GANITA, Vol.73(2), 2023, 141-147

SOME NEW CLASSES OF PERMUTATION TRINOMIALS OVER $\mathbb{F}_{2^{2m}}$

P. L. SHARMA ✉, **SHALINI GUPTA and SUSHIL KUMAR**

Abstract

A polynomial f over finite field $\mathbb{F}_q$ is called a permutation polynomial if f permutes the elements of $\mathbb{F}_q$. We present the constructions of permutation trinomials over finite fields with even characteristic by using the known permutations of the set of $(2^m + 1)$-th roots of unity.

2010 *Mathematics subject classification:* 11T06; 11T55; 12E20.

Keywords and phrases: Finite fields, Permutation polynomials, Permutation trinomials, Trace function.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^*$ denotes its multiplication group, where q is a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a permutation polynomial over $\mathbb{F}_q$ if the associated function $f : c \to f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is one-to-one. Hermite and Dickson were the first to study permutation polynomials for finite prime fields and arbitrary finite fields. We refer the reader to [10, 11] for an overview of permutation polynomials. Permutation polynomials have many applications in mathematics and engineering such as coding theory, cryptography and combinatorial designs. A survey of recent advances paper on permutation polynomials is [5].

Permutation polynomials with few terms have been extensively explored because of their simple algebraic form and their extraordinary properties. Hence, we are especially interested in permutation trinomials over finite fields with even characteristic. The existence of the permutation polynomials of the form $x^r h(x^{(q-1)/d})$ can be found in [13], where r and d are positive integers with $d \mid (q-1)$. For the construction of classes of permutation polynomials with few terms, see [1, 4, 6–9, 16]. Some new classes of permutation trinomials over finite fields with even characteristic can be found in [2, 3, 12, 15]. Xu at el. [14] found some permutation pentanomials and trinomials over finite fields with even characteristic. We extend the work of [3, 14, 15] by constructing five classes of permutation trinomials over finite fields with even characteristic.

2. Preliminaries

Throughout this paper, μ_d denotes the set of d-th roots of unity in the algebraic closure of $\mathbb{F}_q$. For each $x \in \mathbb{F}_q$, we denote x^{2^m} by $\bar{x}$ in analogy with the usual complex conjugation. The unit circle of $\mathbb{F}_{2^m}$ is defined as

$$\mu_{2^m+1} = \{x \in \mathbb{F}_q : x^{2^m+1} = x\bar{x} = 1\}.$$

The trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by

$$Tr_1^m(x) = x + x^2 + ... + x^{2^{m-1}}.$$

Trace function $Tr_1^m(.)$ is linear and for $k \in \mathbb{N}$,

$$Tr_1^m(x^{2^k}) = Tr_1^m(x).$$

The following results are needed in the next sections.

Lemma 2.1. *[16] Let $d, r > 0$ with $d|(q-1)$ and $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h(x^{(q-1)/d})$ permute $\mathbb{F}_q$ if and only if the following two conditions hold:*

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

Lemma 2.2. *[9] For a positive integer m, the quadratic equation $x^2 + ax + b = 0, a, b \in \mathbb{F}_{2^m}, a \neq 0$, has solutions in $\mathbb{F}_{2^m}$ if and only if $Tr_1^m(\frac{b}{a^2}) = 0$.*

Lemma 2.3. *[3] For $m \in \mathbb{N}$, the polynomial $1 + x + x^3$ has no roots in μ_{2^m+1}.*

Lemma 2.4. *For a positive integer m, the polynomials $1 + x^2 + x^5$ and $1 + x^3 + x^5$ have no roots in μ_{2^m+1}.*

Proof. Suppose $\alpha \in \mu_{2^m+1}$ is a root of $1 + x^2 + x^5$, that is,

$$1 + \alpha^2 + \alpha^5 = 0. \tag{2.1}$$

Raising both sides of (2.1) to the power 2^m and multiplying it by α^5, we get

$$1 + \alpha^3 + \alpha^5 = 0. \tag{2.2}$$

On adding (2.1) and (2.2), we obtain $\alpha^3 + \alpha^2 = 0$, which implies that $\alpha = 1$. But $\alpha = 1$ does not satisfy (2.1), which is a contradiction. Hence the polynomial $1 + x^2 + x^5$ has no roots in μ_{2^m+1}. Using similar arguments, it is easy to show that polynomial $1 + x^3 + x^5$ has no roots in μ_{2^m+1}. □

3. Main Results

In this section, we present permutation trinomials of the form $x^r h(x^{q-1/d})$ over $\mathbb{F}_{2^{2m}}$, where $d = 2^m + 1$.

