

# On inverse of permutation polynomials of small degree over finite fields, II<sup>☆</sup>

Yanbin Zheng<sup>a</sup>, Yuyin Yu<sup>b</sup>

<sup>a</sup>*School of Mathematical Sciences, Qufu Normal University, Qufu 273165, China*

<sup>b</sup>*School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China*

---

## Abstract

We investigate the permutation property of polynomials of the form  $x^r(x^s - a)^t$ , and give the expressions of their inverses. In particular, explicit expressions of inverses of permutation polynomials  $x(x^3 - a)^2$  and  $x(x^2 - a)^3$  on  $\mathbb{F}_{7^n}$  are presented. Then, using some known results, we obtain the inverses of all permutation polynomials of degree 6, 7, 8 over finite fields.

*Keywords:* Finite fields, Permutation polynomials, Inverses

*2010 MSC:* 11T06, 11T71

---

## 1. Introduction

For  $q$  a prime power, let  $\mathbb{F}_q$  denote the finite field with  $q$  elements,  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ , and  $\mathbb{F}_q[x]$  the ring of polynomials over  $\mathbb{F}_q$ . A polynomial  $f \in \mathbb{F}_q[x]$  is called a *permutation polynomial* (PP) of  $\mathbb{F}_q$  if it induces a bijection from  $\mathbb{F}_q$  to itself. For any PP  $f$  of  $\mathbb{F}_q$ , there exists a polynomial  $f^{-1} \in \mathbb{F}_q[x]$  such that  $f^{-1}(f(c)) = c$  for each  $c \in \mathbb{F}_q$  or equivalently  $f^{-1}(f(x)) \equiv x \pmod{x^q - x}$ , and the polynomial  $f^{-1}$  is unique in the sense of reduction modulo  $x^q - x$ . Hence  $f^{-1}$  is defined as the *composition inverse* of  $f$ , and we simply call it the *inverse* of  $f$  on  $\mathbb{F}_q$ .

A polynomial over  $\mathbb{F}_q$  is called an *exceptional polynomial* over  $\mathbb{F}_q$  if it is a PP of  $\mathbb{F}_{q^n}$  for infinitely many positive integers  $n$ . Two polynomials  $f$  and  $g$  over  $\mathbb{F}_q$  are called *affine equivalence* if  $g(x) = \alpha f(\beta x + \gamma) + \delta$  for some  $\alpha, \beta \in \mathbb{F}_q^*$  and  $\gamma, \delta \in \mathbb{F}_q$ . Affine equivalent  $f$  and  $g$  share the same degree, and  $f$  is a PP of  $\mathbb{F}_q$  if and only if so is  $g$ .

The classification of PPs of finite fields has a long history. In 1896, Dickson [9] obtained all *normalized* PPs of degree  $\leq 5$  of  $\mathbb{F}_q$  for all  $q$ , and classified all PPs of degree 6 of  $\mathbb{F}_q$  for odd  $q$ . In 2010, a complete classification of all PPs of degree 6 or 7 of  $\mathbb{F}_{2^n}$  was settled in [15], up to affine equivalence and a special transformation. However, each class of resulting PPs is invariant under the special transformation [10]. For a verification of the classification of normalized PPs of degree 6 of  $\mathbb{F}_q$  for all  $q$ , see [25]. More recently, under affine equivalence, Fan [10–12] gives a complete classification of all PPs of degree 7 of  $\mathbb{F}_q$  for odd  $q$  and degree 8 of  $\mathbb{F}_q$  for all  $q$ . All such PPs of degree  $\leq 8$  can be divided into two classes: exceptional and non-exceptional. According to the results in the above literature, a non-exceptional PP of degree  $\leq 8$  over  $\mathbb{F}_q$  exists only if  $q < 64$ .

The inverses of all normalized PPs of degree  $\leq 5$  were listed in [38]. In this paper, we consider the inverses of all PPs of degree 6, 7, 8. For non-exceptional PPs of degree

---

*Email addresses:* zhengyanbin16@126.com (Yanbin Zheng), yuyuyin@163.com (Yuyin Yu)

6, 7, 8 of  $\mathbb{F}_q$ , since  $q < 64$  is very small, one can use the Lagrange interpolation formula to compute their inverses, i.e.,

$$f^{-1}(x) = \sum_{c \in \mathbb{F}_q} c(1 - (x - f(c))^{q-1}). \quad (1)$$

But for exceptional PPs of degree 6, 7, 8 of  $\mathbb{F}_{q^n}$  with infinitely many  $n$ , finding explicit expressions of their inverses on  $\mathbb{F}_{q^n}$  is not an easy problem.

There are several papers on the inverses of some classes of PPs, see for example [24, 32, 34] for linearized PPs, [18, 21, 29, 39] for PPs of the form  $x^r h(x^{(q-1)/d})$ , [6, 23, 36] for involutions over  $\mathbb{F}_{2^n}$ , [30, 39] for generalized cyclotomic mapping PPs, [37, 39, 40] for more general piecewise PPs, [22, 27, 28] for PPs constructed by the AGW criterion. The results in [22, 27, 28] contain some concrete classes such as bilinear PPs [8, 33], linearized PPs of the form  $L(x) + K(x)$ [24], and PPs of the form  $x + \gamma f(x)$  [14]. For a brief summary of the results concerning the inverses of PPs, we refer the reader to [38] and the references therein.

In this paper, we study the PPs of the form  $f(x) = x^r(x^s - a)^t$  on  $\mathbb{F}_{q^n}$ , where  $a \in \mathbb{F}_{q^n}^*$ ,  $st = q^m - 1$ ,  $r \equiv 1 \pmod{\ell}$  and  $\ell = (q^n - 1)/(s, q^n - 1)$ . According to the Akbary-Ghioca-Wang (AGW) criterion [1],  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $(r, s, q^n - 1) = 1$  and another polynomial  $g(x) := x(x - a)^{st}$  permutes the subset  $(\mathbb{F}_q^*)^s$ . By solving the equation  $g(x) = c$  for any  $c \in (\mathbb{F}_q^*)^s$ , we find the inverse  $g^{-1}$  of  $g$  on  $(\mathbb{F}_q^*)^s$ , and prove that  $g$  permutes  $(\mathbb{F}_q^*)^s$  if and only if  $a^\ell \neq 1$ . Substituting  $g^{-1}$  into a slightly modified version of a result in [22] concerning the inverse of more general PP  $x^r h(x^s)$ , we obtain an expression of the inverse of  $f$  on  $\mathbb{F}_{q^n}$ .

By considering special cases such as  $m = n$ ,  $q^{(m,n)} - 1 \mid s$ , and  $t = 2$  or  $3$ , we get some new classes of PPs and their inverses. In particular, explicit expressions of inverses of exceptional polynomials  $x(x^3 - a)^2$  and  $x(x^2 - a)^3$  on  $\mathbb{F}_{7^n}$  are given. Then, based on the known formulae for the inverses of Dickson PPs and linearized PPs, we find the inverses of all exceptional polynomials of degree 6, 7, 8; see Table 1.

