On a conjecture about a class of permutation quadrinomials

Kangquan Li, Longjiang Qu, Chao Li and Hao Chen

Abstract

Very recently, Tu et al. presented a sufficient condition about (a_1, a_2, a_3), see Theorem 1.1, such that $f(x) = x^{3 \cdot 2^m} + a_1 x^{2^{m+1}+1} + a_2 x^{2^m+2} + a_3 x^3$ is a class of permutation polynomials over $\mathbb{F}_{2^n}$ with $n = 2m$ and m odd. In this present paper, we prove that the sufficient condition is also necessary.

Index Terms

Permutation polynomials, Permutation quadrinomials, Finite Fields

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ be the multiplicative group with the nonzero elements in $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) if the induced mapping $x \to f(x)$ is a permutation of $\mathbb{F}_q$. The study about PPs over finite fields attracts people's interest for many years due to their wide applications in coding theory, cryptography and combinatorial designs.

PPs with few terms attract people's interest due to their simple algebraic form and additional extraordinary properties. Recently, many scholars studied permutation trinomials over $\mathbb{F}_{2^n}$ with $n = 2m$ from Niho exponents of the form

$$f(x) = x^r \left(1 + a_1 x^{s(2^m-1)} + a_2 x^{t(2^m-1)} \right),$$

where $a_1, a_2 \in \mathbb{F}_{2^n}$ and the integers s, t can be viewed as elements of $\mathbb{Z}/(2^m + 1)\mathbb{Z}$, see [1, 2, 5–8, 12, 13], etc. For more relative results, readers can refer in two recent survey papers [9, 15]. However, up to now, there are only four cases of parameters (r, s, t) that have been determined completely:

(1) $(r, s, t) = (1, 1, 2)$ [3];

(2) $(r, s, t) = (1, -1/2, 1/2)$ [12];

(3) $(r, s, t) = (1, -1, 2)$ [1, 5, 13];

(4) $(r, s, t) = (1, 1/4, 3/4)$ [2, 12].

Very recently, in [11], the authors presented a class of permutation quadrinomials as follows. Note that for each element x in $\mathbb{F}_{2^n}$ with $n = 2m$, we define $\overline{x} = x^{2^m}$. Moreover, we use $\mathrm{Tr}_1^m(\cdot)$ to denote the absolute trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, i.e., for any $x \in \mathbb{F}_{2^m}$, $\mathrm{Tr}_1^m(x) = x + x^2 + \cdots + x^{2^{m-1}}$.

Theorem 1.1. *[11] 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

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

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

$$f(x) = \overline{x}^3 + a_1 \overline{x}^2 x + a_2 x^2 \overline{x} + a_3 x^3$$

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

The authors in [11] conjectured that the sufficient condition in Theorem 1.1 is also necessary. In the present paper, we prove that their conjecture is right. Namely,

Theorem 1.2. *Let $n = 2m$. Then the quadrinomial*

$$f(x) = \overline{x}^3 + a_1 \overline{x}^2 x + a_2 x^2 \overline{x} + a_3 x^3$$

is a permutation of $\mathbb{F}_{2^n}$ if and only if m is odd and $(a_1, a_2, a_3) \in \Gamma$, where Γ is defined as in Theorem 1.1.

Firstly, as pointed out in [11], the assumption $a_1 \in \mathbb{F}_{2^m}$ is reasonable since

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

where $\beta \in \mathbb{F}_{2^n}^*$ satisfies $\beta^2 a_1 = 1$ and $a_1(\beta/\overline{\beta}) = \beta^{-1-2^m} \in \mathbb{F}_{2^m}$. Next, if $1 + a_1 + a_2 + a_3 = 0$, then $f(0) = f(1) = 0$ and f is not a permutation. Thus in this paper, we always assume

$$1 + a_1 + a_2 + a_3 \neq 0.$$

In addition, it is clear that $f(x) = x^3 h\left(x^{2^m - 1}\right)$, where $h(x) = x^3 + a_1 x^2 + a_2 x + a_3$. The PPs of the form $x^r h\left(x^{(q-1)/d}\right)$ over $\mathbb{F}_q$ are interesting and have been paid particular attention. There is a connection between the PPs of this type and certain permutations of the subgroup of order d of $\mathbb{F}_q^*$.

Lemma 1.3. *[10, 14, 16] Pick $d, r > 0$ with $d \mid (q - 1)$, and let $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h\left(x^{(q-1)/d}\right)$ permutes $\mathbb{F}_q$ if and only if both*

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

(2) $g(x) = x^r h(x)^{(q-1)/d}$ *permutes* μ_d, *where* $\mu_d = \{x \in \mathbb{F}_q : x^d = 1\}$.

Since $\gcd(3, 2^m - 1) = 1$ if and only if m is odd, together with Lemma 1.3, we know that $f(x)$ is a PP over $\mathbb{F}_{2^n}$ if and only if m is odd and

$$
\begin{aligned}
g(x) &= x^3 h(x)^{2^m - 1} \\
&= \frac{\overline{a}_3 x^3 + \overline{a}_2 x^2 + a_1 x + 1}{x^3 + a_1 x^2 + a_2 x + a_3}
\end{aligned}
$$

permutes $\mu_{2^m + 1}$. Let $\phi(x) = \frac{x + \omega^2}{x + \omega}$ be a bijection from $\mathbb{F}_{2^m}$ to $\mu_{2^m+1} \backslash \{1\}$, where $\omega \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$ and $\omega^2 + \omega + 1 = 0$. Then g permutes $\mu_{2^m + 1}$ if and only if $g(\phi(x))$ is a bijection. This happens if and only if

$$
F(x) = g(\phi(x))|_{\mathbb{F}_{2^m}} : \mathbb{F}_{2^m} \to \mu_{2^m+1} \backslash \{(1 + a_1 + a_2 + a_3)^{2^m - 1}\} \tag{2}
$$

is a bijection. Let

$$
L(x, y) = N\left(\frac{F(x) - F(y)}{x - y} \right) = 0,
$$

where $N\left(\frac{F(x) - F(y)}{x-y} \right)$ denotes the numerator of $\frac{F(x) - F(y)}{x-y}$. Clearly, $F(x)$ is a bijection if and only if $L(x, y) = 0$ has no $\mathbb{F}_{2^m}$-rational points off the line $x = y$.

Our method to show that the sufficient condition in Theorem 1.1 is also necessary is based on the Hasse-Weil bound, which has been applied in the study of PPs, e.g. [1, 5].

Lemma 1.4. *[4, Hasse-Weil bound] Let* $L(x, y)$ *be a polynomial in* $\mathbb{F}_q[x, y]$ *of degree* d *and let* $\#V_{\mathbb{F}_q^2}(L)$ *be the number of zeros of* L. *If* L *has an absolutely irreducible component over* $\mathbb{F}_q$, *then*

$$
\left| \#V_{\mathbb{F}_q^2}(L) - q \right| \le (d-1)(d-2)q^{1/2} + \frac{1}{2}d(d-1)^2 + 1.
$$

In addition, in our proof, some relations obtained in [11] between θ_i for $i = 1, 2, 3, 4$ are also useful.

Lemma 1.5. *[11] For* θ_i *(*$i = 1, 2, 3, 4$*) defined as (1), we have*

1) $\theta_2 \overline{\theta}_2 + \theta_3 \overline{\theta}_3 = \theta_4 (\theta_1 + \theta_4)$ *(note that the relation always holds just from the definition of* θ_i, *without the assumption* $(a_1, a_2, a_3) \in \Gamma$*);*
2) *if* $(a_1, a_2, a_3) \in \Gamma$, *we have* $\theta_2 \theta_3 + \overline{\theta}_2 \overline{\theta}_3 = \frac{\theta_2 \overline{\theta}_2 (\theta_2 + \overline{\theta}_2)}{\theta_1}$;
3) *if* $(a_1, a_2, a_3) \in \Gamma$, *if there exists an element* $\lambda \in \mu_{2^m + 1}$ *such that* $\theta_1 + \theta_2 \overline{\lambda} + \overline{\theta}_2 \lambda = 0$, *then* $\theta_2 \overline{\theta}_2 = \theta_1 \theta_4$.

