Cryptogr. Commun. (2019) 11:227–236
https://doi.org/10.1007/s12095-018-0284-7

More classes of permutation trinomials with Niho exponents

Huali Deng[1] · **Dabin Zheng**[1]

Received: 3 July 2017 / Accepted: 26 January 2018 / Published online: 8 February 2018

Abstract This paper presents two classes of permutation trinomials with the form $x^{s(2^m-1)+1}+x^{t(2^m-1)+1}+x$ over the finite field $\mathbb{F}_{2^{2m}}$ as a supplement of the recent works of Li and Helleseth, and a class of permutation trinomials like this form over $\mathbb{F}_{3^{2m}}$. Moreover, we give a method to construct permutation polynomials from known ones.

Keywords Finite field · Permutation polynomial · Niho exponent

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

1 Introduction

Let q be a power of a prime, and $\mathbb{F}_q$ be a finite field with q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if the associated polynomial function $f : a \mapsto f(a)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$ [15]. Permutation polynomials over finite fields have important applications in cryptography [17, 20, 21], coding theory [8, 22] and combinatorial design theory [4]. Finding new permutation polynomials is of great interest in both theoretical and applied aspects.

The construction of permutation polynomials with few terms attracts many authors to work on this topic due to their simple form and wide applications. The recent progress on construction of permutation binomials and trinomials can be seen in [2, 3, 5–7, 9, 10, 12–14, 23, 26] and the references therein. In particular, Li and Helleseth in [12, 13] investigated permutation polynomials with the following form

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1}, \tag{1}$$

✉ Dabin Zheng
dzheng@hubu.edu.cn

[1] Hubei Province Key Laboratory of Applied Mathematics, Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China

where s, t are integers satisfying $1 \leq s, t \leq 2^m$. For simplicity, when s, t are written as fractions or negative integers, then they are interpreted as modulo $2^m + 1$. By solving equations with low degree over finite fields and using the property of linear fractional polynomials over the finite fields $\mathbb{F}_{2^m}$, they obtained some new permutation polynomials over $\mathbb{F}_{2^{2m}}$ of the form (1).

In this paper, we will further study the permutation polynomials of the form (1) following the works in [12, 13]. By some delicate operation of solving equations with low degrees over finite fields, we find two new pairs (s, t) such that (1) are permutation polynomials over $\mathbb{F}_{2^{2m}}$. By using the technique provided in [6] we obtain a new class of permutation trinomials like this form over $\mathbb{F}_{3^{2m}}$. Moreover, we present a method to construct permutation polynomials from known ones.

2 Preliminaries

Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements for a prime p. Let k be a divisor of n. The trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$ is defined by

$$\mathrm{Tr}_k^n(x) = \sum_{i=0}^{n/k-1} x^{p^{ik}},$$

where $x \in \mathbb{F}_{p^n}$. Let q be a power of a prime p. A positive integer s is called a *Niho exponent* with respect to the finite field $\mathbb{F}_{q^2}$ if $s \equiv p^i \mod (q-1)$ for some nonnegative integer i. s is called a normalized Niho exponent if $i = 0$. The Niho exponents were first introduced by Niho in [18] for studying the cross-correlation between an m-sequence and its d-decimation. Let d be a positive integer with $d \mid (q-1)$, and μ_d denote the set of d-th roots of unity in $\mathbb{F}_q^*$, i.e.,

$$\mu_d = \left\{x \in \mathbb{F}_q^* \ : \ x^d = 1\right\}.$$

A main technique to investigate permutation behavior of polynomials of the form (1) is the following lemma.

Lemma 1 ([19, 24, 25]) *Let q be a power of a prime. Let $\mathbb{F}_q$ be a finite field with q elements and $h(x) \in \mathbb{F}_q[x]$. Let d, r be positive integers with $d \mid (q-1)$. Then $f(x) = x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if the following two conditions hold:*

(1) $\gcd(r, (q-1)/d) = 1$,
(2) $x^r h(x)^{(q-1)/d}$ *permutes* μ_d.

For later usage we need the following lemmas.

Lemma 2 ([5, 26]) *Let m be a positive integer. Each of the polynomials $1 + x + x^3$, $1 + x^3 + x^4$, $1 + x + x^4$ and $1 + x + x^5$ (m is even) has no roots in μ_{2^m+1}.*

Lemma 3 *Let m be an odd positive integer. Each of the polynomials $x^2 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x + 1$ has no roots in $\mathbb{F}_{2^m}$.*

Lemma 4 (Theorem 2 in [1]) *Let $q = 2^m$ and $\mathbb{F}_q$ be a finite field. Let $a, b \in \mathbb{F}_q$ with $b \neq 0$. Then the cubic equation $x^3 + ax + b = 0$ has a unique solution in $\mathbb{F}_q$ if and only if $Tr_1^m(\frac{a^3}{b^2} + 1) \neq 0$.*

