Turkish Journal of Mathematics

Volume 46 | Number 3 Article 17

1-1-2022

Two classes of permutation polynomials with Niho exponents over finite fields with even characteristic

QIAN LIU

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2022) 46: 919 – 928

doi:10.55730/1300-0098.3132

Two classes of permutation polynomials with Niho exponents over finite fields with even characteristic

Qian LIU*
College of Computer and Data Science, Key Laboratory of Information Security of Network Systems, Fuzhou University, Fuzhou, P.R. China

Received: 02.09.2021 • **Accepted/Published Online:** 31.01.2022 • **Final Version:** 11.03.2022

Abstract: In this paper, by transforming the permutation problem into the root distribution problem in the unit circle of certain quadratic and cubic equations, we investigate the permutation behavior of the type $f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$ over $\mathbb{F}_{2^{4m}}$ and $f(x)=x+x^{2^m}+x^{2^{m+1}-1}+ax^{2^{2m}-2^m+1}$ over $\mathbb{F}_{2^{2m}}$, respectively.

Key words: Finite field, permutation trinomial, permutation quadrinomial

1. Introduction

Let q be a power of a prime p, $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{F}_q^*$ denote its multiplicative group. A polynomial $f\in\mathbb{F}_q[x]$ is called a permutation polynomial if its associated polynomial mapping $f:c\mapsto f(c)$ from $\mathbb{F}_q$ into itself is a bijection [12]. Permutation polynomials over finite fields have been a hot topic of study for many years due to their significant applications areas such as cryptography [17], combinatorial design theory [4], coding theory [8], and other areas of mathematics and engineering [15]. Finding new constructions of permutation polynomials is of tremendous interest in both theoretical and applied aspects. The reader is referred to the survey paper [6] for a detailed introduction about the developments on permutation polynomials.

The study of permutation polynomials with few terms, especially binomials and trinomials, has attracted the researcher's interest due to their simple algebraic form and additional extraordinary properties. Only a few classes of permutation binomials and trinomials are known. This motivates us to find new families of permutation trinomials with coefficients over finite fields with even characteristic. A Niho exponent [16] with respect to the finite field $\mathbb{F}_{q^2}$ is a positive integer d satisfying $d\equiv p^j \mod (q-1)$ for some nonnegative integer j. When $j=0$, the integer d is then called a normalized Niho exponent. The Niho exponents are good resources that lead to desirable objects in sequence design and communications [5]. By utilizing various methods in solving equations with low degree over finite fields, some new permutation trinomials with Niho exponents were proposed in [1–3, 7, 9–11, 13, 14, 18, 21–23]. However, only a small number of classes of permutation quadrinomials are known in the literature. To the best of our knowledge, the permutation behavior of quadrinomials having the form $x^{2^{m+1}+2^m}+ax^{2^{m+1}+1}+bx^{2^m+2}+cx^3$ over $\mathbb{F}_{2^{2m}}$ for odd m were investigated in [19], where a,b,c satisfying some restrictions.

*Correspondence: lqmova@foxmail.com
2010 *AMS Mathematics Subject Classification:* 11T06, 11T71, 05A05

The purpose of this paper is to construct several classes of permutation polynomials with Niho exponents. Recently, a class of permutation quadrinomials of the form $x + a_1x^{2^{2m}-2^m+1} + a_2x^{2^m} + a_2^2x^{2^{m+1}-1}$ over $\mathbb{F}_{2^{2m}}$ was proposed in [20], where $a_1, a_2 \in \mathbb{F}_{2^{2m}}^*$ and two sets of coefficient triples were obtained with the restriction $a_2^{2^m+1} \neq 1$. Inspired by this work, we study a class of permutation quadrinomials with the form $f(x) = x + x^{2^m} + x^{2^{m+1}-1} + ax^{2^{2m}-2^m+1}$ over $\mathbb{F}_{2^{2m}}$. Moreover, we propose a class of permutation trinomials over finite fields with even characteristic. We reduce the problem of determining the solutions of the equation $f(x) = \gamma$ to that of the root distribution in the unit circle of certain related quadratic and cubic equations.

The remainder of this paper is organized as follows. In Section 2, some preliminaries and notations are introduced, including some useful lemmas. In Section 3, two classes of permutation polynomials with Niho exponents over finite fields with even characteristic are given.

