Cryptogr. Commun. (2018) 10:531–554
DOI 10.1007/s12095-017-0236-7

# Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic

**Kangquan Li[1] · Longjiang Qu[1,2] · Xi Chen[1] · Chao Li[1]**

Received: 25 November 2016 / Accepted: 16 June 2017 / Published online: 1 July 2017


**Abstract** Permutation polynomials over finite fields constitute an active research area and have applications in many areas of science and engineering. Particularly, permutation polynomials with few terms are more popular for their simple algebraic form and additional extraordinary properties. Very recently, G. Kyureghyan and M.E. Zieve (2016) studied permutation polynomials over $\mathbb{F}_{q^n}$ of the form $x+\gamma \mathrm{Tr}_{q^n/q}(x^k)$, where $q$ is odd, and nine classes of permutation polynomials were constructed. In this paper, we present fifteen new classes of permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ over finite fields with even characteristic, which explain most of the examples with $q = 2^k$, $k > 1$, $kl < 14$ and $c \in \mathbb{F}_{q^l}^*$. Furthermore, we also construct four classes of permutation trinomials.

**Keywords** Finite fields · Permutation polynomials · Trinomials

This work is supported by the National Basic Research Program of China (Grant No. 2013CB338002), the Nature Science Foundation of China (NSFC) under Grant 61272484, 11531002, 61572026, the Program for New Century Excellent Talents in University (NCET), the Basic Research Fund of National University of Defense Technology (No. CJ 13-02-01), and the Open Foundation of State Key Laboratory of Cryptology.

This article is part of the Topical Collection on *Special Issue on Sequences and Their Applications*

✉ Longjiang Qu
ljqu_happy@hotmail.com

Kangquan Li
likangquan11@nudt.edu.cn

Xi Chen
1138470214@qq.com

Chao Li
lichao_nudt@sina.com

[1] College of Science, National University of Defense Technology, Changsha, 410073, China

[2] State Key Laboratory of Cryptology, Beijing 100878, China

**Mathematics Subject Classification (2010)** 05A05 · 11T06 · 11T55

## 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 $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the induced mapping $x \to f(x)$ is a permutation of $\mathbb{F}_q$. Permutation polynomials have various applications in coding theory [20, 30], cryptography [22, 26, 27] and combinatorial designs [8]. Therefore, the study about permutation polynomials attracts people's interest for many years. Particularly, permutation polynomials with few terms are more popular thanks to their simple algebraic form and additional extraordinary properties. For example, in [10], Dobbertin first proved a well-known conjecture of Welch stating that the power function $x^{2^m+3}$ on $\mathbb{F}_{2^{2m+1}}$ is even maximally nonlinear, or, in other words the crosscorrelation function between a binary maximum-length linear shift register sequence of degree $n$ and a decimation of that sequence by $2^m+3$ takes on precisely the three values $-1, -1 \pm 2^{m+1}$. And the key of his proof was a discovery of a class of permutation trinomials. More results about permutation polynomials can be found in [5, 6, 12, 13, 15–18, 24, 29].

Let $q = 2^k$. For $\alpha \in \mathbb{F}_{q^l}$, *the trace function* from $\mathbb{F}_{q^l}$ to its subfield $\mathbb{F}_q$ is defined as

$$\mathrm{Tr}_{q^l/q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{l-1}}.$$

If $q = 2$, $\mathrm{Tr}_{q^l/q}(\alpha)$ is called *the absolute trace function*, and it is simply denoted by $\mathrm{Tr}_{q^l}(\alpha)$. The trace function is often used in constructing permutation polynomials over finite fields [5–7, 18, 33, 37]. In [5], P. Charpin and G. Kyureghyan considered a class of permutation polynomials of the shape $G(x) + \gamma \mathrm{Tr}_q(H(x))$ over $\mathbb{F}_q$, where $q = 2^k$. They found that the considered problem can be reduced to looking for Boolean functions with linear structures. With this idea, they constructed sparse permutation polynomials by choosing both $G(x)$ and $H(x)$ to be monomials. In [7], they extended these results from finite fields with even characteristic to arbitrary finite fields. Very recently, G. Kyureghyan and M.E. Zieve [18] studied all permutation polynomials over $\mathbb{F}_{q^n}$ of the form $x + \gamma \mathrm{Tr}_{q^n/q}(x^k)$ with $\gamma \in \mathbb{F}_{q^n}^*$, $q$ odd, $n > 1$, and $q^n < 5000$. They constructed nine classes of permutation polynomials with this special form, which explained most of the experimental results under the aforementioned condition. This motivates us to study such permutation polynomials over finite fields with even characteristic. Hence this paper is devoted to construct new permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$, where $q = 2^k$. To avoid repetitive work from [5], we do not consider the absolute trace function, in other words, we assume that $q > 2$.

We notice that a permutation polynomial of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ is a permutation trinomial when $l = 2$. Permutation trinomials have been widely studied for their simple structure and wide applications. For instances, the discovery of a class of permutation trinomials by Ball and Zieve [3] provided a way to prove the construction of the Ree-Tits symplectic spreads of $\mathbf{PG}(3, q)$. Hou [16, 17] acquired a necessary and sufficient condition about determining a special permutation trinomial. For more recent results about permutation trinomials, please refer to [9, 14, 24, 25, 28].

We also notice that a permutation polynomial of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ may also with the form $x^r h\left(x^{(q^l-1)/d}\right)$ in some special cases, while there are many results about the polynomials with this form over $\mathbb{F}_{q^l}$. For instances, let $Q = q_0^m$, where $q_0 \equiv 1 \pmod d$ and $d \mid m$, and $h \in \mathbb{F}_{q_0}[x]$. Akbary and Wang [2], Laigle-Chapug [20] proved that $x^r h\left(x^{(Q-1)/d}\right)$ permutes $\mathbb{F}_Q$ if and only if $\gcd(r+n, d) = \gcd\left(r, (Q-1)/d\right) = 1$.

Zieve made important contributions to determining permutation polynomials with this form. In [34], Zieve obtained a necessary and sufficient condition about a complex form $h(x) = h_k(x)^t \hat{h}\left(h_l(x)^{d_0}\right)$, where $h_k(x) = 1 + x + \cdots + x^{k-1}$ and $t, d_0, \hat{h}$ satisfy some conditions. For more results about permutation polynomials with this form, one can consult [14, 35, 36].

In this paper, we construct fifteen new classes of permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ over finite fields with even characteristic. Moreover, four classes of permutation trinomials are also presented. According to the difference on the Hamming weight of $a$, which is defined to be the number of nonzero coefficients $a_i$ in the binary expansion $\sum_{i=0}^{s} a_i 2^i$ of $a$, we use three different methods to prove these results. In the following, we give the sketches of these methods. The first one is called *the elementary approach*. It was used in the case where the Hamming weight of $a$ is small. Let $f(x) = cx + \mathrm{Tr}_{q^l/q}(x^a) = d$ and $u = cx + d$. Then $u = \mathrm{Tr}_{q^l/q}(x^a) \in \mathbb{F}_q$ and $x = \frac{1}{c}(u + d)$. Plugging $x = \frac{1}{c}(u + d)$ into $f(x) = d$ leads to an equation of $u$ with low degree. It is not difficult to show that this low degree equation has at most one solution in $\mathbb{F}_q$. We call the second method *the fractional approach*. It has been used in [12, 25], where the permutation trinomials over $\mathbb{F}_{q^2}$ of the form $x^r h\left(x^{q-1}\right)$ were mainly considered, and $p(x) = x^r h(x)^{q-1}$ was called a *fractional polynomial*. In the present paper, several new classes of permutation trinomials over $\mathbb{F}_{q^2}$,where $q = 2^k$ with such form are constructed, some of which are the generalizations of those in [25]. The final method is *the multivariate method* introduced by Dobbertin [11]. That is to prove the permutation property of a polynomial by algebraic calculations with multivariate equations. It had been widely used to prove permutation polynomials, such as [9, 18] and so on.

By using Magma, we search all permutation polynomials over $\mathbb{F}_{q^l}$ of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$ with $q = 2^k$, $kl < 14$, $c \in \mathbb{F}_{q^l}^*$ and $a \in [1, q^l - 2]$. We also add some conditions in the process of obtaining the data in Table 1. First, the restriction $k > 1$ is added to distinguish our study from that of P. Charpin and G. Kyureghyan [5]. Second, we rule out the trivial cases that $\mathrm{Tr}_{q^l/q}(x^a) \equiv 0$ for $x \in \mathbb{F}_{q^l}$, $a$ is divided by $q$, and $a$ is a power of 2, where the last case is corresponding to linearized polynomials. All experiment examples are given in Table 1. In Table 1, $\omega$ is a primitive element of the corresponding finite field and the overbar of an element denotes the set consisting of all its conjugate elements. Column Ref. refers to the theorem that explains the corresponding examples. It should be noted that an example may be explained by several theorems, however, we only list one for simplicity. Lastly, the symbol "-" means that an example can not be explained by us up to now. We can see from Table 1 that most of the examples of this form can be generalized to a class of permutation polynomials.

The rest of this paper is organized as follows. In Section 2 we introduce some useful lemmas. Section 3 contains the permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$. It is divided into three subsections according to the value of $l$, which are the case that $l > 2$ is even, the case that $l$ is odd and the case that $l = 2$. Four classes of permutation trinomials are introduced in Section 4.

## 2 Preliminary

The following result was discovered independently by several authors. It is also worth pointing out that it is actually the multiplicative case of a more general AGW criterion [1, Lemma 1.2]. Lemma 2.1 will be frequently employed in the sequel.

**Table 1** Permutation polynomials of the form $cx + \mathrm{Tr}_{2^{kl}/2^k}(x^a)$ over $\mathbb{F}_{2^{kl}}$, $k > 1$, $kl < 14$