In the following, we firstly determine the necessary and sufficient conditions about (a_1, a_2, a_3) for $L(x, y)$ to split completely into absolutely irreducible components not defined over $\mathbb{F}_{2^m}$, see Theorem 1.6, whose proof will be given in the next section. For convenience, if L can be factorized as a product of four linear factors, we write $L = (1, 1, 1, 1)$; if L can be factorized as a product of two quadratic absolute irreducible factors, we write $L = (2, 2)$.

Theorem 1.6. *Let* $L(x, y) \neq 0$ *defined as (5) and* $1 + \theta_1 + \theta_2 + \theta_3 \neq 0$. *Then the factorizations of* $L(x, y)$ *into absolute irreducible components not defined over* $\mathbb{F}_{2^m}$ *are characterized as follows:*

(a) $L = (1, 1, 1, 1)$ *if and only if*

$$\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_2^2 = \theta_1\overline{\theta}_3, \theta_4^2 = \theta_1^2 + \theta_3\overline{\theta}_3, \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1;$$

(b) $L = (2, 2)$ *if and only if*

$$\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_2^2 = \theta_1\overline{\theta}_3, \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1;$$

(c) $L = (1, 1)$ *if and only if*

$$\theta_1 = \theta_2 + \overline{\theta}_2 \neq 0, \theta_3 = \theta_2 + \gamma, \theta_4 = \gamma + \theta_2 + \overline{\theta}_2 \quad and \quad \gamma = \frac{\theta_2^2 + \overline{\theta}_2^2 + \theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2}.$$

In the last of this section, we give the proof of Theorem 1.2.

Proof. Firstly, according to the item (1) of Lemma 1.3, we know that if f is a PP, then m is odd since $\gcd(3, 2^m - 1) = 1$ if and only if m is odd. Let

$$\Gamma_1 := \{(a_1, a_2, a_3) \in \Gamma : \theta_1 \neq \theta_3 + \overline{\theta}_3\} \quad \text{and} \quad \Gamma_2 := \{(a_1, a_2, a_3) \in \Gamma : \theta_1 = \theta_3 + \overline{\theta}_3\}.$$

Then, it is clear that the condition of (a) in Theorem 1.6 belongs to Γ_1 and that of (b) is indeed Γ_1. In the following, we show that the condition of (c) in Theorem 1.6 is Γ_2. Recall that

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

Then for $(a_1, a_2, a_3) \in \Gamma_2$, i.e., $\theta_1 = \theta_3 + \overline{\theta}_3$, we have $\theta_2^2 = \theta_1\overline{\theta}_3 = (\theta_3 + \overline{\theta}_3)\overline{\theta}_3$ and thus $\overline{\theta}_2^2 = (\theta_3 + \overline{\theta}_3)\theta_3$. Adding the above two equations, we obtain $\theta_2 + \overline{\theta}_2 = \theta_3 + \overline{\theta}_3$. Let $\gamma = \theta_2 + \theta_3$. Then $\gamma \in \mathbb{F}_{2^m}$. In addition, from Lemma 1.5, we have $\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 = \frac{\theta_2\overline{\theta}_2(\theta_2 + \overline{\theta}_2)}{\theta_1}$ and thus $\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 = \theta_2\overline{\theta}_2$. Plugging $\theta_3 = \theta_2 + \gamma$ and $\overline{\theta}_3 = \overline{\theta}_2 + \gamma$ into the above equation, we get

$$\gamma = \frac{\theta_2^2 + \overline{\theta}_2^2 + \theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2}.$$

Furthermore, from Lemma 1.5, we have $\theta_2\overline{\theta}_2 = \theta_1\theta_4$. Thus

$$\theta_4 = \frac{\theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2} = \gamma + \theta_2 + \overline{\theta}_2.$$

Therefore, the condition of (c) in Theorem 1.6 is indeed Γ_2.

All in all, L can split completely into absolute irreducible components not defined over $\mathbb{F}_{2^m}$ if and only if $(a_1, a_2, a_3) \in \Gamma$. When $(a_1, a_2, a_3) \notin \Gamma$, L with degree 4 has an absolutely irreducible factor over $\mathbb{F}_{2^m}$ and thus according to Lemma 1.4, we have

$$\begin{aligned}
\#V_{\mathbb{F}_{2^m}}(L) &\geq 2^m - (d-1)(d-2)2^{m/2} - \frac{1}{2}d(d-1)^2 - 1 \\
&= 2^m - 6 \cdot 2^{m/2} - 19.
\end{aligned}$$

Let $\lambda \in \mathbb{R}$ denote the larger solution of $x^2 - 6x - 21 = 0$. Then $\lambda < 9$ and thus $\#V_{\mathbb{F}_{2^m}^2}(L) > 2$ when $m \geq 4$. By (5), $L(x,x) = \ell_{22}x^4 + \ell_{11}x^2 + \ell_{00}$, which has at most two zeros in $\mathbb{F}_{2^m}$. Hence $L(x,y)$ has at least a zero $(x,y) \in \mathbb{F}_{2^m}^2$ with $x \neq y$ when $m \geq 4$. Consequently, when $(a_1, a_2, a_3) \notin \Gamma$ with $m \geq 4$, f is not a permutation over $\mathbb{F}_{2^n}$. For the case $m < 4$, the same conclusion can be obtained by the MAGMA.

Together with the sufficient proof in [11], the proof of Theorem 1.2 has been finished completely. $\square$

Therefore, in the following we only suffice to provide the proof of Theorem 1.6, which will be given in the next section. Through the paper, the algebraic closure of $\mathbb{F}_{2^m}$ is denoted by $\overline{\mathbb{F}}_{2^m}$.

2. The proof of Theorem 1.6

In this section, we prove Theorem 1.6. After direct computation, we have

$$
\begin{aligned}
F(x) &= g\left(\phi(x)\right) \\
&= \frac{\overline{a}_3 \left(\frac{x+\omega^2}{x+\omega}\right)^3 + \overline{a}_2 \left(\frac{x+\omega^2}{x+\omega}\right)^2 + a_1 \left(\frac{x+\omega^2}{x+\omega}\right) + 1}{\left(\frac{x+\omega^2}{x+\omega}\right)^3 + a_1 \left(\frac{x+\omega^2}{x+\omega}\right)^2 + a_2 \left(\frac{x+\omega^2}{x+\omega}\right) + a_3} \\
&= \frac{\epsilon_1 x^3 + \epsilon_2 x^2 + \epsilon_3 x + \epsilon_4}{\tau_1 x^3 + \tau_2 x^2 + \tau_3 x + \tau_4},
\end{aligned}
$$

where

$$
\begin{cases}
\epsilon_1 = a_1 + \overline{a}_2 + \overline{a}_3 + 1 \\
\epsilon_2 = \omega^2 a_1 + \omega \overline{a}_2 + \omega^2 \overline{a}_3 + \omega \\
\epsilon_3 = \omega^2 a_1 + \omega \overline{a}_2 + \omega \overline{a}_3 + \omega^2 \\
\epsilon_4 = \omega a_1 + \omega^2 \overline{a}_2 + \overline{a}_3 + 1,
\end{cases}
$$

and

$$
\begin{cases}
\tau_1 = a_1 + a_2 + a_3 + 1 \\
\tau_2 = \omega a_1 + \omega^2 a_2 + \omega a_3 + \omega^2 \\
\tau_3 = \omega a_1 + \omega^2 a_2 + \omega^2 a_3 + \omega \\
\tau_4 = \omega^2 a_1 + \omega a_2 + a_3 + 1.
\end{cases}
$$

