

# A New Method of Construction of Permutation Trinomials with Coefficients 1

Hua Guo<sup>1,2</sup>, Shuo Wang<sup>3</sup>, Hutao Song<sup>1,4</sup>, Xiyong Zhang<sup>5,\*</sup>, Jianwei Liu<sup>1</sup>

<sup>1</sup> School of Cyber Science and Technology, Beihang University, Beijing 100191, China

<sup>2</sup> State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

<sup>3</sup> School of Electronic and Information Engineering, Beihang University, Beijing 100191, China

<sup>4</sup> State Key Laboratory of Software Development Environment, Beihang University, Beijing 100191, China

<sup>5</sup> Beijing Institute of Satellite Information Engineering, Beijing 100086, China

## Abstract

Permutation polynomials over finite fields are an interesting and constantly active research subject of study for many years. They have important applications in areas of mathematics and engineering. In recent years, permutation binomials and permutation trinomials attract people's interests due to their simple algebraic forms. In this paper, by reversely using Tu's method for the characterization of permutation polynomials with exponents of Niho type, we propose a new method to construct permutation trinomials with coefficients 1. Moreover, we give the explicit compositional inverses of a class of permutation trinomials for a special case.

**Keywords:** *Finite field, Permutation trinomial, Fractional reciprocal polynomial, Polar decomposition, Exponential sum*

## 1 Introduction

Let  $p$  be a prime number,  $n$  be a positive integer,  $q = p^n$ ,  $\mathbb{F}_q$  be a finite field with  $q$  elements, and  $\mathbb{F}_q^\times$  be its multiplicative group. Let  $f(x)$  be a polynomial over  $\mathbb{F}_q$ . If  $f : \alpha \mapsto f(\alpha)$  is a permutation of  $\mathbb{F}_q$ ,  $f(x)$  is called a permutation polynomial (abbreviated as PP) of  $\mathbb{F}_q$ . The algebraic closure of  $\mathbb{F}_q$  is denoted by  $\overline{\mathbb{F}}_q$ . For integer  $s, d > 0$  such that  $sd = q - 1$ , let  $\mu_d = \{x \in \overline{\mathbb{F}}_q : x^d = 1\}$  denote the unique cyclic subgroup of  $\mathbb{F}_q^\times$  of order  $d$ . Especially when  $q = 2^{2m}$  for some positive integer  $m$  and  $d = 2^m + 1$ ,  $\mu_d$  is written as  $U$  in this paper. Permutation polynomials have wide applications in various areas of mathematics and engineering, such as coding theory [17], cryptography [7, 16] and combinatorial designs [2]. Permutation binomials and trinomials with coefficients 1 have the simplest algebraic form. These types of PPs attract people's interests in recent years due to their important applications in cryptography (such as multivariate public key cryptography), integer sequences, and finite geometry, etc.

---

\*Corresponding author

Email addresses:

hguo@buaa.edu.cn (Hua Guo)

nicolas\_wangshuo@buaa.edu.cn (Shuo Wang)

htsong@buaa.edu.cn (Hutao Song)

Xiyong.Zhang@hotmail.com (Xiyong Zhang)

liujianwei@buaa.edu.cn (Jianwei Liu)

In general by Lagrange interpolation it is not difficult to construct a random PP for a given finite field. However it is difficult to find PPs with simple or nice algebraic appearance. Only a few classes of permutation binomials and trinomials are known by now. In 2009, Akbary, Ghioca and Wang proposed a useful criterion referred as AGW criterion to decide whether a map is a permutation function over a finite set in [1]. In fact it is a generalization of numerous earlier results, one of which is the following theorem that has been used in many previous constructions of PPs.

**Theorem 1.1** [8] *Let  $q$  be a prime power number,  $r, d$  be positive integers,  $d \mid (q-1)$ ,  $h \in \mathbb{F}_q[x]$ , then  $f(x) := x^r h(x^{(q-1)/d})$  is a permutation polynomial over  $\mathbb{F}_q$  if and only if*

- (1)  $\gcd(r, (q-1)/d) = 1$ , and
- (2)  $x^r h(x)^{(q-1)/d}$  is a permutation polynomial over  $\mu_d$ .