2. Preliminaries

For two positive integers m and n with $m|n$, let $\mathbb{F}_{p^n}$ be a finite field with p^n elements, we use $Tr_m^n(\cdot)$ to denote the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, i.e.

$$Tr_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(n/m-1)m}}.$$

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

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

Lemma 2.1 *([20]) Let $A \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_{2^m}$ be fixed. Then*

$$U\backslash\{1\} = \left\{ \frac{u + \overline{A}}{u + A} : u \in \mathbb{F}_{2^m} \right\}.$$

Lemma 2.2 *([21]) Let $n = 2m$ be an even positive integer and $a, b \in \mathbb{F}_{2^n}^*$ satisfy $Tr_1^n(\frac{b}{a^2}) = 0$. Then for the quadratic equation $x^2 + ax + b = 0$, we have (i) both two solutions are in the unit circle, if and only if $b = \frac{a}{\overline{a}}$ and*

$$Tr_1^m(\frac{b}{a^2}) = Tr_1^m(\frac{1}{a\overline{a}}) = 1.$$

(ii) there is exactly one solution in the unit circle, if and only if $b \neq \frac{a}{\overline{a}}$ and

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

Lemma 2.3 *([20]) Let m be a positive integer, $B_1, B_2, B_3, B_4 \in \mathbb{F}_{2^m}$ and $B_1(B_2B_3 + B_1B_4) \neq 0$. Then the cubic equation*

$$B_1x^3 + B_2x^2 + B_3x + B_4 = 0$$

has a unique solution in $\mathbb{F}_{2^m}$ if and only if one of the following two conditions holds: (i) $B_2^2 + B_1B_3 = 0$ and m is odd. (ii) $B_2^2 + B_1B_3 \neq 0$ and $Tr_1^m(1 + \frac{(B_2^2+B_1B_3)(B_3^2+B_2B_4)}{(B_2B_3+B_1B_4)^2}) = 1$.

3. Main results

In this section, we consider two classes of permutation polynomials with Niho exponents over finite fields with even characteristic. More precisely, we investigate the permutation behavior of the type $f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$ over $\mathbb{F}_{2^{4m}}$ and $f(x)=x+x^{2^m}+x^{2^{m+1}-1}+ax^{2^{2m}-2^m+1}$ over $\mathbb{F}_{2^{2m}}$, respectively.

Theorem 3.1 *Let m be a positive integer, then $f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$ is a permutation trinomial over $\mathbb{F}_{2^{4m}}$.*

Proof Here, for each element x in the finite fields $\mathbb{F}_{2^{4m}}$, we define $\overline{x}=x^{2^{2m}}$ and $U_{2^{2m}}=\{x\in\mathbb{F}_{2^{4m}}: x^{2^{2m}+1}=x\overline{x}=1\}$. To prove that $f(x)=x+x^{2^{3m}-2^m+1}+x^{2^{4m}-2^{3m}+2^m}$ permutes $\mathbb{F}_{2^{4m}}$, it is sufficient to show that for any $\gamma\in\mathbb{F}_{2^{4m}}$, the equation

$$x+x^{2^m(2^{2m}-1)+1}+x^{(2^{2m}-2^m+1)(2^{2m}-1)+1}=\gamma \tag{3.1}$$

has a unique solution in $\mathbb{F}_{2^{4m}}$.To this end, we discuss the proof according to the following two cases. Case I: $\gamma=0$, i.e., $f(x)=0$. Obviously, $x=0$ is a solution of (3.1). Next we show that there is no $x\in\mathbb{F}_{2^{4m}}^*$ satisfying (3.1). Otherwise, we have

$$1+x^{2^m(2^{2m}-1)}+x^{(2^{2m}-2^m+1)(2^{2m}-1)}=0. \tag{3.2}$$

Denote $\lambda=x^{2^{2m}-1}$, then $\lambda\in U_{2^{2m}}$. From (3.2) we can deduce

$$1+\lambda^{2^m}+\lambda^{2^{2m}-2^m+1}=0, \tag{3.3}$$

which implies that

$$1+\lambda^{2^m}+\lambda^{-2^m}=0. \tag{3.4}$$

Multiplying both sides of (3.4) by λ^{2^m}, we obtain

$$(\lambda^{2^m})^2+\lambda^{2^m}+1=0. \tag{3.5}$$

It can be seen that $Tr_1^{2m}(1)=0$. Then we know that (3.5) has no solution in $U_{2^{2m}}$ from Lemma 2.2, which implies that (3.2) has no nonzero solution in $\mathbb{F}_{2^{4m}}$. This is a contraction. So, (3.1) has only one solution $x=0$ in $\mathbb{F}_{2^{4m}}$ for $\gamma=0$. Case II: $\gamma\neq 0$ and $f(x)=\gamma$. Obviously, $x=0$ is not a solution of (3.1), we only need to prove that (3.1) has only one solution in $\mathbb{F}_{2^{4m}}^*$. Substituting $x=\frac{\gamma}{y}$ into (3.1), we have

$$\frac{\gamma}{y}(1+(\frac{\gamma}{y})^{2^m(2^{2m}-1)}+(\frac{\gamma}{y})^{(2^{2m}-2^m+1)(2^{2m}-1)})=\gamma,$$

and then replacing γ and y with γ^{2^m} and y^{2^m}, respectively, we obtain

$$1+\frac{\gamma\overline{y}}{\overline{\gamma}y}+\frac{\overline{\gamma}y}{\gamma\overline{y}}=y^{2^m}, \tag{3.6}$$

which is equivalent to

$$\gamma\overline{\gamma}y\overline{y}+\gamma^2\overline{y}^2+\overline{\gamma}^2y^2=\gamma\overline{\gamma}y\overline{y}y^{2^m}. \tag{3.7}$$