Lemma 5 ([16]) *Let $\mathbb{F}_q$ be a finite field with $q = 2^m$. Let $h(x) = x^4 + a_2x^2 + a_1x + a_0$ and $g(y) = y^3 + a_2y + a_1$ be polynomials over $\mathbb{F}_q$ with $a_0a_1 \neq 0$. Let γ_i be the roots of $g(y) = 0$ when they exist in $\mathbb{F}_q$ and $\omega_i = a_0\gamma_i^2/a_1^2$ for $i = 1, 2, 3$. Then $h(x)$ has no solution in $\mathbb{F}_q$ if one of the following conditions is satisfied:*

(1) *$g(y) = 0$ has exactly one solution in $\mathbb{F}_q$ and $Tr_1^m(\omega_1) = 1$;*
(2) *$g(y) = 0$ has exactly three solution in $\mathbb{F}_q$ and $Tr_1^m(\omega_1) = 0$, $Tr_1^m(\omega_2) = Tr_1^m(\omega_3) = 1$.*

Lemma 6 (Theorem 2.10 in [10]) *Let $q = 2^m$ and $\mathbb{F}_q$ be a finite field. The polynomial $g(x) = x^7(1 + x^4 + x^6)^{q-1}$ permutes the unite circle μ_{q+1} in $\mathbb{F}_{q^2}$ if $\gcd(m, 3) = 1$.*

Lemma 7 (Lemma 4.1 in [26]) *The mapping $g(x) = x^3(1 + x^2 + x^3)^{2^m-1}$ permutes μ_{2^m+1} in the finite field $\mathbb{F}_{2^{2m}}$.*

Lemma 8 (Lemma 4 in [13]) *Let $q = 2^m$ and $\mathbb{F}_q$ be a finite field. Let $(s, t) = (i, j)$ be a pair such that $f(x)$ defined by (1) is a permutation polynomial over $\mathbb{F}_{q^2}$, then $f(x)$ defined by (1) is also a permutation polynomial over $\mathbb{F}_{q^2}$ for the following pairs:*

(1) $(s, t) = (\frac{i}{2i-1}, \frac{i-j}{2i-1})$ *if* $\gcd(2i - 1, 2^m + 1) = 1$, *or*
(2) $(s, t) = (\frac{j}{2j-1}, \frac{j-i}{2j-1})$ *if* $\gcd(2j - 1, 2^m + 1) = 1$.

These pairs are called equivalent pairs if they exist.

If (s, t) is a pair such that (1) is a permutation polynomial, then from Lemma 8 one can easily get equivalent pairs of (s, t) such that (1) is a permutation polynomial. So, from this property of Niho exponents one easily checks multiplicative equivalence of two permutation trinomials of the form (1) [12].

3 Two classes of permutation trinomials over $\mathbb{F}_{2^{2m}}$

In this section, we investigate the permutation behavior of two classes of trinomials of the form (1) over $\mathbb{F}_{2^{2m}}$, and present a method to construct new permutation polynomials from known ones.

Theorem 1 *Let $\mathbb{F}_q$ be a finite field with $q = 2^m$ and* $\gcd(m, 2) = 1$. *The trinomial $f(x)$ defined by (1) is a permutation over $\mathbb{F}_{q^2}$ if $(s, t) = (\frac{2}{7}, \frac{8}{7})$.*

Proof By Lemma 1 we only need to show $\phi(x) = x(1 + x^s + x^t)^{q-1}$ permutes the unite circle μ_{q+1}. This is equivalent to showing that $g(x) = \phi(x^7) = x^7(1 + x^{7s} + x^{7t})^{q-1} = x^7(1 + x^2 + x^8)^{q-1}$ permutes the unite circle μ_{q+1} since $\gcd(7, q + 1) = 1$. By Lemma 2 we know that $1 + x^2 + x^8 \neq 0$ for all $x \in \mu_{q+1}$. So $g(\mu_{q+1}) \subseteq \mu_{q+1}$. For $x \in \mu_{q+1}$, $g(x)$ is reduced to the following fraction,

$$g(x) = x^7(1 + x^2 + x^8)^{q-1} = \frac{1 + x^6 + x^8}{x + x^3 + x^9}.$$

Next we show that there is no pair $(x, y) \in \mu_{q+1}^2$ with $x \neq y$ satisfying $g(x) = g(y)$. From

$$\frac{1 + x^6 + x^8}{x + x^3 + x^9} = \frac{1 + y^6 + y^8}{y + y^3 + y^9},$$

we get

$$\begin{aligned}&(x + y) + xy(x^5 + y^5) + xy(x^7 + y^7) + (x^3 + y^3) + x^3y^3(x^3 + y^3)\\&+x^3y^3(x^5 + y^5) + (x^9 + y^9) + x^6y^6(x^3 + y^3) + x^8y^8(x + y) = 0.\end{aligned} \tag{2}$$