Theorem 3.1. *The polynomial $f_1(x) = x^5 + x^{2^{m+1}+3} + x^{5.2^m}$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$ if and only if $m \not\equiv 0 \ mod\ 4$.*

Proof. The polynomial $f_1(x)$ is of the type $x^r h_1(x^{(q-1)/d})$, where $r = 5$ and $h_1(x) = 1 + x^2 + x^5 \in \mathbb{F}_{2^{2m}}[x]$. Since $\gcd(5, 2^m - 1) = 1$ as $m \not\equiv 0 \ mod\ 4$, therefore by Lemma 2.1, $f_1(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if the polynomial $u_1(x) = x^5 h_1(x)^{2^m-1}$ permutes μ_{2^m+1}.
The Lemma 2.4 concludes that $h_1(x)$ has no roots in μ_{2^m+1}, which implies $u_1(x) \neq 0$ for $x \in \mu_{2^m+1}$. It is easy to check that $u_1(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$.
Therefore, $u_1(x)$ permutes μ_{2^m+1} if and only if $u_1(x)$ is one-one on μ_{2^m+1}. For this, assume that $u_1(x)$ is not one-one, that is, there exist $x, y \in \mu_{2^m+1}$ and $x \neq y$ such that $u_1(x) = u_1(y)$. Then we have

$$\frac{x^5 + x^3 + 1}{x^5 + x^2 + 1} = \frac{y^5 + y^3 + 1}{y^5 + y^2 + 1}. \tag{3.1}$$

$$\left\{ \because u_1(x) = x^5 h_1(x)^{2^m-1} = x^5(1 + x^2 + x^5)^{2^m-1} = \frac{x^5 + x^3 + 1}{x^5 + x^2 + 1} \right\}$$

From (3.1), we obtain

$$(1 + x^2y^2)(x + y)^3 + (1 + x^3y^3)(x + y)^2 + (xy + x^2y^2 + x^3y^3)(x + y) = 0. \tag{3.2}$$

As $x \neq y$, so dividing both sides of (3.2) by $(x + y)^5$, we obtain

$$\frac{(1 + x^2y^2)}{(x + y)^2} + \frac{(1 + x^3y^3)}{(x + y)^3} + \frac{(xy + x^2y^2 + x^3y^3)}{(x + y)^4} = 0. \tag{3.3}$$

This implies that

$$(ab)^2 + ((a + b) + (a + b)^2)ab + (a + b)^2 + (a + b)^3 = 0, \tag{3.4}$$

where $a = \frac{1}{x+y}$ and $b = \frac{xy}{x+y}$. Note that $a + b$ and $ab \in \mathbb{F}_{2^m}$.
It follows from the Lemma 2.2 that the quadratic equation $x^2 + ax + b = 0; a, b \in \mathbb{F}_{2^m}, a \neq 0$ has solutions in $\mathbb{F}_{2^m}$ if and only if $Tr_1^m(\frac{b}{a^2}) = 0$.
Therefore, from (3.4), we have

$$Tr_1^m\left[\frac{(a + b)^2 + (a + b)^3}{(a + b)^2 + (a + b)^4}\right] = 0. \tag{3.5}$$

This implies that

$$Tr_1^m(\frac{1}{1 + a + b}) = 0,$$

which is a contradiction, that means $u_1(x)$ is one-one. Hence, $f_1(x)$ is permutation polynomial over $\mathbb{F}_{2^{2m}}$.
Conversely, if $f_1(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$, then by Lemma 2.1, we have $\gcd(5, 2^m - 1) = 1$, which implies that $m \not\equiv 0 \ mod\ 4$. □

Theorem 3.2. *The polynomial $f_2(x) = x^5 + x^{3.2^m+2} + x^{5.2^m}$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$ if and only if $m \not\equiv 0 \ mod\ 4$.*

