\theta_2\theta_1\theta_4(\theta_1+\theta_4).\end{aligned}$$

Then

$$\begin{aligned}I_1\theta_2\theta_4^3 &= (a_1^2\theta_1\theta_4^2 + \theta_1\theta_4(\theta_1+\theta_4))(1+a_1^2)\theta_4 + (a_1^2\theta_1\theta_4^2 + \theta_1\theta_4(\theta_1+\theta_4))a_1\theta_2 \\ &\quad + (a_1\theta_2\theta_3\theta_4 + a_1\theta_2(\theta_1+\theta_4)^2)(1+a_1^2)\theta_4 \\ &\quad + (a_1\theta_2\theta_3\theta_4 + a_1\theta_2(\theta_1+\theta_4)^2)a_1\theta_2 + a_1\theta_1\theta_4^3\theta_2 + a_1^2u\theta_2\theta_4(\theta_1+\theta_4)\end{aligned} \tag{36}$$

and

$$\begin{aligned}
&(I_1\theta_2+\overline{I}_1\overline{\theta}_2)\theta_4^3\\
&=\left(a_1^2\theta_1\theta_4^2+\theta_1\theta_4(\theta_1+\theta_4)\right)a_1u+\left(a_1\theta_4(\theta_2\theta_3+\overline{\theta}_2\overline{\theta}_3)+a_1u(\theta_1+\theta_4)^2\right)(1+a_1^2)\theta_4\\
&\quad+a_1^2u^2(\theta_1+\theta_4)^2+a_1u\theta_1\theta_4^3+a_1^2u^2\theta_4(\theta_1+\theta_4)\\
&=a_1^3u\theta_1\theta_4^2+a_1u(\theta_1^2\theta_4+\theta_1\theta_4^2)+a_1u\theta_1^2(\theta_4+a_1^2\theta_4)\\
&\quad+a_1^2u^2(\theta_1+\theta_4)^2+a_1u\theta_1\theta_4^3+a_1^2u^2\theta_4(\theta_1+\theta_4)\\
&=a_1^3u\theta_1\theta_4^2+a_1u\theta_1\theta_4^2+a_1^3u\theta_1^2\theta_4+a_1^2u^2\theta_1^2+a_1u\theta_1\theta_4^3+a_1^2u^2\theta_1\theta_4\\
&=a_1^2u^2\theta_1^2+a_1u\theta_1\theta_4(a_1^2\theta_4+\theta_4+a_1^2\theta_1+\theta_4^2+a_1u)\\
&=a_1^2u^2\theta_1^2.
\end{aligned}$$

That's to say,

$$I_1\theta_2+\overline{I}_1\overline{\theta}_2=\frac{a_1^2u^2\theta_1^2}{\theta_4^3}.$$

It's easy to see that

$$I_2\theta_2+\overline{I}_2\overline{\theta}_2=\frac{\overline{a}_2^2\theta_2^4+a_2^2\overline{\theta}_2^4}{\theta_4^3}=\frac{\theta_1^2(a_2\theta_3+\overline{a}_2\overline{\theta}_3)^2}{\theta_4^3}=\frac{a_1^2u^2\theta_1^2}{\theta_4^3}=I_1\theta_2+\overline{I}_1\overline{\theta}_2,$$

which means that (34) holds.

In the following, we begin to compute $I_1\overline{I}_2+\overline{I}_1I_2$. By multiplying both sides of (36) by

$$\overline{I}_2\overline{\theta}_2\theta_4^3=a_2^2\overline{\theta}_2^4=\theta_1^2(a_2\theta_3)^2=\theta_1^2(a_1\overline{\theta}_2+\theta_4)^2,$$

we have

$$\begin{aligned}
&I_1\overline{I}_2\theta_2\overline{\theta}_2\theta_4^6/\theta_1^2\\
&=(a_1\overline{\theta}_2+\theta_4)^2\left((1+a_1^2)\theta_4+a_1\theta_2\right)\left(a_1^2\theta_1\theta_4^2+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2+\theta_1\theta_4(\theta_1+\theta_4)\right)\\
&\quad+(a_1\overline{\theta}_2+\theta_4)^2\left(a_1\theta_1\theta_4^3\theta_2+a_1^2u\theta_2\theta_4(\theta_1+\theta_4)\right)\\
&=\Big((1+a_1^2)\theta_4^3+a_1\theta_2\theta_4^2+a_1^2(1+a_1^2)\overline{\theta}_2^2\theta_4+a_1^3\theta_1\theta_4\overline{\theta}_2\Big)\\
&\quad\cdot\left(a_1^2\theta_1\theta_4^2+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2+\theta_1\theta_4(\theta_1+\theta_4)\right)\\
&\quad+(a_1\overline{\theta}_2+\theta_4)^2\left(a_1\theta_1\theta_4^3\theta_2+a_1^2u\theta_2\theta_4(\theta_1+\theta_4)\right).
\end{aligned}$$