Raising (3.7) to the 2^{2m}-th power, we can get

$$\gamma\overline{\gamma}y\overline{y} + \overline{\gamma}^2y^2 + \gamma^2\overline{y}^2 = \gamma\overline{\gamma}y\overline{y}\overline{y}^{2^m}. \tag{3.8}$$

Combining (3.7) and (3.8), we have $y^{2^m} = \overline{y}^{2^m}$, i.e. $y = \overline{y}$. Then we have $1 + \frac{\gamma}{\overline{\gamma}} + \frac{\overline{\gamma}}{\gamma} = y^{2^m}$ which is the unique solution of (3.6), and substituting it into $x = \frac{\gamma}{y}$, we know that the solution of (3.1) is unique in the case $\gamma \neq 0$. To summarize, we conclude that (3.1) has at most one solution. The proof is completed. □

Theorem 3.2 *Let $n = 2m$ be an even positive integer with m even and $m > 2$. Assume that $a, \mu \in \mathbb{F}_2^m$ satisfying $1 + a \neq 0$, $1 + a + \mu \neq 0$, $Tr_1^m(\frac{1}{1+a}) = 0$ and $Tr_1^m(1 + \frac{\mu}{(1+a+\mu)^2}) = 0$. Then the quadrinomial*

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

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

Proof To prove that $f(x) = x + x^{2^m} + x^{2^{m+1}-1} + ax^{2^{2m}-2^m+1}$ permutes $\mathbb{F}_{2^n}$, it is sufficient to show that for any $\gamma \in \mathbb{F}_{2^n}$, the equation

$$f(x) = x + x^{2^m} + x^{2^{m+1}-1} + ax^{2^{2m}-2^m+1} = \gamma \tag{3.9}$$

has at most one solution in $\mathbb{F}_{2^n}$. To this end, we discuss the proof according to the following two situations. Case I: $\gamma = 0$, i.e. $f(x) = 0$. It is clear that (3.9) has a solution $x = 0$. Next we show that there is no $x \in \mathbb{F}_{2^n}^*$ satisfying (3.9). Otherwise, we have

$$1 + x^{2^m-1} + x^{2^{m+1}-2} + ax^{2^{2m}-2^m} = 0. \tag{3.10}$$

Denote by $\theta = x^{2^m-1}$, then $\theta \in U$. From (3.10) we can deduce

$$1 + a\overline{\theta} + \theta + \theta^2 = 0,$$

which implies that

$$\theta + a = \theta^2(1 + \theta). \tag{3.11}$$

Taking 2^m-th power on both sides of (3.11) and multiplying by (3.11), it leads to

$$(\overline{\theta} + a)(\theta + a) = (1 + \overline{\theta})(1 + \theta),$$

which implies

$$1 + \overline{\theta}a + \theta a + a^2 = \theta + \overline{\theta}. \tag{3.12}$$

Multiplying both sides of (3.12) by θ, we obtain

$$\theta^2(1 + a) + \theta(1 + a^2) + 1 + a = 0. \tag{3.13}$$

Note that $1+a \neq 0$, let $\alpha = 1+a$ and $\beta = 1$. It can be seen that $\beta = \frac{\alpha}{\overline{\alpha}}$ and $Tr_1^m(\frac{1}{\alpha\overline{\alpha}}) = Tr_1^m(\frac{1}{1+a}) = 0$. Then we know that (3.13) has no solution in U by Lemma 2.2, which implies that (3.10) has no nonzero solution in $\mathbb{F}_{2^n}$. This is a contradiction. Therefore, (3.9) has only one solution $x = 0$ in $\mathbb{F}_{2^n}$ for $\gamma = 0$. Case II: $\gamma \neq 0$

and $f(x)=\gamma$. Obviously, $x=0$ is not a solution of (3.9), we only need to prove that (3.9) has only one solution in $\mathbb{F}_{2^n}^*$. Substituting $x=\frac{\gamma}{y}$ into (3.9), we have

$$\frac{1}{y}(1+a\frac{\gamma\overline{y}}{\overline{\gamma}y}+\frac{\overline{\gamma}y}{\gamma\overline{y}}+(\frac{\overline{\gamma}y}{\gamma\overline{y}})^2)=1.$$