Theorem 1.1 shows that polynomials of the form  $x^r h(x^{(q-1)/d})$  have a close connection with the  $d$ -order subgroup  $\mu_d$  of  $\mathbb{F}_q^\times$ . Indeed there have been many construction results by using the method of constructing PPs over  $\mu_d$  to obtain PPs over the original finite field.

All permutation binomials  $x^m + ax^n \in \mathbb{F}_q[x]$  have been characterized by Zieve [8]. The necessary and sufficient condition for  $x^r(x^{(q-1)/l} + a)$  being a permutation polynomial is given by the following Theorem.

**Theorem 1.2** [8] *Let  $q$  be a prime power number,  $r, d$  be positive integers,  $d \mid (q-1)$ ,  $a \in \mathbb{F}_q^\times$ , and  $\eta + \frac{a}{\eta} \in \mu_{(q-1)/d}$  for all  $\eta \in \mu_{2d}$ , then  $x^r(x^{(q-1)/d} + a)$  is a permutation polynomial over  $\mathbb{F}_q$  if and only if  $-a \notin \mu_d$ ,  $\gcd(r, (q-1)/d) = 1$ , and  $\gcd(2d, 2r + (q-1)/d) \leq 2$ .*

Theorem 1.2 indicates that there are no permutation binomials with both nonzero coefficients equal to 1 over finite fields with even characteristic, while permutation trinomials with coefficients 1 exist [11, 13, 19]. This motivates us to find a new method to construct permutation trinomials with coefficients 1.

We list some permutation trinomials with coefficients 1 constructed in recent years in Table 1. The main construction methods include Hermite's criterion, Dobbertin's multivariate approach([4]), discussions of the number of solutions of special equations ([3]), polar decomposition ([3]), etc. It should be noted that in many cases proving the permutation properties of PPs constructed by the method of polar decomposition or Theorem 1.1 is equivalent to proving that the corresponding fractional polynomials permute  $\mu_{\sqrt{q}+1}$ . Then is it possible to obtain PPs of the original finite field by reversely using Tu's polar decomposition method by exponential sum? It seems that this idea has not appeared previously to our knowledge. The bulk of our effort in this paper is placed in this direction, and the main contribution is to present a novel construction method of PPs by using the above idea.

As for fractional permutation polynomials over  $U$  which play important roles in the constructions of PPs by Theorem 1.1, Li et al. [5] proved the permutation properties of  $\frac{x^3+x^2+1}{x^3+x+1}$  and  $\frac{x^7+x^5+1}{x^7+x^2+1}$  by determining the solutions of quadratic and quartic equations respectively. Later Li et al. [11] proved the permutation properties of  $\frac{x^{2^k+1}+x^{2^k}+1}{x^{2^k+1}+x+1}$  over  $U$  by rewriting it as  $x^{2^k} = \frac{ax+b}{cx+d}$ . Main fractional permutation polynomials of  $U$  over a finite field with even characteristic up to now are listed in Table 2.

Table 1: Some permutation trinomials with coefficients 1

Permutation polynomial of $F_{2^{2m}}$	$m$	Reference
$x + x^3 + x^{2^{(m+1)/2+2}}$	odd	[4]
$x^{3 \times 2^{(m+1)/2+4}} + x^{2^{(m+1)/2+2}} + x^{2^{(m+1)/2}}$	odd	[15]
$x + x^{2^{(m+1)/2-1}} + x^{2^m - 2^{(m+1)/2+1}}$	odd	[3]
$x + x^3 + x^{2^m - 2^{(m+3)/2+2}}$	odd	[3]
$x + x^{2^{(m+1)/2-1}} + x^{2^m - 2^{m/2+1}}$	odd	[3]
$x^{2^{m/2+4}} + x^{2^{m/2+1}+3} + x^{2^{m/2+2}+1}$	$m \equiv 2 \pmod{4}$	[9]
$x^5 + x^{2^{m/2+4}} + x^{5 \times 2^{m/2}}$	$m \equiv 4 \pmod{8}$	[13], Theorem 3.1
$x^9 + x^{8+7 \times 2^m} + x^{9 \times 2^m}$	$m \equiv 2 \pmod{4}$	Theorem 3.1

This paper is organized as follows. In Section 2, we introduce some basic notations and Lemmas. In Section 3, we propose a new method to construct permutation trinomials with coefficients 1, which is the main result of this paper. Then in Subsection 3.2, we give the explicit compositional inverses of a class of permutation trinomials for a special case. Some concluding remarks are given in Section 4.