| | $k$ | $l$ | $a$ | $c$ | Ref. | | $k$ | $l$ | $a$ | $c$ | Ref. |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 7 | 1 | Th 3.6 | 21 | 3 | 4 | 9 | $\mathbb{F}_{64}^*$ | Th 3.1 |
| 2 | 3 | 2 | 15 | $\mathbb{F}_4^*$ | Th 3.6 | 22 | 3 | 4 | 18 | $\mathbb{F}_{64}^*$ | Th 3.1 |
| 3 | 3 | 2 | 22 | $\overline{\omega^9}$ | Th 3.9 | 23 | 3 | 4 | 36 | $\mathbb{F}_{64}^*$ | Th 3.1 |
| 4 | 2 | 3 | 10 | $\mathbb{F}_4\backslash\{0,1\}$ | Th 3.5 | 24 | 4 | 3 | 34 | $C_1$ | Th 3.4 |
| 5 | 4 | 2 | 31 | 1 | Th 3.6 | 25 | 4 | 3 | 136 | $\mathbb{F}_{16}\backslash\{0,1\}$ | Th 3.5 |
| 6 | 4 | 2 | 61 | 1 | Th 2.7 | 26 | 6 | 2 | 127 | 1 | Th 3.6 |
| 7 | 4 | 2 | 91 | 1 | Th 2.6 | 27 | 6 | 2 | 136 | $C_2$ | – |
| 8 | 4 | 2 | 76 | $1, \overline{\omega^{119}}$ | Th 2.8(2) | 28 | 6 | 2 | 505 | 1 | Th 2.8(1) |
| 9 | 4 | 2 | 106 | $\mathbb{F}_4^*$ | Th 3.7 | 29 | 6 | 2 | 505 | $\overline{\omega^{819}}$ | – |
| 10 | 2 | 4 | 5 | $\mathbb{F}_{16}^*$ | Th 3.1 | 30 | 6 | 2 | 568 | 1 | Th 2.8(2) |
| 11 | 2 | 4 | 10 | $\mathbb{F}_{16}^*$ | Th 3.1 | 31 | 6 | 2 | 1072 | $C_3$ | Th 3.9 |
| 12 | 3 | 3 | 36 | $\mathbb{F}_8\backslash\{0,1\}$ | Th 3.5 | 32 | 6 | 2 | 1324 | 1 | Th 3.12 |
| 13 | 2 | 5 | 10 | $\mathbb{F}_4\backslash\{0,1\}$ | Th 3.4 | 33 | 6 | 2 | 1387 | 1 | Th 2.6 |
| 14 | 2 | 5 | 34 | $\mathbb{F}_4\backslash\{0,1\}$ | Th 3.4 | 34 | 6 | 2 | 1450 | $\mathbb{F}_{16}^*$ | Th 2.7 |
| 15 | 5 | 2 | 63 | $\mathbb{F}_4^*$ | Th 3.6 | 35 | 6 | 2 | 1639 | 1 | – |
| 16 | 5 | 2 | 435 | $\mathbb{F}_4^*$ | Th 3.8 | 36 | 6 | 2 | 1828 | $\mathbb{F}_8^*$ | Th 3.13 |
| 17 | 5 | 2 | 125 | 1 | – | 37 | 2 | 6 | 5 | $\mathbb{F}_{16}^*$ | Th 3.1 |
| 18 | 5 | 2 | 466 | 1 | Th 3.10 | 38 | 2 | 6 | 10 | $\mathbb{F}_{16}^*$ | Th 3.1 |
| 19 | 5 | 2 | 187 | $1, \overline{\omega^{93}}$ | Th 3.11 | 39 | 2 | 6 | 17 | $\mathbb{F}_4^*$ | Th 3.2 |
| 20 | 5 | 2 | 280 | $1, \overline{\omega^{231}}, \overline{\omega^{363}}$ | Th 3.9 | 40 | 2 | 6 | 34 | $C_4$ | Th 3.3 |

$C_1 : \mathbb{F}_{16}^*\backslash\{c : c^3 \neq 1\}$
$C_2 : \{c : c \in \mathbb{F}_{32}, x^3 + x + c = 0 \text{ has no solution in } \mathbb{F}_{32}\}$
$C_3 : \overline{\omega^{117}}, \overline{\omega^{273}}, \overline{\omega^{351}}, \overline{\omega^{429}}, \overline{\omega^{507}}, \overline{\omega^{819}}$
$C_4 : 1, \overline{\omega^{231}}, \overline{\omega^{819}}, \overline{\omega^{1365}}$

**Lemma 2.1** [23, 31, 34] *Pick $d, r > 0$ with $d \mid (q-1)$, and let $h \in \mathbb{F}_q[x]$. Then $f(x) = x^r h\left(x^{(q-1)/d}\right)$ permutes $\mathbb{F}_q$ if and only if both*

(1) $\gcd\left(r, (q-1)/d\right) = 1$ *and*
(2) $x^r h(x)^{(q-1)/d}$ *permutes $\mu_d$, where $\mu_d = \{x \in \overline{\mathbb{F}}_q : x^d = 1\}$, and $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$.*

The following results on the number of the solutions of quadratic and cubic equations in $\mathbb{F}_q$ are useful in the subsequent proof.

**Lemma 2.2** [19] *Let $q = 2^k$, where $k$ is a positive integer. The quadratic equation $x^2 + ux + v = 0$, where $u, v \in \mathbb{F}_q$ and $u \neq 0$, has roots in $\mathbb{F}_q$ if and only if $\mathrm{Tr}_q\left(\frac{v}{u^2}\right) = 0$.*

**Lemma 2.3** [4] *Let $a, b \in \mathbb{F}_q$, where $q = 2^k$ and $b \neq 0$. Then the cubic equation $x^3 + ax + b = 0$ has a unique solution in $\mathbb{F}_q$ if and only if $\mathrm{Tr}_q\left(\frac{a^3}{b^2} + 1\right) \neq 0$.*

We can work out a solution of a cubic equation by the following method.

**Theorem 2.4** [32] *Let $q = 2^k$ and $f(x) = x^3 + ax + b \in \mathbb{F}_q[x]$ and $b \neq 0$. Let $t_1$ be one solution of the quadratic derived equation $t^2 + bt + a^3 = 0$. And let $\epsilon$ be one solution of $x^3 = t_1$. Then $\epsilon + \frac{a}{\epsilon}$ is a root of $f(x)$.*

Philip A. Leonard and Kenneth S. Williams characterized the factorization of a quartic polynomial over $\mathbb{F}_{2^k}$ in [21].

**Lemma 2.5** [21] *Let $q = 2^k$ and $f(x) = x^4 + a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$, where $a_0 \neq 0$. Let $g(y) = y^3 + a_2y + a_1$. Then $f(x)$ is irreducible if and only if $g(y)$ only has one solution $r$ in $\mathbb{F}_q$ and $\mathrm{Tr}_q\left(\frac{a_0r^2}{a_1^2}\right) = 1$.*

The following two theorems were obtained by G. Kyureghyan and M.E. Zieve in [18]. We list them here because they can explain some examples in Table 1.

**Theorem 2.6** [18] *If $q \equiv 1 \pmod 3$, then $f(x) = x + \mathrm{Tr}_{q^2/q}\left(x^{\frac{q^2+q+1}{3}}\right)$ permutes $\mathbb{F}_{q^2}$.*

**Theorem 2.7** [18] *For any prime power $q$ and any positive integers $l, n$ with $2l \mid n$, if $\gamma \in \mathbb{F}_{q^n}$ satisfies $\gamma^{q^{2l}-1} = -1$, then the polynomial $f(x) = x + \gamma \mathrm{Tr}_{q^n/q}(x^{q^l+1})$ permutes $\mathbb{F}_{q^n}$.*

The following results can be proved similarly as [18, Theorem 6.1].

**Theorem 2.8** *Let $q = 2^k$ and $f(x) = cx + \mathrm{Tr}_{q^4/q^2}(x^a) \in \mathbb{F}_{q^4}[x]$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^4}$ if one of the following conditions occurs:*

(1) $a = q^3 - q + 1$ *and* $c = 1$;
(2) $a = q^4 - q^3 + q$ *and* $c = 1$.

## 3 Permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$

In this section, we describe a few classes of permutation polynomials of the form $cx + \mathrm{Tr}_{q^l/q}(x^a)$. We divide the results into three subsections according to the value of $l$. More precisely, they are the case $l > 2$ is even, $l$ is odd and $l = 2$. We put the case $l = 2$ alone out since the results in this case constitute the majority.

### 3.1 The case $l > 2$ is even

**Theorem 3.1** *Let $q = 2^k$ and $f(x) = cx + \mathrm{Tr}_{q^{2n}/q}\left(x^{2^i(q+1)}\right)$, where $c \in \mathbb{F}_{q^2}^*$ and $n, k, i > 0$ are integers. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n}}$.*

*Proof* We show that for any $d \in \mathbb{F}_{q^{2n}}$, the equation $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$. Let $u = cx + d$. Then $u = \mathrm{Tr}_{q^{2n}/q}(x^{2^i(q+1)}) \in \mathbb{F}_q$ and $x = \frac{1}{c}(u + d)$. Plugging $x = \frac{1}{c}(u + d)$ into $f(x) = d$, we get

$$u + \frac{\mathrm{Tr}_{q^{2n}/q}\left(u^{2^{i+1}} + \left(d^{2^iq} + d^{2^i}\right)u^{2^i} + d^{2^i(q+1)}\right)}{c^{2^i(q+1)}} = 0.$$

Thanks to $u \in \mathbb{F}_q$, $\mathrm{Tr}_{q^{2n}/q}(1) \equiv 0$ and $\mathrm{Tr}_{q^{2n}/q}\left(d^{2^i q} + d^{2^i}\right) \equiv 0$, we have

$$u = \frac{\mathrm{Tr}_{q^{2n}/q}\left(d^{2^i(q+1)}\right)}{c^{2^i(q+1)}}.$$

Hence $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$. Moreover, $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n}}$. □

**Theorem 3.2** *Let $q = 2^k$ and $f(x) = cx + \mathrm{Tr}_{q^{2n}/q}\left(x^{q^2+1}\right)$, where $c \in \mathbb{F}_q^*$ and $n, k > 0$ are integers. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n}}$.*

*Proof* It suffices to prove that for any $d \in \mathbb{F}_{q^{2n}}$, $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$. Let $u = cx + d$. Then $u = \mathrm{Tr}_{q^{2n}/q}\left(x^{q^2+1}\right) \in \mathbb{F}_q$ and $x = \frac{1}{c}(u + d)$. Plugging the above expression of $x$ into $f(x) = d$, we get

$$u + \mathrm{Tr}_{q^{2n}/q}\left(\frac{1}{c^2}(u^2 + (d^{q^2} + d)u + d^{q^2+1})\right) = 0,$$

i.e.,

$$u = \frac{\mathrm{Tr}_{q^{2n}/q}\left(d^{q^2+1}\right)}{c^2}.$$

Hence $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$. We finish the proof. □

**Theorem 3.3** *Let $q = 2^k$ and $f(x) = cx + \mathrm{Tr}_{q^{2n}/q}\left(x^{2^i(q^2+1)}\right)$, where $c \in \mathbb{F}_{q^2}^*$ and $n, k, i > 0$ are integers. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n}}$ if one of the following conditions occurs:*

(1) *$n$ is even;*

(2) *$n$ is odd and $\left(\frac{1}{c^{2^{i+1}}} + \frac{1}{c^{2^{i+1}q}}\right)^{\frac{q-1}{\gcd(2^{i+1}-1, 2^k-1)}} \neq 1$.*

*Proof* We claim that $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$ for any $d \in \mathbb{F}_{q^{2n}}$ in the above two cases. Let $u = cx + d$. Then $u = \mathrm{Tr}_{q^{2n}/q}\left(x^{2^i(q^2+1)}\right) \in \mathbb{F}_q$ and $x = \frac{1}{c}(u + d)$. Moreover,

$$\begin{aligned} x^{2^i(q^2+1)} &= \frac{1}{c^{2^{i+1}}}(u + d)^{2^i(q^2+1)} \\ &= \frac{1}{c^{2^{i+1}}}\left(u^{2^i} + d^{2^i q^2}\right)\left(u^{2^i} + d^{2^i}\right) \\ &= \frac{1}{c^{2^{i+1}}}\left[u^{2^{i+1}} + (d^{2^i q^2} + d^{2^i})u^{2^i} + d^{2^i q^2 + 2^i}\right]. \end{aligned}$$

Then plugging the above equation and $x = \frac{1}{c}(u + d)$ into $f(x) = d$, we get:

(1) If $n$ is even,

$$u = \frac{1}{c^{2^{i+1}}}\mathrm{Tr}_{q^{2n}/q^2}\left(d^{2^i q^2 + 2^i}\right) + \frac{1}{c^{2^{i+1}q}}\mathrm{Tr}_{q^{2n}/q^2}\left(d^{2^i q^3 + 2^i q}\right).$$

Under the first condition, $f(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n}}$.