Set $x + y = u$ and $xy = v$. We know that $u \neq 0$ and $v \neq 0$ since $x \neq y$. It follows that $u^{1-q} = \frac{x+y}{x^{-1}+y^{-1}} = xy = v$ since $x, y \in \mu_{q+1}$. Plugging them into (2) and simplifying it, we get

$$\begin{aligned}&1 + vu^4 + v^2u^2 + v^3 + u^2 + v + v^3u^2 + v^4\\&+v^3u^4 + v^4u^2 + v^5 + u^8 + v^6u^2 + v^7 + v^8 = 0.\end{aligned} \tag{3}$$

Let $u = z^{-1}$ for $z \in \mathbb{F}_{q^2}^*$, and then $v = z^{q-1}$. Multiplying both sides of (3) by z^8 we get

$$\begin{aligned}&(z^8 + z^{8q}) + z^{q+1}(z^2 + z^{2q}) + z^{2(q+1)}(z^2 + z^{2q}) + z^{3(q+1)}(z^2 + z^{2q})\\&+(z^6 + z^{6q}) + z^{q+1}(z^6 + z^{6q}) + z^{3(q+1)} + z^{4(q+1)} + 1 = 0.\end{aligned} \tag{4}$$

Let α, β denote $z + z^q$ and z^{q+1} respectively. Then $\alpha, \beta \in \mathbb{F}_q$ and from (4) we have

$$\alpha^8 + \alpha^6 + \beta\alpha^6 + \beta\alpha^2 + 1 + \beta^3 + \beta^4 = 0. \tag{5}$$

Next we show that (5) has no solutions $(\alpha, \beta) \in \mathbb{F}_q^2$.

If $z \in \mathbb{F}_q$ then $\alpha = z + z^q = 0$. From (5) we obtain

$$\beta^4 + \beta^3 + 1 = 0.$$

By Lemma 3 we know this is a contradiction since $\beta \in \mathbb{F}_q$ and $\gcd(2, m) = 1$.
If $z \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ then $\alpha = z + z^q \neq 0$. Let $\nu = \alpha^2$. From (5) we have

$$\nu^4 + \nu^3 + \beta\nu^3 + \beta\nu + 1 + \beta^3 + \beta^4 = 0. \tag{6}$$

Multiplying both sides of (6) by ν^{-4} and let $\gamma = \frac{1}{\nu}$, $\delta = \frac{\beta}{\nu}$, we get

$$\gamma^4 + \delta\gamma^2 + (1 + \delta^3)\gamma + 1 + \delta + \delta^4 = 0. \tag{7}$$

From Lemma 3 we know that $1 + \delta + \delta^4 \neq 0$ for $\delta \in \mathbb{F}_q$ since $\gcd(2, m) = 1$. Next we show that there is no pair $(\gamma, \delta) \in \mathbb{F}_q^2$ satisfying (7).

Assume that $1 + \delta^3 = 0$. We have $\delta = 1$ since $\delta \in \mathbb{F}_q$ and $\gcd(2, m) = 1$. Substituting $\delta = 1$ into (7) we get

$$\gamma^4 + \gamma^2 + 1 = 0.$$

This is a contradiction from Lemma 3 since $\gamma \in \mathbb{F}_q$ and $\gcd(2, m) = 1$.
Assume that $1 + \delta^3 \neq 0$. Let $h(y) = y^3 + \delta y + (1 + \delta^3)$. Since $\gcd(2, m) = 1$ we have

$$\mathrm{Tr}_1^m\left(\frac{\delta^3}{(1 + \delta^3)^2} + 1\right) = \mathrm{Tr}_1^m\left(\frac{1}{1 + \delta^3} + \frac{1}{(1 + \delta^3)^2} + 1\right) = \mathrm{Tr}_1^m(1) \neq 0.$$

From Lemma 4 we know that $h(y)$ has exactly one solution, which is $\delta + 1$. Let

$$\omega = \frac{(1 + \delta + \delta^4)(1 + \delta)^2}{(1 + \delta^3)^2} = 1 + \frac{\delta}{1 + \delta^3} + \frac{\delta^2}{(1 + \delta^3)^2} + \frac{1}{1 + \delta^3} + \frac{1}{(1 + \delta^3)^2}.$$

It is clear that $\mathrm{Tr}_1^m(\omega) = 1$ since $\gcd(m, 2) = 1$. By Lemma 5 we know that there is no pair $(\gamma, \delta) \in \mathbb{F}_q^2$ satisfying (7). Therefore, there is no pair (x, y) in μ_{q+1}^2 with $x \neq y$ satisfying $g(x) = g(y)$, that is, $g(x)$ permutes the unite circle μ_{q+1}. □

Theorem 2 *Let m be a positive integer with $m \equiv 2, 4 \mod 6$. Let $\mathbb{F}_q$ be a finite field with $q = 2^m$. The trinomial $f(x)$ defined by (1) is a permutation over $\mathbb{F}_{q^2}$ if $(s, t) = (-\frac{2}{7}, \frac{8}{7})$.*