Let $\varepsilon=\frac{\gamma}{\overline{\gamma}}\in U$, we obtain

$$\frac{1}{y}(1+a\varepsilon\frac{\overline{y}}{y}+\overline{\varepsilon}\frac{y}{\overline{y}}+\overline{\varepsilon}^2\frac{y^2}{\overline{y}^2})=1,$$

which implies that

$$y\overline{y}^2+a\varepsilon\overline{y}^3+\overline{\varepsilon}y^2\overline{y}+\overline{\varepsilon}^2y^3+y^2\overline{y}^2=0. \tag{3.14}$$

Taking 2^m-th power on both sides of (3.14), we have

$$y^2\overline{y}+a\overline{\varepsilon}y^3+\varepsilon y\overline{y}^2+\varepsilon^2\overline{y}^3+y^2\overline{y}^2=0. \tag{3.15}$$

Adding (3.14) and (3.15), we obtain

$$A\overline{y}^3+\overline{A}y^3+By\overline{y}^2+\overline{B}y^2\overline{y}=0, \tag{3.16}$$

where $A=a\varepsilon+\varepsilon^2$ and $B=1+\varepsilon$. If $\varepsilon=1$, then $\gamma=\overline{\gamma}$. And (3.16) turns to $(1+a)\overline{y}^3+(1+a)y^3=0$, which means that $y=\overline{y}$. Thus plugging $y=\overline{y}$ into (3.14), we have $y=1+a$ is a unique solution of (3.16). Thus, (3.9) has unique solution in $\mathbb{F}_{2^m}$. For each $\varepsilon\in U\backslash\{1\}$, we know that there exists a unique $\gamma\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ by Lemma 2.1, then x can be determined uniquely by y. So we only need to prove that for each $\varepsilon\in U\backslash\{1\}$, (3.16) has a unique solution in $\mathbb{F}_{2^n}^*$. Now the solution of (3.16) is divided into the following two cases.
(i) $A+B+\overline{A}+\overline{B}=0$. From (3.16), we can easily get that $y=\overline{y}$ is the unique solution. Furthermore, plugging $y=\overline{y}$ into (3.14), we have $y=1+a\varepsilon+\overline{\varepsilon}+\overline{\varepsilon}^2$. Hence, (3.16) has a unique solution in $\mathbb{F}_{2^m}$. Next we need to prove that there is no other solution in $\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ satisfying (3.16). Set $C=A+B$, since $A+B+\overline{A}+\overline{B}=0$, we can get $C+\overline{C}=0$, which implies $C\in\mathbb{F}_{2^m}$. Therefore, (3.16) is equivalent to

$$A\overline{y}^3+\overline{A}y^3+(A+C)y\overline{y}^2+(\overline{A}+C)y^2\overline{y}=0,$$

which can be written as

$$A\overline{y}^2(y+\overline{y})+\overline{A}y^2(y+\overline{y})+Cy\overline{y}(y+\overline{y})=0. \tag{3.17}$$

Note that $y\neq\overline{y}$, dividing (3.17) by $y+\overline{y}$ results in

$$A\overline{y}^2+\overline{A}y^2+Cy\overline{y}=0,$$

then by eliminating y^2 on both sides of above equation, we can get

$$A(\frac{\overline{y}}{y})^2+C\frac{\overline{y}}{y}+\overline{A}=0.$$

Denote $\lambda=\frac{\overline{y}}{y}$, then above equation is equivalent to

$$\lambda^2+\frac{C}{A}\lambda+\frac{\overline{A}}{A}=0. \tag{3.18}$$

Since $\frac{\overline{A}}{A} = \frac{\frac{C}{A}}{\frac{C}{\overline{A}}}$, to prove that there is no other solution in $\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ satisfying (3.16), it suffices to prove that $Tr_1^m(\frac{A\overline{A}}{C^2}) = 0$ by Lemma 2.2. Let $\mu = \varepsilon + \overline{\varepsilon}$, we have

$$A\overline{A} = (a\varepsilon + \varepsilon^2)(a\overline{\varepsilon} + \overline{\varepsilon}^2) = a^2 + a\overline{\varepsilon} + a\varepsilon + 1 = a^2 + 1 + a\mu,$$

$$B\overline{B} = (1+\varepsilon)(1+\overline{\varepsilon}) = \varepsilon + \overline{\varepsilon} = \mu,$$

$$\begin{aligned} A\overline{B} + \overline{A}B &= (a\varepsilon + \varepsilon^2)(1+\overline{\varepsilon}) + (a\overline{\varepsilon} + \overline{\varepsilon}^2)(1+\varepsilon) \\ &= (1+a)\mu + \mu^2, \end{aligned}$$

$$C^2 = (A+B)(\overline{A}+\overline{B}) = A\overline{A} + A\overline{B} + \overline{A}B + B\overline{B} = 1 + a^2 + \mu^2.$$