(2) If $n$ is odd,

$$\left(\frac{1}{c^{2^{i+1}}}+\frac{1}{c^{2^{i+1}q}}\right)u^{2^{i+1}}+u=\frac{1}{c^{2^{i+1}}}\mathrm{Tr}_{q^{2n}/q^2}\left(d^{2^iq^2+2^i}\right)+\frac{1}{c^{2^{i+1}q}}\mathrm{Tr}_{q^{2n}/q^2}\left(d^{2^iq^3+2^iq}\right). \tag{1}$$

If $c\in\mathbb{F}_q^*$, then $u=\mathrm{Tr}_{q^{2n}/q}\left(\frac{d^{2^iq^2+2^i}}{c^{2^{i+1}}}\right)$. It follows that $f(x)=d$ has at most one solution in $\mathbb{F}_{q^{2n}}$.

If $c\in\mathbb{F}_{q^2}\backslash\mathbb{F}_q$, let $a=\left(\frac{1}{c^{2^{i+1}}}+\frac{1}{c^{2^{i+1}q}}\right)^{-1}$ and $g(x)=x^{2^{i+1}}+ax\in\mathbb{F}_q[x]$. Obviously, $a\neq 0,1$. Notice that $g(x)$ permutes $\mathbb{F}_q$ if and only if $g(x)$ only has zero root in $\mathbb{F}_q$. Considering $x^{2^{i+1}}=ax$, then either $x=0$ or $x^{2^{i+1}-1}=a$ which is impossible since $\left(\frac{1}{c^{2^{i+1}}}+\frac{1}{c^{2^{i+1}q}}\right)^{\frac{q-1}{\gcd(2^{i+1}-1,2^k-1)}}\neq 1$. This means that $x=0$ is the unique solution of $g(x)=0$ in $\mathbb{F}_q$. Thus $g(x)$ is a permutation polynomial over $\mathbb{F}_q$. Therefore, (1) has at most one solution in $\mathbb{F}_{q^{2n}}$.

Hence $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n}}$ in the above two cases. □

### 3.2 The case $l$ is odd

In this subsection, we construct two classes of permutation polynomials of the form $cx+\mathrm{Tr}_{q^l/q}(x^a)$.

**Theorem 3.4** *Let $q=2^k$, where $k$ is even and $k\not\equiv 0 \pmod 3$. Let $n>0, i\neq j\geq 0$ be integers and $f(x)=cx+\mathrm{Tr}_{q^{2n+1}/q}\left(x^{2q^i+2q^j}\right)$, where $c\in\mathbb{F}_q^*$ and $c^{\frac{q-1}{3}}\neq 1$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n+1}}$.*

*Proof* It suffices to show that for any $d\in\mathbb{F}_{q^{2n+1}}$, $f(x)=d$ has at most one solution in $\mathbb{F}_{q^{2n+1}}$. Let $u=cx+d$. Then $u=\mathrm{Tr}_{q^{2n+1}/q}\left(x^{2q^i+2q^j}\right)\in\mathbb{F}_q$. Plugging $x=\frac{1}{c}(u+d)$ into $f(x)=d$, we get

$$u^4+c^4u=\mathrm{Tr}_{q^{2n+1}/q}\left(d^{2q^i+2q^j}\right). \tag{2}$$

Let $g(u)=u^4+c^4u\in\mathbb{F}_q[u]$. Then $g(u)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $g(u)=0$ only has one solution in $\mathbb{F}_q$. If there exists $u\in\mathbb{F}_q^*$ such that $g(u)=0$. Then $u^3=c^4$, we have $c^{\frac{q-1}{3}}=\left(u^{q-1}\right)^{\frac{q}{4}}=1$, which is a contradiction. Therefore, $g(u)$ is a permutation polynomial over $\mathbb{F}_q$. Moreover, (2) only has one solution in $\mathbb{F}_q$ for any $d\in\mathbb{F}_{q^{2n+1}}$. It follows that $f(x)=d$ has at most one solution in $\mathbb{F}_{q^{2n+1}}$. The proof is finished. □

**Theorem 3.5** *Let $q=2^k$ and $f(x)=cx+\mathrm{Tr}_{q^{2n+1}/q}\left(x^{\frac{q^2+q}{2}}\right)$, where $c\in\mathbb{F}_q\backslash\{0,1\}$ and $n,k>0$ are integers. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^{2n+1}}$.*

*Proof* Let $g(x)=f\left(x^2\right)=cx^2+\mathrm{Tr}_{q^{2n+1}/q}\left(x^{q^2+q}\right)$. Then $f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if so does $g(x)$. We show that for any $d\in\mathbb{F}_{q^2}$, the equation $g(x)=d$ has at most one solution in $\mathbb{F}_{q^2}$.

Let $u = cx^2 + d = \mathrm{Tr}_{q^{2n+1}/q}\left(x^{q^2+q}\right) \in \mathbb{F}_q$. Then $x = \left(\frac{u+d}{c}\right)^{\frac{1}{2}}$, and

$$x^{q^2+q} = \frac{\left(u^2 + (d^{q^2} + d^q)u + d^{q^2+q}\right)^{\frac{1}{2}}}{c}.$$

Plugging the above equation into $g(x) = d$, we have

$$u + \frac{1}{c}\left(u^2 + \mathrm{Tr}_{q^{2n+1}/q}\left(d^{q^2+q}\right)\right)^{\frac{1}{2}} = 0,$$

i.e.,

$$u = \frac{1}{1+c}\left(\mathrm{Tr}_{q^{2n+1}/q}\left(d^{q^2+q}\right)\right)^{\frac{1}{2}}.$$

Hence, $g(x) = d$ has at most one solution in $\mathbb{F}_{q^{2n+1}}$. It follows that $g(x)$ permutes $\mathbb{F}_{q^{2n+1}}$. Then so $f(x)$ does. The proof is complete. □

### 3.3 The case $l = 2$

**Theorem 3.6** *Let $q = 2^k$ and $f(x) = cx + \mathrm{Tr}_{q^2/q}\left(x^{2q-1}\right) \in \mathbb{F}_{q^2}[x]$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$ if one of the following conditions occurs.*

(i) *$k$ is even and $c = 1$,*
(ii) *$k$ is odd and $c^3 = 1$.*

*Proof* (i) When $k$ is even and $c = 1$, $f(x) = x + x^{2q-1} + x^{2-q}$. We refer the proof to Th 3.2 in [9].

(ii) Now, $f(x) = cx + x^{2q-1} + x^{2q^2-q}$. We show that for any $d \in \mathbb{F}_{q^2}$, $f(x) = d$ has at most one solution in $\mathbb{F}_{q^2}$. Put $u = cx + d = \mathrm{Tr}_{q^2/q}\left(x^{2q-1}\right) \in \mathbb{F}_q$. Then $x = c^2(u + d)$ since $c^3 = 1$.

If $d \in \mathbb{F}_q$, so does $cx$, i.e., $c^q x^q = cx$. On the other hand, $c^q = c^2$ since $k$ is odd and $c^3 = 1$. Then $x^q = c^2 x$. Therefore, $x^{2q-1} = \frac{c^4 x^2}{x} = cx \in \mathbb{F}_q$. Moreover, $f(x) = cx + \mathrm{Tr}_{q^2/q}(x^{2q-1}) = cx = d$. Hence $x = \frac{d}{c}$ is the unique solution of $f(x) = d$ in $\mathbb{F}_{q^2}$.

If $d \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, then $u + d = 0$ is impossible. And $x^{2q-1} = c^{4q-2}(u+d)^{2q-1} = \frac{u^2+d^{2q}}{u+d}$ thanks to $c^q = c^2$. Then plugging the above expressions of $x$ and $x^{2q-1}$ into $f(x) = d$, we get

$$u + \frac{u^2 + d^{2q}}{u + d} + \frac{u^2 + d^2}{u + d^q} = 0,$$

i.e.,

$$u^3 + \left(d^{q+1} + d^{2q} + d^2\right)u + d^{3q} + d^3 = 0. \tag{3}$$

Let $e = d^{q-1}$ and $g(x) = x^2 + x + \frac{e}{e^2+1}$. Then it is easy to verify that $e \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$. Considering the equation $g(x) = 0$, we get

$$g(x) = \left(x + \frac{1}{e+1}\right)\left(x + \frac{e}{e+1}\right) = 0.$$

Then $\frac{1}{e+1}, \frac{e}{e+1}$ are the solutions of $g(x) = 0$ in $\mathbb{F}_{q^2}$. Thanks to $\frac{1}{e+1}, \frac{e}{e+1} \notin \mathbb{F}_q$, $g(x) = 0$ has no solution in $\mathbb{F}_q$. Therefore, according to Lemma 2.2,

$$\mathrm{Tr}_q\left(\frac{e}{e^2+1}\right) = 1. \tag{4}$$

Let us return to (3): $u^3+au+b=0$, where $a=d^2\left(e^2+e+1\right)$ and $b=d^3\left(e^3+1\right)$. Then

$$\begin{aligned}\mathrm{Tr}_q\left(\frac{a^3}{b^2}+1\right) &= \mathrm{Tr}_q\left[\frac{\left(e^2+e+1\right)^3}{\left(e^3+1\right)^2}+1\right]\\ &= \mathrm{Tr}_q\left(\frac{e^2+e+1}{e^2+1}+1\right)\\ &= \mathrm{Tr}_q\left(\frac{e}{e^2+1}\right)=1.\end{aligned}$$

Therefore, according to Lemma 2.3, (3) only has one solution in $\mathbb{F}_q$. Then $f(x)=d$ has at most one solution in $\mathbb{F}_{q^2}$. We finish the proof. □

**Theorem 3.7** *Let $q=2^k$, where $k>0$ is even. Let $a=\frac{(3q-2)\left(q^2+q+1\right)}{3}$ and $f(x)=cx+\mathrm{Tr}_{q^2/q}\left(x^a\right)\in\mathbb{F}_{q^2}[x]$, where $c^3=1$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $g(x)=f\left(x^{q-2}\right)=cx^{q-2}+x^{2q-3}+x^{2-3q}=x^{q-2}h(x^{q-1})$, where $h(x)=c+x+x^{-4}$. If $g(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$, then $f(x)$ also permutes $\mathbb{F}_{q^2}$ since $\gcd\left(q-2,q^2-1\right)=\gcd(q-2,3)=1$. From Lemma 2.1, it suffices to show that the fractional polynomial

$$p(x)=x^{q-2}h(x)^{q-1}=\frac{x^5+cx+1}{x^5+cx^4+1}$$

permutes $\mu_{q+1}$. If $c=1$, then $p(x)=\frac{x^3+x^2+1}{x^3+x+1}$, one can refer the proof in [25].