Proof. The polynomial $f_2(x)$ is of the type $x^r h_2(x^{(q-1)/d})$, where $r = 5$ and $h_2(x) = 1 + x^3 + x^5 \in \mathbb{F}_{2^{2m}}[x]$. Since $\gcd(5, 2^m - 1) = 1$ as $m \not\equiv 0 \ mod\ 4$. Thus, Lemma 2.1 concludes that $f_2(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if the polynomial $u_2(x) = x^5 h_2(x)^{2^m-1}$ permutes μ_{2^m+1}.
It follows from Lemma 2.4 that the polynomial $h_2(x)$ has no roots in μ_{2^m+1}, which implies $u_2(x) \neq 0$ for $x \in \mu_{2^m+1}$. It is easy to check that $u_2(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$.
Therefore, $u_2(x)$ permutes μ_{2^m+1} if and only if $u_2(x)$ is one-one on μ_{2^m+1}. For this, assume that $u_2(x)$ is not one-one, that is, there exist $x, y \in \mu_{2^m+1}$ and $x \neq y$ such that $u_2(x) = u_2(y)$. Then for $x \in \mu_{2^m+1}$,

$$u_2(x) = x^5(1 + x^3 + x^5)^{2^m-1} = \frac{x^5 + x^2 + 1}{x^5 + x^3 + 1} = \frac{1}{u_1(x)}. \tag{3.6}$$

It is clear from (8) that $u_2(x)$ permutes μ_{2^m+1} if and only if $u_1(x)$ permutes μ_{2^m+1}. Since $u_1(x)$ permutes μ_{2^m+1}, see [Theorem 3.1]. Therefore, $u_2(x)$ permutes μ_{2^m+1}. Hence, Lemma 2.1 concludes that $f_2(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$. □

Theorem 3.3. *The polynomial $f_3(x) = x^6 + x^{2^{m+1}+4} + x^{5.2^m+1}$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$ if and only if m is odd.*

Proof. The polynomial $f_3(x)$ is of the form $x^r h_3(x^{(q-1)/d})$, where $r = 6$ and $h_3(x) = 1 + x^2 + x^5 \in \mathbb{F}_{2^{2m}}[x]$. Since $\gcd(6, 2^m - 1) = 1$ as m is odd, therefore by Lemma 2.1, $f_3(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if the polynomial $u_3(x) = x^6 h_3(x)^{2^m-1} = \frac{x^6+x^4+x}{x^5+x^2+1}$ permutes μ_{2^m+1}.
It follows from Lemma 2.4 that $h_3(x)$ has no roots in μ_{2^m+1}, which implies $u_3(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$.
Now, we need to prove that $u_3(x)$ is one-one on μ_{2^m+1}, assume that there exist $x, y \in \mu_{2^m+1}$ and $x \neq y$ such that $u_3(x) = u_3(y)$. Then

$$\frac{x^6 + x^4 + x}{x^5 + x^2 + 1} = \frac{y^6 + y^4 + y}{y^5 + y^2 + 1}. \tag{3.7}$$

After solving (3.7), we have

$$(x + y)^6 + (1 + xy + x^2y^2)(x + y)^4 + (1 + xy + x^4y^4 + x^5y^5)(x + y) = 0. \tag{3.8}$$

Dividing both sides of (3.8) by $(x + y)^6$ leads to

$$1 + \frac{(1 + xy + x^2y^2)}{(x + y)^2} + \frac{(1 + xy + x^4y^4 + x^5y^5)}{(x + y)^5} = 0. \tag{3.9}$$

Let $a = \frac{1}{x+y}$ and $b = \frac{xy}{x+y}$, clearly $a + b$ and $ab \in \mathbb{F}_{2^m}$. By substituting the values of a and b in (3.9), we obtain

$$(a + b)^5 + (a + b)^2 + ab + 1 = 0. \tag{3.10}$$

Dividing both sides of (3.10) by $(a+b)$, we get

$$(a+b)^4 + (a+b) + \frac{(ab+1)}{(a+b)} = 0. \tag{3.11}$$

Using the property $Tr_1^m(x)^2 = Tr_1^m(x)$ for any $x \in \mathbb{F}_{2^m}$, (3.11) turns out to be

$$Tr_1^m\left(\frac{ab+1}{a+b}\right) = 0,$$

which is a contradiction. Therefore, $u_3(x)$ permutes μ_{2^m+1}. Hence, $f_3(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$.
Conversely, if $f_3(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$, then the Lemma 2.1 concludes that $\gcd(6, 2^m - 1) = 1$, which implies that m is odd. □

THEOREM 3.4. *The polynomial* $f_4(x) = x^4 + x^{3.2^m+1} + x^{5.2^m-1}$ *is a permutation polynomial over* $\mathbb{F}_{2^{2m}}$.