In summary, under affine equivalence, Table 1 and [38, Tabel I] list the inverses of all PPs of degree  $\leq 8$  over all finite fields, except for the inverses of non-exceptional PPs of degree 6, 7, 8 which can be obtained by (1).

Some notations of this paper are as follows. The sets of integers and positive integers are denoted by  $\mathbb{Z}$  and  $\mathbb{N}$  respectively. The greatest common divisor of two integers  $m$  and  $n$  is written as  $(m, n)$ . For  $a \in \mathbb{F}_{q^n}$  and  $d \mid n$ , the norm of  $a$  over  $\mathbb{F}_{q^d}$  is defined by  $N_{q^n/q^d}(a) = a^{(q^n - 1)/(q^d - 1)}$ .

Table 1: All exceptional polynomials of degree 6, 7, 8 and their inverses

Exceptional polynomials over $\mathbb{F}_q$	Inverses	$q$	Reference
$x^6$	$x^{(5q-4)/6}$	$q = 2^n$ , odd $n \geq 3$	<a href="#">Lemma 1</a>
$x^7$	$x^{(kq-k+1)/7}$ with $k \equiv (1-q)^5 \pmod{7}$	$q \not\equiv 1 \pmod{7}$	<a href="#">Lemma 1</a>
$x^7 - ax$ ( $a$ not a sixth power)	$a^{\frac{q-1}{6}} (1 - a^{\frac{q-1}{6}})^{-1} \sum_{i=0}^{n-1} a^{-\frac{\tau^{i+1}-1}{6}} x^{\tau^i}$	$q = 7^n$ , $n \geq 2$	<a href="#">[7, 32]</a>
$x^7 - 2ax^4 + a^2x$ ( $a$ not a cube)	$2x(2a^{\frac{q-1}{6}} x^{\frac{q-1}{2}} + a^{\frac{q-1}{3}} + 1) (\sum_{i=0}^{n-1} a^{-\frac{\tau^{i+1}-1}{6}} x^{\frac{\tau^i-1}{2}})^2$	$q = 7^n$ , $n \geq 2$	<a href="#">Corollary 6</a>
$x^7 - 3ax^5 + 3a^2x^3 - a^3x$ ( $a$ not a square)	$x(3(ax^4)^{\frac{q-1}{6}} - 3(ax)^{\frac{q-1}{3}} - 2) (\sum_{i=0}^{n-1} a^{-\frac{\tau^{i+1}-1}{6}} x^{\frac{\tau^i-1}{3}})^3$	$q = 7^n$ , $n \geq 2$	<a href="#">Corollary 8</a>
$x^7 - 7ax^5 + 14a^2x^3 - 7a^3x$ ( $a \neq 0$ )	$\sum_{i=0}^{\lfloor m/2 \rfloor} \frac{m}{m-i} \binom{m-i}{i} (-a^7)^i x^{m-2i}$ where $m = (kq^2 - k + 1)/7$ with $k \equiv (1 - q^2)^5 \pmod{7}$ and $\lfloor m/2 \rfloor$ denotes the largest integer $\leq m/2$ .	$q \equiv \pm 2, \pm 3 \pmod{7}$	<a href="#">[18]</a> <a href="#">Lemma 1</a>
$x^8 + a_2x^4 + a_1x^2 + a_0x$ (if its only root in $\mathbb{F}_{2^n}$ is 0)	$(\det(D_L))^{-1} \sum_{i=0}^{n-1} \bar{a}_i x^{q^i}$ where $D_L$ and $\bar{a}_i$ are defined as in <a href="#">Lemma 3</a> .	$q = 2^n$ , $n \geq 4$	<a href="#">[34]</a>

<sup>†</sup> This list is complete up to affine transformations:  $g(x) = \alpha f(\beta x + \gamma) + \delta$  with  $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$  and  $\alpha\beta \neq 0$ .

<sup>‡</sup> All non-exceptional permutation polynomials of degree 6, 7, 8 are listed in [\[10–12, 15, 25\]](#), and all of them are over small fields  $\mathbb{F}_q$  with  $q \leq 64$ . Hence their inverses can be obtained by the Lagrange interpolation formula.

## 2. Permutation polynomials of small degree and their inverses

Since the inverses of all normalized PPs of degree  $\leq 5$  were listed in [38], we only consider the PPs of degree 6, 7, 8 which can be divided into two classes: exceptional and non-exceptional. Combining the results in [4, 10–12, 15, 25] gives the following theorems.

**Theorem 1.** *A non-exceptional PP of degree  $m \in \{6, 7, 8\}$  over  $\mathbb{F}_q$  exists if and only if one of the following conditions holds:*

- (i)  $m = 6$  and  $q \in \{8, 9, 11, 16, 27, 32\}$ ;
- (ii)  $m = 7$  and  $q \in \{9, 11, 13, 16, 17, 19, 23, 25, 27, 31, 49\}$ ;
- (iii)  $m = 8$  and  $q \in \{11, 13, 16, 19, 23, 27, 29, 31, 32, 64\}$ .

*Under affine equivalence, all such PPs are explicitly listed in [10–12, 15, 25].*

**Theorem 2.** *Each exceptional polynomial of degree 6, 7, 8 is affine equivalent to one of the following:*

- (i)  $x^6$  over  $\mathbb{F}_{2^n}$  with odd  $n \geq 3$ ;
- (ii)  $x^7$  over  $\mathbb{F}_q$  with  $q \not\equiv 1 \pmod{7}$ ;
- (iii)  $x^7 - ax$  over  $\mathbb{F}_{7^n}$  with  $a$  not a sixth power in  $\mathbb{F}_{7^n}$ , i.e.,  $a \in \mathbb{F}_{7^n}^*$  such that  $a^{(7^n-1)/6} \neq 1$ ;
- (iv)  $x(x^3 - a)^2$  over  $\mathbb{F}_{7^n}$  with  $a$  not a cube in  $\mathbb{F}_{7^n}$ , i.e.,  $a \in \mathbb{F}_{7^n}^*$  such that  $a^{(7^n-1)/3} \neq 1$ ;
- (v)  $x(x^2 - a)^3$  over  $\mathbb{F}_{7^n}$  with  $a$  not a square in  $\mathbb{F}_{7^n}$ , i.e.,  $a \in \mathbb{F}_{7^n}^*$  such that  $a^{(7^n-1)/2} \neq 1$ ;
- (vi)  $x^7 - 7ax^5 + 14a^2x^3 - 7a^3x$  with  $a \in \mathbb{F}_q^*$  and  $q \equiv \pm 2, \pm 3 \pmod{7}$ ;
- (vii)  $x^8 + a_2x^4 + a_1x^2 + a_0x$  over  $\mathbb{F}_{2^n}$  if its only root in  $\mathbb{F}_{2^n}$  is 0.

The inverses of PPs in Theorem 1 can be obtained directly by the Lagrange interpolation formula (1) due to  $q < 64$ . To obtain the inverses of PPs in Theorem 2, we need the following results.