Therefore, we have

$$
L(x,y) = N\left(\frac{F(x) - F(y)}{x - y}\right) = \ell_{22}x^2y^2 + \ell_{21}x^2y + \ell_{12}xy^2 + \ell_{20}x^2 + \ell_{11}xy + \ell_{02}y^2 + \ell_{10}x + \ell_{01}y + \ell_{00},
$$

$$(5)$$

where

$$
\begin{aligned}
\ell_{22} &= a_1^2 + a_1 a_3 + a_1 \overline{a}_3 + a_2 \overline{a}_2 + a_2 + a_3 \overline{a}_3 + \overline{a}_2 + 1 \\
&= \theta_1 + \theta_3 + \overline{\theta}_3,
\end{aligned}
$$

$$\ell_{21} = a_1^2 + a_2\overline{a}_2 + a_2\overline{a}_3 + a_3\overline{a}_2 + a_3\overline{a}_3 + 1$$
$$= \theta_1 + \theta_2 + \overline{\theta}_2,$$

$$\ell_{20} = a_1^2 + \omega^2 a_1 a_3 + \omega a_1\overline{a}_3 + a_1 + a_2\overline{a}_2 + \omega^2 a_2\overline{a}_3 + \omega^2 a_2 + \omega a_3\overline{a}_2 + \omega\overline{a}_2$$
$$= \theta_4 + \omega\theta_3 + \omega^2\overline{\theta}_3 + \omega\theta_2 + \omega^2\overline{\theta}_2,$$

$$\ell_{11} = a_1^2 + a_2\overline{a}_2 + a_3\overline{a}_3 + 1 = \theta_1,$$

$$\ell_{10} = a_1^2 + a_1 + a_2\overline{a}_2 + \omega a_2\overline{a}_3 + \omega^2 a_3\overline{a}_2 + a_3\overline{a}_3 + 1$$
$$= \theta_1 + \omega^2\theta_2 + \omega\overline{\theta}_2,$$

$$\ell_{00} = a_1^2 + \omega a_1 a_3 + \omega^2 a_1\overline{a}_3 + a_2\overline{a}_2 + \omega a_2 + a_3\overline{a}_3 + \omega^2\overline{a}_2 + 1$$
$$= \theta_1 + \omega^2\theta_3 + \omega\overline{\theta}_3,$$

and $\ell_{12} = \ell_{21}$, $\ell_{02} = \ell_{20}$, $\ell_{01} = \ell_{10}$, θ_i for $i = 1, 2, 3, 4$ are defined as (1).

In the following, we determine the necessary and sufficient conditions for $L(x, y)$ to split completely into absolutely irreducible components not defined over $\mathbb{F}_{2^m}$. The factorization can be divided into two cases: $\ell_{22} \neq 0$ and $\ell_{22} = 0$.

Case 1: $\ell_{22} \neq 0$. Namely, $\theta_1 \neq \theta_3 + \overline{\theta}_3$.

In the case, $\deg L = 4$ and it is clear that the morphisms $(x, y) \to (y, x)$ and $(x, y) \to (\overline{x}, \overline{y})$ fix $L = 0$ and therefore they act on its components, which means that if $x + a$ with $a \in \overline{\mathbb{F}}_{2^m} \backslash \mathbb{F}_{2^m}$ is a component of L, then $y + a$ and $x + \overline{a}$ are also the components of L directly. Moreover, if $L(x, y)$ can split completely into absolute irreducible components not defined over $\mathbb{F}_{2^m}$, then the only possibilities are $(1, 1, 1, 1)$ and $(2, 2)$. The reason is as follows. If $x + a$ with $a \in \overline{\mathbb{F}}_{2^m} \backslash \mathbb{F}_{2^m}$ is a component not defined over $\mathbb{F}_{2^m}$ of L, then $y + a$, $x + \overline{a}$ and $y + \overline{a}$ are also the components of L, i.e., $L = (1, 1, 1, 1)$. If L has a component not defined over $\mathbb{F}_{2^m}$ with degree 2, denoted by L_1, then $\overline{L}_1$ with degree 2 is also a component of L, where $\overline{L}_1$ denotes the polynomial from raising all the coefficients of L_1 into their 2^m-th power respectively. Obviously, $L_1 \neq \overline{L}_1$. Thus, $L = (2, 2)$, i.e., L can not be $(2, 1, 1)$. In addition, the impossibility of $L = (3, 1)$ is trivial.

Subcase 1.1: $L = (1, 1, 1, 1)$. In the subcase, there must exist some $a \in \overline{\mathbb{F}}_{2^m} \backslash \mathbb{F}_{2^m}$ such that

$$L = \ell_{22}(x + a)(x + \overline{a})(y + a)(y + \overline{a})$$
$$= \ell_{22}\left(x^2 y^2 + (a + \overline{a})x^2 y + a\overline{a}x^2 + (a + \overline{a})xy^2 + (a^2 + \overline{a}^2)xy\right.$$
$$\left. + (a^2\overline{a} + a\overline{a}^2)x + a\overline{a}y^2 + (a^2\overline{a} + a\overline{a}^2)y + a^2\overline{a}^2\right).$$

Comparing the coefficients of the above expression and (5), we have

$$\begin{cases} \ell_{21} = (a + \overline{a})\ell_{22} & \text{(6.1)} \\ \ell_{20} = a\overline{a}\ell_{22} & \text{(6.2)} \\ \ell_{11} = (a^2 + \overline{a}^2)\ell_{22} & \text{(6.3)} \\ \ell_{10} = (a^2\overline{a} + a\overline{a}^2)\ell_{22} & \text{(6.4)} \\ \ell_{00} = a^2\overline{a}^2\ell_{22}. & \text{(6.5)} \end{cases}$$

Computing $(6.1)^2 + \ell_{22} \times (6.3)$, $(6.2)^2 + \ell_{22} \times (6.5)$ and $(6.1) \times (6.2) + \ell_{22} \times (6.4)$ respectively, we obtain

$$\begin{cases} \ell_{21}^2 = \ell_{11}\ell_{22} \\ \ell_{20}^2 = \ell_{00}\ell_{22} \\ \ell_{21}\ell_{20} = \ell_{10}\ell_{22}, \end{cases}$$

namely,

$$\begin{cases} \theta_1\theta_3 + \theta_1\overline{\theta}_3 + \theta_2^2 + \overline{\theta}_2^2 = 0 & \text{(8.1)} \\ \theta_1^2 + \omega\theta_1\theta_3 + \omega^2\theta_1\overline{\theta}_3 + \omega^2\theta_2^2 + \omega\overline{\theta}_2^2 + \theta_3\overline{\theta}_3 + \theta_4^2 = 0 & \text{(8.2)} \\ \theta_1^2 + \theta_1\theta_2 + \omega^2\theta_1\theta_3 + \theta_1\theta_4 + \theta_1\overline{\theta}_2 + \omega\theta_1\overline{\theta}_3 + \omega\theta_2^2 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_2\overline{\theta}_2 + \theta_4\overline{\theta}_2 + \omega^2\overline{\theta}_2^2 + \overline{\theta}_2\overline{\theta}_3 = 0. & \text{(8.3)} \end{cases}$$

Computing $(8.2) \times (\theta_1 + \theta_2 + \overline{\theta}_2)^2 + (8.3)^2$, we get

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

Since $\ell_{22} = \theta_1 + \theta_3 + \overline{\theta}_3 \neq 0$ in the case, we have

$$\omega\theta_1^2\theta_3 + \omega^2\theta_1^2\overline{\theta}_3 + \omega^2\theta_1\theta_2^2 + \omega\theta_1\overline{\theta}_2^2 + \theta_2^2\theta_3 + \overline{\theta}_2^2\overline{\theta}_3 = 0. \tag{9}$$

Moreover, from Eq. (8.1), we can assume that $\theta_2^2 + \theta_1\overline{\theta}_3 = \gamma \in \mathbb{F}_{2^m}$. Then $\theta_2^2 = \gamma + \theta_1\overline{\theta}_3$ and $\overline{\theta}_2^2 = \gamma + \theta_1\theta_3$. Plugging them into Eq. (9), we have

$$\begin{aligned} & \omega\theta_1^2\theta_3 + \omega^2\theta_1^2\overline{\theta}_3 + \omega^2\theta_1\theta_2^2 + \omega\theta_1\overline{\theta}_2^2 + \theta_2^2\theta_3 + \overline{\theta}_2^2\overline{\theta}_3 \\ = & \omega\theta_1^2\theta_3 + \omega^2\theta_1^2\overline{\theta}_3 + \omega^2\theta_1\left(\gamma + \theta_1\overline{\theta}_3\right) + \omega\theta_1\left(\gamma + \theta_1\theta_3\right) + \left(\gamma + \theta_1\overline{\theta}_3\right)\theta_3 + \left(\gamma + \theta_1\theta_3\right)\overline{\theta}_3 \\ = & \gamma(\theta_1 + \theta_3 + \overline{\theta}_3) = 0, \end{aligned}$$