If $c\neq 1$, $p(x)$ can not be simplified. However, we can also prove that $p(x)$ permutes $\mu_{q+1}$. Assume that there exist two distinct elements $x_1,x_2\in\mu_{q+1}$ such that

$$\frac{x_1^5+cx_1+1}{x_1^5+cx_1^4+1}=\frac{x_2^5+cx_2+1}{x_2^5+cx_2^4+1}.$$

Let $u=x_1+x_2$ and $v=x_1x_2$. Simplifying the above equation, we obtain

$$(1+v)u^3+cvu^2+v^4+cv^2+1=0. \tag{5}$$

Let $y=u^{-1}\neq 0$. The following relationship between $u$ and $v$ will be employed in the sequel. And for convenience, we will use it directly in the following.

$$u^q=x_1^q+x_2^q=\frac{1}{x_1}+\frac{1}{x_2}=\frac{x_1+x_2}{x_1x_2}=\frac{u}{v}.$$

Then $v=u^{1-q}=y^{q-1}$ and $u=y^{-1}$. Substituting $y^{q-1}$ and $y^{-1}$ for $u$ and $v$ respectively in (5), we have

$$y^q+y+cy^{q+1}+y^{4q}+cy^{2q+2}+y^4=0. \tag{6}$$

Let $\alpha=y+y^q$ and $\beta=y^{q+1}$. Then $\alpha,\beta\in\mathbb{F}_q$. Plugging them into the above equation, we get

$$\alpha+\alpha^4+c\beta+c\beta^2=0, \tag{7}$$

i.e.,

$$\beta^2+\beta+c^2\alpha^4+c^2\alpha=0.$$

Then $\beta=c\alpha^2+c^2\alpha$ or $c\alpha^2+c^2\alpha+1$. If $\beta=c\alpha^2+c^2\alpha$, recalling that $u=x_1+x_2$ and $v=x_1x_2$, we know $x_1,x_2$ are the solutions of $x^2+ux+v=0$, i.e., $(yx)^2+yx+y^{q+1}=0$.

That is $(yx)^2 + yx + c\alpha^2 + c^2\alpha = 0$. Without loss of generality, let $x_1 = c^2(1 + y^{q-1})$ and $x_2 = c^2(1 + y^{q-1}) + y^{-1}$. Since $x_2 \in \mu_{q+1}$, we have

$$x_2^{q+1} = \left[c^2\left(1+y^{1-q}\right)+y^{-q}\right]\left[c^2\left(1+y^{q-1}+y^{-1}\right)\right] = c\left(y^{1-q}+y^{q-1}\right)+y^{-1-q} = 1.$$

Hence, $y^{q+1} = c\left(y^2 + y^{2q}\right) + 1$, i.e., $\beta = c\alpha^2 + 1$. However, $\beta = c\alpha^2 + c^2\alpha$. Then $c^2\alpha = 1$, $\alpha = c$ and $\beta = y = 0$. It is a contradiction.

If $\beta = c\alpha^2 + c^2\alpha + 1$, $x_1$ and $x_2$ are the solutions of $(yx)^2 + yx + c\alpha^2 + c^2\alpha + 1 = 0$. Without loss of generality, let $x_1 = c^2(1 + y^{q-1}) + cy^{-1}$ and $x_2 = c^2(1 + y^{q-1}) + c^2y^{-1}$. Similarly, we can check that it is impossible in the case.

Therefore, $p(x)$ permutes $\mu_{q+1}$. It follows from Lemma 2.1 that $f(x)$ permutes $\mathbb{F}_{q^2}$. We complete the proof. □

**Theorem 3.8** *Let $q = 2^k$, where $k > 0$ is odd. Let $a = \frac{(3q^2-2)(q+4)}{5}$ and $f(x) = cx + \mathrm{Tr}_{q^2/q}(x^a) \in \mathbb{F}_{q^2}[x]$, where $c^3 = 1$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $g(x) = f(x^5) = cx + \mathrm{Tr}_{q^2/q}\left(x^{q+4}\right)$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$ if and only if $g(x)$ permutes $\mathbb{F}_{q^2}$ since $\gcd(5, q^2 - 1) = \gcd\left(5, 4^{2k+1} - 1\right) = \gcd(5, 2) = 1$. According to Lemma 2.1, it suffices to show that the fractional polynomial

$$p(x) = \frac{c^2x^5 + x^4 + x}{x^4 + x + c}$$

permutes $\mu_{q+1}$. Assume that there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that

$$\frac{c^2x_1^5 + x_1^4 + x_1}{x_1^4 + x_1 + c} = \frac{c^2x_2^5 + x_2^4 + x_2}{x_2^4 + x_2 + c}.$$

Let $u = x_1 + x_2$ and $v = x_1x_2$. After simplifying the above equation, we get

$$u^4 + \left(c^2v + c\right)u^3 + vu^2 + c^2v^4 + v^2 + c = 0.$$

Let $y = u^{-1}$. Then $u = y^{-1}$ and $v = y^{q-1}$. Plugging them into the above equation, we yield

$$1 + c^2y^q + cy + y^{q+1} + y^{2q+2} + cy^4 + c^2y^{4q} = 0.$$

Then

$$\mathrm{Tr}_q\left(1 + c^2y^q + cy + y^{q+1} + y^{2q+2} + cy^4 + c^2y^{4q}\right) = 0.$$

However, we also have

$$\begin{aligned}&\mathrm{Tr}_q\left(c^2y^q + cy + y^{q+1} + y^{2q+2} + cy^4 + c^2y^{4q}\right)\\ &\quad= \mathrm{Tr}_q\left[cy + c^2y^q + \left(cy + c^2y^q\right)^4 + y^{q+1} + y^{2q+2}\right] = 0.\end{aligned}$$

It follows that $\mathrm{Tr}_q(1) = 0$, which contradicts the assumption that $k$ is odd. Hence, $p(x)$ permutes $\mu_{q+1}$.

Therefore, $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$. □

**Theorem 3.9** *Let $q = 2^k$, $a = 2^{2k-2} + 3 \cdot 2^{k-2}$, $c \in \mathbb{F}_q$ and the equation $x^3 + x + c = 0$ has no solution in $\mathbb{F}_q$. Then $f(x) = cx + \mathrm{Tr}_{q^2/q}(x^a)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $g(x) = f(x^4) = cx^4 + \mathrm{Tr}_{q^2/q}\left(x^{3q+1}\right) = cx^4 + x^{3q+1} + x^{3+q} = x^4(c + x^{3q-3} + x^{q-1}) = x^4 h\left(x^{q-1}\right)$, where $h(x) = c + x + x^3$. Because of $\gcd\left(4, q^2-1\right) = 1$, it suffices to show that $g(x)$ permutes $\mathbb{F}_{q^2}$. In the following, we will prove that

$$p(x) = x^4 h(x)^{q-1} = \frac{cx^4 + x^3 + x}{x^3 + x + c}$$

permutes $\mu_{q+1}$.

If the assertion would not hold, then there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that $p(x_1) = p(x_2)$. We have

$$\frac{cx_1^4 + x_1^3 + x_1}{x_1^3 + x_1 + c} = \frac{cx_2^4 + x_2^3 + x_2}{x_2^3 + x_2 + c}.$$

Let $u = x_1 + x_2$ and $v = x_1 x_2$. After simplifying the above equation and substituting $u$ and $v$ for $x_1 + x_2$ and $x_1 x_2$ respectively, we obtain

$$cu^3 + (v+1)u^2 + v^3 + v^2 + v + 1 = 0. \tag{8}$$

Let $y = u^{-1}$. Then $u = y^{-1}$, $v = y^{q-1}$ and we have

$$c + y^q + y + y^{3q} + y^{2q+1} + y^{q+2} + y^3 = 0,$$

i.e.,

$$\alpha^3 + \alpha + c = 0,$$

where $\alpha = y + y^q \in \mathbb{F}_q$. This leads to a contradiction thanks to our assumption on $c$.

Thus we conclude that $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$ according to Lemma 2.1. □

**Theorem 3.10** *Let $q = 2^k$ and $f(x) = x + \mathrm{Tr}_{q^2/q}(x^a)$, where*

$$a = \begin{cases} \frac{(2q^2-1)(q+6)}{7}, & \text{if} \quad k \equiv 1 \pmod 3; \\ -\frac{(q^2-2)(q+6)}{7}, & \text{if} \quad k \equiv 2 \pmod 3. \end{cases}$$

*Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Put $g(x) = f(x^7) = x^7 + x^{6q+1} + x^{q+6} = x^7 h(x^{q-1})$,where $h(x) = 1 + x + x^6$. We show that

$$p(x) = x^7 h(x)^{q-1} = \frac{x^7 + x^6 + x}{x^6 + x + 1}$$

permutes $\mu_{q+1}$ when $k \not\equiv 0 \pmod 3$. If there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that

$$\frac{x_1^7 + x_1^6 + x_1}{x_1^6 + x_1 + 1} = \frac{x_2^7 + x_2^6 + x_2}{x_2^6 + x_2 + 1}.$$

Let $u = x_1 + x_2$ and $v = x_1 x_2$. We get

$$u^6 + (1+v)u^5 + vu^4 + (v^3 + v^2)u + v^6 + v^3 + 1 = 0.$$

Denote $y = u^{-1}$. Then $u = y^{-1}$ and $v = y^{q-1}$. Let $\alpha = y + y^q$ and $\beta = y^{1+q}$. Then we have

$$\beta^3 + (\alpha^2 + \alpha)\beta^2 + \beta + \alpha^6 + \alpha + 1 = 0. \tag{9}$$

Let $\gamma = \beta + \alpha^2 + \alpha$. Then we get

$$\gamma^3 + a\gamma + b = 0, \tag{10}$$

where

$$\begin{aligned} a &= \alpha^4 + \alpha^2 + 1, \\ b &= \alpha^6 + \alpha^2 + 1. \end{aligned}$$

Now we compute the number of the solution of (10).

Since

$$\begin{aligned} \frac{a^3}{b^2} &= \frac{\left(\alpha^4 + \alpha^2 + 1\right)^3}{\left(\alpha^6 + \alpha^2 + 1\right)^2} \\ &= 1 + \frac{\alpha^{10} + \alpha^6 + \alpha^4 + \alpha^2}{\alpha^{12} + \alpha^4 + 1} \\ &= 1 + \frac{\alpha^4}{\alpha^6 + \alpha^2 + 1} + \frac{\alpha^8}{\alpha^{12} + \alpha^4 + 1} + \frac{\alpha^2}{\alpha^6 + \alpha^2 + 1} + \frac{\alpha^4}{\alpha^{12} + \alpha^4 + 1} \\ &= \left(w + \frac{\alpha^4 + \alpha^2}{\alpha^6 + \alpha^2 + 1}\right) + \left(w + \frac{\alpha^4 + \alpha^2}{\alpha^6 + \alpha^2 + 1}\right)^2, \end{aligned}$$

where $w^3 = 1$ and $w \neq 1$, $\mathrm{Tr}_q\left(\frac{a^3}{b^2} + 1\right) = 0$. According to Lemma 2.3, (10) has no solution or three solutions in $\mathbb{F}_q$. In the following, we claim that (10) has one solution which is not in $\mathbb{F}_q$. Then it follows that (10) has no solution in $\mathbb{F}_q$.