PROOF. The polynomial $f_4(x)$ is of the form $x^r h_4(x^{(q-1)/d})$, where $r = 4$ and $h_4(x) = 1 + x^3 + x^5 \in \mathbb{F}_{2^{2m}}[x]$. From Lemma 2.1, $f_4(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if $\gcd(4, 2^m - 1) = 1$ and the polynomial $u_4(x) = x^4 h_4(x)^{2^m-1}$ permutes μ_{2^m+1}.
Lemma 2.4 concludes that $h_4(x)$ has no roots in μ_{2^m+1}, which implies $u_4(x) \neq 0$ for $x \in \mu_{2^m+1}$ and hence $g_4(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$. Because μ_{2^m+1} is a finite set, $u_4(x)$ permutes μ_{2^m+1} if and only if $u_4(x)$ is one-one on μ_{2^m+1}.
For $x \in \mu_{2^m+1}$, we have

$$u_4(x) = x^4(1 + x^3 + x^5)^{2^m-1} = \frac{x^5 + x^2 + 1}{x^6 + x^4 + x} = \frac{1}{u_3(x)}.$$

Therefore, $u_4(x)$ permutes μ_{2^m+1} if and only if $u_3(x)$ permutes μ_{2^m+1}. It follows from Theorem 3.3 that $u_3(x)$ permutes μ_{2^m+1}, and thus, $u_4(x)$ permutes μ_{2^m+1}. Hence, the Lemma 2.1 concludes that $f_4(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$. □

THEOREM 3.5. *The polynomial* $f_5(x) = x^5 + x^{2^m+4} + x^{3.2^m+2}$ *is a permutation polynomial over* $\mathbb{F}_{2^{2m}}$ *if and only if* $m \not\equiv 0 \ mod\ 4$.

PROOF. The polynomial $f_5(x)$ is of the type $x^r h_5(x^{(q-1)/d})$, where $r = 5$ and $h_5(x) = 1 + x + x^3 \in \mathbb{F}_{2^{2m}}[x]$. Since $\gcd(5, 2^m - 1) = 1$ as $m \not\equiv 0 \ mod\ 4$, so by Lemma 2.1, $f_5(x)$ permutes $\mathbb{F}_{2^{2m}}$ if and only if the polynomial $u_5(x) = x^5 h_5(x)^{2^m-1}$ permutes μ_{2^m+1}.
It follows from Lemma 2.3 that $h_5(x) \neq 0$ for all $x \in \mu_{2^m+1}$, which implies that $u_5(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$. Now, we need to prove that $u_5(x)$ is one-one on μ_{2^m+1}, assume that there exist $x, y \in \mu_{2^m+1}$ and $x \neq y$ such that $u_5(x) = u_5(y)$. Then

$$\frac{x^5 + x^4 + x^2}{x^3 + x + 1} = \frac{y^5 + y^4 + y^2}{y^3 + y + 1}, \tag{3.12}$$

$$\left\{ \because u_5(x) = x^5 h_5(x)^{2^m-1} = x^5(1 + x + x^3)^{2^m-1} = \frac{x^5 + x^4 + x^2}{x^3 + x + 1} \right\}$$

Now (3.12) implies that

$$(x+y)^5 + (1+xy)(x+y)^4 + (1+x^3y^3)(x+y)^2 + (xy+x^2y^2+x^3y^3)(x+y) = 0.$$

Since $x \neq y$. Therefore, we have

$$1 + \frac{1+xy}{(x+y)} + \frac{1+x^3y^3}{(x+y)^3} + \frac{xy+x^2y^2+x^3y^3}{(x+y)^4} = 0. \tag{3.13}$$