Proof By Lemma 1 we need to show $\phi(x) = x(1 + x^s + x^t)^{q-1}$ permutes the unite circle μ_{q+1}. This is equivalent to showing that $g(x) = \phi(x^7) = x^7(1 + x^{-2} + x^8)^{q-1}$ permutes the unite circle μ_{q+1} since $\gcd(7, q + 1) = 1$. By Lemma 2 we know that $1 + x^2 + x^{10} \neq 0$ for all $x \in \mu_{q+1}$ when m is even. So $g(\mu_{q+1}) \subseteq \mu_{q+1}$. For $x \in \mu_{q+1}$, $g(x)$ is reduced to the following form,

$$g(x) = x^7(1 + x^{-2} + x^8)^{q-1} = \frac{x(1 + x^8 + x^{10})}{1 + x^2 + x^{10}}.$$

Dividing the common divisor $1 + x^2 + x^4$ of numerator and denominator of the above fraction we get

$$g(x) = \frac{x(1 + x^8 + x^{10})}{1 + x^2 + x^{10}} = \frac{x(1 + x^2 + x^6)}{1 + x^4 + x^6} = x^7(1 + x^4 + x^6)^{q-1}.$$

Since $m \equiv 2, 4 \mod 6$, we have that $\gcd(m, 3) = 1$. By Lemma 6 we know that $g(x)$ permutes the unite circle μ_{q+1}. So, $f(x)$ is a permutation over $\mathbb{F}_{q^2}$. □

Inspired by the proof of Theorem 2 we present a method to construct new permutation polynomials from known ones. To this end, we introduce some symbols as follows. Let n and k_i be integers satisfying $n \geq 2$, $k_0 = 0$ and $k_i + k_{n-i} = k_n$ for $0 \leq i \leq n$. Let $q = 2^m$ and $R(x) = \sum_{i=0}^{n} x^{k_i}$ be a polynomial over $\mathbb{F}_{q^2}$.

Theorem 3 *Let r and ℓ be positive integers. Let $h(x)$ be a polynomial over $\mathbb{F}_{q^2}$. Assume that $R(x) \neq 0$ for $x \in \mu_{q+1}$, then the polynomial $F(x) = x^{r+k_n\ell}R(x^{q-1})^{\ell}h(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r + k_n\ell, q - 1) = 1$ and the polynomial $g(x) = x^r h(x)^{q-1}$ permutes μ_{q+1}.*

Proof By Lemma 1 we know that $F(x)$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r + k_n l, q - 1) = 1$ and the polynomial $G(x) = x^{r+k_n\ell}R(x)^{(q-1)\ell}h(x)^{q-1}$ permutes μ_{q+1}. Since $R(x) \neq 0$ for $x \in \mu_{q+1}$ and $k_i + k_{n-i} = k_n$ for $0 \leq i \leq n$, we have

$$\begin{aligned} G(x) &= x^{r+k_n\ell}\left(R(x)^{\ell}h(x)\right)^{q-1} = x^{r+k_n\ell}\left(\sum_{i=0}^{n} x^{k_i}\right)^{(q-1)\ell} h(x)^{q-1} \\ &= x^r \left(\frac{\sum\limits_{i=0}^{n} x^{k_n-k_i}}{\sum\limits_{i=0}^{n} x^{k_i}}\right)^{\ell} h(x)^{q-1} \\ &= g(x). \end{aligned}$$

So $G(x)$ permutes μ_{q+1} if and only if $g(x) = x^r h(x)^{q-1}$ permutes μ_{q+1}. This completes the proof. □

By this theorem we can obtain a new permutation polynomial $F(x)$ over $\mathbb{F}_{q^2}$ from a permutation polynomial over the unite circle μ_{q+1} if the desired polynomial $R(x)$ is provided. The following corollary presents a method to construct $R(x)$, and then obtains new permutation polynomials over $\mathbb{F}_{q^2}$ from known permutation polynomials over the unit circle μ_{q+1}.

Corollary 1 *Let k, r, ℓ be positive integers and n be an even number. Let $R(x) = \sum_{i=0}^{n} x^{ki}$ and $h(x)$ be a polynomial over $\mathbb{F}_{q^2}$. Then the polynomial $F(x) = x^{r+kn\ell}R(x^{q-1})^{\ell}h(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if the following three conditions hold:*

(1) $\gcd((n+1)k, q+1) = 1$,
(2) $\gcd(r + kn\ell, q-1) = 1$,
(3) $g(x) = x^r h(x)^{q-1}$ *permutes* μ_{q+1}.

Proof If the condition (1) holds then $R(x) \neq 0$ for $x \in \mu_{q+1}$. In fact, assume that $\alpha \in \mu_{q+1}$ is a root of $R(x)$, i.e., $\sum_{i=0}^{n} \alpha^{ki} = 0$. We have

$$\alpha^{(n+1)k} + 1 = (\alpha^k + 1)\left(\sum_{i=0}^{n} \alpha^{ki}\right) = 0.$$

From $\gcd((n+1)k, q+1) = 1$, we get $\alpha = 1$. But $\alpha = 1$ is not a root of $R(x)$ since n is even. This proves that $R(x) \neq 0$ for $x \in \mu_{q+1}$. By Theorem 3 and conditions (2) and (3) we know that $F(x)$ permutes $\mathbb{F}_{q^2}$.

