



Article ID 1007-1202(2025)03-0231-04 DOI <https://doi.org/10.1051/wujns/2025303231>

Cite this article: QIN Xiaoer, GUO Xiaonan, QIU Yinuo, *et al.* A Note on a Class of Permutation Quadrinomials of  $F_{q^2}[J]$ . *Wuhan Univ J of Nat Sci*, 2025, 30(3): 231-234.

# A Note on a Class of Permutation Quadrinomials of $F_{q^2}$

□ QIN Xiaoer<sup>1</sup>, GUO Xiaonan<sup>1</sup>, QIU Yinuo<sup>1</sup>, YAN Li<sup>2†</sup>

1. School of Mathematics and Big Data, Chongqing University of Education, Chongqing 400065, China;
2. School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China

**Abstract:** Constructing permutation polynomials is a hot topic in finite fields, and permutation polynomials have many applications in different areas. In this paper, by using monomials on the cosets of a subgroup to characterize the permutational property of rational functions on  $\mu_{q+1}$ , we construct a class of permutation quadrinomials with the form  $f_{r,a,b,c,s,t,u}(x) = x^r(1 + ax^{s(q-1)} + bx^{t(q-1)} + cx^{u(q-1)})$  of  $F_{q^2}$ .

**Key words:** permutation quadrinomials; monomials; finite fields

**CLC number:** O156.1

## 0 Introduction

Let  $F_q$  be the finite field with  $q$  elements. A polynomial  $f(x) \in F_q[x]$  is called a permutation polynomial if  $f$  induces a bijection from  $F_q$  to itself. Permutation polynomials have wide applications in coding theory, cryptography and combinatorial designs. We refer the readers to Refs. [1-3] for more details of the recent advances.

Permutation polynomials with a few terms have attracted more attention in recent years for their simple algebraic forms and some special properties. There are several classes of permutation trinomials of the form  $x^r h(x^{q-1})$  over  $F_{q^2}$  constructed in recent years. Kyureghyan and Zieve<sup>[4]</sup> described a class of permutation trinomials having the form  $x + \gamma \text{Tr}_{q^2/q}(x^{(q^2+1)/4})$  of  $F_{q^2}$ , where  $\text{Tr}_{q^2/q}$  is the trace function from  $F_{q^2}$  to  $F_q$ . We note that this kind of permutation trinomials actually has the form

$x(1 + \gamma x^{\frac{q+3}{4}(q-1)} + \gamma x^{\frac{q^2+3q+1}{4}(q-1)})$ . Zheng *et al*<sup>[5]</sup> showed a class of permutation trinomials of the form  $cx - x^s + x^{sq}$ , where  $s = \frac{3q^2+2q-1}{4}$ , which can be rewritten as  $x(c - x^{\frac{3q+5}{4}(q-1)} + x^{\frac{3q^2+5q+1}{4}(q-1)})$ . In Ref. [6], the authors got several classes of more generalized permutation trinomials having similar forms to  $x^r(c + x^{\frac{q+3}{4}+k(q-1)} + x^{\frac{q^2+3q}{4}+k+1(q-1)})$  and  $x^r(c - x^{\frac{q+3}{4}+k(q-1)} + x^{\frac{q^2+3q}{4}+k+1(q-1)})$ . By using a similar idea to Ref. [6], Lavorante<sup>[7]</sup> constructed a few new families of permutation trinomials with the form  $x^r(c + x^{s(q-1)} + x^{t(q-1)})$ . By using monomial functions on the cosets of a subgroup of  $\mu_{q+1}$ , Hou and Lavorante<sup>[8]</sup> gave a general method to construct permutation polynomials over  $F_{q^2}$ . Specially, they presented several classes of permutation binomials and trinomials.

On the other hand, permutation quadrinomials also

**Received date:** 2024-07-15 © Wuhan University 2025

**Foundation item:** Supported by the National Natural Science Foundation of China (11926344), Science and Technology Research Program of Chongqing Municipal Education Commission (KJZD-K202401601), Doctor Talent Program of Chongqing University of Education (2023BSRC003) and Undergraduate Science Research Program of Chongqing University of Education (KY20240046)