Recall that

$$A + \overline{A} + B + \overline{B} = a\varepsilon + \varepsilon^2 + a\overline{\varepsilon} + \overline{\varepsilon}^2 + 1 + \varepsilon + 1 + \overline{\varepsilon} = a\mu + \mu + \mu^2 = 0,$$

then we get $\mu = 0$ or $\mu = 1 + a$. Note that $\mu \neq 1 + a$, we only consider $\mu = 0$. It can be verified that

$$Tr_1^m(\frac{A\overline{A}}{C^2}) = Tr_1^m(\frac{1+a^2}{1+a^2}) = Tr_1^m(1) = 0,$$

since m is even. So (3.16) has no other solution in $\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. That is to say, $y = \overline{y} = 1 + a\varepsilon + \overline{\varepsilon} + \overline{\varepsilon}^2$ is the unique solution of (3.16), then (3.9) has a unique solution in $\mathbb{F}_{2^n}^*$.

(ii) $A + B + \overline{A} + \overline{B} \neq 0$. It can easy to check $y = \overline{y}$ does not satisfy (3.16), so we only consider $y \neq \overline{y}$. Then by eliminating y^3 on both sides of (3.16) gives

$$A\lambda^3 + \overline{A} + B\lambda^2 + \overline{B}\lambda = 0, \tag{3.19}$$

where $\lambda = \frac{\overline{y}}{y} \in U\backslash\{1\}$. Next we need to prove (3.19) has unique solution in $U\backslash\{1\}$. Since $\varepsilon \in U$, then $\varepsilon \neq \overline{\varepsilon}$, which implies that $B \neq \overline{B}$. By Lemma 2.1, λ can be represented as $\lambda = \frac{X+\overline{B}}{X+B}$, where $X \in \mathbb{F}_{2^m}$ and $B \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, then (3.19) can be rewritten as

$$A(\frac{X+\overline{B}}{X+B})^3 + B(\frac{X+\overline{B}}{X+B})^2 + \overline{B}(\frac{X+\overline{B}}{X+B}) + \overline{A} = 0,$$

which can be simplified as

$$D_1X^3 + D_2X^2 + D_3X + D_4 = 0, \tag{3.20}$$

over $\mathbb{F}_{2^m}$, where

$$\begin{cases} D_1 = A + \overline{A} + B + \overline{B}, \\ D_2 = A\overline{B} + \overline{A}B + B^2 + \overline{B}^2, \\ D_3 = A\overline{B}^2 + \overline{A}B^2 + B^2\overline{B} + B\overline{B}^2, \\ D_4 = A\overline{B}^3 + \overline{A}B^3. \end{cases}$$

Therefore, we only need to prove that (3.20) has a unique solution in $\mathbb{F}_{2^m}$. From Lemma 2.3 (ii), we will show that $D_2^2 + D_1D_3 \neq 0$ and $Tr_1^m(1 + \frac{(D_2^2+D_1D_3)(D_3^2+D_2D_4)}{(D_2D_3+D_1D_4)^2}) = 1$. First, denote $\nu = A\overline{A} + B\overline{B} = 1 + a^2 + \mu(a+1)$, and we can get

$$D_2^2 = A^2\overline{B}^2 + \overline{A}^2B^2 + B^4 + \overline{B}^4,$$

and

$$\begin{aligned} D_1D_3 &= (A+\overline{A}+B+\overline{B})(A\overline{B}^2+\overline{A}B^2+B^2\overline{B}+B\overline{B}^2) \\ &= A^2\overline{B}^2+\overline{A}^2B^2+A\overline{A}B^2+A\overline{A}\overline{B}^2+AB^2\overline{B}+\overline{A}B\overline{B}^2 \\ &+ \overline{A}B^3+A\overline{B}^3+B^3\overline{B}+B\overline{B}^3. \end{aligned}$$

Then, we have

$$\begin{aligned} D_2^2+D_1D_3 &= B^4+\overline{B}^4+\overline{A}B^3+A\overline{B}^3+B^3\overline{B}+B\overline{B}^3 \\ &+ A\overline{A}B^2+A\overline{A}\overline{B}^2+AB^2\overline{B}+\overline{A}B\overline{B}^2 \\ &= (B^2+\overline{B}^2)(B^2+\overline{B}^2+A\overline{A}+A\overline{B}+\overline{A}B+B\overline{B}) \\ &= (B+\overline{B})^2(\nu+D_2). \end{aligned}$$