Conversely, if $F(x)$ permutes $\mathbb{F}_{q^2}$ then (2) holds and the polynomial $G(x) = x^{r+kn\ell}(R(x)^{\ell}h(x))^{q-1}$ permutes μ_{q+1} by Lemma 1. From $G(x)$ permutes μ_{q+1} we know that conditions (1) and (3) hold. □

From Corollary 1 we list some examples of permutation polynomials over $\mathbb{F}_{q^2}$ from permutation polynomials over the unite circle μ_{q+1}.

Example 1 Let m be a positive integer and $q = 2^m$. The following polynomials permute the finite field $\mathbb{F}_{q^2}$.

(1) $x^7 + x^{3q+4} + x^{4q+3} + x^{6q+1} + x^{7q}$ for an m satisfying $\gcd(m, 3) = 1$ and $m \not\equiv 2 \mod 4$.
(2) $x^{11} + x^{q+10} + x^{2q+9} + x^{4q+7} + x^{6q+5} + x^{8q+3} + x^{11q}$ for an m satisfying $m \not\equiv 0 \mod 10$ and $m \not\equiv 2 \mod 4$.
(3) $x^{11} + x^{q+10} + x^{3q+8} + x^{4q+7} + x^{5q+6} + x^{6q+5} + x^{7q+4} + x^{8q+3} + x^{11q}$ for an even m satisfying $m \not\equiv 0 \mod 10$.
(4) $x^{2^k+3} + x^{3q+2^k} + x^{2^k \cdot q+3} + x^{(2^k+1)q+2} + x^{(2^k+2)q+1}$ for a positive integer k and an even m satisfying $\gcd(2^k+3, q-1) = 1$ and $\gcd(2^k+1, q+1) = 1$.
(5) $x^{2^k+3} + x^{3q+2^k} + x^{(2^k+1)q+2} + x^{(2^k+2)q+1} + x^{(2^k+3)q}$ for a positive integer k and an even m satisfying $\gcd(2^k+3, q-1) = 1$ and $\gcd(2^k-1, q+1) = 1$.

Proof We only prove the case (1) and the proofs of the other cases are similar, and omit the details here.

Let $R(x) = 1 + x + x^2 + x^3 + x^4$ and $h(x) = 1 + x + x^3$. It is verified that $F(x) = x^7+x^{3q+4}+x^{4q+3}+x^{6q+1}+x^{7q} = x^7R(x^{q-1})h(x^{q-1})$. This is $F(x)$ in Corollary 1 for $n = 4, r = 3, k = 1$ and $\ell = 1$. We easily verify that $\gcd((n+1)k, q+1) = \gcd(5, 2^m + 1) = 1$ since $m \not\equiv 2 \mod 4$, and $\gcd(r + kn\ell, q - 1) = \gcd(7, 2^m - 1) = 1$ since $\gcd(m, 3) = 1$. By Lemma 7, we know that $g(x) = x^rh(x)^{q-1} = x^3(1 + x + x^3)^{q-1}$ permutes μ_{q+1}. So, the polynomial in (1) is a permutation polynomial over $\mathbb{F}_{q^2}$ from Corollary 1. □

In the end of this section, we list all the known pairs (s, t) such that the polynomials of the form (1) are permutations in Table 1.

4 A class of permutation trinomials over $\mathbb{F}_{3^{2m}}$

It is clear that polynomials of the form (1) are a special case of polynomials of the form $x^rh(x^{\frac{q-1}{d}})$, where r, d are positive integers satisfying $d \mid (q - 1)$, $1 \le r < \frac{q-1}{d}$ and $h(x) \in \mathbb{F}_q[x]$. Recently, some new permutation trinomials of this form were obtained in [9–11] over finite fields with odd characteristic. Permutation property of trinomials in those papers is derived by using Lemma 1. At the same time, Hou [6, 7] proposed several classes of permutation trinomials with this form by highly technical calculations. Following some techniques in [6] we obtain a new class of permutation trinomials having the form,

$$f(x) = x^{4(q-1)+1} + x^{(q-1)^2+1} - x, \tag{8}$$

over $\mathbb{F}_{q^2}$, where $q = 3^m$.

To this end, we need some preparations. Denote by $\lambda = \mathrm{Tr}_m^{2m}(x) = x+x^q$ and $\mu = x\cdot x^q$ for $x \in \mathbb{F}_{q^2}$. The following lemma can be verified by routine calculations.