**Biography:** QIN Xiaoer, male, Ph.D., research direction: number theory. E-mail: qincn328@sina.com

† Corresponding author. E-mail: yanl930@163.com

have attracted attention in recent years. Especially, constructing permutation quadrinomials of the form

$$f_{r,s,t,u}(x) = x^r(1 + ax^{s(q-1)} + bx^{t(q-1)} + cx^{u(q-1)}) \in F_{q^2}[x] \quad (1)$$

where  $r, s, t$  are integers, attracted great interest recently. Gupta<sup>[9]</sup> studied several classes of permutation quadrinomials of the form (1) over  $F_{q^2}$  with  $\text{Char}(F_q) = 3, 5$ . Tu et al<sup>[10]</sup> proposed a class of permutation quadrinomials having the form  $x^3(1 + ax^{q-1} + bx^{2(q-1)} + cx^{3(q-1)})$  of  $F_{2^{2m}}$ . In Ref. [11], the authors investigated some permutation quadrinomials of  $F_{2^{2m}}$  with the case of  $(r, s, t, u) = (1, -1, 1, 2)$  in (1) under some restrictive conditions. In Ref. [12], the authors provided more classes of permutation quadrinomials of the form (1) in characteristic two. Lavorante<sup>[13]</sup> used the Hasse-Weil type theorems to prove the necessary conditions for a polynomial in Ref. [12] to be a permutation polynomial. Ding and Zieve<sup>[14]</sup> determined all permutation polynomials over  $F_{q^2}$  having the form  $x^r h(x^{q-1})$ , where, for some  $Q$  which is the power of the character of  $F_q$ , the terms of  $h(x)$  have degrees  $\{0, 1, Q, Q + 1\}$  and  $r \equiv Q + 1 \pmod{q + 1}$ . The authors in Ref. [15] characterized two classes of permutation quadrinomials over  $F_{2^n}$  by using self-reciprocal polynomials. In this paper, motivated by the method in Ref. [6], we continue to construct a new class of permutation quadrinomials of  $F_{q^2}$ .

This paper is organized as follows: In Section 1, we list some results, which will be used in our paper. In Section 2, by using monomials of  $\mu_{\frac{q+1}{2}}$  and  $-\mu_{\frac{q+1}{2}}$ , we construct a class of permutation quadrinomials over  $F_{q^2}$  of the form  $x^r(1 + ax^{s(q-1)} + bx^{t(q-1)} + cx^{u(q-1)})$  for some integers  $r, s, t, u$ .

## 1 Preliminary

The following result was discovered independently by several authors.

**Lemma 1**<sup>[16-17]</sup> Let  $r$  be a positive integer. Then  $f(x) = x^r h(x^{q-1}) \in F_{q^2}[x]$  is a permutation polynomial of  $F_{q^2}$  if and only if each of the following is true:

- (1)  $\text{gcd}(r, q - 1) = 1$ ,
- (2)  $x^r h(x)^{q-1}$  permutes  $q + 1$ -th roots of unity  $\mu_{q+1}$ .

Specially, by using Lemma 1, constructing permutation polynomials of the form  $x^r h(x^{q-1})$  over  $F_{q^2}$  translates to finding permutations having the form  $x^r h(x)^{q-1}$  on the set of  $q + 1$ -th roots of unity  $\mu_{q+1}$ . For  $x \in \mu_{q+1}$ , one has

$$x^r h(x)^{q-1} = x^r \frac{h(x)^q}{h(x)} = x^r \frac{h^q(x^{-1})}{h(x)},$$

where  $h^q(x)$  denotes the polynomial obtained  $h(x)$  by raising every coefficient to the  $q$ -th power. Thus to show that  $x^r h(x)^{q-1}$  permutes  $F_{q^2}$ , the point is to prove that the rational function  $x^r \frac{h^q(x^{-1})}{h(x)}$  permutes  $\mu_{q+1}$ .

Let  $d|q + 1$  with  $d \geq 2$  be a positive integer and  $\zeta$  be a primitive  $d$ -th root of unity. We make some denotations:  $S_0 = \mu_{\frac{q+1}{d}}$  and  $S_i = \zeta^i S_0$  for  $1 \leq i \leq d - 1$ . It is easy to imply that  $\mu_{q+1} = \bigcup_{i=0}^{d-1} S_i$  and  $S_i \cap S_j = \emptyset$  for  $0 \leq i \neq j \leq d - 1$ .

For  $g(x) \in F_{q^2}[x]$ , if  $g(x)$  is a monomial on each subset of  $\mu_{q+1}$ , then by using the piecewise method, we can easily determine the permutational property of  $g(x)$  on  $\mu_{q+1}$  in the following lemma.