which means $\gamma = \theta_2^2 + \theta_1\overline{\theta}_3 = 0$, also thanks to $\ell_{22} = \theta_1 + \theta_3 + \overline{\theta}_3 \neq 0$ in the case. Furthermore, $a + \overline{a} = \frac{\ell_{21}}{\ell_{22}}$ and $a\overline{a} = \frac{\ell_{20}}{\ell_{22}}$ and thus $a, \overline{a}$ are solutions of

$$x^2 + \frac{\ell_{21}}{\ell_{22}}x + \frac{\ell_{20}}{\ell_{22}} = 0,$$

which does not have solutions in $\mathbb{F}_{2^m}$ if and only if

$$\ell_{21}^2 = \theta_1^2 + \theta_2^2 + \overline{\theta}_2^2 = \theta_1(\theta_1 + \theta_3 + \overline{\theta}_3) \neq 0,$$

i.e., $\theta_1 \neq 0$ and $\mathrm{Tr}_1^m\left(\frac{\ell_{20}}{\ell_{22}} \cdot \frac{\ell_{22}^2}{\ell_{21}^2}\right) = \mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right) = 1$. Moreover,

$$\begin{aligned}
&\mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{(\theta_1 + \theta_3 + \overline{\theta}_3)(\theta_4 + \omega\theta_3 + \omega^2\overline{\theta}_3 + \omega\theta_2 + \omega^2\overline{\theta}_2)}{\theta_1^2 + \theta_2^2 + \overline{\theta}_2^2}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{(\theta_1 + \theta_3 + \overline{\theta}_3)(\theta_4 + \omega\theta_3 + \omega^2\overline{\theta}_3 + \omega\theta_2 + \omega^2\overline{\theta}_2)}{\theta_1^2 + \theta_1\theta_3 + \theta_1\overline{\theta}_3}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{\theta_4 + \omega\theta_3 + \omega^2\overline{\theta}_3 + \omega\theta_2 + \omega^2\overline{\theta}_2}{\theta_1}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right)
\end{aligned}$$

and thus $\mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1$. Furthermore, when $\theta_2^2 = \theta_1\overline{\theta}_3$, it is easy to show that Eq. (8.2) and Eq. (8.3) holds if and only if $\theta_4^2 = \theta_1^2 + \theta_3\overline{\theta}_3$. Thus, $L(x,y)$ can split completely into absolute irreducible components not defined over $\mathbb{F}_{2^m}$ with $(1,1,1,1)$ if and only if

$$\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_2^2 = \theta_1\overline{\theta}_3, \theta_4^2 = \theta_1^2 + \theta_3\overline{\theta}_3, \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1.$$

Subcase 1.2: $L = (2,2)$. In the subcase, we firstly consider the possibilities about the factorization of L. (i) If $x^2 + ay^2 + bxy + cx + dy + e$ is a component of L, then clearly, $y^2 + ax^2 + bxy + cy + dx + e$ is the other component of L. Since the coefficients of x^4 and x^3y in L are 0, we have $a = b = 0$. (ii) If $xy + ax + ay + b$ is a component of L, then $xy + \overline{a}x + \overline{a}y + \overline{b}$ is the other component of L. (iii) If $xy + ax + by + c$ with $b \neq a$ is a component of L, then $xy + ay + bx + c$ is the other component of L. Moreover, $xy + \overline{a}x + \overline{b}y + \overline{c}$ is also a component of L and thus $xy + \overline{a}x + \overline{b}y + \overline{c} = xy + ay + bx + c$. Furthermore, we have $b = \overline{a}$ and $c \in \mathbb{F}_{2^m}$.

Hence there are three possibilities about the factorization of L:

(i)
$$L = \ell_{22}(x^2 + ax + by + c)(y^2 + ay + bx + c),$$

(ii)
$$L = \ell_{22}(xy + ax + ay + b)(xy + \overline{a}x + \overline{a}y + \overline{b}),$$

(iii)
$$L = \ell_{22}(xy + ax + \overline{a}y + b)(xy + \overline{a}x + ay + b).$$

As for (i), after comparing the coefficients (mainly x^3 and y^3) of the hypothetic expression of L and (5),

we obtain $b = 0$ directly and thus the possibility becomes the Subcase 1.1.

As for (ii), there exist some $a, b \in \overline{\mathbb{F}}_{2^m}$ such that

$$
\begin{aligned}
L &= \ell_{22}(xy + ax + ay + b)(xy + \overline{a}x + \overline{a}y + \overline{b}) \\
&= \ell_{22}\left(x^2y^2 + (\overline{a} + a)x^2y + (\overline{a} + a)xy^2 + a\overline{a}x^2 + (\overline{b} + b)xy \right. \\
&\quad \left. + a\overline{a}y^2 + (a\overline{b} + \overline{a}b)x + (a\overline{b} + \overline{a}b)y + b\overline{b}\right).
\end{aligned}
$$

Comparing the coefficients of the above expression and (5), we have

$$
\begin{cases}
\ell_{21} = (a + \overline{a})\ell_{22} & (10.1) \\
\ell_{20} = a\overline{a}\ell_{22} & (10.2) \\
\ell_{11} = (b + \overline{b})\ell_{22} & (10.3) \\
\ell_{10} = (a\overline{b} + \overline{a}b)\ell_{22} & (10.4) \\
\ell_{00} = b\overline{b}\ell_{22}. & (10.5)
\end{cases}
$$

When $\ell_{21} \neq 0$ and $\ell_{11} \neq 0$, i.e., $a, b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$, from (10.1) and (10.2), we know that a and $\overline{a}$ are solutions of $x^2 + \frac{\ell_{21}}{\ell_{22}}x + \frac{\ell_{20}}{\ell_{22}} = 0$, which does not have solutions in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right) = 1$. Thus we can assume that $\frac{\ell_{20}\ell_{22}}{\ell_{21}^2} = 1 + \gamma + \gamma^2$, where $\gamma \in \mathbb{F}_{2^m}$ and in the case, we have

$$
a = \frac{\ell_{21}}{\ell_{22}}(\omega + \gamma) \quad \text{and} \quad \overline{a} = \frac{\ell_{21}}{\ell_{22}}(\omega^2 + \gamma).
$$

Also, the similar discussion about b and $\overline{b}$ holds. We have $\mathrm{Tr}_1^m\left(\frac{\ell_{00}\ell_{22}}{\ell_{11}^2}\right) = 1$ and assume that $\frac{\ell_{00}\ell_{22}}{\ell_{11}^2} = 1 + \eta + \eta^2$, where $\eta \in \mathbb{F}_{2^m}$. Moreover,

$$
b = \frac{\ell_{11}}{\ell_{22}}(\omega + \eta) \quad \text{and} \quad \overline{b} = \frac{\ell_{11}}{\ell_{22}}(\omega^2 + \eta).
$$

Furthermore, together with (10.4) and the expressions of $a, \overline{a}, b, \overline{b}$, we obtain

$$
\frac{\ell_{10}\ell_{22}}{\ell_{21}\ell_{11}} = \gamma + \eta.
$$

After direct computing, we get

$$
\frac{\ell_{00}\ell_{22}}{\ell_{11}^2} + \frac{\ell_{20}\ell_{22}}{\ell_{21}^2} = \frac{\ell_{10}\ell_{22}}{\ell_{21}\ell_{11}} + \frac{\ell_{10}^2\ell_{22}^2}{\ell_{21}^2\ell_{11}^2},
$$

i.e.,

$$
\ell_{00}\ell_{21}^2 + \ell_{20}\ell_{11}^2 + \ell_{10}\ell_{21}\ell_{11} + \ell_{10}^2\ell_{22} = 0.
$$

Plugging the expressions of ℓ_{ij} for $0 \leq i, j \leq 2$ into the above equation, we have

$$
\theta_1^3 + \theta_1^2\theta_4 + \theta_1\theta_2\overline{\theta}_2 + \theta_2^2\theta_3 + \overline{\theta}_2^2\theta_3 = 0,
$$

i.e.,

$$\theta_4 = \frac{\theta_1^3 + \theta_1\theta_2\overline{\theta}_2 + \theta_2^2\theta_3 + \overline{\theta}_2^2\overline{\theta}_3}{\theta_1^2}. \tag{11}$$