Lemma 9 *Let $q = 3^m$ and $\mathbb{F}_{q^2}$ be a finite field. For $x \in \mathbb{F}_{q^2}$,*

$$Tr_m^{2m}(x^7) = \lambda^7 - \mu\lambda^5 - \mu^2\lambda^3 - \mu^3\lambda, \quad Tr_m^{2m}(x^5) = \lambda^5 + \mu\lambda^3 - \mu^2\lambda,$$

Table 1 Known pairs (s, t) such that $f(x)$ defined by (1) are permutation polynomials

(s, t)	$g(x)$	Conditions	Equivalent Pairs	Proven in
$(k, -k)$	x	see Thm. 3.4 in [3]	$(\frac{\pm k}{2k\mp 1}, \frac{\pm 2k}{2k\mp 1})$	[3]
$(2, -1)$	$\frac{1+x^2+x^3}{1+x+x^3}$	positive m	$(1, \frac{1}{3}), (1, \frac{2}{3})$	[3, 26]
$(1, -\frac{1}{2})$	$\frac{x(1+x^2+x^3)}{1+x+x^3}$	$\gcd(3, m) = 1$	$(1, \frac{3}{2}), (\frac{1}{4}, \frac{3}{4})$	[5, 9, 10]
$(-\frac{1}{3}, \frac{4}{3})$	$\frac{1+x^4+x^5}{1+x+x^5}$	m even	$(1, \frac{1}{5}), (1, \frac{4}{5})$	[10, 13, 26]
$(3, -1)$	$\frac{1+x^3+x^4}{x(1+x+x^4)}$	m even	$(\frac{3}{5}, \frac{4}{5}), (\frac{1}{3}, \frac{4}{3})$	[10, 13, 26]
$(-\frac{2}{3}, \frac{5}{3})$	$\frac{1+x^5+x^7}{1+x^2+x^7}$	m even	$(1, \frac{2}{7}), (1, \frac{5}{7})$	[13]
$(\frac{1}{5}, \frac{4}{5})$	$\frac{x(1+x^3+x^4)}{1+x+x^4}$	$\gcd(5, 2^m + 1) = 1$	$(1, -\frac{1}{3}), (1, \frac{4}{3})$	[5, 10, 13]
$(2, -\frac{1}{2})$	$\frac{x(1+x+x^5)}{1+x^4+x^5}$	$m \equiv 2, 4 \mod 6$	$(\frac{2}{3}, \frac{5}{6}), (\frac{1}{4}, \frac{5}{4})$	[10]
$(4, -2)$	$\frac{1+x^4+x^6}{x(1+x^2+x^6)}$	$\gcd(3, m) = 1$	$(\frac{4}{7}, \frac{6}{7}), (\frac{2}{5}, \frac{6}{5})$	[10]
$(\frac{2^k}{2^k-1}, \frac{-1}{2^k-1})$	$\frac{1+x^{2^k}+x^{2^k+1}}{1+x+x^{2^k+1}}$	$\gcd(2^k - 1, 2^m + 1) = 1$	$(1, \frac{1}{2^k+1}), (1, \frac{2^k}{2^k+1})$	[12]
$(\frac{1}{2^k+1}, \frac{2^k}{2^k+1})$	$\frac{x+x^{2^k}+x^{2^k+1}}{1+x+x^{2^k}}$	$\gcd(2^k + 1, 2^m + 1) = 1$	$(1, \frac{2^k}{2^k-1}), (1, \frac{-1}{2^k-1})$	[12]
$(\frac{2}{7}, \frac{8}{7})$	$\frac{1+x^6+x^8}{x(1+x^2+x^8)}$	$\gcd(m, 2) = 1$	$(2, -\frac{2}{3}), (\frac{2}{3}, \frac{8}{9})$	Theorem 1
$(-\frac{2}{7}, \frac{8}{7})$	$\frac{x(1+x^8+x^{10})}{1+x^2+x^{10}}$	$m \equiv 2, 4 \mod 6$	$(\frac{10}{9}, \frac{8}{9}), (\frac{2}{11}, \frac{10}{11})$	Theorem 2

$$Tr_m^{2m}(x^4) = \lambda^4 - \mu\lambda^2 - \mu^2, \quad Tr_m^{2m}(x^{12}) = \lambda^{12} - \mu^3\lambda^6 - \mu^6,$$
$$Tr_m^{2m}(x^8) = \lambda^8 + \mu\lambda^6 - \mu^2\lambda^4 - \mu^3\lambda^2 - \mu^4.$$

Using above lemma we can prove the following theorem.

Theorem 4 *Let m be a positive integer with $m \not\equiv 0 \pmod 6$. Let $q = 3^m$ and $\mathbb{F}_{q^2}$ be a finite field with q^2 elements. The polynomial $f(x) = x^{4q-3} + x^{q^2-2q+2} - x$ is a permutation trinomial over $\mathbb{F}_{q^2}$.*

Proof We first show that $f(x)$ permutes $\mathbb{F}_q$. If $f(x) \in \mathbb{F}_q$ for $x \in \mathbb{F}_{q^2}$ then $f(x)^q = f(x)$, i.e.,

$$x^{4-3q} + x^{3q-2} - x^q = x^{4q-3} + x^{3-2q} - x. \tag{9}$$

Denote by $y = x^{q-1}$. Assume $x \neq 0$ then $y \neq 0$. From (9) we get

$$y^4 + y^{-2} - 1 = y^{-3} - y^3 + y. \tag{10}$$

Equation (10) is reduced to

$$(y-1)^7 = 0.$$

So, $y = 1$, i.e., $x^{q-1} = 1$. Hence, $x \in \mathbb{F}_q$. On the other hand, if $x \in \mathbb{F}_q$ then $f(x) = x^{4q-3} + x^{3-2q} - x = x$. So, $f(x)$ permutes $\mathbb{F}_q$.