Denote these two products by P_1 and P_2. It's easy to see

$$P_2=a_1^3\theta_1\theta_4^3\theta_2\overline{\theta}_2^2+a_1\theta_1\theta_4^5\theta_2+a_1^4u\theta_2\overline{\theta}_2^2\theta_4(\theta_1+\theta_4)+a_1^2u\theta_2\theta_4^3(\theta_1+\theta_4)$$

and

$$\begin{aligned}P_2+\overline{P}_2 &= a_1^3u\theta_1^2\theta_4^4+a_1^4u^2\theta_1\theta_4^2(\theta_1+\theta_4)+a_1u\theta_1\theta_4^5+a_1^2u^2\theta_4^3(\theta_1+\theta_4)\\ &= a_1^3u\theta_1^2\theta_4^4+a_1^4u^2\theta_1^2\theta_4^2+a_1^4u^2\theta_1\theta_4^3+a_1u\theta_1\theta_4^5+a_1^2u^2\theta_1\theta_4^3+a_1^2u^2\theta_4^4.\end{aligned}$$

To compute $P_1+\overline{P}_1$, we write $\overline{(\cdot)}$ to denote the conjugation of the front terms for short, that's to say,

$$\begin{aligned}&(1+a_1^2)\theta_4^3\left(a_1^2\theta_1\theta_4^2+\theta_1\theta_4(\theta_1+\theta_4)+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2\right)+\overline{(\cdot)}\\ =\ &(1+a_1^2)\theta_4^3\left(a_1\theta_4(\theta_2\theta_3+\overline{\theta}_2\overline{\theta}_3)+a_1u(\theta_1+\theta_4)^2\right)\\ =\ &(1+a_1^2)\theta_4^3\left(a_1\theta_4^2u+a_1u(\theta_1^2+\theta_4^2)\right)\\ =\ &a_1u\theta_1^2\theta_4^3+a_1^3u\theta_1^2\theta_4^3.\end{aligned}$$

Similarly we have the other three sums of the terms and the corresponding conjugations of P_1 as

$$\begin{aligned}&a_1\theta_2\theta_4^2\left(a_1^2\theta_1\theta_4^2+\theta_1\theta_4(\theta_1+\theta_4)+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2\right)+\overline{(\cdot)}\\ =\ &a_1^3u\theta_1\theta_4^4+a_1u\theta_1^2\theta_4^3+a_1u\theta_1\theta_4^4+a_1^2u^2\theta_1^2\theta_4^2+a_1^2u^2\theta_4^4,\\ &a_1^2(1+a_1^2)\overline{\theta}_2^2\theta_4\left(a_1^2\theta_1\theta_4^2+\theta_1\theta_4(\theta_1+\theta_4)+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2\right)+\overline{(\cdot)}\\ =\ &a_1^6u^2\theta_1\theta_4^3+a_1^2u^2\theta_1^2\theta_4^2+a_1^2u^2\theta_1\theta_4^3+a_1^4u^2\theta_1^2\theta_4^2+a_1^3u^3\theta_4^3+a_1^5u^3\theta_4^3+a_1^3u\theta_1^3\theta_4^2+a_1^5u\theta_1^3\theta_4^2\end{aligned}$$

and

$$\begin{aligned}&a_1^3\theta_1\theta_4\overline{\theta}_2\left(a_1^2\theta_1\theta_4^2+\theta_1\theta_4(\theta_1+\theta_4)+a_1\theta_2\theta_3\theta_4+a_1\theta_2(\theta_1+\theta_4)^2\right)+\overline{(\cdot)}\\ =\ &a_1^5u\theta_1^2\theta_4^3+a_1^3u\theta_1^3\theta_4^2+a_1^3u\theta_1^2\theta_4^3+a_1^4u^2\theta_1\theta_4^3.\end{aligned}$$