The quadratic derived equation of (10) is

$$t^2 + bt + a^3 = 0. \tag{11}$$

Let $t = bz$. Plugging it into the above equation, we get

$$z^2 + z + \frac{a^3}{b^2} = z^2 + z + \left(w + \frac{\alpha^4 + \alpha^2}{\alpha^6 + \alpha^2 + 1}\right) + \left(w + \frac{\alpha^4 + \alpha^2}{\alpha^6 + \alpha^2 + 1}\right)^2 = 0.$$

Then $z = w + \frac{\alpha^4 + \alpha^2}{\alpha^6 + \alpha^2 + 1}$ and $t = bz = \left(\alpha^6 + \alpha^2 + 1\right) w + \alpha^4 + \alpha^2 = w\left(w\alpha^2 + 1\right)^3$. Thus $\epsilon^3 = t$ has the solution $\epsilon = \sigma(w\alpha^2 + 1)$, where $\sigma^3 = w$, i.e., $\sigma^9 = 1$ and $\sigma^3 \neq 1$. Therefore,

$$\begin{aligned} \epsilon + \frac{\alpha^4 + \alpha^2 + 1}{\epsilon} &= \sigma(w\alpha^2 + 1) + \sigma^8(w^2\alpha^2 + 1) \\ &= (\sigma^4 + \sigma^5)\alpha^2 + \sigma + \sigma^8 \\ &= e^4\alpha^2 + e, \end{aligned}$$

where $e = \sigma + \frac{1}{\sigma}$, is one solution of (10). Next we show that $e^4\alpha^2 + e \notin \mathbb{F}_q$. The following of the proof is split into two cases.

**Case I**: $k \equiv 1 \pmod 3$.

Let $k = 3l + 1$. Since $\sigma^q = (\sigma^{8^l})^2 = \sigma^{\pm 2}$, $e^q = \sigma^2 + \frac{1}{\sigma^2} = e^2$. Then $(e^4\alpha^2 + e)^q = e^8\alpha^2 + e^2$. If $e^4\alpha^2 + e \in \mathbb{F}_q$, then $e^4\alpha^2 + e = e^8\alpha^2 + e^2$. Therefore, we get

$$\alpha^2 = \frac{e^2 + e}{e^8 + e^4}.$$

It follows from $\alpha^2 \in \mathbb{F}_q$ that

$$\alpha^{2q} = \frac{e^4 + e^2}{e^{16} + e^8} = \frac{e^2 + e}{e^8 + e^4},$$

i.e., $\alpha^4 = \alpha^2, \alpha = 1$. Then according to (9), we have $\beta^3 + \beta + 1 = 0$. So $\beta \in \mathbb{F}_{2^3} \cap \mathbb{F}_q = \mathbb{F}_2$, i.e., $\beta = 1$. Moreover, we have $y^2 + y + 1 = 0$, $y^3 = 1$ since $y + y^q = 1$ and $y^{q+1} = 1$. Due to $y \notin \mathbb{F}_q$ and $y^3 = 1$, $k$ is odd. So $v = y^{q-1} = y$. On the other hand, $x_1, x_2 \in \mathbb{F}_{q^2}$ is the solutions of $x^2 + ux + v = 0$, i.e., $x^2 + y^{-1}x + y = 0$. According to Lemma 2.2 and $\mathrm{Tr}_q\left(\frac{v}{u^2}\right) = \mathrm{Tr}_q\left(y^3\right) = \mathrm{Tr}_q(1) = 1$, we know that the equation $x^2 + ux + v = 0$ has no solution in $\mathbb{F}_{q^2}$. It is impossible. Hence, in the case, $e^4\alpha^2 + e \notin \mathbb{F}_q$.

**Case II**: $k \equiv 2 \pmod 3$.

This case can be proved similarly as **Case I**. We omit it here.

Hence (10) has a solution which is not in $\mathbb{F}_q$. It follows that $p(x)$ permutes $\mu_{q+1}$ when $k \not\equiv 0 \pmod 3$. Moreover, $g(x)$ permutes $\mathbb{F}_{q^2}$ according to Lemma 2.1, so does $f(x)$ since $\gcd(7, q^2 - 1) = 1$ when $k \not\equiv 0 \pmod 3$. □

**Theorem 3.11** *Let $q = 2^k$, where $k$ is odd. Let $a = \frac{2^{2k-1}+3\cdot 2^{k-1}+1}{3}$ and $f(x) = cx + \mathrm{Tr}_{q^2/q}(x^a) \in \mathbb{F}_{q^2}[x]$, where $c^{\frac{q+1}{3}} = 1$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $h(x) = c + x^{\frac{2^{k-1}+2}{3}} + x^{\frac{1-2^{k-1}}{3}}$. Then $f(x) = cx + x^{\frac{2^{k-1}+2}{3}(2^k-1)+1} + x^{\frac{1-2^{k-1}}{3}(2^k-1)+1} = xh(x^{q-1})$. Let $p(x) = xh(x)^{q-1}$. Then for $x \in \mu_{q+1}$, we have

$$p(x) = x\frac{c^{-1} + x^{-\frac{2^{k-1}+2}{3}} + x^{\frac{2^{k-1}-1}{3}}}{c + x^{\frac{2^{k-1}+2}{3}} + x^{\frac{1-2^{k-1}}{3}}} = \frac{c^{-1}x^{\frac{2^{k-1}+2}{3}} + x^{\frac{2^k+1}{3}} + 1}{cx^{\frac{2^{k-1}-1}{3}} + x^{\frac{2^k+1}{3}} + 1}.$$

Let $p_1(x) = p(x)^2$. In the following, we show that $p_1(x)$ permutes $\mu_{q+1}$. Then according to Lemma 2.1 and $\gcd(2, q + 1) = 1$, we can conclude that $f(x)$ permutes $\mathbb{F}_{q^2}$.

Let $y = x^{\frac{2^k+1}{3}}$. Obviously, $y^3 = 1$. And we have

$$p_1(x) = \frac{yx^2 + c^2\left(y^2 + 1\right)x}{c^4 y + c^2\left(y^2 + 1\right)x}.$$

Let $S_1 = \{x : x \in \mu_{q+1}, y = 1\}$ and $S_2 = \{x : x \in \mu_{q+1}, y \neq 1\}$. Assume there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that $p_1(x_1) = p_1(x_2)$. The following proof is divided into four cases.

**Case I**: $x_1, x_2 \in S_1$.

Then $p_1(x_1) = \frac{1}{c^4}x_1^2$ and $p_1(x_2) = \frac{1}{c^4}x_2^2$. It is clear that we can conclude $x_1 = x_2$ from $p_1(x_1) = p_1(x_2)$, a contradiction.

**Case II**: $x_1, x_2 \in S_2$.

Then $p_1(x_1) = \frac{1}{c^2}x_1$ and $p_1(x_2) = \frac{1}{c^2}x_2$. We have $x_1 = x_2$ from $p_1(x_1) = p_1(x_2)$, which is also impossible.

**Case III**: $x_1 \in S_1$ and $x_2 \in S_2$.

Then $p_1(x_1) = \frac{1}{c^4}x_1^2$ and $p_1(x_2) = \frac{1}{c^2}x_2$. So $x_2 = \frac{1}{c^2}x_1^2$. But $x_2^{\frac{q+1}{3}} = \left(\frac{1}{c^2}x_1^2\right)^{\frac{q+1}{3}} = 1$, which is a contradiction with $x_2 \in S_2$.

**Case IV**: $x_1 \in S_2$ and $x_2 \in S_1$.
This case is similar as Case III.
Hence, $p_1(x)$ permutes $\mu_{q+1}$. Moreover, $f(x)$ permutes $\mathbb{F}_{q^2}$. □

**Theorem 3.12** *Let $q = 2^k$ and $k$ be even. Then $f(x) = x + \mathrm{Tr}_{q^2/q}\left(x^{\frac{q^2-2q+4}{3}}\right)$ is a permutation polynomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $h(x) = 1 + x^{\frac{q-1}{3}} + x^{\frac{4-q}{3}}$. Then $f(x) = x + x^{\frac{q-1}{3}(q-1)+1} + x^{\frac{4-q}{3}(q-1)+1} = xh(x^{q-1})$. According to Lemma 2.1, it suffices to show that

$$p(x) = xh(x)^{q-1} = x\frac{1 + x^{\frac{1-q}{3}} + x^{\frac{q-4}{3}}}{1 + x^{\frac{q-1}{3}} + x^{\frac{4-q}{3}}}$$

permutes $\mu_{q+1}$. Let $p_1(x) = p(x^3)$. Since $\gcd(3, q+1) = 1$, we only need to consider $p_1(x)$ whether permutes $\mu_{q+1}$. A direct computation leads to

$$p_1(x) = \frac{x^5 + x^4 + x^3 + x + 1}{x^5 + x^4 + x^2 + x + 1}.$$

Assume there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that $p_1(x_1) = p_1(x_2)$. Let $u = x_1 + x_2$ and $v = x_1x_2$. After a lengthy but direct computation, we get

$$\left(v^2 + 1\right)u^2 + (v+1)^3 u + v^2 = 0.$$

Obviously, we have $v \neq 1$ from the above equation. Multiplying both sides of $\frac{1}{v^4+1}$ yields

$$\left(\frac{u}{v+1}\right)^2 + \frac{u}{v+1} + \frac{1}{v^2+1} + \frac{1}{v^4+1} = 0. \tag{12}$$

Then $u = \frac{1}{v+1}$ or $u = \frac{1}{v+1} + v + 1$. If $u = \frac{1}{v+1}$, then $u^q = \frac{1}{v^q+1} = \frac{v}{v+1}$. However, $u^q = x_1^q + x_2^q = \frac{1}{x_1} + \frac{1}{x_2} = \frac{u}{v}$. So $\frac{v}{v+1} = \frac{u}{v} = \frac{1}{v^2+v}$, i.e., $v^2 = 1$, a contradiction. If $u = \frac{1}{v+1} + v + 1$, we can also obtain $v^2 = 1$, which is impossible. Thus $p_1(x)$ permutes $\mu_{q+1}$.
Hence, $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^2}$. The proof is complete. □

The following theorem is proved by the multivariate method.

**Theorem 3.13** *Let $q = 2^k$, $a = 2^{4k-1} - 2^{3k-1} + 2^{2k-1} + 2^{k-1}$ and $c \in \mathbb{F}_q^*$. Then $f(x) = cx + \mathrm{Tr}_{q^4/q^2}(x^a)$ is a permutation polynomial over $\mathbb{F}_{q^4}$.*

*Proof* Let $g(x) = f(x^2) = cx^2 + \mathrm{Tr}_{q^4/q^2}\left(x^{2a}\right) = cx^2 + x^{q^4-q^3+q^2+q} + x^{q^3+q^2-q+1}$. It suffices to show that $g(x)$ permutes $\mathbb{F}_{q^4}$.

First of all, we claim that $g(x) = 0$ only has zero solution in $\mathbb{F}_{q^4}$. If $g(x) = 0$, then either $x = 0$ or $c + x^{-q^3+q^2+q-1} + x^{q^3+q^2-q-1} = 0$. So we only need to prove the equation

$$c + x^{-q^3+q^2+q-1} + x^{q^3+q^2-q-1} = 0 \tag{13}$$

has no solution in $\mathbb{F}_{q^4}^*$. Raising (13) to its $q$-th power leads to

$$c + x^{q^3+q^2-q-1} + x^{q^3-q^2-q+1} = 0. \tag{14}$$

Adding (13) and (14), we have

$$x^{-q^3+q^2+q-1} = x^{q^3-q^2-q+1},$$

i.e.,

$$x^{q^3-q^2-q+1} = 1.$$

Since $\gcd\left(q^3 - q^2 - q + 1, q^4 - 1\right) = q^2 - 1$, we have $x \in \mathbb{F}_{q^2}$. Plugging it into (13), we get $c = 0$, which is contradiction. Thus $g(x) = 0$ only has zero solution in $\mathbb{F}_{q^4}$.