From above analysis we know that $f(\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \subset \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Next, for any $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, we show that the equation

$$f(x) = x^{4q-3} + x^{q^2-2q+2} - x = \alpha \tag{11}$$

has one solution in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ only depending on α. Taking trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ on both sides of (11) and using Lemma 9 we have

$$\begin{aligned}\beta = \mathrm{Tr}_m^{2m}(\alpha) &= \mathrm{Tr}_m^{2m}(x^{4q-3}) + \mathrm{Tr}_m^{2m}(x^{3-2q}) - \mathrm{Tr}_m^{2m}(x)\\ &= \frac{\mathrm{Tr}_m^{2m}(x^7)}{x^{3(1+q)}} + \frac{\mathrm{Tr}_m^{2m}(x^5)}{x^{2(1+q)}} - \mathrm{Tr}_m^{2m}(x)\\ &= \frac{\lambda^7 - \mu\lambda^5 - \mu^2\lambda^3 - \mu^3\lambda}{\mu^3} + \frac{\lambda^5 + \mu\lambda^3 - \mu^2\lambda}{\mu^2} - \lambda\\ &= \frac{\lambda^7}{\mu^3}.\end{aligned} \tag{12}$$

Taking norm function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ on both sides of (11) and using Lemma 9 we have

$$\begin{aligned}\gamma = \alpha \cdot \alpha^q &= (x^{4q-3} + x^{3-2q} - x)(x^{4-3q} + x^{3q-2} - x^q)\\ &= \frac{\mathrm{Tr}_m^{2m}(x^{12})}{x^{5(1+q)}} - \frac{\mathrm{Tr}_m^{2m}(x^8)}{x^{3(1+q)}} - \frac{\mathrm{Tr}_m^{2m}(x^4)}{x^{1+q}}\\ &= \frac{\lambda^{12} - \mu^3\lambda^6 - \mu^6}{\mu^5} - \frac{\lambda^4 - \mu\lambda^2 - \mu^2}{\mu}\\ &\quad - \frac{\lambda^8 + \mu\lambda^6 - \mu^2\lambda^4 - \mu^3\lambda^2 - \mu^4}{\mu^3}\\ &= \frac{\lambda^{12}}{\mu^5} - \frac{\lambda^8}{\mu^3} + \frac{\lambda^6}{\mu^2} - \lambda^2 + \mu.\end{aligned} \tag{13}$$

From (12) and (13) we calculate $\frac{\gamma}{\beta^2}$ as follows,

$$\begin{aligned}\frac{\gamma}{\beta^2} &= \frac{\mu}{\lambda^2} - \frac{\mu^3}{\lambda^6} + \frac{\mu^4}{\lambda^8} - \frac{\mu^6}{\lambda^{12}} + \frac{\mu^7}{\lambda^{14}} \\ &= \left(\frac{\mu}{\lambda^2} - 1\right)^7 + 1. \qquad (14)\end{aligned}$$

It is clear that $\lambda, \mu \in \mathbb{F}_q$. Since $m \not\equiv 0 \pmod 6$, we have $\gcd(7, q-1) = 1$, and denote the inverse of 7 modulo $q-1$ by $\frac{1}{7}$. So, from (14) we have

$$\frac{\mu}{\lambda^2} = \left(\frac{\gamma}{\beta^2} - 1\right)^{\frac{1}{7}} + 1. \qquad (15)$$

Combining (12) and (15) we have

$$x + x^q = \lambda = \beta\left((\frac{\gamma}{\beta^2} - 1)^{\frac{1}{7}} + 1\right)^3. \qquad (16)$$

Substituting the value of λ into (15) we get

$$x \cdot x^q = \mu = \beta^2\left((\frac{\gamma}{\beta^2} - 1)^{\frac{1}{7}} + 1\right)^7. \qquad (17)$$

It is know that $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So, $x^q \neq x$. From (16) and (17) we know that x and x^q are two distinct solutions of the following quadratic equation

$$z^2 - \beta\left((\frac{\gamma}{\beta^2} - 1)^{\frac{1}{7}} + 1\right)^3 z + \beta^2\left((\frac{\gamma}{\beta^2} - 1)^{\frac{1}{7}} + 1\right)^7 = 0.$$

So, (11) has only one solution x in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, i.e., $f(x)$ permutes the set $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Combining above two cases we know that $f(x)$ permutes $\mathbb{F}_{q^2}$. □

5 Concluding remark

In this paper, we present two classes of permutation trinomials with the form (1) over the finite field $\mathbb{F}_{2^{2m}}$ and a class of permutation trinomials like this form over $\mathbb{F}_{3^{2m}}$. Moreover, a method to construct permutation polynomials from known ones is provided. During the study of permutation trinomials of the form (1), we have come across the pair $(s,t) = (\frac{4}{11}, \frac{10}{11})$ such that the polynomial of the form (1) for an m with $\gcd(m, 5) = 1$ can possibly be a permutation trinomial over $\mathbb{F}_{2^{2m}}$. We have verified the conjecture for m from 2 to 12 using computers. It would be nice if this conjecture can be settled.