Adding these equations together, we obtain

$$\begin{aligned}&(I_1\overline{I}_2+\overline{I}_1I_2)\theta_1\theta_4^7=\theta_1^2(P_1+\overline{P}_1+P_2+\overline{P}_2)\\ =\ &\theta_1^2(a_1^3u\theta_1^2\theta_4^4+a_1u\theta_1\theta_4^5+a_1^3u\theta_1\theta_4^4+a_1u\theta_1\theta_4^4+a_1^6u^2\theta_1\theta_4^3+a_1^3u^3\theta_4^3\\ &+a_1^5u^3\theta_4^3+a_1^5u\theta_1^3\theta_4^2+a_1^5u\theta_1^2\theta_4^3)\end{aligned}$$

and

$$\begin{aligned}&(I_1\overline{I}_2+\overline{I}_1I_2)\theta_1\theta_4^5\\ =\ &\theta_1^2(a_1^3u\theta_1^2\theta_4^2+a_1u\theta_1\theta_4^3+a_1^3u\theta_1\theta_4^2+a_1u\theta_1\theta_4^2+a_1^6u^2\theta_1\theta_4\\ &+a_1^3u^3\theta_4+a_1^5u^3\theta_4+a_1^5u\theta_1^3+a_1^5u\theta_1^2\theta_4)\\ =\ &a_1u\theta_1^2(a_1^2\theta_1^2(\theta_4^2+a_1^2\theta_1+a_1^2\theta_4)+a_1^5u\theta_1\theta_4+a_1^4u^2\theta_4+a_1^2u^2\theta_4+a_1^2\theta_1\theta_4^2+\theta_1\theta_4^3+\theta_1\theta_4^2)\end{aligned}$$

$$
\begin{aligned}
&= a_1u\theta_1^2(a_1^2\theta_1^2(a_1u+\theta_4)+a_1^5u\theta_1\theta_4+a_1^4u^2\theta_4+a_1^2u^2\theta_4+a_1^2\theta_1\theta_4^2+\theta_1\theta_4^3+\theta_1\theta_4^2)\\
&= a_1u\theta_1^2(a_1^3u\theta_1^2+a_1^5u\theta_1\theta_4+a_1^4u^2\theta_4+a_1^2u^2\theta_4+\theta_1\theta_4(a_1^2\theta_1+a_1^2\theta_4+\theta_4+\theta_4^2))\\
&= a_1u\theta_1^2(a_1^5u\theta_1\theta_4+a_1^4u^2\theta_4+a_1^3u\theta_1^2+a_1^2u^2\theta_4+a_1u\theta_1\theta_4)\\
&= a_1^2u^2\theta_1^2(a_1^4\theta_1\theta_4+a_1^3u\theta_4+a_1^2\theta_1^2+a_1u\theta_4+\theta_1\theta_4).
\end{aligned}
$$

Since

$$
\begin{aligned}
&\left((I_1\theta_2+\overline{I}_1\overline{\theta}_2)J_2+(I_2\theta_2+\overline{I}_2\overline{\theta}_2)J_1\right)\theta_4^6 = a_1^2u^2\theta_1^2\theta_4^3(J_1+J_2)\\
&= a_1^2u^2\theta_1^2\left((1+a_1^2)\theta_1\theta_4^3+a_1^3u(\theta_1+\theta_4)\theta_4+a_1^2u^2\theta_1+a_1u\theta_4(\theta_1+\theta_4)\right.\\
&\quad \left.+(1+a_1^4+\theta_4^2)\theta_4^3+a_1^2u^2(\theta_1+\theta_4)\right)\\
&= a_1^2u^2\theta_1^2\theta_4\left((1+a_1^2)\theta_1\theta_4^2+a_1^3u(\theta_1+\theta_4)+a_1u(\theta_1+\theta_4)+(1+a_1^4+\theta_4^2)\theta_4^2+a_1^2u^2\right),
\end{aligned}
$$