## 2 Preliminaries

We recall Tu's method in this section, which gave a criterion for permutation polynomials in terms of additive characters of the underlying finite fields. Let  $Tr_1^n(\cdot)$  be the absolute trace function from  $\mathbb{F}_{2^n}$  to  $\mathbb{F}_2$ , i.e.  $\forall x \in \mathbb{F}_{2^n}, Tr_1^n(x) = x + x^2 + \cdots + x^{2^{n-1}}$ . The following Lemma characterizes permutation polynomials by using additive characters.

**Lemma 2.1** [19] *A mapping  $g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$  is a permutation polynomial over  $\mathbb{F}_{2^n}$  if and only if for every nonzero  $\gamma \in \mathbb{F}_{2^n}$ ,*

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\gamma g(x))} = 0.$$

Table 2: Some fractional permutation polynomials over  $U$

Fraction polynomial	Condition	Reference
$\frac{x^3+x^2+1}{x^3+x+1}$		[3]
$\frac{x(x^3+x^2+1)}{x^3+x+1}$	$\gcd(3, m) = 1$	[3]
$\frac{x^5+x^4+1}{x^5+x+1}$	$m$ is odd	[5, 11]
$\frac{x^4+x^3+1}{x(x^4+x+1)}$	$m$ is odd	[11]
$\frac{x^7+x^5+1}{x^7+x^2+1}$	$m$ is odd	[11]
$\frac{x(x^5+x+1)}{x^5+x^4+1}$	$m = 2, 4 \pmod{6}$	[5]
$\frac{x^6+x^4+1}{x(x^6+x^2+1)}$	$\gcd(3, m) = 1$	[5]
$\frac{x^{2^k+1}+x^{2^k}+1}{x^{2^k+1}+x+1}$	$\gcd(2^k - 1, 2^m + 1) = 1$	[11]
$\frac{x^{2^k+1}+x^{2^k}+1}{x^{2^k+1}+x+1}$	$\gcd(2^k + 1, 2^m + 1) = 1$	[11]

If  $f(x) = \sum_{i=1}^t u_i x^{d_i}$  with  $u_1 = 1$  and  $\gcd(d_1, 2^n - 1) = 1$ , then

$$\begin{aligned}
 \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\gamma f(x))} &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\gamma(\sum_{i=1}^t u_i x^{d_i}))} \\
 &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n((\delta x)^{d_1} + \sum_{i=2}^t u_i \delta^{d_1 - d_i} (\delta x)^{d_i})} \\
 &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(x^{d_1} + \sum_{i=2}^t u_i \delta^{d_1 - d_i} x^{d_i})}.
 \end{aligned}$$

Let  $m$  be a positive integer,  $n = 2m$ . For  $i = 1, 2, \dots, t$ ,  $d_i = s_i(2^m - 1) + e$ , then the computation of the above exponential sum can be converted to equation problem over  $U$ .

**Corollary 2.2** [19] Let  $f(x) = x^{d_1} + \sum_{i=2}^t u_i x^{d_i}$ ,  $\gcd(d_1, 2^n - 1) = 1$ , and  $d_i = s_i(2^m - 1) + e$  for every  $i \in [1, t]$ . Then the polynomial  $f$  is a permutation polynomial over  $\mathbb{F}_{2^n}$  if and only if  $\forall \delta \in \mathbb{F}_{2^n}$ ,

$$\begin{aligned}
 &\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(x^{d_1} + \sum_{i=2}^t u_i \delta^{d_1 - d_i} x^{d_i})} \\
 &= (N(u_2, \dots, u_t) - 1) \cdot 2^m \\
 &= 0.
 \end{aligned}$$

where  $N(u_2, \dots, u_t)$  is the number of  $\lambda$ 's in  $U$  such that

$$\lambda^{d_1} + \sum_{i=2}^t u_i \delta^{d_1-d_i} \lambda^{d_i} + (\lambda^{d_1} + \sum_{i=2}^t u_i \delta^{d_1-d_i} \lambda^{d_i})^{2^m} = 0. \quad (1)$$