Substituting $a = \frac{1}{x+y}$ and $b = \frac{xy}{x+y}$ in (3.13), we obtain

$$(ab)^2 + ((a+b) + (a+b)^2)(ab) + 1 + (a+b) + (a+b)^3 = 0. \tag{3.14}$$

As $a+b$ and $ab \in \mathbb{F}_{2^m}$, therefore, Lemma 2.2 concludes that the quadratic equation $x^2 + ax + b = 0; a, b \in \mathbb{F}_{2^m}, a \neq 0$ has solutions in $\mathbb{F}_{2^m}$ if and only if $Tr_1^m(\frac{b}{a^2}) = 0$. Therefore, from (3.14), we have

$$Tr_1^m\left[\frac{1+(a+b)+(a+b)^3}{(a+b)^2+(a+b)^4}\right] = 0,$$

which leads to a contradiction that $u_5(x)$ is not one-one which implies $u_5(x)$ permutes μ_{2^m+1}. Thus, $f_5(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$.
Conversely, if $f_5(x)$ is a permutation polynomial over $\mathbb{F}_{2^{2m}}$, therefore by Lemma 2.1, $\gcd(5, 2^m - 1) = 1$, which implies that $m \not\equiv 0 \ mod\ 4$. □

Acknowledgements: The authors gratefully acknowledge the support of UGC-SAP. The third author thankfully acknowledge the financial support of UGC.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] S. Ball and M. Zieve, *Sympectic spreads and permutation polynomials*, Finite Fields Appl., Lect. Notes Comput. Sci. **2948** (2004) 79–88.
[2] C. Ding, L. Qu, Q. Wang, J. Yuan and P. Yuan, *Permutation trinomials over finite fields with even characteristic*, SIAM J. Discrete Math. **29** (2015) 79–92.
[3] R. Gupta and R. K. Sharma, *Some new classes of permutation trinomials over finite field with even characteristic*, Finite Fields Appl. **41** (2016) 89–96.
[4] X. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl. **35** (2015) 16–35.
[5] X. Hou, *Permutation polynomials over finite fields – a survey of recent advances*, Finite Fields Appl. **32** (2015) 82–119.
[6] J. B. Lee and Y. H. Park, *Some permutation trinomials over finite fields*, Acta Math. Sci. **17** (1997) 250–254.
[7] K. Li, L. Qu and X. Chen, *New classes of permutation binomials and permutation trinomials over finite fields*, Finite Fields Appl. **43** (2017) 69–85.
[8] K. Li, L. Qu, C. Li and S. Fu, *New permutation trinomials constructed from fractional polynomials*, Acta Arithmetica **183** (2018) 101–116.
[9] N. Li and T. Helleseth, *Several classes of permutation trinomials from Niho exponents*, Cryptogr. Commun. **9** (2017) 693–705.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Application, Addision-Wesley, Reading, MA. **20** (1983).
[11] G. L. Mullen and D. Panario, *Handbook of Finite Fields*, Taylor & Francis, Boca Raton (2013).
[12] P. L. Sharma, M. Harish and S. Kumar, *Some permutation trinomials over finite fields* $\mathbb{F}_{2^{2m}}$, J. Indian Math. Soc., Accepted for Publication.
[13] D. Wan and R. Lidl, *Permutation polynomials of the form* $x^r h(x^{(q-1)/d})$ *and their group structure*, Monatshefte Math. **31** (1991) 12–24.
[14] G. Xi, X. Cao and J. Ping, *Some permutation pentanomials over finite fields with even characteristic*, Finite Fields Appl. **49** (2018) 212–226.
[15] Z. Zha, L. Hu and S. Fan, *Further results on permutation trinomials over finite fields with even characteristic*, Finite Fields Appl. **45** (2017) 43–52.
[16] M. E. Zieve, *Some families of permutation polynomials over finite fields*, Int. J. Number Theory **4** (2008) 851–857.

P. L. Sharma, (Corresponding Author) Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
e-mail: plsharma1964@gmail.com

Shalini Gupta, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
e-mail: shalini.garga1970@gmail.com

Sushil Kumar, Department of Mathematics & Statistics, Himachal Pradesh University, Shimla, India
e-mail: skthakur0304@gmail.com