Acknowledgements The authors wish to thank the anonymous referees for their helpful comments. The work was partially supported by National Natural Science Foundation of China (NSFC) under Grant 11101131.

References

1. Berlekamp, E.R., Rumsey, H., Solomon, G.: On the solution of algebraic equations over finite fields. Inf. Control. **10**(67), 553–564 (1967)
2. Bassalygo, L.A., Zinoviev, V.A.: Permutation and complete permutation polynomials. Finite Field Appl. **33**, 198–211 (2015)

3. Ding, C., Qu, L., Wang, Q., Yuan, J., Yuan, P.: Permutation trinomials over finite fields with even characteristic. SIAM J. Discrete Math. **29**, 79–92 (2015)
4. Ding, C., Yuan, J.: A family of skew Hadamard difference sets. J. Combin. Theory Ser. A **113**, 1526–1535 (2006)
5. Gupta, R., Sharma, R.K.: Some new classes of permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **41**, 89–96 (2016)
6. Hou, X.: Determination of a type of permutation trinomials over finite fields. Acta Arithmetica **166**, 253–278 (2014)
7. Hou, X.: Determination of a type of permutation trinomials over finite fields II. Finite Fields Appl. **35**, 16–35 (2015)
8. Laigle-Chapuy, Y.: Permutation polynomial and application to coding theory. Finite Fields Appl. **13**, 58–70 (2007)
9. Li, K., Qu, L., Chen, X.: New classes of permutation bionmials and permutation trinomials over finite fields. Finite Fields Appl. **43**, 16–23 (2017)
10. Li, K., Qu, L., Li, C., Fu, S.: New Permutation Trinomials Constructed from Fractional Polynomials. arXiv:1605.06216 (2016)
11. Li, N.: On two conjectures about permutation trinomials over $\mathbb{F}_{3^{2k}}$. Finite Fields Appl. **47**, 1–10 (2017)
12. Li, N., Helleseth, T.: New Permutation Trinomials from Niho Exponents over Finite Fields with even Characteristic. arXiv:1606.03768 (2016)
13. Li, N., Helleseth, T.: Several classes of permutation trinomials from Niho exponents. Cryptogr. Commun. **9**(6), 693–705 (2017)
14. Li, N., Helleseth, T., Tang, X.: Further results on a class of permutation polynomials over finite fields. Finite Fields Appl. **22**, 16–23 (2013)
15. Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Cambridge University Press, Cambridge (1997)
16. Leonard, P.A., Williams, K.S.: Quartics over $GF(2^n)$. Proc. Amer. Math. Soc. **36**(2), 347–350 (1972)
17. Muller, W.B., Nobauer, R.: Cryptanalysis of the Dickson-scheme. In: Proceedings of EUROCRYPT 85, pp. 215–230. Springer, New York (1986)
18. Niho, Y.: Multivalued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences. Ph.D. Dissertation, University of Southern California, Los Angeles (1972)
19. Park, Y.H., Lee, J.B.: Permutation polynomials and group permutation polynomials. Bull. Aust. Math. Soc. **63**, 67–74 (2001)
20. Qu, L., Tan, Y., Tan, C.H., Li, C.: Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Inform. Theory **59**, 4675–4686 (2013)
21. Rivest, R.L., Shamir, A., Aselman, L.M.: A method for obtaining gigital signatures and public-key cryptosytems. Commun. ACM **21**, 120–126 (1978)
22. Sun, J., Takeshita, O.Y.: Interleavers for turdo codes using permutation polynomials over integer rings. IEEE Trans. Inform. Theory **51**, 101–119 (2005)
23. Tu, Z., Zeng, X., Hu, L.: Several classes of complete permutation polynomials. Finite Fields Appl. **25**, 182–193 (2014)
24. Wang, Q.: Cyclotomic mapping permutation polynomials over finite fields. In: Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, Los Angeles, CA, USA, May 31–June 2, 2007, Lect. Notes Comput. Sci., vol. 4893, pp. 119–128 (2007)
25. Zieve, M.E.: On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$. Proc. Amer. Math. Soc. **137**, 209–216 (2009)
26. Zha, Z., Hu, L., Fan, S.: Further results on permutation trinomials over finite fields with even characteristic. Finite Fields Appl. **45**, 43–52 (2017)