Next, we show that $g(x) = \alpha$ has at most one solution in $\mathbb{F}_{q^4}$ for any $\alpha \in \mathbb{F}_{q^4}^*$. Obviously, $x = 0$ is not a solution of $g(x) = \alpha$ if $\alpha \neq 0$. Let $y = x^q$, $z = y^q$, $w = z^q$, $\beta = \alpha^q$, $\gamma = \beta^q$ and $\delta = \gamma^q$. Then $x, y, z, w, \alpha, \beta, \gamma, \delta \neq 0$, and we have

$$cx^2 + \frac{xyz}{w} + \frac{xzw}{y} = \alpha. \tag{15}$$

Raising (15) into its $q$-th, $q^2$-th and $q^3$-th power, we get the following equations respectively.

$$cy^2 + \frac{yzw}{x} + \frac{xyw}{z} = \beta, \tag{16}$$

$$cz^2 + \frac{xzw}{y} + \frac{xyz}{w} = \gamma \tag{17}$$

and

$$cw^2 + \frac{xyw}{z} + \frac{yzw}{x} = \delta. \tag{18}$$

We compute the sum of (15) and (17), and get $z = x + B$, where $B = \left(\frac{\alpha+\gamma}{c}\right)^{\frac{1}{2}}$. Likely, we have $w = y + A$, where $A = \left(\frac{\beta+\delta}{c}\right)^{\frac{1}{2}}$ through adding (16) and (18). Plugging $z = x + B$ and $w = y + A$ into (15) and (16) and then simplifying, we obtain

$$\left(\alpha + cx^2\right) y^2 + \left(\alpha A + cAx^2\right) y + BA^2x + A^2x^2 = 0 \tag{19}$$

and

$$\left(B^2 + Bcx + cx^2\right) y^2 + B^2Ay + \beta x(B + x) = 0. \tag{20}$$

Computing (19) $*B^2+$ (20) $*\left(\alpha + cx^2\right)$, we yield

$$D_1 y^2 = D_0, \tag{21}$$

where

$$D_1 = c\left(\alpha + cx^2\right)$$

and

$$D_0 = B^2A^2 + \alpha\beta + \beta cx^2.$$

We compute (19) $*c+$ (21), we get

$$D_3 y = D_2, \tag{22}$$

where

$$D_3 = cA\left(\alpha + cx^2\right)$$

and

$$D_2 = B^2A^2 + \alpha\beta + cBA^2x + cA^2x^2 + \beta cx^2.$$

If $\alpha + cx^2 = 0$, then $x = \left(\frac{\alpha}{c}\right)^{\frac{1}{2}}$. Then $g(x) = \alpha$ has at most one solution in $\mathbb{F}_{q^4}$. Otherwise, computing (22) $^2$/ (21) and simplifying it, we obtain

$$D_5 x^4 = D_4,$$

where

$$D_5 = \beta A^2 c^3 + c^2 A^4 + \beta^2 c^2$$

and

$$D_4 = B^4 A^4 + \alpha^2 \beta^2 + \alpha^2 \beta A^2 c + \alpha B^2 A^4 c.$$

We claim that $D_5 \neq 0$ when $\beta \neq 0$. If $D_5 = 0$, then we have

$$\beta^2 + \delta^2 + c^2 \beta \delta = 0. \tag{23}$$

Let $t = \frac{\delta}{\beta}$. Then $c^2 = t + \frac{1}{t} \in \mathbb{F}_q$. Thus $\left(t + \frac{1}{t}\right)^q = t + \frac{1}{t}$, i.e., $\left(t^{q+1} + 1\right)\left(t^{q-1} + 1\right) = 0$. Therefore, $t^{q+1} = 1$ or $t^{q-1} = 1$. In the first case, $\beta^{(q^2-1)(q-1)} = 1$. Due to $\gcd\left(q^4 - 1, \left(q^2 - 1\right)(q-1)\right) = q^2 - 1$, $\beta \in \mathbb{F}_{q^2}$. Then $\delta = \beta$. Moreover, it follows that $c = 0$ from (23), which is a contradiction. The other case is the same as the first one, we omit it here.

Above all, $x^4 = \frac{D_4}{D_5}$. Thus, $g(x) = \alpha$ has at most one solution in $\mathbb{F}_{q^4}$. We finish the proof. □

## 4 Permutation trinomials

In this section, we construct four classes of permutation trinomials over finite fields with even characteristic.

**Theorem 4.1** *Let $q = 2^k$, $k \geq 1, l$ be integers and $f(x) = x^{lq+l+3} + x^{(l+6)q+l-3} + x^{(l-2)q+l+5}$. Then $f(x)$ is a permutation trinomial over $\mathbb{F}_{q^2}$ if* $\gcd(3 + 2l, q - 1) = 1$ *and* $k \not\equiv 0 \pmod 4$.

*Proof* Let $h(x) = 1 + x^6 + x^{-2}$. Then $f(x) = x^{lq+l+3} h(x^{q-1})$. According to Lemma 2.1, $f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(lq + l + 3, q - 1) = 1$,i.e., $\gcd(3 + 2l, q - 1) = 1$ and

$$p(x) = x^{3+lq+l} h(x)^{q-1} = \frac{x^8 + x^6 + 1}{x^9 + x^3 + x}$$

permutes $\mu_{q+1}$. Assume that there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that

$$\frac{x_1^8 + x_1^6 + 1}{x_1^9 + x_1^3 + x_1} = \frac{x_2^8 + x_2^6 + 1}{x_2^9 + x_2^3 + x_2}.$$

After a complex computation and substituting $u$ and $v$ for $x_1 + x_2$ and $x_1 x_2$ respectively, we get

$$u^8 + (v^3 + v)u^4 + (v^6 + v^4 + v^3 + v^2 + 1)u^2 + v^8 + v^7 + v^5 + v^4 + v^3 + v + 1 = 0. \tag{24}$$

Let $y = u^{-1}$. Then $u = y^{-1}$ and $v = y^{q-1}$. Plugging them into (24), we obtain

$$\beta^4 + \beta^3 + (\alpha^6 + \alpha^2)\beta + \alpha^8 + \alpha^6 + 1 = 0, \tag{25}$$

where

$$\begin{aligned} \beta &= y^{q+1}, \\ \alpha &= y + y^q. \end{aligned}$$

Let $g(x) = x^4 + x^3 + (\alpha^6 + \alpha^2)x + \alpha^8 + \alpha^6 + 1 \in \mathbb{F}_q[x]$. In the following, we prove that $g(x)$ has no root in $\mathbb{F}_q$ when $k \not\equiv 0 \pmod 4$. The rest of the proof is split into two cases.

**Case I: $k$ is odd.**

We show that $g(x)$ is an irreducible polynomial. Let $g_1(x) = x^4 g\left(\frac{1}{x} + \alpha^3 + \alpha\right)$. Then we can compute

$$g_1(x) = a_1 x^4 + a_2 x^2 + x + 1,$$

where

$$\begin{aligned} a_1 &= \alpha^{12} + \alpha^8 + \alpha^6 + \alpha^4 + 1, \\ a_2 &= \alpha^3 + \alpha. \end{aligned}$$

We claim that $a_1 \neq 0$ for any $\alpha \in \mathbb{F}_q$. Otherwise, there exists $\alpha \in \mathbb{F}_q$ such that $a_1 = 0$. Then

$$\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0,$$

i.e.,

$$\left(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1\right)\left(\alpha^2 + \alpha + 1\right) = 0.$$

Thus, $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$ or $\alpha^2 + \alpha + 1 = 0$. In the first case, let $\alpha_1 = \alpha + 1$. Then $\alpha_1^4 + \alpha_1^3 = 1$. Moreover, we have

$$\left(\frac{1}{\alpha_1}\right)^4 + \frac{1}{\alpha_1} = 1. \tag{26}$$

Raising the above equation to its 4-th power, we obtain

$$\left(\frac{1}{\alpha_1}\right)^{16} + \left(\frac{1}{\alpha_1}\right)^4 = 1. \tag{27}$$

Computing (26) + (27) , we get $\left(\frac{1}{\alpha_1}\right)^{15} = 1$. Then thanks to $\gcd(15, q-1) = 1$ when $k$ is odd, we get $\alpha_1 = 1$. However $\alpha_1 = 1$ is not the solution of (26). Therefore, $\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 \neq 0$. In the other case, let $t(\alpha) = \alpha^2 + \alpha + 1 \in \mathbb{F}_q[\alpha]$. Obviously, $t(\alpha)$ is irreducible in $\mathbb{F}_2[\alpha]$. Thanks to $\gcd(2, k) = 1$, $t(\alpha)$ is also irreducible in $\mathbb{F}_q[\alpha]$. So, $\alpha^2 + \alpha + 1 \neq 0$ for any $\alpha \in \mathbb{F}_q$. Hence, $a_1 \neq 0$.

Next we let $g_2(x) = \frac{1}{a_1} g_1(x) = x^4 + \frac{a_2}{a_1} x^2 + \frac{1}{a_1} x + \frac{1}{a_1} \in \mathbb{F}_q[x]$. Then it suffices to show that $g_2(x)$ is irreducible in $\mathbb{F}_q[x]$. Let us consider the cubic equation

$$y^3 + \frac{a_2}{a_1} y + \frac{1}{a_1} = 0. \tag{28}$$

Then the quadratic derived equation of (28) is

$$t^2 + \frac{1}{a_1} t + \left(\frac{a_2}{a_1}\right)^3 = 0. \tag{29}$$

Let $t = \frac{1}{a_1} z$. Then $z^2 + z + \frac{a_2^3}{a_1} = 0$. In fact,

$$\begin{aligned} \frac{a_2^3}{a_1} &= \frac{\left(\alpha^3 + \alpha\right)^3}{\alpha^{12} + \alpha^8 + \alpha^6 + \alpha^4 + 1} \\ &= \frac{\alpha^9 + \alpha^7 + \alpha^5 + \alpha^3}{\alpha^{12} + \alpha^8 + \alpha^6 + \alpha^4 + 1} \\ &= \frac{\alpha^3}{\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1} + \left(\frac{\alpha^3}{\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1}\right)^2. \end{aligned}$$

On one hand, for (28), we have $\mathrm{Tr}_q\left(\frac{(a_2/a_1)^3}{(1/a_1)^2}+1\right)=\mathrm{Tr}_q\left(\frac{a_2^3}{a_1}+1\right)=1$. According to Lemma 2.3, (28) only has one solution in $\mathbb{F}_q$. On the other hand, for (29),

$$\begin{aligned} t_1 &= \frac{1}{\alpha^{12}+\alpha^8+\alpha^6+\alpha^4+1}\cdot\left(\frac{\alpha^3}{\alpha^6+\alpha^4+\alpha^3+\alpha^2+1}\right)\\ &= \left(\frac{\alpha}{\alpha^6+\alpha^4+\alpha^3+\alpha^2+1}\right)^3, \end{aligned}$$

is one solution of (29). Let $\epsilon=\frac{\alpha}{\alpha^6+\alpha^4+\alpha^3+\alpha^2+1}$ be a solution of $x^3=t_1$. Then

$$r=\epsilon+\frac{a_2}{a_1\epsilon}=\frac{1}{\alpha^4+\alpha^3+\alpha^2+\alpha+1}$$

is the unique solution of (28) in $\mathbb{F}_q$. In the following, we compute

$$\begin{aligned} \mathrm{Tr}_q\left(a_1r^2\right) &= \mathrm{Tr}_q\left[\left(\alpha^{12}+\alpha^8+\alpha^6+\alpha^4+1\right)\left(\frac{1}{\alpha^4+\alpha^3+\alpha^2+\alpha+1}\right)^2\right]\\ &= \mathrm{Tr}_q\left(\alpha^4+\alpha^2+1\right)\\ &= 1. \end{aligned}$$

According to Lemma 2.5, in the Case $k$ is odd, $g(x)$ is irreducible in $\mathbb{F}_q[x]$. Particularly, $g(x)$ has no roots in $\mathbb{F}_q$.