**Lemma 2**<sup>[6]</sup> Let  $\frac{q+1}{d}$  be a positive integer and  $A_i \in \mu_{q+1}$  for  $0 \leq i \leq d - 1$ . For  $g(x) \in F_{q^2}[x]$ , if

$$g(x) = A_i x^r, \text{ for } x \in S_i.$$

Then  $g(x)$  permutes  $\mu_{q+1}$  if and only if each of the following is true:

- (1)  $\text{gcd}(r, \frac{q+1}{d}) = 1$ , for  $0 \leq i \leq d - 1$ ;
- (2)  $A_i x_i^{r_i} \neq A_j x_j^{r_j}$  for  $x_i \in S_i$  and  $x_j \in S_j$ .

Lemma 2 provides an approach to study the permutational property of  $x^r \frac{h^q(x^{-1})}{h(x)}$  on  $\mu_{q+1}$  via monomials on the subsets  $S_i$ . In Refs. [4, 5, 7], the authors used the case  $d = 2$  in Lemma 2 to construct a few classes of permutation trinomials of  $F_{q^2}$ . By using the cases  $d = 3$ , the authors obtained several kinds of permutation trinomials of  $F_{q^2}$  in Refs. [16, 18].

## 2 Main Results

Motivated by the method in Ref. [6], we characterize several classes of permutation quadrinomials over  $F_{q^2}$  in this section.

**Theorem 1** Let  $q$  be a prime power with  $q \equiv 1 \pmod{8}$ , and  $a, b, c \in F_{q^2}$  satisfy  $(a + b + c)^{\frac{q+1}{2}} = 1$  and  $(b - c - a)^{\frac{q+1}{2}} = 1$ . Let  $r$  be a positive integer and  $k$  be an even integer. Then  $f(x) = x^r(1 + ax^{\frac{(q+3}{4} + k)(q-1)} + bx^{\frac{(3q+5}{4} + k)(q-1)} + cx^{\frac{(3q^2+5q}{4} + k+1)(q-1)})$  permutes  $F_{q^2}$  if and only if  $\text{gcd}(r, q -$

$1) = 1$  and  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

**Proof** It follows from Lemma 1 that  $f(x)$  permutes  $F_{q^2}$  if and only if  $\gcd(r, q - 1) = 1$  and  $g(x) = x^r(1 + ax^{u+k} + bx^{v+k} + cx^{qv+k+1})^{q-1}$  permutes  $\mu_{q+1}$ , where  $u = \frac{q+3}{4}, v = \frac{3q+5}{4}$ .

In the following, we claim that if  $\gcd(r, q - 1) = 1$ , then  $g(x)$  permutes  $\mu_{q+1}$  if and only if  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

We divide  $\mu_{q+1}$  into two subsets  $\mu_{\frac{q+1}{2}}$  and  $-\mu_{\frac{q+1}{2}}$ , and consider the following cases. For  $x$  in  $\mu_{\frac{q+1}{2}}$ , it is easy to check that  $x^u = x^v = x^{qv+1} = x^{1-v}$ . One has  $g(x) = x^r(1 + (a + b + c)x^{u+k})^{q-1}$ .

Since  $q \equiv 1 \pmod{8}$ , we have that  $\frac{q+1}{2}$  is odd. Then by  $(a + b + c)^{\frac{q+1}{2}} = 1$ , we deduce that the equation  $1 + (a + b + c)x^{u+k} = 0$  has no roots in  $\mu_{\frac{q+1}{2}}$ . Furthermore,

$$g(x) = x^r \frac{1 + (a + b + c)^q x^{-u-k}}{1 + (a + b + c)x^{u+k}} = (a + b + c)^q x^{r-k-u} \frac{1 + \frac{x^{k+u}}{(a + b + c)^q}}{1 + (a + b + c)x^{u+k}}.$$

By using  $(a + b + c)^{\frac{q+1}{2}} = 1$ ,  $g(x)$  can be simplified as  $\frac{1}{a + b + c} x^{r-k-u}$ . Since  $x \in \mu_{\frac{q+1}{2}}$  can be written as  $y^2$  for  $y \in \mu_{\frac{q+1}{2}}$  and  $2u \equiv 1 \pmod{\frac{q+1}{2}}$ , thus  $g(x)$  can be rewritten as  $\frac{1}{a + b + c} y^{2r-2k-1}$ .