**Lemma 1.** *Let  $m, \ell \in \mathbb{N}$  and  $(m, \ell) = 1$ . Then an inverse of  $m$  modulo  $\ell$  is  $(k\ell + 1)/m$ , where  $k \equiv -\ell^{\phi(m)-1} \pmod{m}$  and  $\phi$  is Euler's totient function.*

*Proof.* Clearly,  $k\ell + 1 \equiv 1 - \ell^{\phi(m)} \equiv 0 \pmod{m}$  and  $m(k\ell + 1)/m - k\ell = 1$ . Therefore,  $(k\ell + 1)/m$  is an inverse of  $m$  modulo  $\ell$ .  $\square$

**Lemma 2** ([7, 32]). *Let  $L(x) = x^{q^m} - ax$ , where  $a \in \mathbb{F}_{q^n}^*$  and  $m, n \in \mathbb{N}$ . Then  $L$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $N_{q^n/q^d}(a) \neq 1$ , where  $d = (m, n)$ . In this case, its inverse on  $\mathbb{F}_{q^n}$  is*

$$L^{-1}(x) = \frac{N_{q^n/q^d}(a)}{1 - N_{q^n/q^d}(a)} \sum_{i=1}^{n/d} a^{-\frac{q^{im}-1}{q^m-1}} x^{q^{(i-1)m}}.$$

**Lemma 3.** *Let  $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ . Then  $L$  is a PP of  $\mathbb{F}_{q^n}$  if and only if*

$$D_L := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}$$

*is nonsingular [20, Page 362]. In this case, its inverse was given in [34] by*

$$L^{-1}(x) = \frac{1}{\det(D_L)} \sum_{i=0}^{n-1} \bar{a}_i x^{q^i},$$

*where  $\bar{a}_i$  is the  $(i, 0)$ -th cofactor of  $D_L$ , i.e.,  $\det(D_L) = a_0 \bar{a}_0 + \sum_{i=1}^{n-1} a_i^{q^i} \bar{a}_i$ .*

The Dickson polynomial  $D_n(x, a)$  of degree  $n$  with parameter  $a \in \mathbb{F}_q$  is given as

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i},$$

where  $\lfloor n/2 \rfloor$  denotes the largest integer  $\leq n/2$ . For  $a \in \mathbb{F}_q^*$ ,  $D_n(x, a)$  is a PP of  $\mathbb{F}_q$  if and only if  $\gcd(n, q^2 - 1) = 1$ . Its inverse is determined in [18] by the next lemma.

**Lemma 4** ([18, Lemma 4.8]). *Let  $a \in \mathbb{F}_q^*$  and  $m, n \in \mathbb{N}$  be such that  $mn \equiv 1 \pmod{q^2 - 1}$ . Then the inverse of  $D_n(x, a)$  on  $\mathbb{F}_q$  is  $D_m(x, a^n)$ .*

The PP  $x^7 - 7ax^5 + 14a^2x^3 - 7a^3x$  in Theorem 2 is the Dickson polynomial  $D_7(x, a)$  and, by Lemma 4, its inverse is  $D_m(x, a^7)$ . By Lemma 1, an inverse  $m$  of 7 modulo  $q^2 - 1$  can be written as  $m = (kq^2 - k + 1)/7$ , where  $k \equiv (1 - q^2)^5 \pmod{7}$ .

The inverses of PPs  $x^6$ ,  $x^7$ ,  $x^7 - ax$  and  $x^8 + \sum_{i=0}^2 a_i x^i$  in Theorem 2 can be obtained directly by Lemmas 1 to 3. The inverses of PPs  $x(x^3 - a)^2$  and  $x(x^2 - a)^3$  on  $\mathbb{F}_{7^n}$  are given by Corollaries 6 and 8 in Section 5 respectively.

In short, the inverses of all the PPs in Theorem 2 are known now. For convenience, all the PPs in Theorem 2 and their inverses are listed in Table 1.

### 3. Large class of PPs and its inverse

In this section we slightly modify a known expression of the inverse of PP  $x^r h(x^s)$ . Moreover, we investigate the permutation properties of  $x(x-a)^{st}$  on  $(\mathbb{F}_{q^n}^*)^s$  and  $x^r(x^s - a)^t$  on  $\mathbb{F}_{q^n}$ , and obtain their inverses. The following lemma will be needed.

**Lemma 5** ([1, Proposition 3.1]). *Let  $f(x) = x^r h(x^s)$ , where  $h \in \mathbb{F}_q[x]$  and  $r, s \in \mathbb{N}$ . Then  $f$  is a PP of  $\mathbb{F}_q$  if and only if  $(r, s, q - 1) = 1$  and  $g(x) := x^r h(x)^s$  permutes  $(\mathbb{F}_q^*)^s$ .*

The problem that when special classes of  $g$  permuting  $(\mathbb{F}_q^*)^s$  has been extensively studied, see for example [3, 5, 13, 16, 17, 19, 26, 35]. For a recent survey of this problem, we refer the reader to [31] and the references therein.

The inverse of  $f$  in terms of roots of unity over  $\mathbb{F}_q$  was given in [29, 39]. Let  $g_1 \in \mathbb{F}_q[x]$  be such that  $x^{k_1} \circ g_1 = g \circ x^{k_1}$ , where  $k_1 = s/(s, q - 1)$ . The inverse of  $f$  in terms of the inverse of  $g_1$  on  $(\mathbb{F}_q^*)^s$  was given in [18] when  $(r, q - 1) = 1$ , and given in [22] for all  $r \in \mathbb{N}$ . Using the method in [22], we obtain the following equivalent version of the inverse of  $f$ , which is expressed in terms of the inverse of  $g$  on  $(\mathbb{F}_q^*)^s$ .

**Theorem 3.** *Let  $f(x) = x^r h(x^s)$ , where  $h \in \mathbb{F}_q[x]$  and  $r, s \in \mathbb{N}$ . Let  $\bar{s} = (s, q - 1)$  and  $k$  be an inverse of  $s/\bar{s}$  modulo  $(q - 1)/\bar{s}$ . If  $f$  is a PP of  $\mathbb{F}_q$  and  $g^{-1}$  is the inverse of  $g(x) := x^r h(x)^s$  on  $(\mathbb{F}_q^*)^s$ . Then the inverse of  $f$  on  $\mathbb{F}_q$  is*

$$f^{-1}(x) = x^b (h(g^{-1}(x^s)))^{-b} (g^{-1}(x^s))^{ck},$$

where  $b, c \in \mathbb{Z}$  satisfy  $br + c\bar{s} = 1$ .

*Proof.* We prove it by using the method in [22, Theorem 3.2]. Since the theorem holds for  $x = 0$ , we only consider  $x \in \mathbb{F}_q^*$ . Let  $\phi(x) = (x^r, x^s)$  and  $\psi(y, z) = (y^r h(z)^r, g(z))$ . It is easy to verify that  $\psi \circ \phi = \phi \circ f$ , i.e., the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{F}_q^* & \xrightarrow{f} & \mathbb{F}_q^* \\ \phi \downarrow & & \downarrow \phi \\ \phi(\mathbb{F}_q^*) & \xrightarrow{\psi} & \phi(\mathbb{F}_q^*). \end{array}$$

If  $f$  is a PP, then, by [Lemma 5](#),  $(r, \bar{s}) = 1$  and  $g$  permutes  $(\mathbb{F}_q^*)^s$ . Assume  $br + c\bar{s} = 1$  and  $k(s/\bar{s}) + v(q-1)/\bar{s} = 1$  for some  $b, c, k, v \in \mathbb{Z}$ . Then

$$c\bar{s} = c\bar{s}(k(s/\bar{s}) + v(q-1)/\bar{s}) = cks + cv(q-1),$$

and so, for any  $x \in \mathbb{F}_q^*$ ,

$$(x^r)^b (x^s)^{ck} = x^{br+cks} x^{cv(q-1)} = x^{br+cks+cv(q-1)} = x^{br+c\bar{s}} = x. \quad (2)$$

Hence  $\phi$  is bijective and  $\phi^{-1}(y, z) = y^b z^{ck}$ .