Here, $\nu+D_2=1+a^2+\mu(a+1)+(1+a)\mu+\mu^2+(1+\varepsilon)^2+(1+\bar{\varepsilon})^2=1+a^2\neq 0$. Furthermore, we get $D_2^2+D_1D_3\neq 0$ since $B\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. Next, we still need to prove that

$$Tr_1^m(1+\frac{(D_2^2+D_1D_3)(D_3^2+D_2D_4)}{(D_2D_3+D_1D_4)^2})=1.$$

It is clear to check that

$$D_3^2=A^2\overline{B}^4+\overline{A}^2B^4+B^4\overline{B}^2+B^2\overline{B}^4,$$

$$\begin{aligned} D_2D_4 &= (A\overline{B}+\overline{A}B+B^2+\overline{B}^2)(A\overline{B}^3+\overline{A}B^3) \\ &= A^2\overline{B}^4+\overline{A}^2B^4+A\overline{A}B\overline{B}^3+A\overline{A}B^3\overline{B}+A\overline{B}^5+\overline{A}B^5+AB^2\overline{B}^3+\overline{A}B^3\overline{B}^2, \end{aligned}$$

$$\begin{aligned} D_2D_3 &= (A\overline{B}+\overline{A}B+B^2+\overline{B}^2)(A\overline{B}^2+\overline{A}B^2+B^2\overline{B}+B\overline{B}^2) \\ &= A^2\overline{B}^3+\overline{A}^2B^3+\overline{A}B^4+A\overline{B}^4+A\overline{A}B\overline{B}^2+A\overline{A}B^2\overline{B}+B^4\overline{B}+B\overline{B}^4 \\ &+ B^3\overline{B}^2+B^2\overline{B}^3+AB\overline{B}^3+\overline{A}B^3\overline{B}, \end{aligned}$$

$$\begin{aligned} D_1D_4 &= (A+\overline{A}+B+\overline{B})(A\overline{B}^3+\overline{A}B^3) \\ &= A^2\overline{B}^3+\overline{A}^2B^3+A\overline{A}\overline{B}^3+A\overline{A}B^3+AB\overline{B}^3+\overline{A}\overline{B}B^3+A\overline{B}^4+\overline{A}B^4. \end{aligned}$$

Then, we have

$$\begin{aligned} D_3^2+D_2D_4 &= B^4\overline{B}^2+B^2\overline{B}^4+A\overline{A}B\overline{B}^3+A\overline{A}B^3\overline{B}+A\overline{B}^5+\overline{A}B^5 \\ &+ AB^2\overline{B}^3+\overline{A}B^3\overline{B}^2 \\ &= (B+\overline{B})^2(B\overline{B}\nu+D_4), \end{aligned}$$

and

$$\begin{aligned} D_2D_3+D_1D_4 &= A\overline{A}\overline{B}^3+A\overline{A}B^3+A\overline{A}B\overline{B}^2+A\overline{A}B^2\overline{B}+B^4\overline{B}+B\overline{B}^4 \\ &+ B^3\overline{B}^2+B^2\overline{B}^3 \\ &= (B+\overline{B})^3(A\overline{A}+B\overline{B})=(B+\overline{B})^3\nu. \end{aligned}$$

We will show that $\nu=1+a^2+(a+1)\mu\neq 0$ in the following description. If $\nu=0$, then $\mu=1+a=\varepsilon+\overline{\varepsilon}$, which is equivalent to

$$\varepsilon^2+(1+a)\varepsilon+1=0. \tag{3.21}$$

Since $\frac{1+\overline{a}}{1+a}=1$ and $Tr_1^m(\frac{1}{1+a})=0$. We know that (3.21) has no solution in U from Lemma 2.2, it is a contradiction. It is easy to calculate that

$$B\overline{B}D_2+D_4=B\overline{B}(A\overline{B}+\overline{A}B+B^2+\overline{B}^2)+A\overline{B}^3+\overline{A}B^3,$$

$$\begin{aligned} \frac{B\overline{B}D_2+D_4}{(B+\overline{B})^2\nu} &= \frac{B\overline{B}}{\nu}+\frac{A\overline{B}^3+\overline{A}B^3+B\overline{B}(A\overline{B}+\overline{A}B)}{(B+\overline{B})^2\nu} \\ &= \frac{B\overline{B}}{\nu}+\frac{(B+\overline{B})(A\overline{B}^2+\overline{A}B^2)}{(B+\overline{B})^2\nu} \\ &= \frac{B\overline{B}}{\nu}+\frac{A\overline{B}^2+\overline{A}B^2}{(B+\overline{B})\nu}, \end{aligned}$$

and

$$\frac{D_2D_4}{(B+\overline{B})^2\nu^2}=\frac{A\overline{B}^3+\overline{A}B^3+A\overline{A}B\overline{B}}{\nu^2}+\frac{(A\overline{B}^2+\overline{A}B^2)^2}{(B+\overline{B})^2\nu^2}.$$