In addition, from $\mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right) = 1$, we have

$$\mathrm{Tr}_1^m\left(\frac{(\theta_1 + \theta_3 + \overline{\theta}_3)(\theta_4 + \omega\theta_3 + \omega^2\overline{\theta}_3 + \omega\theta_2 + \omega^2\overline{\theta}_2)}{\theta_1^2 + \theta_2^2 + \overline{\theta}_2^2}\right) = 1. \tag{12}$$

Using the following relation,

$$\mathrm{Tr}_1^m\left(\frac{\omega\theta_3^2 + \omega^2\overline{\theta}_3^2}{\theta_1^2 + \theta_2^2 + \overline{\theta}_2^2}\right) = \mathrm{Tr}_1^m\left(\frac{(\omega^2\theta_3 + \omega\overline{\theta}_3)(\theta_1 + \theta_2 + \overline{\theta}_2)}{\theta_1^2 + \theta_2^2 + \overline{\theta}_2^2}\right),$$

Eq. (12) can be simplified as

$$\mathrm{Tr}_1^m\left(\frac{\omega\theta_1\theta_2 + \omega^2\theta_1\overline{\theta}_2 + \theta_1\theta_3 + \theta_1\overline{\theta}_3 + \theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3 + \theta_3\overline{\theta}_3 + \theta_4(\theta_1 + \theta_3 + \overline{\theta}_3)}{\theta_1^2 + \theta_2^2 + \overline{\theta}_2^2}\right) = 1 \tag{13}$$

Next plugging Eq. (11) into Eq. (13) and simplifying, we obtain

$$\mathrm{Tr}_1^m\left(\frac{\Delta}{\theta_1^2\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2}\right) = 1, \tag{14}$$

where

$$\begin{aligned}
\Delta &= \theta_1^4 + \omega\theta_1^3\theta_2 + \omega^2\theta_1^3\overline{\theta}_2 + \theta_1^2\theta_2\theta_3 + \theta_1^2\theta_2\overline{\theta}_2 + \theta_1^2\theta_3\overline{\theta}_3 + \theta_1^2\overline{\theta}_2\overline{\theta}_3 + \theta_1\theta_2^2\theta_3 \\
&\quad + \theta_1\theta_2\overline{\theta}_2\theta_3 + \theta_1\theta_2\overline{\theta}_2\overline{\theta}_3 + \theta_1\overline{\theta}_2^2\overline{\theta}_3 + \theta_2^2\theta_3^2 + \overline{\theta}_2^2\overline{\theta}_3^2 + \overline{\theta}_2^2\theta_3\overline{\theta}_3 + \theta_2^2\theta_3\overline{\theta}_3.
\end{aligned}$$

Also, using the following relation,

$$\mathrm{Tr}_1^m\left(\frac{\theta_2^2\theta_3^2 + \overline{\theta}_2^2\overline{\theta}_3^2}{\theta_1^2\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2}\right) = \mathrm{Tr}_1^m\left(\frac{\left(\theta_2\theta_3 + \overline{\theta}_2\overline{\theta}_3\right)\theta_1\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)}{\theta_1^2\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2}\right),$$

Eq. (14) becomes

$$\begin{aligned}
1 &= \mathrm{Tr}_1^m\left(\frac{\theta_1^4 + \omega\theta_1^3\theta_2 + \omega^2\theta_1^3\overline{\theta}_2 + \theta_1^2\theta_2\overline{\theta}_2 + \theta_1^2\theta_3\overline{\theta}_3 + \overline{\theta}_2^2\theta_3\overline{\theta}_3 + \theta_2^2\theta_3\overline{\theta}_3}{\theta_1^2\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{\theta_1^2 + \omega\theta_1\theta_2 + \omega^2\theta_1\overline{\theta}_2 + \theta_2\overline{\theta}_2}{\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2}\right) + \mathrm{Tr}_1^m\left(\frac{\theta_3\overline{\theta}_3}{\theta_1^2}\right).
\end{aligned}$$

In addition,

$$
\begin{aligned}
& \mathrm{Tr}_1^m \left(\frac{\theta_1^2 + \omega\theta_1\theta_2 + \omega^2\theta_1\overline{\theta}_2 + \theta_2\overline{\theta}_2}{\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2} \right) \\
= \ & \mathrm{Tr}_1^m \left(\frac{\omega^2\theta_1^2 + \overline{\theta}_2^2 + \omega\theta_1(\theta_1 + \theta_2 + \overline{\theta}_2) + \overline{\theta}_2(\theta_1 + \theta_2 + \overline{\theta}_2)}{\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2} \right) \\
= \ & \mathrm{Tr}_1^m \left(\frac{\omega^2\theta_1^2 + \overline{\theta}_2^2}{\left(\theta_1 + \theta_2 + \overline{\theta}_2\right)^2} + \frac{\omega^2\theta_1 + \overline{\theta}_2}{\theta_1 + \theta_2 + \overline{\theta}_2} \right) \\
= \ & 1
\end{aligned}
$$

since $\omega^2\theta_1 + \overline{\theta}_2 \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$ (if $\omega^2\theta_1 + \overline{\theta}_2 \in \mathbb{F}_{2^m}$, $\theta_1 + \theta_2 + \overline{\theta}_2 = 0$, which contradicts our assumption). Thus we have

$$
\mathrm{Tr}_1^m \left(\frac{\theta_3\overline{\theta}_3}{\theta_1^2} \right) = 0. \tag{15}
$$

Moreover, from Lemma 1.5, we get

$$
\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 = \theta_4\left(\theta_1 + \theta_4\right).
$$

Plugging Eq. (11) into the above equation, we obtain

$$
\theta_1^4\theta_3\overline{\theta}_3 + \theta_1^3\theta_2^2\theta_3 + \theta_1^3\overline{\theta}_2^2\overline{\theta}_3 + \theta_1^2\theta_2^2\overline{\theta}_2^2 + \theta_2^4\theta_3^2 + \overline{\theta}_2^4\overline{\theta}_3^2 = 0. \tag{16}
$$

Assume $\theta_2^2 = \theta_1\overline{\theta}_3 + \epsilon$, where $\epsilon \neq 0$. Then $\overline{\theta}_2^2 = \theta_1\theta_3 + \overline{\epsilon}$. Plugging the expressions of θ_2 and $\overline{\theta}_2$ into Eq. (16) directly and simplifying, we get

$$
\theta_1^2 = \frac{\epsilon}{\overline{\epsilon}}\theta_3^2 + \frac{\overline{\epsilon}}{\epsilon}\overline{\theta}_3^2. \tag{17}
$$

Plugging Eq. (17) into Eq. (15), we obtain

$$
\begin{aligned}
0 & = \mathrm{Tr}_1^m \left(\frac{\epsilon\theta_3\overline{\epsilon}\overline{\theta}_3}{\epsilon^2\theta_3^2 + \overline{\epsilon}^2\overline{\theta}_3^2} \right) \\
& = \mathrm{Tr}_1^m \left(\frac{t}{t^2 + 1} \right) \\
& = \mathrm{Tr}_1^m \left(\frac{1}{t + 1} + \frac{1}{t^2 + 1} \right) \\
& = 1,
\end{aligned}
$$

where $t = \frac{\overline{\epsilon}\overline{\theta}_3}{\epsilon\theta_3} \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. Conflict! Therefore, $\epsilon = 0$, i.e.,

$$
\theta_2^2 = \theta_1\overline{\theta}_3.
$$

Furthermore, when $\theta_2^2 = \theta_1\overline{\theta}_3$, from Eq. (11), we get $\theta_4^2 = \theta_1^2 + \theta_3\overline{\theta}_3$ directly. In addition, we have $\mathrm{Tr}_1^m \left(\frac{\theta_4}{\theta_1} \right) = 1$ according to $\mathrm{Tr}_1^m \left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2} \right) = 1$, see Subcase 1.1. Moreover, $\mathrm{Tr}_1^m \left(\frac{\ell_{00}\ell_{22}}{\ell_{11}^2} \right) = 1$ is also

equivalent to $\mathrm{Tr}_1^m \left(\frac{\theta_4}{\theta_1} \right) = 1$ since

$$
\begin{aligned}
&\mathrm{Tr}_1^m \left(\frac{(\theta_1 + \theta_3 + \overline{\theta}_3)(\theta_1 + \omega^2 \theta_3 + \omega \overline{\theta}_3)}{\theta_1^2} \right) \\
=\ & \mathrm{Tr}_1^m \left(\frac{\theta_1^2 + \omega \theta_1 \theta_3 + \omega^2 \theta_1 \overline{\theta}_3 + \theta_3 \overline{\theta}_3}{\theta_1^2} + \frac{\omega^2 \theta_3^2 + \omega \overline{\theta}_3^2}{\theta_1^2} \right) \\
=\ & \mathrm{Tr}_1^m \left(\frac{\theta_1^2 + \omega \theta_1 \theta_3 + \omega^2 \theta_1 \overline{\theta}_3 + \theta_3 \overline{\theta}_3}{\theta_1^2} + \frac{\theta_1 (\omega \theta_3 + \omega \overline{\theta}_3)}{\theta_1^2} \right) \\
=\ & \mathrm{Tr}_1^m \left(\frac{\theta_1^2 + \theta_3 \overline{\theta}_3}{\theta_1^2} \right) = \mathrm{Tr}_1^m \left(\frac{\theta_4}{\theta_1} \right) = 1.
\end{aligned}
$$