Since  $f$  is a PP of  $\mathbb{F}_q$  and  $\phi$  is bijective,  $\psi$  is also bijective. For  $(y, z) \in \phi(\mathbb{F}_q^*)$ , assume that  $\psi(y, z) = (\alpha, \beta)$  for some  $(\alpha, \beta) \in \phi(\mathbb{F}_q^*)$ , i.e.,

$$y^r h(z)^r = \alpha \quad \text{and} \quad g(z) = z^r h(z)^s = \beta.$$

Because  $z, \beta \in (\mathbb{F}_q^*)^s$  and  $g$  permutes  $(\mathbb{F}_q^*)^s$ , we obtain  $z = g^{-1}(\beta)$ . Denote  $\alpha = x_0^r$  and  $\beta = x_0^s$  for some  $x_0 \in \mathbb{F}_q^*$ . Then  $\alpha^b \beta^{ck} = x_0$  by (2), and so  $(\alpha^b \beta^{ck} h(z)^{-1})^r h(z)^r = \alpha$ . Since  $\psi$  is bijective, we have  $y = \alpha^b \beta^{ck} h(z)^{-1}$ . Hence,

$$\psi^{-1}(\alpha, \beta) = (y, z) = (\alpha^b \beta^{ck} h(g^{-1}(\beta))^{-1}, g^{-1}(\beta)).$$

Substituting  $\phi, \phi^{-1}, \psi^{-1}$  into  $f^{-1} = \phi^{-1} \circ \psi^{-1} \circ \phi$  gives the desire result.  $\square$

The key step in [Theorem 3](#) is to find the inverse of  $g$  on  $(\mathbb{F}_q^*)^s$ , which is possible to be done for special classes of  $g$ , as for instance in the following result.

**Lemma 6.** *Let  $a \in \mathbb{F}_{q^n}^*$  and  $s \mid q^m - 1$ . Then  $g(x) = x(x-a)^{q^m-1}$  permutes  $(\mathbb{F}_{q^n}^*)^s$  if and only if  $a^\ell \neq 1$ , where  $\ell = (q^n - 1)/(s, q^n - 1)$ . In this case, its inverse on  $(\mathbb{F}_{q^n}^*)^s$  is*

$$g^{-1}(x) = \left( (a^{-1}x)^{\frac{q^n-1}{q^d-1}} - 1 \right) \left( \sum_{i=1}^{n/d} a^{-\frac{q^{im}-1}{q^m-1}} x^{\frac{q^{(i-1)m}-1}{q^m-1}} \right)^{-1} + a,$$

where  $d = (m, n)$ .

*Proof.* Since the multiplicative group of  $\mathbb{F}_{q^n}$  is cyclic, we can verify  $(\mathbb{F}_{q^n}^*)^s = (\mathbb{F}_{q^n}^*)^{(s, q^n-1)}$ . Thus  $a \in (\mathbb{F}_{q^n}^*)^s$  if and only if  $a^\ell = 1$ . If  $a^\ell = 1$ , then  $a \in (\mathbb{F}_{q^n}^*)^s$ , and so  $g$  has root in  $(\mathbb{F}_{q^n}^*)^s$ . Hence  $g$  does not permute  $(\mathbb{F}_{q^n}^*)^s$ . Next we only consider  $a^\ell \neq 1$  and  $x \in (\mathbb{F}_{q^n}^*)^s$ .

Since  $g$  introduces a mapping from  $(\mathbb{F}_{q^n}^*)^s$  to itself, we need only show that, for any  $y \in (\mathbb{F}_{q^n}^*)^s$ , the equation  $g(x) = y$  has exactly one solution  $x$  and  $x = g^{-1}(y)$ .

Since  $a^\ell \neq 1$ , we have  $x - a \neq 0$  for any  $x \in (\mathbb{F}_{q^n}^*)^s$ . Let  $z = (x - a)^{-1}$ . Then  $x - a = z^{-1}$  and  $x = z^{-1} + a$ . Substituting them into  $g(x) = y$  yields

$$(z^{-1} + a)z^{1-q^m} = y, \quad \text{i.e.,} \quad z^{q^m} - (a/y)z = 1/y. \quad (3)$$

Recall that  $d = (m, n)$  and  $\ell = (q^n - 1)/(s, q^n - 1)$ . Let  $q^m - 1 = st$ . Then

$$\begin{aligned} q^d - 1 &= q^{(m, n)} - 1 = (q^m - 1, q^n - 1) = (st, q^n - 1) \\ &= (s, q^n - 1)(t, (q^n - 1)/(s, q^n - 1)) \\ &= (s, q^n - 1)(t, \ell), \end{aligned}$$

and so  $\frac{q^n-1}{q^d-1}(t, \ell) = \ell$ . Since  $a^\ell \neq 1$  and  $y \in (\mathbb{F}_{q^n}^*)^s$ , we have

$$(\mathbb{N}_{q^n/q^d}(a/y))^{(t, \ell)} = (a/y)^{\frac{q^n-1}{q^d-1}(t, \ell)} = (a/y)^\ell = a^\ell \neq 1.$$

Therefore,

$$\mathbb{N}_{q^n/q^d}(a/y) \neq 1. \quad (4)$$

It follows from [Lemma 2](#) and [\(3\)](#) that

$$\begin{aligned} z &= \frac{\mathbb{N}_{q^n/q^d}(a/y)}{1 - \mathbb{N}_{q^n/q^d}(a/y)} \sum_{i=1}^{n/d} (a/y)^{-\frac{q^{im}-1}{q^m-1}} (1/y)^{q^{(i-1)m}} \\ &= (\mathbb{N}_{q^n/q^d}(y/a) - 1)^{-1} \sum_{i=1}^{n/d} a^{-\frac{q^{im}-1}{q^m-1}} y^{\frac{q^{(i-1)m}-1}{q^m-1}}. \end{aligned} \quad (5)$$

Substituting [\(5\)](#) into  $x = z^{-1} + a$  gives  $x = g^{-1}(y)$ .  $\square$

After these preparations, we can now give the main theorem.