Then we have

$$\begin{aligned} & Tr_1^m(\frac{(D_3^2+D_2D_4)(D_2^2+D_1D_3)}{(D_2D_3+D_1D_4)^2}) \\ = \; & Tr_1^m(\frac{(B+\overline{B})^2(B\overline{B}\nu+D_4)(B+\overline{B})^2(\nu+D_2)}{(B+\overline{B})^6\nu^2}) \\ = \; & Tr_1^m(\frac{(B\overline{B}\nu+D_4)(\nu+D_2)}{(B+\overline{B})^2\nu^2}) \\ = \; & Tr_1^m(\frac{B\overline{B}}{B^2+\overline{B}^2}+\frac{B\overline{B}D_2+D_4}{(B+\overline{B})^2\nu}+\frac{D_2D_4}{(B+\overline{B})^2\nu^2}) \\ = \; & Tr_1^m(\frac{B\overline{B}}{B^2+\overline{B}^2}+\frac{B\overline{B}}{\nu}+\frac{A\overline{B}^2+\overline{A}B^2}{(B+\overline{B})\nu}+\frac{A\overline{B}^3+\overline{A}B^3}{\nu^2}+\frac{A\overline{A}B\overline{B}}{\nu^2}+\frac{(A\overline{B}^2+\overline{A}B^2)^2}{(B+\overline{B})^2\nu^2}) \\ = \; & Tr_1^m(\frac{B\overline{B}}{B^2+\overline{B}^2}+\frac{A\overline{B}^3+\overline{A}B^3}{\nu^2}+\frac{B\overline{B}}{\nu}+\frac{A\overline{A}B\overline{B}}{\nu^2}) \\ = \; & Tr_1^m(\frac{B\overline{B}}{B^2+\overline{B}^2}+\frac{B\overline{B}}{\nu}+\frac{A\overline{B}^3+\overline{A}B^3}{\nu^2}). \end{aligned}$$

Therefore, to prove (3.20) has a unique solution in $\mathbb{F}_{2^m}$, we only need to prove

$$Tr_1^m(1+\frac{B\overline{B}}{B^2+\overline{B}^2}+\frac{B\overline{B}}{\nu}+\frac{A\overline{B}^3+\overline{A}B^3}{\nu^2})=1. \tag{3.22}$$

Since $B\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ and $B\neq\overline{B}$, the equation $x^2+(B+\overline{B})x+B\overline{B}=0$ has no solution in $\mathbb{F}_{2^m}$, so we can get $Tr_1^m(\frac{B\overline{B}}{B^2+\overline{B}^2})=1$ from Lemma 2.2. Thus (3.22) is equivalent to

$$Tr_1^m(1+\frac{B\overline{B}}{\nu}+\frac{A\overline{B}^3+\overline{A}B^3}{\nu^2})=0.$$

It is clear that $B\overline{B}=\mu,\nu=1+a^2+a\mu+\mu$, and

$$A\overline{B}^3+\overline{A}B^3=(a\varepsilon+\varepsilon^2)(1+\bar{\varepsilon})^3+(a\bar{\varepsilon}+\bar{\varepsilon}^2)(1+\varepsilon)^3=(1+a)\mu^2,$$

we have

$$\begin{aligned} Tr_1^m(1+\frac{B\overline{B}}{\nu}+\frac{\overline{A}B^3+A\overline{B}^3}{\nu^2}) &= Tr_1^m(1+\frac{\mu}{1+a^2+a\mu+\mu}+\frac{(1+a)\mu^2}{(1+a^2+a\mu+\mu)^2}) \\ &= Tr_1^m(1+\frac{\mu}{(1+a+\mu)^2})=0, \end{aligned}$$

since $Tr_1^m(1+\frac{\mu}{(1+a+\mu)^2})=0$. Thus (3.19) has a unique solution in $\mathbb{F}_{2^m}$ from Lemma 2.3 (ii), which implies that (3.20) has exactly one solution λ in $U\backslash\{1\}$. Moreover, we can plug $\overline{y}=\lambda y$ into (3.14), then we have that $y=\frac{\lambda^2+a\varepsilon\lambda^3+\bar{\varepsilon}\lambda+\bar{\varepsilon}^2}{\lambda^2}$ is the unique solution of (3.14) in $\mathbb{F}_{2^m}$. Therefore, (3.9) has a unique solution in $\mathbb{F}_{2^n}^*$. To summarize, we conclude that (3.9) has at most one solution. The proof is completed. □

Acknowledgement

The author is grateful to the anonymous reviewers and the editor for their detailed comments and suggestions which highly improve the presentation and quality of this paper. This work was supported by the Educational Research Project of Young and Middle-aged Teachers of Fujian Province under Grant JAT200033 and the Talent Fund Project of Fuzhou University under Grant GXRC-20002.