As already mentioned in Section 1, there is a close connection between the fractional PPs over subgroup of order  $d$  and the permutations of form  $x^r h(x^{(q-1)/d})$  over  $\mathbb{F}_q$ . Thus constructing corresponding fractional PPs over  $\mu_d$  is the key point for constructing certain permutations with the above form. The following Theorem gives a general fractional PPs over  $U$  which would be needed later in this paper.

**Theorem 2.3** [11] *Let  $U$  be the  $(2^m + 1)$ -order multiplicative subgroup of the finite field  $\mathbb{F}_{2^{2m}}$ . If  $\gcd(2^k - 1, 2^m + 1) = 1$ , the reciprocal polynomial  $\frac{x^{2^k+1} + x^{2^k} + 1}{x^{2^k+1} + x + 1}$  is a permutation fractional polynomial of  $U$ .*

### 3 A new method of construction of permutation trinomials with coefficients 1

In this section, we firstly give a new construction method in Subsection 3.1. In order to illustrate how to use the new method, we give the construction process of a class of trinomials, and the explicit compositional inverses of this class of permutation trinomials for a special case are given in Subsection 3.2.

#### 3.1 New method

In [19], Tu et al. proposed a criterion for permutation polynomials by using polar decomposition. They characterized the permutation properties of polynomials by calculating Walsh spectra of the corresponding Boolean functions in terms of additive characters of finite fields. Specifically, the study of permutation behavior of polynomials  $\sum_{i=1}^t u_i x^{d_i}$  satisfying  $d_i \equiv d_j \pmod{2^{n/2-1}}$  for each pair of exponents  $(d_i, d_j)$  is converted to the study of permutation behavior of polynomials  $g(x) + g(x)^{2^m}$  over  $U$ . In this subsection, we are inspired by the research of [19], and reversely use the polar decomposition method to deduce a large class of permutation trinomials with coefficients 1.

**Theorem 3.1** *Let  $n = 2m, m > 0, i, j \in \mathbb{N}^+, i \neq j, u \in \mathbb{Z}, J = 2^j, I = 2^i$ . Suppose  $\gcd(d_1, 2^{2m} - 1) = 1$  and  $\gcd(2^i - 2^j, 2^m + 1) = 1$ . And*

$$\begin{cases} d_1 &= 2^{i-1} - 2^{j-1} + u \times (2^m + 1), \\ d_2 &= 2^{i-1} + 2^{j-1} + (u - 2^{j-1}) \times (2^m + 1), \\ d_3 &= -(2^{i-1} + 2^{j-1}) + (u + 2^{i-1}) \times (2^m + 1). \end{cases}$$

where  $\frac{1}{J-1} \pmod{2^m + 1} \equiv t, 0 < t < 2^m + 1$ . Then

$$x^{d_1} + x^{d_2} + x^{d_3}$$

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

**Proof.** Write  $k := j - i$ . Since  $\gcd(2^i - 2^j, 2^m + 1) = \gcd(2^k - 1, 2^m + 1) = 1$ , by Theorem 2.3,

$$f_k(x) = \frac{x^{K+1} + x^K + 1}{x^{K+1} + x + 1}, K = 2^k,$$

permutes  $U$ .

Note  $\gcd(I, 2^k - 1) = 1$ , we have  $g(x) = x^I$  is a permutation polynomial over  $U$ , and  $g(f_k(x)) = (\frac{x^{K+1} + x^K + 1}{x^{K+1} + x + 1})^I$  is also a permutation polynomial of  $U$ . Therefore, for all  $\beta \in U$ ,

$$(x^{K+1} + x^K + 1)^I = \beta(x^{K+1} + x + 1)^I$$

has only one solution in  $U$ . That is,

$$(1 + \beta)x^{I+J} + x^J + \beta x^I + 1 + \beta = 0, J = KI, \quad (2)$$

has only one solution in  $U$ .