**Theorem 4.** *Let  $f(x) = x^r(x^s - a)^t$ , where  $a \in \mathbb{F}_{q^n}^*$  and  $r, s, t \in \mathbb{N}$  are such that  $st = q^m - 1$  and  $r \equiv 1 \pmod{\ell}$  with  $\ell = (q^n - 1)/(s, q^n - 1)$ . Then  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $(r, q^n - 1) = 1$  and  $a^\ell \neq 1$ . In this case, the inverse of  $f$  on  $\mathbb{F}_{q^n}$  is*

$$f^{-1}(x) = x^u(G(x)H(x))^{tu}, \quad (6)$$

where  $u$  is an inverse of  $r$  modulo  $q^n - 1$ ,

$$G(x) = ((a^{-1}x^s)^{\frac{q^n-1}{q^d-1}} - 1)^{-1}, \quad (7)$$

$$H(x) = \sum_{i=1}^{n/d} a^{-\frac{q^{im}-1}{q^m-1}} x^{\frac{q^{(i-1)m}-1}{t}}, \text{ and } d = (m, n). \quad (8)$$

*Proof.* From [Lemma 5](#),  $f$  is a PP if and only if  $(r, s, q^n - 1) = 1$  and  $g(x) := x^r(x - a)^{st}$  permutes  $(\mathbb{F}_q^*)^s$ . Since  $r \equiv 1 \pmod{\ell}$ , we have  $x^r = x$  and so  $g(x) = x(x - a)^{st}$  for any  $x \in (\mathbb{F}_q^*)^s$ . By [Lemma 6](#),  $g$  permutes  $(\mathbb{F}_q^*)^s$  if and only if  $a^\ell \neq 1$ . It follows from  $r \equiv 1 \pmod{\ell}$  that  $(r, \ell) = 1$ , and so  $(r, s, q^n - 1) = 1$  if and only if  $(r, q^n - 1) = 1$ .

Let  $ru + (q^n - 1)v = 1$  for some  $u, v \in \mathbb{Z}$ . Then  $ru + (\ell v)\bar{s} = 1$ , where  $\bar{s} = (s, q^n - 1)$ . For any  $x \in \mathbb{F}_{q^n}^*$ , we have  $g^{-1}(x^s) \in (\mathbb{F}_q^*)^s$ , and so  $(g^{-1}(x^s))^\ell = 1$ . Substituting  $b := u$ ,  $c := \ell v$  and  $g^{-1}$  in [Lemma 6](#) into [Theorem 3](#) gives the expression of  $f^{-1}$ .  $\square$

The following are two examples of [Theorem 4](#) where  $r^2 \equiv 1 \pmod{q^n - 1}$ .

**Example 1.** *Let  $f(x) = x^r(x^3 + a)^5$ , where  $a \in \mathbb{F}_{2^8}^*$  and  $r \equiv 1 \pmod{85}$ . Then  $f$  is a PP of  $\mathbb{F}_{2^8}$  if and only if  $(r, 3) = 1$  and  $a^{85} \neq 1$ . In this case, its inverse on  $\mathbb{F}_{2^8}$  is*

$$f^{-1}(x) = x^r(x^{51} + a^{17})^{-5r}(x^3 + a^{16})^{5r}.$$

**Example 2.** *Let  $f(x) = x^r(x^{16} - a)^5$ , where  $a \in \mathbb{F}_{3^6}^*$  and  $r \equiv 1 \pmod{91}$ . Then  $f$  is a PP of  $\mathbb{F}_{3^6}$  if and only if  $(r, 8) = 1$  and  $a^{91} \neq 1$ . In this case, its inverse on  $\mathbb{F}_{3^6}$  is*

$$f^{-1}(x) = (1 - a^{91})^{-5r} x^r (a^{90} + a^9 x^{16} + x^{584})^{5r}.$$

#### 4. Simplified versions of the main theorem

In this section we aim to simplify the expressions of  $G$  and  $H$  in [Theorem 4](#). On the one hand, we consider small  $n/(m, n)$  which is the number of the terms of  $H$ . On the other hand, we study the cases  $q^d - 1 \mid s$  and  $q^d - 1 \mid t$ , in which  $G$  and  $G^t$  are reduced to constants respectively.

#### 4.1. The case $H$ is a constant

Applying [Theorem 4](#) to  $m = n$ , we obtain that  $G(x) = a(x^s - a)^{-1}$  and  $H(x) = a^{-1}$ . Hence we arrive at the following result.

**Corollary 1.** *Let  $f(x) = x^r(x^s - a)^t$ , where  $a \in \mathbb{F}_q^*$ ,  $st = q - 1$  and  $r \equiv 1 \pmod{t}$ . Then  $f$  is a PP of  $\mathbb{F}_q$  if and only if  $(r, q - 1) = 1$  and  $a^t \neq 1$ . If  $f$  is a PP of  $\mathbb{F}_q$  and  $u$  is an inverse of  $r$  modulo  $q - 1$ , then its inverse on  $\mathbb{F}_q$  is*

$$f^{-1}(x) = x^u(x^s - a)^{-tu}.$$

The binomial  $x^s - a$  in [Corollary 1](#) can be generalized to  $H(x^s)$  which has no nonzero root in  $\mathbb{F}_q$ ; see the next theorem.

**Theorem 5.** *Let  $f(x) = x^r(h(x^s))^t$ , where  $h \in \mathbb{F}_q[x]$  and  $st = q - 1$ . Then  $f$  is a PP of  $\mathbb{F}_q$  if and only if  $(r, q - 1) = 1$  and  $h(x^s)$  has no nonzero root in  $\mathbb{F}_q$  (see [[2](#), Corollary 3.2]). If  $f$  is a PP of  $\mathbb{F}_q$  and  $r \equiv 1 \pmod{t}$ , then its inverse on  $\mathbb{F}_q$  is*

$$f^{-1}(x) = x^u(h(x^s))^{-tu},$$

where  $u$  is an inverse of  $r$  modulo  $q - 1$ .

*Proof.* The permutation part is [[2](#), Corollary 3.2]. Let  $r = kt + 1$  for some  $k \in \mathbb{Z}$ . Then

$$rs = (kt + 1)s = kst + s \equiv s \pmod{q - 1}.$$

Now it is easy to verify that  $f^{-1}(f(e)) = e$  for any  $e \in \mathbb{F}_q$ . This completes the proof.  $\square$

#### 4.2. The case $G$ or $G^t$ is a constant

If  $f$  in [Theorem 4](#) is a PP, then [\(4\)](#) holds, and so  $G(c) \in \mathbb{F}_{q^d}^*$  for any  $c \in \mathbb{F}_{q^n}$ . Hence  $G(x)^t = 1$  when  $q^d - 1 \mid t$ . Moreover, if  $q^d - 1 \mid s$ , then  $N_{q^n/q^d}(c^s) = 1$  for any  $c \in \mathbb{F}_{q^n}^*$ . Thus  $G$  is reduced to a constant. The argument above gives the following theorem.