For  $x$  in  $-\mu_{\frac{q+1}{2}}$ , one has  $x^u = -x^v = x^{qv+1} = x^{1-v}$ . Then

$$g(x) = x^r(1 + ax^{u+k} + bx^{v+k} + cx^{qv+1+k})^{q-1} = x^r(1 + (a - b + c)x^{u+k})^{q-1}.$$

Since  $q \equiv 1 \pmod{8}$ , we have that  $u$  and  $\frac{q+1}{2}$  are odd, thus  $u + k$  is odd. Then by  $(b - c - a)^{\frac{q+1}{2}} = 1$ , we know that  $1 + (a - b + c)x^{u+k} \neq 0$  for  $x \in -\mu_{\frac{q+1}{2}}$ . Thus

$$g(x) = x^r \frac{1 + (a - b + c)^q x^{-u-k}}{1 + (a - b + c)x^{u+k}} = (a - b + c)^q x^{r-k-u} \frac{1 + \frac{x^{k+u}}{(a - b + c)^q}}{1 + (a - b + c)x^{u+k}}.$$

Since  $(a - b + c)^q = \frac{1}{a - b + c}$  and  $\frac{1}{(a - b + c)^q} = a - b + c$ , then  $g(x) = \frac{1}{a - b + c} x^{r-k-u}$ . For  $x \in -\mu_{\frac{q+1}{2}}$ , there exists  $y \in \mu_{\frac{q+1}{2}}$  such that  $x$  can be presented by  $-y^2$ . Then  $g(x) = \frac{1}{a - b - c} y^{2r-2k-1}$ .

Note that  $\frac{1}{a + b + c} \in \mu_{\frac{q+1}{2}}$  and  $\frac{1}{a - b + c} \in -\mu_{\frac{q+1}{2}}$ .

Then it follows from Lemma 2 that  $g(x)$  permutes  $\mu_{q+1}$  if and only if  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ . Namely, the claim is true.

Therefore, we can conclude that  $f(x)$  permutes  $F_{q^2}$  if and only if  $\gcd(r, q - 1) = 1$  and  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

We complete the proof of Theorem 1.

Similarly, we can get the following results, and we omit their detailed proofs.

**Theorem 2** Let  $q$  be a prime power with  $q \equiv 1 \pmod{8}$ , and  $a, b, c \in F_{q^2}$  satisfy  $(a + b + c)^{\frac{q+1}{2}} = 1$  and  $(b - a + c)^{\frac{q+1}{2}} = 1$ . Let  $r$  be a positive integer and  $k$  be an even integer. Then  $f(x) = x^r(1 + ax^{\frac{q+3}{4}+k(q-1)} + bx^{\frac{3q+5}{4}+k(q-1)} + cx^{\frac{q^2+3q}{4}+k+1(q-1)})$  permutes  $F_{q^2}$  if and only if  $\gcd(r, q - 1) = 1$  and  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

**Theorem 3** Let  $q$  be a prime power with  $q \equiv 1 \pmod{8}$ , and  $a, b, c \in F_{q^2}$  satisfy  $(a + b + c)^{\frac{q+1}{2}} = 1$  and  $(b - a - c)^{\frac{q+1}{2}} = 1$ . Let  $r$  be a positive integer and  $k$  be an even integer. Then  $f(x) = x^r(1 + ax^{\frac{q+3}{4}+k(q-1)} + bx^{\frac{q^2+3q}{4}+k(q-1)} + cx^{\frac{3q^2+5q}{4}+k+1(q-1)})$  permutes  $F_{q^2}$  if and only if  $\gcd(r, q - 1) = 1$  and  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

**Theorem 4** Let  $q$  be a prime power with  $q \equiv 1 \pmod{8}$ , and  $a, b, c \in F_{q^2}$  satisfy  $(a + b + c)^{\frac{q+1}{2}} = 1$  and  $(a + b - c)^{\frac{q+1}{2}} = 1$ . Let  $r$  be a positive integer and  $k$  be an even integer. Then  $f(x) = x^r(1 + ax^{\frac{3q+5}{4}+k(q-1)} + bx^{\frac{q^2+3q}{4}+k(q-1)} + cx^{\frac{3q^2+5q}{4}+k+1(q-1)})$  permutes  $F_{q^2}$  if and only if  $\gcd(r, q - 1) = 1$  and  $\gcd(2r - 2k - 1, \frac{q+1}{2}) = 1$ .