For all  $t \in \mathbb{Z}$ , let  $x = \beta^t y$ . Substituting it into (2), we get

$$(\beta^{t(I+J)+1} + \beta^{t(I+J)})y^{I+J} + \beta^{tJ}y^J + \beta^{tI+1}y^I + 1 + \beta = 0.$$

If  $\gcd(J - I, 2^m + 1) = 1$ , there exists  $t \equiv \frac{1}{J-I} \pmod{2^m + 1}$ ,  $0 < t < 2^m + 1$ , such that  $tJ = tI + 1 + b(2^m + 1) = L$ , where  $b \in \mathbb{Z}$ . Note  $\beta^L \in U$ . Hence

$$(\beta^{2L} + \beta^{2L-1})y^{I+J} + \beta^L y^J + \beta^L y^I + 1 + \beta = 0. \quad (3)$$

Write  $L_1 := \frac{I+J}{2}$ ,  $L_2 := \frac{I-J}{2}$ . Dividing both sides of equation (3) by  $\beta^L y^{L_1}$ , we have

$$(\beta^L + \beta^{L-1})y^{L_1} + y^{L_2} + y^{-L_2} + (\beta^{-L} + \beta^{-(L-1)})y^{-L_1} = 0,$$

i.e.,

$$\beta^L y^{L_1} + y^{L_2} + \beta^{-(L-1)}y^{-L_1} + (\beta^L y^{L_1} + y^{L_2} + \beta^{-(L-1)}y^{L_1})^{2^m} = 0. \quad (4)$$

According to Lemma 2.2, the three-term polynomial obtained by the method of polar decomposition should be

$$y^{L_2} + \beta^L y^{L_1} + \beta^{-(L-1)}y^{-L_1}. \quad (5)$$

On the other hand, for the three-term polynomial with coefficients 1, the simplified polynomial form deduced from the proof of permutation polynomial over the underlying finite field by Tu's method in [19] is

$$y^{d_1} + \delta^{d_1-d_2}y^{d_2} + \delta^{d_1-d_3}y^{d_3}, y \in U, \delta \in \mathbb{F}_{2^n}. \quad (6)$$

Let  $Q = 2^m + 1$ . According to (5) and (6), we can assume that

$$\begin{cases} L_2 \equiv d_1 \pmod{Q}, \\ L_1 \equiv d_2 \pmod{Q}, \\ -L_1 \equiv d_3 \pmod{Q}. \end{cases} \quad (7)$$

Furthermore we can assume  $\exists u_1, u_2, u_3, u_4, u_5, a \in \mathbb{Z}$ , such that  $\forall y \in U, \delta \in \mathbb{F}_{2^n}$ ,

$$\begin{aligned} & y^{L_2} + \beta^L y^{L_1} + \beta^{-(L-1)}y^{-L_1} \\ = & y^{L_2+u_1Q} + \delta^{(Q-2)aL+u_4Q(Q-2)}y^{L_1+u_2Q} + \delta^{(Q-2)a(1-L)+u_5Q(Q-2)}y^{-L_1+u_3Q}. \end{aligned} \quad (8)$$

By (6) and the polynomial form of (8), we have

$$\begin{cases} d_1 = L_2 + u_1Q, \\ d_1 - d_2 = (Q - 2)aL + u_4Q(Q - 2), \\ d_1 - d_3 = (Q - 2)a(1 - L) + u_5Q(Q - 2). \end{cases} \quad (9)$$

Thus,

$$\begin{cases} d_2 = L_2 + u_1Q - (Q - 2)aL - u_4Q(Q - 2), \\ d_3 = L_2 + u_1Q + (Q - 2)a(L - 1) - u_5Q(Q - 2). \end{cases} \quad (10)$$