References

[1] Bai T, Xia Y. A new class of permutation trinomials constructed from Niho exponents. Cryptography and Communications 2018; 10 (6): 1023-1036. doi: 10.1007/s12095-017-0263-4

[2] Bartoli D. On a conjecture about a class of permutation trinomials. Finite Fields and Their Applications 2018; 52: 30-50. doi: 10.1016/j.ffa.2018.03.003

[3] Deng H, Zheng D. More classes of permutation polynomials with Niho exponents. Cryptography and Communications 2019; 11 (2): 227-236. doi: 10.1007/s12095-018-0284-7

[4] Ding C, Yuan J. A family of skew hadamard difference sets. Journal of Combinatorial Theory, Series A 2006; 113: 1526-1535. doi: 10.1016/j.jcta.2005.10.006

[5] Dobbertin H, Felke P, Helleseth T, Rosendahl P. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums. IEEE Transactions on Information Theory 2006; 52 (2): 613-627. doi: 10.1109/TIT.2005.862094

[6] Hou X. Permutation polynomials over finite fields – a survey of recent advances. Finite Fields and Their Applications 2015; 32: 82-119. doi: 10.1016/j.ffa.2014.10.001

[7] Hou X. On a class of permutation trinomials in characteristic 2. Cryptography and Communications 2019; 11: 1199-1210. doi: 10.1007/s12095-018-0342-1

[8] Laigle-Chapuy Y. Permutation polynomials and applications to coding theory. Finite Fields and Their Applications 2007; 13: 58-70. doi: 10.1016/j.ffa.2005.08.003

[9] Li N, Helleseth T. Several classes of permutation trinomials from Niho exponents. Cryptography and Communications 2017; 9: 693-705. doi: 10.1007/s12095-016-0210-9

[10] Li N, Hu Q. A conjecture on permutation trinomials over finite fields of characteristic two. Advances in Mathematics of Communications 2019; 13 (3): 505-512. doi: 10.3934/amc.2019031

[11] Li N, Zeng X. A survey on the applications of Niho exponents. Cryptography and Communications 2019; 11 (3): 509-548. doi: 10.1007/s12095-018-0305-6

[12] Lidl R, Niederreiter H. Finite Fields, Encyclopedia of Mathematics and its Applications 20. 2nd ed. Cambridge, UK: Cambridge University Press, 1997.

[13] Liu Q, Sun Y. Several classes of permutation trinomials from Niho exponents over finite fields of characteristic 3. Journal of Algebra and Its Applications 2019; 18 (4): 1950069. doi: 10.1142/S0219498819500695

[14] Ma J, Ge G. A note on permutation polynomials over finite fields. Finite Fields and Their Applications 2017; 48: 261-270. doi: 10.1016/j.ffa.2017.08.003

[15] Mullen GL. Permutation polynomials over finite fields. In: Finite Fields, Coding Theory, and Advances in Communications and Computing. Lecture Notes in Pure and Applied Mathematics 141. New York, USA: Marcel Dekker, 1993, pp. 131-151.

[16] Niho Y. Multi type cross-correlation functions between two maximal linear recursive sequences. PhD, University of Southern California, Los Angeles, USA, 1972.

[17] Schwenk J, Huber K. Public key encryption and digital signatures based on permutation polynomials. Electronic Letters 1998; 34: 759-760. doi: 10.1049/el:19980569

[18] Tu Z, Zeng X. Two classes of permutation trinomials with Niho exponents. Finite Fields and Their Applications 2018; 53: 99-112. doi: 10.1016/j.ffa.2018.05.007

[19] Tu Z, Zeng X, Helleseth T. New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$. Finite Fields and Their Applications 2018; 50: 304-318. doi: 10.1016/j.ffa.2017.11.013

[20] Tu Z, Zeng X, Helleseth T. A class of new permutation quadrinomials. Discrete Mathematics 2018; 341: 3010-3020. doi: 10.1016/j.disc.2018.07.021

[21] Tu Z, Zeng X, Li C, Helleseth T. A class of new permutation trinomials. Finite Fields and Their Applications 2018; 50: 178-195. doi: 10.1016/j.ffa.2017.11.009

[22] Zheng L, Kan H, Peng J. Two classes of permutation trinomials with Niho exponents over finite fields with even characteristic. Finite Fields and Their Applications 2020; 68: 101754. doi: 10.1016/j.ffa.2020.101754

[23] Zheng L, Kan H, Peng J, Tang D. Two classes of permutation trinomials with Niho exponents. Finite Fields and Their Applications 2021; 70: 101790. doi: 10.1016/j.ffa.2020.101790