**Theorem 6.** *With the same notation and hypotheses as in [Theorem 4](#), let  $f$  be a PP of  $\mathbb{F}_{q^n}$ .*

- (i) *If  $q^d - 1 \mid t$ , then  $f^{-1}(x) = x^u(H(x))^{tu}$ .*
- (ii) *If  $q^d - 1 \mid s$ , then  $f^{-1}(x) = x^u(AH(x))^{tu}$ , where  $A = (a^{-\frac{q^n-1}{q^d-1}} - 1)^{-1}$ .*

Recall that  $d = (m, n)$  and  $q^m - 1 = st$ . The conditions  $q^d - 1 \mid s$  or  $q^d - 1 \mid t$  in [Theorem 6](#) are easy to satisfied, because

$$st = q^m - 1 = (q^d - 1)(1 + q^d + q^{2d} + \cdots + q^{m-d}). \quad (9)$$

For instance, taking  $t = 1$  and  $n = 2m$  leads to  $q^d - 1 = q^m - 1 = s$  and  $n/d = 2$ . Hence  $H(x) = a^{-1} + a^{-(q^m+1)}x^{q^m-1}$ . Then substituting  $q$  for  $q^m$  yields the following result.

**Corollary 2.** *Let  $f(x) = x^r(x^{q-1} - a)$ , where  $a \in \mathbb{F}_{q^2}^*$  and  $r \equiv 1 \pmod{q + 1}$ . Then  $f$  is a PP of  $\mathbb{F}_{q^2}$  if and only if  $(r, q^2 - 1) = 1$  and  $a^{q+1} \neq 1$ . If  $f$  is a PP of  $\mathbb{F}_{q^2}$  and  $u$  is an inverse of  $r$  modulo  $q^2 - 1$ , then its inverse on  $\mathbb{F}_{q^2}$  is*

$$f^{-1}(x) = (1 - a^{q+1})^{-u}(a^q x + x^q)^u.$$

Next we give another example of the case  $q^d - 1 = s$  over  $\mathbb{F}_{2^n}$ .



**Corollary 3.** Let  $f(x) = x^r(x^3 + a)^5$  where  $a \in \mathbb{F}_{2^n}^*$ ,  $n$  is even,  $r \equiv 1 \pmod{\ell}$  and  $\ell = (2^n - 1)/3$ . Then  $f$  is a PP of  $\mathbb{F}_{2^n}$  if and only if  $(r, 2^n - 1) = 1$  and  $a^\ell \neq 1$ . If  $f$  is a PP of  $\mathbb{F}_{2^n}$  and  $n \equiv 2 \pmod{4}$ , then its inverse on  $\mathbb{F}_{2^n}$  is

$$f^{-1}(x) = a^{\ell u} x^u \left( \sum_{i=1}^{n/2} a^{-\frac{16^i-1}{15}} x^{\frac{16^{i-1}-1}{5}} \right)^{5u},$$

where  $u$  is an inverse of  $r$  modulo  $2^n - 1$ .

*Proof.* The permutation part is a direct consequence of [Theorem 4](#). Let  $\omega = a^\ell$ . Then  $\omega^3 = 1$  and, by  $\omega \neq 1$ ,  $\omega^2 + \omega + 1 = 0$ . Thus  $\omega/(1 + \omega) = \omega^{-1}$  and  $\omega^{-5} = \omega$ . Inserting them into [Theorem 6](#) gives the above expression of  $f^{-1}$ .  $\square$

The next corollary is an example of the case  $q^d - 1 = t$  and  $2n = 3m$ .

**Corollary 4.** Let  $f(x) = x(x^{q+1} - a)^{q-1}$ , where  $a \in \mathbb{F}_{q^3}^*$  and  $q$  is odd. Then  $f$  is a PP of  $\mathbb{F}_{q^3}$  if and only if  $a^{(q^3-1)/2} = -1$ . In this case, its inverse on  $\mathbb{F}_{q^3}$  is

$$f^{-1}(x) = x(a^{q^2+q} + a^q x^{q+1} + x^{q^2+q+2})^{q-1}.$$

## 5. Permutation trinomials and tetranomials

Applying the main theorem to  $t = 2, 3$ , we can obtain some permutation trinomials and tetranomials and their inverses, which contain two classes of exceptional polynomials in [Theorem 2](#). First, we give a simple lemma.

**Lemma 7.** Let  $a$  be odd,  $m, n \in \mathbb{N}$  and  $d = (m, n)$ . Then  $(a^m - 1)/(a^d - 1)$  and  $m/d$  have the same parity, and

$$((a^m - 1)/2, a^n - 1) = \begin{cases} a^d - 1 & \text{if } m/d \text{ is even,} \\ (a^d - 1)/2 & \text{if } m/d \text{ is odd.} \end{cases}$$

*Proof.* Since  $(a^m - 1)/(a^d - 1) = \sum_{i=1}^{m/d} (a^d)^{i-1}$  and  $a$  is odd,  $(a^m - 1)/(a^d - 1)$  is an integer with the same parity as  $m/d$ . Then

$$\begin{aligned} 2((a^m - 1)/2, a^n - 1) &= (a^m - 1, 2(a^n - 1)) \\ &= (a^m - 1, a^n - 1) \left( \frac{a^m - 1}{(a^m - 1, a^n - 1)}, \frac{2(a^n - 1)}{(a^m - 1, a^n - 1)} \right) \\ &= (a^m - 1, a^n - 1) \left( \frac{a^m - 1}{(a^m - 1, a^n - 1)}, 2 \right) \\ &= (a^d - 1) \left( \frac{a^m - 1}{a^d - 1}, 2 \right) \\ &= (a^d - 1)(m/d, 2). \end{aligned} \quad \square$$

Applying [Theorem 4](#) to  $r = 1$  and  $t = 2$ , we derive the following result.

**Theorem 7.** Let  $f(x) = x^q - 2ax^{\frac{q^m+1}{2}} + a^2x$ , where  $a \in \mathbb{F}_{q^n}^*$ ,  $q$  is odd and  $m, n \in \mathbb{N}$ . Let  $d = (m, n)$ ,  $c = a^{(q^n-1)/(q^d-1)}$  and

$$H_2(x) = x \left( \sum_{i=1}^{n/d} a^{-\frac{q^{im}-1}{q^m-1}} x^{\frac{q^{(i-1)m}-1}{2}} \right)^2.$$

(i) If  $m/d$  is even, then  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $c \neq 1$ . In this case,

$$f^{-1}(x) = c^2(1-c)^{-2}H_2(x).$$

(ii) If  $m/d$  is odd, then  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $c^2 \neq 1$ . In this case,

$$f^{-1}(x) = c^2(1-c^2)^{-2}(2cx^{\frac{q^n-1}{2}} + c^2 + 1)H_2(x). \quad (10)$$