By (7) and (10), we have

$$\begin{cases} d_2 \equiv L_2 + 2aL \equiv L_1 \pmod{Q}, \\ d_3 \equiv L_2 - 2a(L - 1) \equiv -L_1 \pmod{Q}. \end{cases} \quad (11)$$

Since  $L_1 = \frac{I+J}{2}$ ,  $L_2 = \frac{I-J}{2}$ ,  $t \equiv \frac{1}{J-I} \pmod{2^m + 1}$ , and  $L = tJ = tI + 1 + b(2^m + 1)$ , by solving the equations (11), we get

$$a \equiv \frac{1}{2t} \pmod{Q}. \quad (12)$$

Substitute  $a = \frac{1}{2t} + u_6Q$  ( $u_6 \in \mathbb{Z}$ ) into the equations (10),

$$\begin{cases} d_2 = L_2 + u_1Q - (Q - 2)\frac{J}{2} - (u_4 + u_6tJ)Q(Q - 2), \\ d_3 = L_2 + u_1Q + (Q - 2)\frac{I}{2} + (\frac{b}{2t} + u_6tI + u_6bQ - u_5)Q(Q - 2). \end{cases} \quad (13)$$

Substitute  $L_2$  into  $d_1$ ,  $d_2$  and  $d_3$ , and replace  $u_1$  by  $u$ , we have

$$\begin{cases} d_1 \equiv \frac{I-J}{2} + uQ \pmod{Q(Q-2)}, \\ d_2 \equiv \frac{I-J}{2} + uQ - (Q-2)\frac{J}{2} \pmod{Q(Q-2)}, \\ d_3 \equiv \frac{I-J}{2} + uQ + (Q-2)\frac{I}{2} \pmod{Q(Q-2)}. \end{cases} \quad (14)$$

Thus, we deduce that the trinomial is

$$x^{\frac{I-J}{2}+uQ} + x^{\frac{I-J}{2}+uQ-(Q-2)\frac{J}{2}} + x^{\frac{I-J}{2}+uQ+(Q-2)\frac{I}{2}}. \quad (15)$$

It can be seen that the equation (4) deduced from polar decomposition of (15) has one and only one solution of  $U$  for every  $\beta \in U$ .

Therefore,

$$\begin{cases} d_1 = 2^{i-1} - 2^{j-1} + u \times (2^m + 1), \\ d_2 = 2^{i-1} + 2^{j-1} + (u - 2^{j-1}) \times (2^m + 1), \\ d_3 = -(2^{i-1} + 2^{j-1}) + (u + 2^{i-1}) \times (2^m + 1). \end{cases}$$

By Corollary 2.2, we have proved that for all  $i, j \in \mathbb{N}^+$ ,  $i \neq j$ ,  $u \in \mathbb{Z}$ , if  $\gcd(2^{i-1} - 2^{j-1} + u \times (2^m + 1), 2^{2^m - 1}) = 1$  and  $\gcd(2^i - 2^j, 2^m + 1) = 1$ , the polynomial

$$x^{d_1} + x^{d_2} + x^{d_3}$$

is a permutation polynomial over  $\mathbb{F}_{2^n}$ . The proof is complete.  $\blacksquare$

### 3.2 Compositional inverses of permutation trinomials in Subsection 3.1 for $i = j + m - 1$

Compositional inverses of permutation polynomials have important applications in cryptography. For instance, in multivariate public key cryptography, permutation polynomials with coefficients 1 can be used as central map due to their simple form, thus, their explicit compositional inverses will be needed in the decryption process.

For a polynomial  $f(x)$  over  $\mathbb{F}_q$ ,  $f^{-1}(x)$  is the compositional inverse of  $f(x)$  if  $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x \pmod{x^q - x}$ . In this subsection, we give the explicit compositional inverses of the permutation trinomials in Subsection 3.1 for a special case  $i = j + m - 1$ .