Thus there exist some $a, b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$, such that $L(x, y) = \ell_{22}(xy + ax + ay + b)(xy + \overline{a}x + \overline{a}y + \overline{b})$ if and only if

$$
\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_1 \neq \theta_2 + \overline{\theta}_2, \theta_2^2 = \theta_1 \overline{\theta}_3, \theta_4^2 = \theta_1^2 + \theta_3 \overline{\theta}_3, \mathrm{Tr}_1^m \left(\frac{\theta_4}{\theta_1} \right) = 1.
$$

When $\ell_{11} = \theta_1 \neq 0$ and $\ell_{21} = \theta_1 + \theta_2 + \overline{\theta}_2 = 0$, we have $\theta_2 \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^m}$, $a = \overline{a}$ and $a^2 = \frac{\ell_{20}}{\ell_{22}}$. From (10.3) and (10.5), we have $\mathrm{Tr}_1^m \left(\frac{\ell_{00} \ell_{22}}{\ell_{11}^2} \right) = 1$, i.e.,

$$
\mathrm{Tr}_1^m \left(\frac{\theta_1^2 + \omega \theta_1 \theta_3 + \omega^2 \theta_1 \overline{\theta}_3 + \omega^2 \theta_3^2 + \theta_3 \overline{\theta}_3 + \omega \overline{\theta}_3^2}{\theta_1^2} \right) = 1.
$$

Moreover, it is clear that

$$
\begin{aligned}
&\mathrm{Tr}_1^m \left(\frac{\omega \theta_1 \theta_3 + \omega^2 \theta_1 \overline{\theta}_3 + \omega^2 \theta_3^2 + \omega \overline{\theta}_3^2}{\theta_1^2} \right) \\
=\ & \mathrm{Tr}_1^m \left(\frac{\omega \theta_3 + \omega^2 \overline{\theta}_3}{\theta_1} + \frac{(\omega \theta_3 + \omega^2 \overline{\theta}_3)^2}{\theta_1^2} \right) \\
=\ & 0,
\end{aligned}
$$

and thus

$$
\mathrm{Tr}_1^m \left(\frac{\theta_3 \overline{\theta}_3}{\theta_2^2 + \overline{\theta}_2^2} \right) = \mathrm{Tr}_1^m \left(\frac{\theta_3 \overline{\theta}_3}{\theta_1^2} \right) = 0.
$$

In addition, from Lemma 1.5, we get

$$
\theta_2 \overline{\theta}_2 + \theta_3 \overline{\theta}_3 = \theta_4 \left(\theta_1 + \theta_4 \right).
$$

Plugging $\theta_1 = \theta_2 + \overline{\theta}_2$ into the above equation, we have

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

Therefore,

$$
\mathrm{Tr}_1^m\left(\frac{\theta_3\overline{\theta}_3}{\theta_2^2+\overline{\theta}_2^2}\right)
$$

$$
= \mathrm{Tr}_1^m\left(\frac{\theta_4(\theta_2+\overline{\theta}_2)+\theta_4^2+\theta_2\overline{\theta}_2}{\theta_2^2+\overline{\theta}_2^2}\right)
$$

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

$$
= \mathrm{Tr}_1^m\left(\frac{1}{t+1}+\frac{1}{t^2+1}\right)=1,
$$

where $t=\frac{\overline{\theta}_2}{\theta_2}\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$. Conflict! Hence, there does not exist any $a\in\mathbb{F}_{2^m},b\in\mathbb{F}_{2^n}$ such that $L(x,y)=\ell_{22}(xy+ax+ay+b)(xy+\overline{a}x+\overline{a}y+\overline{b})$.

When $\ell_{21}=\theta_1+\theta_2+\overline{\theta}_2\neq 0$ and $\ell_{11}=\theta_1=0$, $b=\overline{b}$ and $b^2=\frac{\ell_{00}}{\ell_{22}}$. From (10.1) and (10.2), we have $\mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right)=1$. Moreover, computing $(10.4)^2\times\ell_{22}+(10.5)\times(10.1)^2$, we get

$$
\ell_{10}^2\ell_{22}=\ell_{00}\ell_{21}^2,
$$

i.e.,

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

Thus $\theta_2^2\theta_3\in\mathbb{F}_{2^m}$, denoted by $\epsilon\in\mathbb{F}_{2^m}$. In addition, from $\mathrm{Tr}_1^m\left(\frac{\ell_{20}\ell_{22}}{\ell_{21}^2}\right)=1$, we have

$$
\mathrm{Tr}_1^m\left(\frac{\omega\theta_2\theta_3+\omega\theta_2\overline{\theta}_3+\theta_3\theta_4+\omega^2\overline{\theta}_2\theta_3+\theta_3\overline{\theta}_3+\overline{\theta}_3\theta_4+\omega^2\overline{\theta}_2\overline{\theta}_3+\omega\theta_3^2+\omega^2\overline{\theta}_3^2}{\theta_2^2+\overline{\theta}_2^2}\right)=1. \tag{18}
$$

Also, thanks to

$$
\mathrm{Tr}_1^m\left(\frac{\omega\theta_3^2+\omega^2\overline{\theta}_3^2}{\theta_2^2+\overline{\theta}_2^2}\right)=\mathrm{Tr}_1^m\left(\frac{\left(\omega^2\theta_3+\omega\overline{\theta}_3\right)\left(\theta_2+\overline{\theta}_2\right)}{\theta_2^2+\overline{\theta}_2^2}\right),
$$

together with Eq. (18), we obtain

$$
\mathrm{Tr}_1^m\left(\frac{\theta_2\theta_3+\theta_3\theta_4+\theta_3\overline{\theta}_3+\overline{\theta}_3\theta_4+\overline{\theta}_2\overline{\theta}_3}{\theta_2^2+\overline{\theta}_2^2}\right)=1. \tag{19}
$$

Plugging $\theta_3 = \frac{\epsilon}{\theta_2^2}$ and $\overline{\theta}_3 = \frac{\epsilon}{\overline{\theta}_2^2}$ into Eq. (19) and simplifying, we get

$$
\begin{aligned}
& \mathrm{Tr}_1^m \left(\frac{\theta_2\theta_3 + \theta_3\theta_4 + \theta_3\overline{\theta}_3 + \overline{\theta}_3\theta_4 + \overline{\theta}_2\overline{\theta}_3}{\theta_2^2 + \overline{\theta}_2^2} \right) \\
= \ & \mathrm{Tr}_1^m \left(\frac{\epsilon/\theta_2 + \theta_4\epsilon(1/\theta_2^2 + 1/\overline{\theta}_2^2) + \epsilon^2/(\theta_2^2\overline{\theta}_2^2) + \epsilon/\overline{\theta}_2}{\theta_2^2 + \overline{\theta}_2^2} \right) \\
= \ & \mathrm{Tr}_1^m \left(\frac{\epsilon\theta_2\overline{\theta}_2(\theta_2 + \overline{\theta}_2) + \epsilon^2 + \theta_4\epsilon(\theta_2^2 + \overline{\theta}_2^2)}{\theta_2^2\overline{\theta}_2^2\left(\theta_2^2 + \overline{\theta}_2^2\right)} \right) \\
= \ & \mathrm{Tr}_1^m \left(\frac{\theta_4\epsilon}{\theta_2^2\overline{\theta}_2^2} \right) = 1.
\end{aligned}
$$