*Proof.* Note that  $f(x) = x(x^{\frac{q^m-1}{2}} - a)^2$ . In the notation of [Theorem 4](#), we have  $t = 2$  and  $s = (q^m - 1)/2$ . If  $m/d$  is even, then  $(s, q^n - 1) = q^d - 1$  by [Lemma 7](#), and  $\ell = (q^n - 1)/(q^d - 1)$ . According to [Theorem 4](#),  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $c \neq 1$ . It is easy to verify  $f^{-1}(f(0)) = 0$ . Next we only consider  $x \in \mathbb{F}_{q^n}^*$  for computing  $f^{-1}(x)$ . Since  $q^d - 1 \mid s$ , we have

$$(x^s)^{\frac{q^n-1}{q^d-1}} = (x^{q^n-1})^{\frac{s}{q^d-1}} = 1 \quad (11)$$

for any  $x \in \mathbb{F}_{q^n}^*$ . Substituting [\(11\)](#) into [\(7\)](#), we obtain

$$G(x) = c(1-c)^{-1}. \quad (12)$$

If  $m/d$  is odd, then  $(s, q^n - 1) = (q^d - 1)/2$  by [Lemma 7](#), and  $\ell = 2(q^n - 1)/(q^d - 1)$ . According to [Theorem 4](#),  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $c^2 \neq 1$ . If  $m/d$  is odd, then  $(q^m - 1)/(q^d - 1)$  is also odd by [Lemma 7](#), and so

$$(x^s)^{\frac{q^n-1}{q^d-1}} = x^{\frac{q^m-1}{2} \cdot \frac{q^n-1}{q^d-1}} = x^{\frac{q^n-1}{2} \cdot \frac{q^m-1}{q^d-1}} = x^{\frac{q^n-1}{2}}$$

for any  $x \in \mathbb{F}_{q^n}^*$ . Since

$$1 - c^2 = (x^{\frac{q^n-1}{2}})^2 - c^2 = (x^{\frac{q^n-1}{2}} + c)(x^{\frac{q^n-1}{2}} - c).$$

We have

$$(x^{\frac{q^n-1}{2}} - c)^{-1} = (1 - c^2)^{-1}(x^{\frac{q^n-1}{2}} + c). \quad (13)$$

Note that  $c = a^{(q^n-1)/(q^d-1)}$ . Inserting [\(13\)](#) into [\(7\)](#), we obtain

$$G(x) = c(1 - c^2)^{-1}(x^{\frac{q^n-1}{2}} + c). \quad (14)$$

Then, for any  $x \in \mathbb{F}_{q^n}^*$ ,

$$(x^{\frac{q^n-1}{2}} + c)^2 = 2cx^{\frac{q^n-1}{2}} + c^2 + 1. \quad (15)$$

Substituting [\(12\)](#), [\(14\)](#) and [\(15\)](#) into [Theorem 4](#) gives the desire result.  $\square$

Taking  $q^m = 5, 7, 9$  in [Theorem 7](#) leads to the following corollaries.

**Corollary 5.** Let  $f(x) = x^5 - 2ax^3 + a^2x$ , where  $a \in \mathbb{F}_{5^n}^*$  and  $n \in \mathbb{N}$ . Then  $f$  is a PP of  $\mathbb{F}_{5^n}$  if and only if  $a^{(5^n-1)/2} = -1$ . In this case, the inverse of  $f$  on  $\mathbb{F}_{5^n}$  is

$$f^{-1}(x) = 2a^{\frac{5^n-1}{4}}x^{\frac{5^n+1}{2}} \left( \sum_{i=0}^{n-1} a^{-\frac{5^i+1-1}{4}}x^{\frac{5^i-1}{2}} \right)^2.$$

[Corollary 5](#) is essentially [[38](#), Theorem 8] or [[18](#), Lemma 4.9].

**Corollary 6.** Let  $f(x) = x^7 - 2ax^4 + a^2x$ , where  $a \in \mathbb{F}_{7^n}^*$  and  $n \in \mathbb{N}$ . Then  $f$  is a PP

of  $\mathbb{F}_{7^n}$  if and only if  $a^{(7^n-1)/3} \neq 1$ . In this case, the inverse of  $f$  on  $\mathbb{F}_{7^n}$  is

$$f^{-1}(x) = 2x \left( 2a^{\frac{7^n-1}{6}} x^{\frac{7^n-1}{2}} + a^{\frac{7^n-1}{3}} + 1 \right) \left( \sum_{i=0}^{n-1} a^{-\frac{7^{i+1}-1}{6}} x^{\frac{7^i-1}{2}} \right)^2.$$

*Proof.* The permutation part is a direct consequence of [Theorem 7](#). Let  $\omega = a^{(7^n-1)/3}$ . Then  $\omega^3 = 1$  and  $\omega \neq 1$  if  $f$  is a PP. Hence  $\omega^2 + \omega + 1 = 0$ , and so  $(1 - \omega)^2 = -3\omega$ . Inserting them into [\(10\)](#) gives the above expression of  $f^{-1}$ .  $\square$

**Corollary 7.** Let  $f(x) = x^9 + ax^5 + a^2x$ , where  $a \in \mathbb{F}_{3^n}^*$  and  $n \in \mathbb{N}$ .

(i) If  $n$  is odd, then  $f$  is a PP of  $\mathbb{F}_{3^n}$  if and only if  $a^{(3^n-1)/2} = -1$ . In this case, the inverse of  $f$  on  $\mathbb{F}_{3^n}$  is

$$f^{-1}(x) = x \left( \sum_{i=0}^{n-1} a^{-\frac{9^{i+1}-1}{8}} x^{\frac{9^i-1}{2}} \right)^2.$$

(ii) If  $n$  is even, then  $f$  is a PP of  $\mathbb{F}_{3^n}$  if and only if  $c^2 \neq 1$ , where  $c = a^{(3^n-1)/8}$ . In this case, the inverse of  $f$  on  $\mathbb{F}_{3^n}$  is

$$f^{-1}(x) = x \left( c^5 x^{\frac{3^n-1}{2}} + c^2 + 1 \right) \left( \sum_{i=1}^{n/2} a^{-\frac{9^i-1}{8}} x^{\frac{9^{i-1}-1}{2}} \right)^2. \quad (16)$$

*Proof.* We only verify [\(16\)](#), because the rest parts are direct consequences of [Theorem 7](#). Let  $\omega = c^2 = a^{(3^n-1)/4}$ . Then  $\omega^4 = 1$  and  $\omega \neq 1$  if  $f$  is a PP. Thus  $\omega^3 + \omega^2 + \omega + 1 = 0$ , and so  $(1 - \omega)^2 = 1 + \omega + \omega^2 = -\omega^3$  in  $\mathbb{F}_{3^n}$ . Then  $\omega/(-\omega^3) = -\omega^{-2} = -\omega^2$  and  $-\omega^2(\omega + 1) = \omega + 1$ . Inserting them into [\(10\)](#) gives [\(16\)](#).  $\square$

Applying [Theorem 4](#) to  $r = 1$ ,  $t = 3$  and  $q^m = 7$  gives the following corollary.