**Lemma 3.2** [6] *Let  $q$  be a prime power and  $f(x) = x^r h(x^s) \in \mathbb{F}_q[x]$  be a permutation polynomial, where  $s|(q-1)$ ,  $\gcd(r, q-1) = 1$  and  $h(0) \neq 0$ . Let  $r'$  be an integer which satisfies  $rr' \equiv 1 \pmod{q-1}$ ,  $\alpha(x) = x^{q-s}$ ,  $\beta(x) = x^s$  and  $l(x)$  be the compositional inverse of  $g(x) = x^r h(x^s)$  over  $\mu_{(q-1)/s}$ , then*

$$f^{-1}(x) = (\alpha(x)h(l(\beta(x)))^{s-1})^{r'}l(\beta(x))$$

is the compositional inverse of  $f(x)$  over  $\mathbb{F}_q$ .

The permutation trinomials over  $\mathbb{F}_{2^{2m}}$  constructed by Theorem 3.1 can be written as  $f(x) = x^{d_1}(1 + (x^{2^m-1})^{-2^{j-1}} + (x^{2^m-1})^{2^{i-1}})$ , thus the corresponding polynomials over  $U$  are  $g(x) = x^{d_1}(1 + x^{-2^{j-1}} + x^{2^{i-1}})^{2^{m-1}}$ . According to Lemma 3.2, the key of finding explicit compositional inverses of  $f(x)$  over  $\mathbb{F}_{2^{2m}}$  is the compositional inverses of  $g(x)$  over  $U$ .

**Theorem 3.3** *Let  $i = j + m - 1$ , the compositional inverses of  $g(x) = x^{d_1}(1 + x^{-2^{j-1}} + x^{2^{i-1}})^{2^{m-1}}$  are  $g^{-1}(x) = x^{r_1 r_2}$ , where  $r_1 \cdot 2^{m-1} \equiv 1 \pmod{2^m + 1}$  and  $r_2 \cdot 2^{j-1} \equiv 1 \pmod{2^m + 1}$ .*

**Proof.**  $g(x)$  can be written as:

$$g(x) = \frac{x^{2^{i-1}-2^{j-1}} + x^{2^{i-1}} + x^{-2^{j-1}}}{1 + x^{-2^{j-1}} + x^{2^{i-1}}},$$

thus,

$$\begin{aligned} g(g^{-1}(x)) &= \frac{x^{r_1 r_2 2^{j-1} 2^{m-1} - r_1 r_2 2^{j-1}} + x^{r_1 r_2 2^{j-1} 2^{m-1}} + x^{-r_1 r_2 2^{j-1}}}{1 + x^{-r_1 r_2 2^{j-1}} + x^{r_1 r_2 2^{j-1} 2^{m-1}}} \\ &= \frac{x^{1-r_1} + x + x^{-r_1}}{1 + x^{-r_1} + x} \\ &= \frac{x(x^{-r_1} + 1 + x^{-r_1-1})}{x^{-r_1} + 1 + x}. \end{aligned}$$

Since  $(r_1 + 2)2^{m-1} \equiv r_1 2^{m-1} + 2^m \equiv 2^m + 1 \equiv 0 \pmod{2^m + 1}$  and  $\gcd(2^{m-1}, 2^m + 1) = 1$ ,  $(r_1 + 2) \equiv 0 \pmod{2^m + 1}$ , that is,  $(-r_1 - 1) \equiv 1 \pmod{2^m + 1}$ . Therefore,  $g(g^{-1}(x)) = x$ . The proof is complete. ■

According to Lemma 3.2 and Theorem 3.3, we obtain the next Theorem easily.

**Theorem 3.4** *Let  $i = j + m - 1$ , the explicit compositional inverses of  $f(x) = x^{d_1}(1 + (x^{2^m-1})^{-2^{j-1}} + (x^{2^m-1})^{2^{i-1}})$  is*

$$f^{-1}(x) = (\alpha(x)h(g^{-1}(\beta(x)))^{2^m-2})^{r_3}(\beta(x)),$$

where  $\alpha(x) = x^{2^{2m}-2^{m+1}}$ ,  $\beta(x) = x^{2^m-1}$ ,  $h(x) = 1 + x^{-2^{j-1}} + x^{2^{i-1}}$ ,  $l(x) = x^{r_1 r_2}$ ,  $r_1 \cdot 2^{m-1} \equiv 1 \pmod{2^m + 1}$ ,  $r_2 \cdot 2^{j-1} \equiv 1 \pmod{2^m + 1}$ ,  $r_3 \cdot d_1 \equiv 1 \pmod{2^{2m} - 1}$ .