In addition, from Lemma 1.5, we get

$$
\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 = \theta_4\left(\theta_1 + \theta_4\right).
$$

Plugging $\theta_1 = 0$ into the above equation, we have

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

Furthermore,

$$
\begin{aligned}
\mathrm{Tr}_1^m \left(\frac{\theta_4\epsilon}{\theta_2^2\overline{\theta}_2^2} \right) & = \mathrm{Tr}_1^m \left(\frac{\theta_4^2\epsilon^2}{\theta_2^4\overline{\theta}_2^4} \right) \\
& = \mathrm{Tr}_1^m \left(\frac{\left(\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3\right)\epsilon^2}{\theta_2^4\overline{\theta}_2^4} \right) \\
& = \mathrm{Tr}_1^m \left(\frac{\left(\theta_2\overline{\theta}_2 + \epsilon^2/(\theta_2^2\overline{\theta}_2^2)\right)\epsilon^2}{\theta_2^4\overline{\theta}_2^4} \right) \\
& = \mathrm{Tr}_1^m \left(\frac{\epsilon^4}{\theta_2^6\overline{\theta}_2^6} + \frac{\epsilon^2\theta_2^3\overline{\theta}_2^3}{\theta_2^6\overline{\theta}_2^6} \right) = 0,
\end{aligned}
$$

which is a contradiction! Thus, there does not exist any $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}$ such that $L(x, y) = \ell_{22}(xy + ax + ay + b)(xy + \overline{a}x + \overline{a}y + \overline{b})$.

All in all, there exist some $a, b \in \mathbb{F}_{2^n}$ with a, b not in $\mathbb{F}_{2^m}$ at the same time such that $L(x, y) = \ell_{22}(xy + ax + ay + b)(xy + \overline{a}x + \overline{a}y + \overline{b})$ if and only if

$$
\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_1 \neq \theta_2 + \overline{\theta}_2, \theta_2^2 = \theta_1\overline{\theta}_3, \theta_4^2 = \theta_1^2 + \theta_3\overline{\theta}_3, \mathrm{Tr}_1^m \left(\frac{\theta_4}{\theta_1} \right) = 1.
$$

As for (iii), there exist some $a \in \overline{\mathbb{F}}_{2^m} \backslash \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{2^m}$ such that

$$
\begin{aligned}
L &= \ell_{22}(xy + ax + \overline{a}y + b)(xy + \overline{a}x + ay + b) \\
&= \ell_{22}\left(x^2y^2 + (\overline{a} + a)x^2y + (\overline{a} + a)xy^2 + a\overline{a}x^2 +\right. \\
&\quad \left. (a^2 + \overline{a}^2)xy + a\overline{a}y^2 + (ab + \overline{a}b)x + (ab + \overline{a}b)y + b^2\right).
\end{aligned}
$$

Comparing the coefficients of the above expression and (5), we have

$$
\begin{cases}
\ell_{21} = (a + \overline{a})\ell_{22} & (20.1) \\
\ell_{20} = a\overline{a}\ell_{22} & (20.2) \\
\ell_{11} = (a^2 + \overline{a}^2)\ell_{22} & (20.3) \\
\ell_{10} = (ab + \overline{a}b)\ell_{22} & (20.4) \\
\ell_{00} = b^2\ell_{22}. & (20.5)
\end{cases}
$$

Computing $(20.1)^2 + (20.3) \times \ell_2$ and $(20.4)^2 + (20.3) \times (20.5)$, we obtain

$$
\ell_{21}^2 + \ell_{11}\ell_{22} = 0 \text{ and } \ell_{11}\ell_{00} + \ell_{10}^2 = 0,
$$

i.e.,

$$
\theta_1\theta_3 + \theta_1\overline{\theta}_3 + \theta_2^2 + \overline{\theta}_2^2 = 0 \tag{21}
$$

and

$$
\omega^2\theta_1\theta_3 + \omega\theta_1\overline{\theta}_3 + \omega\theta_2^2 + \omega^2\overline{\theta}_2^2 = 0. \tag{22}
$$

Computing $(21) + \omega \times (22)$, we have $\omega^2\left(\theta_1\overline{\theta}_3 + \theta_2^2\right) = 0$ and thus $\theta_2^2 = \theta_1\overline{\theta}_3$. In addition, since $a + \overline{a} \neq 0$ and $\ell_{11} = (a^2 + \overline{a}^2)\ell_{22}$, we know $\theta_1 = \ell_{11} \neq 0$. Furthermore, when $\theta_1 \neq 0$ and $\theta_2^2 = \theta_1\overline{\theta}_3$, $a, \overline{a}$ are solutions in $\mathbb{F}_{2^n}$ of

$$
x^2 + \frac{\ell_{21}}{\ell_{22}}x + \frac{\ell_{20}}{\ell_{22}} = 0
$$

and thus $\mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1$, see Subcase 1.1. Hence, there exist some $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}$ such that $L = \ell_{22}(xy + ax + \overline{a}y + b)(xy + \overline{a}x + ay + b)$ if and only if

$$
\theta_1 \neq 0, \theta_1 \neq \theta_3 + \overline{\theta}_3, \theta_2^2 = \theta_1\overline{\theta}_3, \mathrm{Tr}_1^m\left(\frac{\theta_4}{\theta_1}\right) = 1.
$$

Case 2: $\ell_{22} = 0$. Namely, $\theta_1 = \theta_3 + \overline{\theta}_3$.

In the case, if $\ell_{21} \neq 0$, then $\deg L = 3$. We also use the important property that the morphisms $(x, y) \to (y, x)$ and $(x, y) \to (\overline{x}, \overline{y})$ fix $L = 0$. If L has a component L_1 not defined over $\mathbb{F}_{2^m}$ with degree 1. Then $\overline{L}_1 \neq L$ with degree 1 is also a component of L, where $\overline{L}_1$ denotes the polynomial from raising all the coefficients of L_1 into their 2^m-th power. Thus if L can split completely into absolute irreducible components not defined over $\mathbb{F}_{2^m}$, the only possibility is $(1, 1, 1)$. Namely, there exist some $a, b \in \overline{\mathbb{F}}_{2^m} \backslash \mathbb{F}_{2^m}$ such that

$L(x, y) = \ell_{21}(x + y + a)(x + b)(y + b)$. However, since $L(\overline{x}_0, \overline{y}_0) = 0$ if $L(x_0, y_0) = 0$, we have $a, b \in \mathbb{F}_{2^m}$. Conflict! Therefore, $\ell_{21} = 0$.

When $\ell_{22} = \ell_{21} = 0$, $\theta_1 = \theta_2 + \overline{\theta}_2 = \theta_3 + \overline{\theta}_3$ and thus $\theta_2 + \theta_3 \in \mathbb{F}_{2^m}$, denoted by $\gamma \in \mathbb{F}_{2^m}$. Moreover, we have

$$L(x, y) = \ell_{20}x^2 + \ell_{11}xy + \ell_{02}y^2 + \ell_{10}x + \ell_{01}y + \ell_{00}, \tag{23}$$

where

$$
\begin{cases}
\ell_{20} = \ell_{02} = \theta_4 + \gamma & (24.1) \\
\ell_{11} = \theta_2 + \overline{\theta}_2 & (24.2) \\
\ell_{10} = \ell_{01} = \omega\theta_2 + \omega^2\overline{\theta}_2 & (24.3) \\
\ell_{00} = \omega\theta_2 + \omega^2\overline{\theta}_2 + \gamma, & (24.4)
\end{cases}
$$

If $\ell_{20} = 0$, i.e., $\theta_4 = \gamma$, to make sure that $L(x, y)$ does not have absolute irreducible components defined over $\mathbb{F}_{2^m}$ different from $y = x$, we have $\ell_{11} = \ell_{00} = 0$. Namely, $\theta_2 \in \mathbb{F}_{2^m}$ and $\gamma = \theta_2$. Furthermore, $\theta_3 = 0$ and $\theta_1 = 0$. Considering the expressions of θ_i, we have

$$
\begin{cases}
1 + a_1^2 + a_2\overline{a}_2 + a_3\overline{a}_3 = 0 & (25.1) \\
\overline{a}_2 + a_1\overline{a}_3 = 0 & (25.2) \\
a_1 + \overline{a}_2 a_3 = a_1 + a_2\overline{a}_3 & (25.3) \\
a_1 + \overline{a}_2 a_3 = a_1^2 + a_2\overline{a}_2. & (25.4)
\end{cases}
$$

Plugging (25.4) into (25.1), we have

$$1 + a_1 + \overline{a}_2 a_3 + a_3\overline{a}_3 = 0,$$

i.e.,

$$(a_1 + 1)(a_3\overline{a}_3 + 1) = 0.$$

Thus $a_1 = 1$ or $a_3\overline{a}_3 = 1$. If $a_1 = 1$, we have $a_2 = a_3$ from (25.2), which means $1 + a_1 + a_2 + a_3 = 0$, which is a contradiction. If $a_3\overline{a}_3 = 1$, then $\theta_2 = \theta_4 = a_1^2 + a_2\overline{a}_2 = 0$, which means $L = 0$, which is also impossible.