## References

- [1] Hou X D. Permutation polynomials over finite fields: A survey of recent advances[J]. *Finite Fields and Their Applications*, 2015, **32**: 82-119.
- [2] Li N, Zeng X Y. A survey on the applications of niho exponents[J]. *Cryptography and Communications*, 2019, **11**(3): 509-548.
- [3] Wang Q. *Combinatorics and Finite Fields*[M]. Berlin: De

- Gruyter, 2019.
- [4] Kyureghyan G, Zieve M. *Contemporary Developments in Finite Fields and Applications*[M]. Singapore: World Scientific, 2016.
- [5] Zheng D B, Yuan M, Yu L. Two types of permutation polynomials with special forms[J]. *Finite Fields and Their Applications*, 2019, **56**: 1-16.
- [6] Qin X E, Yan L. Constructing permutation trinomials via monomials on the subsets of  $\mu_{q+1}$ [J]. *Applicable Algebra in Engineering, Communication and Computing*, 2021, **34**(2): 321-334.
- [7] Lavorante V P. New families of permutation trinomials constructed by permutations of  $\mu_{q+1}$ [EB/OL]. [2023-2-15]. <https://arxiv.org/abs/2105.12012>.
- [8] Hou X D, Lavorante V. P. A general construction of permutation polynomials of  $F_q$ [J]. *Finite Fields Appl*, 2023, **89**: 102193.
- [9] Gupta R. Several new permutation quadrinomials over finite fields of odd characteristic[J]. *Designs, Codes and Cryptography*, 2020, **88**(1): 223-239.
- [10] Tu Z, Zeng X Y, Helleseht T. New permutation quadrinomials over  $F_{2^m}$ [J]. *Finite Fields Appl*, 2018, **50**: 304-318.
- [11] Tu Z R, Zeng X Y, Helleseht T. A class of permutation quadrinomials[J]. *Discrete Mathematics*, 2018, **341**(11): 3010-3020.
- [12] Zheng L J, Liu B X, Kan H B, *et al*. More classes of permutation quadrinomials from Niho exponents in characteristic two[J]. *Finite Fields and Their Applications*, 2022, **78**: 101962.
- [13] Pallozzi Lavorante V P. On permutation quadrinomials from Niho exponents in characteristic two[J]. *Finite Fields and Their Applications*, 2024, **96**: 102418.
- [14] Ding Z G, Zieve M E. Determination of a class of permutation quadrinomials[J]. *Proceedings of the London Mathematical Society*, 2023, **127**(2): 221-260.
- [15] Brochero Martínez F E, Gupta R, Quoos L. Classification of some permutation quadrinomials from self reciprocal polynomials over  $F_2$ [J]. *Finite Fields and Their Applications*, 2023, **91**: 102276.
- [16] Akbary A, Wang Q. On polynomials of the form  $x^r f(x^{q-l})$ [J]. *Int J Math Math Sci*, 2007, **2007**: 23408.
- [17] Wang Q. Cyclotomic mapping permutation polynomials over finite fields[C]//*Sequences, Subsequences, and Consequences*. Berlin: Springer-Verlag, 2007: 119-128.
- [18] Li K Q, Qu L J, Chen X, *et al*. Permutation polynomials of the form  $cx + \text{Tr}_{q|q^3}(x^a)$  and permutation trinomials over finite fields with even characteristic[J]. *Cryptography and Communications*, 2018, **10**(3): 531-554.

## 有限域上一类置换四项式的注记

秦小二<sup>1</sup>, 郭筱楠<sup>1</sup>, 仇怡诺<sup>1</sup>, 鄢丽<sup>2</sup>

1. 重庆第二师范学院 数学与大数据学院, 重庆 400065

2. 重庆师范大学 数学科学学院, 重庆 401331

**摘要:** 构造置换多项式是有限域上的一个热点问题, 置换多项式在诸多领域都有应用。本文利用  $\mu_{q+1}$  的子群陪集上的单项式来刻画  $\mu_{q+1}$  上有理函数的置换性质, 构造了一类有限域  $F_{q^3}$  上形如  $f_{r,a,b,c,s,t,u}(x) = x^r(1 + ax^{s(q-1)} + bx^{t(q-1)} + cx^{u(q-1)})$  的置换四项式。

**关键词:** 置换四项式; 单项式; 有限域

□