## 4 Conclusion

In this paper, we have proposed a new method to construct permutation trinomials with coefficients 1. Moreover, we have given the explicit compositional inverses of a class of permutation trinomials for a special case.

By using fractional permutation polynomials over  $U$ , we reversely deduced some PPs over the original finite fields. This construction method (or reversion usage of Tu's method) by polar decomposition has not appeared previously, and may be employed to discover more PPs (especially PPs with coefficients 1 since there were no simple characterization of these PPs over finite fields in the literature by now).

## Acknowledgment

This work was supported by Natural Science Foundation of Beijing Municipality (No. 4202037), NSF of China with contract (No.61972018).

## References

- [1] A.Akbari, D.Ghioca, Q.Wang, On permutation polynomials of prescribed shape, *Finite Fields and Their Applications*, 15(2), 195-206(2009)
- [2] C. Ding, J. Yuan, A family of skew Hadamard difference sets, *J. Combinatorial Theory Ser. A*, 113(7), 1526-1535(2006)
- [3] C.Ding, L.Qu, Q.Wang, Permutation trinomials over finite fields with even characteristic, *Siam Journal on Discrete Mathematics*, 29(1), 79-92(2015)
- [4] H.Dobbertin, Almost perfect nonlinear power functions on  $GF(2^n)$ : The Niho Case, *IEEE Trans.inf.theory*, 45(4), 1271-1275(1999)
- [5] K.Li, L.Qu, C.Li, et al, New permutation trinomials constructed from fractional polynomials, *Acta Arithmetica*, 183(2), 101-116(2018)
- [6] K.Li, L.Qu, Q.Wang, Compositional inverses of permutation polynomials of the form  $x^r h(x^s)$  over finite fields, *Cryptography and Communications*, 11, 279-298(2019)
- [7] L.Qu, Y.Tan, C.Li, et al, More constructions of differentially 4-uniform permutations on  $\mathbb{F}_{2^{2k}}$ , *Designs Codes Cryptography*, 78(2), 1-18(2013)
- [8] M.E.Zieve, On some permutation polynomials over  $F_q$  of the form  $x^r h(x^{(q-1)/d})$ , *Proceedings of the American Mathematical Society*, 137(7), 2209-2216(2007)
- [9] M.E.Zieve, Permutation polynomials on  $F_q$  induced from Redei function bijections on subgroups of  $F_q$ , *Mathematics*, 2013.
- [10] M.E.Zieve, Some families of permutation polynomials over finite fields, *International Journal of Number Theory*, 4(5), 851-857(2008)

- [11] N.Li, T.Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *Cryptography and Communications*, 11(1), 129-136(2019)
- [12] N.Li, T.Helleseth, Several classes of permutation trinomials from Niho exponents, *Cryptography and Communications*, 9(6), 693-705(2017)
- [13] R.Gupta, R.K.Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields and Their Applications*, 41, 89-96(2016)
- [14] T.Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Mathematics*, 16(3), 209-232(1976)
- [15] W.Cherowitzo,  $\alpha$ -Flocks and Hyperovals, *Geometriae Dedicata*, 72(3), 221-245(1998)
- [16] X. Xu, C. Li, X.Zeng, and Tor Helleseth, Constructions of complete permutation polynomials, *Designs, Codes and Cryptography*, 86(12), 1-24(2018)
- [17] Y.Laigle-chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.*, 13(1), 58-70(2007)
- [18] Y.Park, J.B.Lee, Permutation polynomials and group permutation polynomials, *Bulletin of the Australian Mathematical Society*, 63(1), 67-74(2001)
- [19] Z.Tu, X.Zeng, L.Hu, et al, A Class of binomial permutation polynomials, available online: <http://arxiv.org/pdf/1310.0337v1.pdf>.