Therefore, $\ell_{20} \neq 0$. Suppose that there exist some $a, b \in \mathbb{F}_{2^n}$ such that

$$L = \ell_{20}(x + ay + b)(x + \overline{a}y + \overline{b}).$$

After comparing the coefficients of the above expression and (23), we have $a = 1$ or $a = \frac{b}{\overline{b}}$.

If $a = 1$, then $L = \ell_{20}\left(x^2 + y^2 + (b + \overline{b})x + (b + \overline{b})y + b\overline{b}\right)$ and thus $\ell_{11} = \theta_2 + \overline{\theta}_2 = 0$, i.e., $\theta_2 \in \mathbb{F}_{2^m}$. Furthermore, $\theta_1 = 0$ and $\theta_3 = \gamma + \theta_2 \in \mathbb{F}_{2^m}$. In addition, from Lemma 1.5, we get $\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 = \theta_4(\theta_1 + \theta_4)$ and thus $\theta_4 = \theta_2 + \theta_3 = \gamma$, which means $\ell_{20} = 0$. Conflict.

If $a = \frac{b}{\overline{b}}$, then $L = \ell_{20}\left(x^2 + y^2 + (\frac{b}{\overline{b}} + \frac{\overline{b}}{b})xy + (b + \overline{b})x + (b + \overline{b})y + b\overline{b}\right)$ and thus

$$
\begin{cases}
(\frac{b}{\overline{b}} + \frac{\overline{b}}{b})\ell_{20} = \ell_{11} = \theta_2 + \overline{\theta}_2 & (26.1) \\[2mm]
(b + \overline{b})\ell_{20} = \ell_{10} = \omega\theta_2 + \omega^2\overline{\theta}_2 & (26.2) \\[2mm]
b\overline{b}\ell_{20} = \ell_{00} = \omega\theta_2 + \omega^2\overline{\theta}_2 + \gamma, . & (26.3)
\end{cases}
$$

Computing $(26.2)^2/(26.3) + (26.1)$, we obtain $\ell_{10}^2 = \ell_{00}\ell_{11}$, i.e.,

$$
\gamma = \frac{\theta_2^2 + \overline{\theta}_2^2 + \theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2}.
$$

In addition, from Lemma 1.5, we get $\theta_2\overline{\theta}_2 + \theta_3\overline{\theta}_3 = \theta_4(\theta_1 + \theta_4)$. Plugging $\theta_3 = \theta_2 + \gamma$ and $\theta_1 = \theta_2 + \overline{\theta}_2$ into the above equation and simplifying, we have

$$
(\theta_4 + \gamma)(\theta_4 + \gamma + \theta_2 + \overline{\theta}_2) = 0.
$$

Hence, $\theta_4 = \gamma + \theta_2 + \overline{\theta}_2$ since $\ell_{20} = \theta_4 + \gamma \neq 0$. Moreover, from (26.2) and (26.3), we know that $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m\left(\frac{\ell_{00}\ell_{20}}{\ell_{10}^2}\right) = 1$, which holds under our assumption. In fact,

$$
\begin{aligned}
\mathrm{Tr}_1^m\left(\frac{\ell_{00}\ell_{20}}{\ell_{10}^2}\right) &= \mathrm{Tr}_1^m\left(\frac{(\omega\theta_2 + \omega^2\overline{\theta}^2 + \gamma)(\theta_2 + \overline{\theta}_2)}{\omega^2\theta_2^2 + \omega\overline{\theta}_2^2}\right) \\
&= \mathrm{Tr}_1^m\left(\frac{\omega\theta_2^2 + \omega^2\overline{\theta}_2^2 + \theta_2\overline{\theta}_2 + \gamma(\theta_2 + \overline{\theta}_2)}{\omega^2\theta_2^2 + \omega\overline{\theta}_2^2}\right) \\
&= \mathrm{Tr}_1^m(1) = 1
\end{aligned}
$$

since $\gamma = \frac{\theta_2^2 + \overline{\theta}_2^2 + \theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2}$ and m is odd. Therefore, there exist some $a, b \in \mathbb{F}_{2^n}$ such that $L = \ell_{20}(x + ay + b)(x + \overline{a}y + \overline{b})$ if and only if

$$
\theta_1 = \theta_2 + \overline{\theta}_2 \neq 0, \theta_3 = \theta_2 + \gamma, \theta_4 = \gamma + \theta_2 + \overline{\theta}_2 \quad \text{and} \quad \gamma = \frac{\theta_2^2 + \overline{\theta}_2^2 + \theta_2\overline{\theta}_2}{\theta_2 + \overline{\theta}_2}.
$$

REFERENCES

[1] Daniele Bartoli. On a conjecture about a class of permutation trinomials. *Finite Fields and Their Applications*, 52:30–50, 2018.

[2] Xiang-dong Hou. On the Tu-Zeng permutation trinomial of type $(1/4, 3/4)$. *arXiv preprint arXiv:1906.07240*.

[3] Xiang-dong Hou. Determination of a type of permutation trinomials over finite fields, II. *Finite Fields and Their Applications*, 35:16–35, 2015.

[4] Xiang-dong Hou. *Lectures on Finite Fields*, volume 190. American Mathematical Soc., 2018.

[5] Xiang-dong Hou. On a class of permutation trinomials in characteristic 2. *Cryptography and Communications*, pages 1–12, 2018.

[6] Kangquan Li, Longjiang Qu, and Xi Chen. New classes of permutation binomials and permutation trinomials over finite fields. *Finite Fields and Their Applications*, 43:69–85, 2017.

[7] Kangquan Li, Longjiang Qu, Chao Li, and Shaojing Fu. New permutation trinomials constructed from fractional polynomials. *Acta Arithmetica*, 183:101–116, 2018.

[8] Nian Li and Tor Helleseth. New permutation trinomials from Niho exponents over finite fields with even characteristic. *Cryptography and Communications*, 11(1):129–136, 2019.

[9] Nian Li and Xiangyong Zeng. A survey on the applications of Niho exponents. *Cryptography and Communications*, 11(3):509–548, 2019.

[10] Young Ho Park and June Bok Lee. Permutation polynomials and group permutation polynomials. *Bulletin of the Australian Mathematical Society*, 63(1):67–74, 2001.

[11] Ziran Tu, Xianping Liu, and Xiangyong Zeng. A revisit to a class of permutation quadrinomials. *Finite Fields and Their Applications*, 59:57–85, 2019.

[12] Ziran Tu and Xiangyong Zeng. Two classes of permutation trinomials with Niho exponents. *Finite Fields and Their Applications*, 53:99–112, 2018.

[13] Ziran Tu, Xiangyong Zeng, Chunlei Li, and Tor Helleseth. A class of new permutation trinomials. *Finite Fields and Their Applications*, 50:178–195, 2018.

[14] Qiang Wang. Cyclotomic mapping permutation polynomials over finite fields. In *Sequences, Subsequences, and Consequences*, pages 119–128. Springer, 2007.

[15] Qiang Wang. Polynomials over finite fields: an index approach. *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, 23, 2019.

[16] Michael Zieve. On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. *Proceedings of the American Mathematical Society*, 137(7):2209–2216, 2009.