**Case II:** $k\equiv 2 \pmod 4$**.**

Assume that $\omega$ satisfies $\omega^2+\omega=1$. Then $g(x)=G_1(x)G_2(x)$, where

$$\begin{aligned} G_1(x) &= x^2+(\alpha+\omega)x+\omega^2\alpha^2+\omega\alpha+\omega,\\ G_2(x) &= x^2+(\alpha+\omega^2)x+\omega\alpha^2+\omega^2\alpha+\omega^2. \end{aligned}$$

We have

$$\begin{aligned} \mathrm{Tr}_q\left(\frac{\omega^2\alpha^2+\omega\alpha+\omega}{\alpha^2+\omega^2}\right) &= \mathrm{Tr}_q\left(\frac{\omega\alpha}{\alpha^2+\omega^2}+\omega^2\right)\\ &= \mathrm{Tr}_q\left(\frac{\omega\alpha}{\alpha^2+\omega^2}\right)+1\\ &= \mathrm{Tr}_q\left(\frac{\omega}{\alpha+\omega}+\frac{\omega^2}{\alpha^2+\omega^2}\right)+1\\ &= 1, \end{aligned}$$

since

$$\mathrm{Tr}_q(\omega)=\underbrace{\omega+\omega^2+\cdots+\omega+\omega^2}_{k}=\underbrace{1+\cdots+1}_{\frac{k}{2}}=\frac{k}{2}=1$$

when $k\equiv 2 \pmod 4$. Hence $G_1(x)$ has no roots in $\mathbb{F}_q$ according to Lemma 2.2. Similarly, we claim that $G_2(x)=0$ has no solution in $\mathbb{F}_q$. Thus $g(x)=G_1(x)G_2(x)$ has no roots in $\mathbb{F}_q$.

Therefore, $g(x)$ has no roots in $\mathbb{F}_q$ when $k\not\equiv 0 \pmod 4$. Moreover, (25) can not hold. Then $p(x)$ permutes $\mu_{q+1}$. We complete the proof. □

**Theorem 4.2** *Let $q = 2^k$, where $k$ is odd, and $f(x) = x + x^{\frac{q^2-3q+5}{3}} + x^{\frac{2q^2-3q+4}{3}}$. Then $f(x)$ is a permutation trinomial over $\mathbb{F}_{q^2}$.*

*Proof* Let $f(x) = x\left(1 + x^{\frac{q-2}{3}(q-1)} + x^{\frac{2q-1}{3}(q-1)}\right) = xh\left(x^{q-1}\right)$, where $h(x) = 1+x^{\frac{q-2}{3}} + x^{\frac{2q-1}{3}}$. Put $p(x) = xh(x)^{q-1} \in \mu_{q+1}[x]$ and $y = x^{\frac{q+1}{3}}$. Obviously, $y^3 = 1$. Then for $x \in \mu_{q+1}$,we have

$$p(x) = x\frac{1 + x^{\frac{2-q}{3}} + x^{\frac{1-2q}{3}}}{1 + x^{\frac{q-2}{3}} + x^{\frac{2q-1}{3}}} = x^2\frac{\left(y^2+y\right)x+1}{y^2+y+x},$$

Let $S_1 = \{x|x \in \mu_{q+1}, y = 1\}$ and $S_2 = \{x|x \in \mu_{q+1}, y \neq 1\}$. We claim that $p(x)$ permutes $\mu_{q+1}$. Otherwise, there exist two distinct elements $x_1, x_2 \in \mu_{q+1}$ such that $p(x_1) = p(x_2)$. The following proof is divided into four cases.

**Case I**: $x_1, x_2 \in S_1$.

Then $p(x_1) = x_1$ and $p(x_2) = x_2$. So $x_1 = x_2$ from $p(x_1) = p(x_2)$.

**Case II**: $x_1, x_2 \in S_2$.

Then $p(x_1) = x_1^2$ and $p(x_2) = x_2^2$. We have $x_1 = x_2$ from $p(x_1) = p(x_2)$.

**Case III**: $x_1 \in S_1$ and $x_2 \in S_2$.

Then $p(x_1) = x_1$ and $p(x_2) = x_2^2$. So $x_1 = x_2^2$. But $x_1^{\frac{q+1}{3}} = \left(x_2^2\right)^{\frac{q+1}{3}} \neq 1$, which is a contradiction with $x_1 \in S_1$.

**Case IV**: $x_1 \in S_2$ and $x_2 \in S_1$.

This case is similar as Case III.

Hence, $p(x)$ permutes $\mu_{q+1}$. Moreover, $f(x)$ permutes $\mathbb{F}_{q^2}$ according to Lemma 2.1. □

**Theorem 4.3** *Let $q = 2^k$ and $k \not\equiv 1 \pmod 3$. Then $f(x) = x + x^{q^2+q-1} + x^{q^3-q^2+q}$ is a permutation polynomial over $\mathbb{F}_{q^3}$.*

*Proof* First, we show that $f(x) = 0$ only has zero solution in $\mathbb{F}_{q^3}$. If $f(x) = 0$, then either $x = 0$ or $1 + x^{q-q^2} + x^{q^2+q-2} = 0$. Thus, we only need to prove that the equation

$$1 + x^{q-q^2} + x^{q^2+q-2} = 0 \tag{30}$$

has no solution in $\mathbb{F}_{q^3}^*$. Let $t = x^{q-1} \neq 0$. Then $t^{q^2+q+1} = 1$, and (30) turns to

$$1 + t^{-q} + t^{q+2} = 0,$$

i.e.,

$$1 + t^q + t^{2q+2} = 0. \tag{31}$$

Raising (31) to its $q$-th power, we get

$$1 + t^{q^2} + t^{2q^2+2q} = 0.$$

Plugging $t^{q^2+q+1} = 1$ into the above equation leads to

$$t + t^q + t^{q+2} = 0. \tag{32}$$

Computing (31) + (32), we get $\left(1 + t^{q+1}\right)\left(1 + t + t^{q+1}\right) = 0$. Then either $t^{q+1} + 1 = 0$ or $t^{q+1} + t + 1 = 0$.

If $t^{q+1}=1$, then $t=1$ since $\gcd\left(q+1,q^2+q+1\right)=\gcd\left(q+1,q^2\right)=1$. However, $t=1$ is not the solution of (31). Therefore,

$$1+t+t^{q+1}=0. \tag{33}$$

Computing (31) + (33)$^2$, we yield $t^{q-2}=1$, then $t^{\gcd(q-2,q^2+q+1)}=1$. Moreover, $t=1$ thanks to $\gcd\left(q-2,q^2+q+1\right)=\gcd(2^{k-1}-1,7)=1$ when $k\not\equiv 1 \pmod 3$. However, it is impossible!

Therefore, $f(x)=0$ only has zero solution in $\mathbb{F}_{q^3}$.

Next, we prove $f(x)=a$ has at most one solution in $\mathbb{F}_{q^3}$ for any $a\in\mathbb{F}_{q^3}^*$. It is obvious that $x=0$ is not the solution of $f(x)=a$ when $a\neq 0$. Let $y=x^q, z=y^q, b=a^q, c=b^q$ and $A=a+b+c$. Then $a,b,c,x,y,z\neq 0$ and $A\in\mathbb{F}_q$. And it follows from $f(x)=a$ that

$$x+\frac{xy}{z}+\frac{yz}{x}=a. \tag{34}$$

Raising (34) to its $q$-th and $q^2$-th power respectively, we get

$$y+\frac{yz}{x}+\frac{xz}{y}=b \tag{35}$$

and

$$z+\frac{zx}{y}+\frac{xy}{z}=c. \tag{36}$$

Computing (34) + (35) + (36), we have

$$x+y+z=a+b+c=A.$$

On one hand, after computing $xz*$ (34) $+xy*$ (35), we get $y(x+z)A+x(by+az)=0$. Plugging $y=x+z+A$ into the above equation and simplifying it, we have

$$(A+b)x^2+Az^2+(a+b)xz+A(A+b)x+A^2z=0. \tag{37}$$

Let $x=uz$. Plugging it into (37), we have

$$B_1z+B_0=0, \tag{38}$$

where

$$B_1=(A+b)u^2+(a+b)u+A,$$
$$B_0=A(A+b)u+A^2.$$

On the other hand, plugging $y=x+z+A$ into (34) $*xz$, we get $x^3+z^3+xz^2+A(x^2+z^2)+axz=0$. And plugging $x=uz$ into the above equation, we obtain

$$C_1z+C_0=0, \tag{39}$$

where

$$C_1=u^3+u+1,$$
$$C_0=Au^2+au+A.$$

Computing (38) $*C_1+$ (39) $*B_1$, we have

$$B_0C_1+B_1C_0=0,$$

i.e.,

$$D_1u+D_0=0, \tag{40}$$

where

$$D_1=A^2+Ab+ab,$$
$$D_0=A^2+a^2+ab.$$

We claim that $D_1 \neq 0$. Otherwise,

$$A^2 + Ab + ab = 0. \tag{41}$$

Computing (41) + (41)$^q$ + (41)$^{q^2}$, we get $ab + ac + bc = 0$, i.e., $1 + a^{q^2-q} + a^{q^2-1} = 0$. Let $e = a^{1-q}$. Then $1 + e + e^{q+1} = 0$, which is (33). And it is impossible. Thus

$$u = \frac{D_0}{D_1}.$$

Recalling the definition of $A$, we know $y = A + x + z = A + (1+u)z$. Plugging $x = uz$ and $y = A + (1+u)z$ into (34), we get

$$\left(u^3 + u + 1\right) z = \left(u^2 + 1\right) A + au.$$

If $u^3 + u + 1 = 0$, we can conclude that $u^7 = 1$ easily. In fact,

$$u^q = \begin{cases} u^2, & \text{if } k \equiv 1 \pmod 3, \\ u^4, & \text{if } k \equiv 2 \pmod 3, \\ u, & \text{if } k \equiv 0 \pmod 3. \end{cases}$$

When $k \equiv 2 \pmod 3$, $z = u^{-1}x = u^6 x$ and $y = x^q = (uz)^q = u^q x = u^4 x$. Plugging them into (34), we get $\left(1 + u^3 + u^5\right) x = a$. If $1 + u^3 + u^5 = 0$, then $1 + u^3 + u^{-2} = 0$,i.e., $1 + u^2 + u^5 = 0$ due to $u^7 = 1$. So $u^3 = u^2$, $u = 1$. However, $u = 1$ does not satisfy $1 + u^3 + u^5 = 0$. Therefore, $1 + u^3 + u^5 \neq 0$. It follows that $x = \frac{a}{1+u^3+u^5}$ is the unique solution of $f(x) = a$ in the case. When $k \equiv 0 \pmod 3$,the case is similar as the above one, we omit it here.