to prove the equation (35), it suffices to prove that

$$
\begin{aligned}
&(1+a_1^2)\theta_1\theta_4^2+a_1^3u(\theta_1+\theta_4)+a_1u(\theta_1+\theta_4)+(1+a_1^4+\theta_4^2)\theta_4^2+a_1^2u^2\\
&+a_1^4\theta_1\theta_4+a_1^3u\theta_4+a_1^2\theta_1^2+a_1u\theta_4+\theta_1\theta_4=0,
\end{aligned}
$$

which holds since its left-hand side can be expanded and simplified as

$$
\begin{aligned}
&\theta_1\theta_4^2+a_1^2\theta_1\theta_4^2+a_1^3u\theta_1+a_1u\theta_1+\theta_4^2+a_1^4\theta_4^2+\theta_4^4+a_1^2u^2+a_1^4\theta_1\theta_4+a_1^2\theta_1^2+\theta_1\theta_4\\
&= \theta_1(\theta_4^2+a_1u+a_1^2\theta_1+\theta_4)+a_1^2\theta_1(\theta_4^2+a_1u+a_1^2\theta_4)+\theta_4^2+a_1^4\theta_4^2+\theta_4^4+a_1^2u^2\\
&= a_1^2\theta_1\theta_4+a_1^2\theta_1(a_1^2\theta_1+\theta_4)+\theta_4^2+a_1^4\theta_4^2+\theta_4^4+a_1^2u^2\\
&= (a_1^2\theta_1+a_1^2\theta_4+\theta_4+\theta_4^2+a_1u)^2=0.
\end{aligned}
$$

Thus, (33) holds and the proof of the claim is finished. □

References

[1] A. Akbary, Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, Int. J. Math. Math. Sci. (2007) 23408.
[2] A. Alahmadi, H. Akhazmi, T. Helleseth, R. Hijazi, N.M. Muthana, P. Solé, On the lifted Zetterberg code, Des. Codes Cryptogr. 80 (3) (2016) 561–576.
[3] D. Bartoli, On a conjecture about a class of permutation trinomials, Finite Fields Appl. 52 (2018) 30–50.
[4] L. Carlitz, C. Wells, The number of solutions of a special system of equations in a finite field, Acta Arith. 12 (1966) 77–84.
[5] L.E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Dover, New York, 1958.
[6] C. Ding, L. Qu, Q. Wang, J. Yuan, P. Yuan, Permutation trinomials over finite fields with even characteristic, SIAM J. Discrete Math. 29 (1) (2015) 79–92.
[7] S.M. Dodunekov, J.E.M. Nilsson, Algebraic decoding of the Zetterberg codes, IEEE Trans. Inf. Theory 38 (5) (1992) 1570–1573.
[8] R. Gupta, R.K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields Appl. 41 (2016) 89–96.
[9] X. Hou, A class of permutation trinomials over finite fields, Acta Arith. 162 (2014) 51–64.

[10] X. Hou, Determination of a type of permutation trinomials over finite fields II, Finite Fields Appl. 35 (2015) 16–35.
[11] X. Hou, On a class of permutation trinomials in characteristic 2, arXiv:1803.04071.
[12] N. Li, T. Helleseth, Several classes of permutation trinomials from Niho exponents, Cryptogr. Commun. 9 (2017) 693–705.
[13] N. Li, T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, Cryptogr. Commun. 11 (1) (2019) 129–136.
[14] K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl. 43 (2017) 69–85.
[15] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., Cambridge University Press, 1997.
[16] G.L. Mullen, D. Panario (Eds.), Handbook of Finite Fields, CRC Press, Boca Raton, 2013.
[17] N. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Aust. Math. Soc. 33 (1982) 197–212.
[18] Y. Niho, Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, PhD dissertation, Univ. Southern Calif, Los Angeles, 1972.
[19] Z. Tu, X. Zeng, C. Li, T. Helleseth, A class of new permutation trinomials, Finite Fields Appl. 50 (2018) 178–195.
[20] Z. Tu, X. Zeng, T. Helleseth, New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$, Finite Fields Appl. 50 (2018) 304–318.
[21] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{\frac{q-1}{d}})$ and their group structure, Monatshefte Math. 112 (1991) 149–163.
[22] Z. Zha, L. Hu, S. Fan, Further results on permutation trinomials over finite fields with even characteristic, Finite Fields Appl. 45 (2017) 43–52.
[23] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{\frac{q-1}{d}})$, Proc. Am. Math. Soc. 137 (2009) 2209–2216.