If $u^3 + u + 1 \neq 0$, then $x = z^q$,where $z = \frac{\left(u^2+1\right)A+au}{u^3+u+1}$. In other words, $f(x) = a$ also has at most one solution in $\mathbb{F}_{q^3}$ in the case.

Therefore, for any $a \in \mathbb{F}_{q^3}$, $f(x) = a$ has at most one solution in $\mathbb{F}_{q^3}$. We finish the proof. □

**Theorem 4.4** *Let $q = 2^k$ and $k \not\equiv 1 \pmod 3$. Let $f(x) = x + x^{q^2} + x^{q^3-q^2+q}$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^3}$.*

*Proof* It suffices to prove that $f(x) = a$ has at most one solution in $\mathbb{F}_{q^3}$ for any $a \in \mathbb{F}_{q^3}$. If $a = 0$, then we obtain $x = 0$ or

$$1 + x^{q^2-1} + x^{q-q^2} = 0. \tag{42}$$

We claim that (42) has no solution in $\mathbb{F}_{q^3}^*$. Otherwise, $\mathrm{Tr}_{q^3/q}\left(1 + x^{q^2-1} + x^{q-q^2}\right) = 0$. Moreover, it follows from $\mathrm{Tr}_{q^3/q}\left(x^{q^2-1} + x^{q-q^2}\right) = 0$ that $\mathrm{Tr}_{q^3/q}(1) = 0$, which is a contradiction.

In the following, we assume that $a \neq 0$. Put $y = x^q$, $z = y^q$, $b = a^q$, $c = b^q$ and $A = a + b + c$. Obviously, $x, y, z, b, c \neq 0$ when $a \neq 0$ and $A \in \mathbb{F}_q$. Then we have

$$\begin{cases} x + \frac{xy}{z} + z = a, \\ y + \frac{yz}{x} + x = b, \\ z + \frac{zx}{y} + y = c. \end{cases} \tag{43}$$

Let $\alpha = \frac{xy}{z}$, $\beta = \frac{yz}{x}$, $\gamma = \frac{zx}{y}$. They are clear that $\beta = \alpha^q$ and $\gamma = \alpha^{q^2}$. Then

$$\begin{cases} x^2 = \alpha\gamma, \\ y^2 = \alpha\beta, \\ z^2 = \beta\gamma. \end{cases} \tag{44}$$

Plugging (44) into (43), we obtain

$$\begin{cases} \alpha^2 + \alpha\gamma + \beta\gamma = a^2, \\ \beta^2 + \alpha\beta + \alpha\gamma = b^2, \\ \gamma^2 + \beta\gamma + \alpha\beta = c^2. \end{cases} \tag{45}$$

Adding the above three equations together leads to $\alpha + \beta + \gamma = a + b + c = A$. Then plugging $\gamma = A + \alpha + \beta$ into (45), we yield

$$\beta^2 + A\beta + A\alpha + a^2 = 0, \tag{46}$$

and

$$\beta^2 + \alpha^2 + A\alpha + b^2 = 0. \tag{47}$$

If $A = 0$,then $(\alpha, \beta, \gamma) = (c, a, b)$,and $x = (\alpha\gamma)^{\frac{1}{2}} = (cb)^{\frac{1}{2}}$ is uniquely determined.

If $A \neq 0$,after adding (46) and (47), we can get $\beta = \frac{1}{A}\left(\alpha^2 + a^2 + b^2\right)$. Then plugging it into (46), we have

$$\alpha^4 + A^2\alpha^2 + A^3\alpha + a^4 + b^4 + A^2b^2 = 0. \tag{48}$$

To finish the proof, it suffices to prove that there exists at most one element $\alpha \in \mathbb{F}_{q^3}$ satisfying (47) and (48) since then $x$ is uniquely determined by $\alpha$ by (44).

Otherwise, suppose that there exist $\alpha_1 \neq \alpha_2 \in \mathbb{F}_{q^3}$ satisfy (47) and (48) and put $\delta = \frac{\alpha_1+\alpha_2}{A} \neq 0$. Then we can obtain

$$\delta^{2q} + \delta^2 + \delta = 0 \tag{49}$$

and

$$\delta^4 + \delta^2 + \delta = 0 \tag{50}$$

from (47) and (48) respectively. It is trivial to obtain $\delta^7 = 1$ from (50). In fact,

$$\delta^{2q} = \begin{cases} \delta^4, & \text{if } k \equiv 1 \pmod 3, \\ \delta, & \text{if } k \equiv 2 \pmod 3, \\ \delta^2, & \text{if } k \equiv 0 \pmod 3. \end{cases}$$

When $k \equiv 2 \pmod 3$,according to (49), we have $\delta^2 = 0$, which is impossible! The case $k \equiv 0 \pmod 3$ is the same as the above case, we omit it here.

Therefore, when $k \not\equiv 1 \pmod 3$, $f(x) = a$ has at most one solution in $\mathbb{F}_{q^3}$ for any $a \in \mathbb{F}_{q^3}$. We finish the proof. □

**Acknowledgments** We would like to thank the editor and the referees whose valuable comments and suggestions improve both the technical quality and the editorial quality of this paper.

## References

1. Akbary, A., Ghioca, D., Wang, Q.: On constructing permutations of finite fields. Finite Fields Appl. **17**, 51–67 (2011)
2. Akbary, A., Wang, Q.: On polynomials of the form $x^r h(x)^{(q-1)/l}$. International Journal of Mathematics and Mathematical Sciences. Article ID 23408, 7 pages (2007)

3. Ball, S., Zieve, M.: Symplectic spreads and permutation polynomials. Finite Fields and Applications. In: Lect. Notes Comput. Sci, vol. 2948, pp. 79–88. Springer, Berlin (2004)
4. Berlekamp, E.R., Rumsey, H., Solomon, G.: On the solution of algebraic equations over finite fields. Information And Control **10**(67), 553–564 (1967)
5. Charpin, P., Kyureghyan, G.: On a class of permutation polynomials over $\mathbb{F}_{2^n}$. Sequences and their Applications-SETA 2008, Lecture Notes in Comput Sci. 5203. Springer **3**, 368–376 (2008)
6. Charpin, P., Kyureghyan, G.: Monmial functions with linear structure and permutation polynomials. Finite Fields: Theory and Applications, Contemp. Math. 518, Amer. Math. Soc.. **3**(16), 99–111 (2010)
7. Charpin, P., Kyureghyan, G.: When does $G(x)+\gamma \mathrm{Tr}(H(x))$ permutes $\mathbb{F}_{p^n}$. Finite Fields Appl. **15**, 615–632 (2009)
8. Ding, C., Yuan, J.: A family of skew Hadamard difference sets. J. Combin. Theory Ser. A **113**, 1526–1535 (2006)
9. Ding, C., Qu, L., Wang, Q., et al.: Permutation trinomials over finite fields with even characteristic. SLAM J. Dis. Math. **29**, 79–92 (2015)
10. Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case. IEEE Trans. Inform. Theory **45**, 1271–1275 (1999)
11. Dobbertin, H.: Uniformly representable permutation polynomials. Sequence andtheir Applications-SETA 2001. Springer **2**(9), 1–22 (2002)
12. Gupta, R., Sharma, R.K.: Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **41**, 89–96 (2016)
13. Hou, X.: A survey of permutation binomials and trinomials over finite fields. In: Kyureghyan, G., Mullen, G.L., Pott, A. (eds.) Topics in Finite Fields, Proceedings of the 11th International Conference on Finite Fields and Their Applications, Contemp. Math, vol. 632, pp. 177–191. Magdeburg, Germany (2015). AMS
14. Hou, X.: Permutation polynomials over finite fields–A survey of recent advances. Finite Fields Appl. **32**, 82–119 (2015)
15. Hou, X.: A class of permutation trinomials over finite fields. Acta Arith **162**, 51–64 (2014)
16. Hou, X.: Determination of a type of permutaiton trinomials over finite fields. Acta Arith. **162**, 253–278 (2014)
17. Hou, X.: Determination of a type of permutaiton trinomials over finite fields, **II**. Finite Fields Appl. **35**, 16–35 (2015)
18. Kyureghyan, G., Zieve, M.E.: Permutation polynomials of the form $X+\gamma \mathrm{Tr}(X^k)$. Contemporary Developments in Finite Fields and Appl. doi:10.1142/9789814719261-0011 (2016)
19. Lidl, R., Niederreiter, H.: Finite Fields, 2nd ed. Cambridge Univ. Press, Cambridge (1997)
20. Laigle-Chapuy, Y.: Permutation polynomials and applications to coding theory. Finite Fields Appl. **13**, 58–70 (2007)
21. Leonard, P.A., Williams, K.S.: Quartics over $\mathbb{GF}(2^n)$. Proc. Am. Math. Soc. **36**, 347–350 (1972)
22. Muller, W.B., Nobauer, R.: Cryptanalysis of the Dickson-scheme. In: Proceedings of EUROCRYPT 85, pp. 215–230. Springer-Verlag, New York (1986)
23. Park, H., Lee, J.B.: Permutation polynomials and group permutation polynomials. Bull. Aust. Math. Soc. **63**, 67–74 (2001)
24. Li, K., Qu, L., Chen, X.: New classes of permutation binomials and permutation trinomials over finite fields. Finite Fields Appl. **43**, 69–85 (2017)
25. Li, K., Qu, L., Li, C., et al: New permutation trinomials constructed from fractional polynomials. arXiv:1605.06216 (2016)
26. Qu, L., Tan, Y., Tan, C.H., et al.: Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Inform. Theory **59**, 4675–4686 (2013)
27. Rivest, R.L., Shamir, A., Aselman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM **21**, 120–126 (1978)
28. Ma, J., Zhang, T., Feng, T., et al.: Some new results on permutation polynomials over finite fields. Des. Codes Cryptog.r **83**(2), 425–443 (2017)
29. Tu, Z., Zeng, X., Hu, L., et al.: A class of binomial permutation polynomials. arXiv:1310.0337 (2013)
30. Sun, J., Takeshita, O.Y.: Interleavers for turdo codes using permutation polynomials over integer rings. IEEE Trans. Inform. Theory **51**, 101–119 (2005)
31. Wang, Q.: Cyclotomic mapping permutation polynomials over finite fields. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) Sequences, Subsequences, and Consequences, Lect. Notes Comput. Sci., vol. 4893, pp. 119–128. Springer, Berlin (2007)
32. Williams, K.S.: Note on Cubics over $\mathbf{GF}(2^n)$ and $\mathbf{GF}(3^n)^*$. J. Number Theory **7**, 361–365 (1975)
33. Yuan, P., Ding, C.: Permutation polynomials over finite fields from a powerful lemma. Finite Fields Appl. **17**, 560–574 (2011)

34. Zieve, M.E.: On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. Proc. Am. Math. Soc. **137**, 2209–2216 (2009)
35. Zieve, M.E.: Permutation polynomials on $\mathbb{F}_q$ induced from bijective Rédei functions on subgroups of the multiplicative group of $\mathbb{F}_q$. arXiv:1310.0776 (2013)
36. Zieve, M.E.: Permutation polynomials over $\mathbb{F}_{q^2}$ induced from novel permutations of the $(q+1)$-th roots of unity. preprint
37. Zeng, X., Tian, S., Tu, Z.: Permutation polynomials from trace functions over finite fields. Finite Fields Appl. **35**, 36–51 (2015)