**Corollary 8.** Let  $f(x) = x^7 - 3ax^5 + 3a^2x^3 - a^3x$ , where  $a \in \mathbb{F}_{7^n}^*$  and  $n \in \mathbb{N}$ . Then  $f$  is a PP of  $\mathbb{F}_{7^n}$  if and only if  $a^{(7^n-1)/2} = -1$ . In this case, its inverse on  $\mathbb{F}_{7^n}$  is

$$f^{-1}(x) = x \left( 3(ax^4)^{\frac{7^n-1}{6}} - 3(ax)^{\frac{7^n-1}{3}} - 2 \right) \left( \sum_{i=0}^{n-1} a^{-\frac{7^{i+1}-1}{6}} x^{\frac{7^i-1}{3}} \right)^3.$$

*Proof.* Clearly,  $f(x) = x(x^2 - a)^3$ , and so  $s = 2$ ,  $t = 3$ ,  $\ell = (7^n - 1)/2$ ,  $m = d = 1$ . From [Theorem 4](#),  $f$  is a PP of  $\mathbb{F}_{q^n}$  if and only if  $a^{(7^n-1)/2} = -1$ . It is easy to verify that  $f^{-1}(f(0)) = 0$ . Next we only consider  $x \in \mathbb{F}_{q^n}^*$  for computing  $f^{-1}(x)$ . Note that

$$2 = 1 - a^{\frac{7^n-1}{2}} = \left( x^{\frac{7^n-1}{3}} \right)^3 - \left( a^{\frac{7^n-1}{6}} \right)^3 = \left( x^{\frac{7^n-1}{3}} - a^{\frac{7^n-1}{6}} \right) \lambda(x),$$

where

$$\lambda(x) = x^{\frac{2(7^n-1)}{3}} + a^{\frac{7^n-1}{6}} x^{\frac{7^n-1}{3}} + a^{\frac{7^n-1}{3}}.$$

Therefore,

$$\left( x^{\frac{7^n-1}{3}} - a^{\frac{7^n-1}{6}} \right)^{-1} = 4\lambda(x). \quad (17)$$

Inserting [\(17\)](#) into [\(7\)](#) yields  $G(x) = 4a^{\frac{7^n-1}{6}} \lambda(x)$ . Then, for any  $x \in \mathbb{F}_{q^n}^*$ ,

$$G(x)^3 = -\lambda(x)^3 = 3(ax^4)^{\frac{7^n-1}{6}} - 3(ax)^{\frac{7^n-1}{3}} - 2. \quad (18)$$

Substituting [\(18\)](#) into [Theorem 4](#) gives the desire result.  $\square$

## References

- [1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2011) 51–67.
- [2] A. Akbary, Q. Wang, On polynomials of the form  $x^r f(x^{(q-1)/l})$ , *Int. J. Math. Math. Sci.* 2007 (2007) 1–7, article ID 23408, doi:[10.1155/2007/23408](https://doi.org/10.1155/2007/23408).
- [3] D. Bartoli, Permutation trinomials over  $\mathbb{F}_{q^3}$ , *Finite Fields Appl.* 61 (2020) 101597.
- [4] D. Bartoli, M. Giulietti, L. Quoos, G. Zini, Complete permutation polynomials from exceptional polynomials, *J. Number Theory* 176 (2017) 46–66, doi:[10.1016/j.jnt.2016.12.016](https://doi.org/10.1016/j.jnt.2016.12.016).
- [5] X. Cao, X.-D. Hou, J. Mi, S. Xu, More permutation polynomials with Niho exponents which permute  $\mathbb{F}_{q^2}$ , *Finite Fields Appl.* 62 (2020) 101626.
- [6] P. Charpin, S. Mesnager, S. Sarkar, Involutions over the Galois Field  $\mathbb{F}_{2^n}$ , *IEEE Trans. Inf. Theory* 62 (4) (2016) 2266–2276.
- [7] R. Coulter, M. Henderson, A note on the roots of trinomials over a finite field, *Bull. Aust. Math. Soc.* 69 (2004) 429–432.
- [8] R. S. Coulter, M. Henderson, The compositional inverse of a class of permutation polynomials over a finite field, *Bull. Aust. Math. Soc.* 65 (2002) 521–526.
- [9] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Part I, *Ann. Math.* 11 (1896) 65–120, <https://www.jstor.org/stable/1967217>.
- [10] X. Fan, A classification of permutation polynomials of degree 7 over finite fields, *Finite Fields Appl.* 59 (2019) 1–21.
- [11] X. Fan, Permutation polynomials of degree 8 over finite fields of characteristic 2, *Finite Fields Appl.* 64 (2020) 101662.
- [12] X. Fan, Permutation polynomials of degree 8 over finite fields of odd characteristic, *Bull. Aust. Math. Soc.* 101 (1) (2020) 40–55.
- [13] X.-D. Hou, Z. Tu, X. Zeng, Determination of a class of permutation trinomials in characteristic three, *Finite Fields Appl.* 61 (2020) 101596.
- [14] G. M. Kyureghyan, Constructing permutations of finite fields via linear translators, *J. Combin. Theory Ser. A* 118 (2011) 1052–1061.
- [15] J. Li, D. B. Chandler, Q. Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, *Finite Fields Appl.* 16 (2010) 406–419.
- [16] K. Li, L. Qu, C. Li, H. Chen, On a conjecture about a class of permutation quadrinomials, *Finite Fields Appl.* 66 (2020) 101690.
- [17] K. Li, L. Qu, Q. Wang, New constructions of permutation polynomials of the form  $x^r h(x^{q-1})$  over  $\mathbb{F}_{q^2}$ , *Des. Codes Cryptogr.* 86 (2018) 2379–2405.
- [18] K. Li, L. Qu, Q. Wang, Compositional inverses of permutation polynomials of the form  $x^r h(x^s)$  over finite fields, *Cryptogr. Commun.* 11 (2019) 279–298.
- [19] N. Li, T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *Cryptogr. Commun.* 11 (1) (2019) 129–136.
- [20] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
- [21] A. Muratović-Ribić, A note on the coefficients of inverse polynomials, *Finite Fields Appl.* 13 (2007) 977–980.

- [22] T. Niu, K. Li, L. Qu, Q. Wang, A general method for finding the compositional inverses of permutations from the AGW criterion, arXiv:2004.12552, <https://arxiv.org/abs/2004.12552v1>, 2020.
- [23] T. Niu, K. Li, L. Qu, Q. Wang, New constructions of involutions over finite fields, *Cryptogr. Commun.* 12 (2020) 165–185, doi:[10.1007/s12095-019-00386-2](https://doi.org/10.1007/s12095-019-00386-2).
- [24] L. Reis, Nilpotent linearized polynomials over finite fields and applications, *Finite Fields Appl.* 50 (2018) 279–292.
- [25] C. J. Shallue, I. M. Wanless, Permutation polynomials and orthomorphism polynomials of degree six, *Finite Fields Appl.* 20 (2013) 84–92.
- [26] Z. Tu, X. Liu, X. Zeng, A revisit to a class of permutation quadrinomials, *Finite Fields Appl.* 59 (2019) 57–85.
- [27] A. Tuxanidy, Q. Wang, On the inverses of some classes of permutations of finite fields, *Finite Fields Appl.* 28 (2014) 244–281.
- [28] A. Tuxanidy, Q. Wang, Compositional inverses and complete mappings over finite fields, *Discrete Appl. Math.* 217 (2017) 318–329.
- [29] Q. Wang, On inverse permutation polynomials, *Finite Fields Appl.* 15 (2009) 207–213.
- [30] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields, *Finite Fields Appl.* 45 (2017) 422–427.
- [31] Q. Wang, Polynomials over finite fields: an index approach, in: K.-U. Schmidt, A. Winterhof (Eds.), *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, 319–346, doi:[10.1515/9783110642094-015](https://doi.org/10.1515/9783110642094-015), 2019.
- [32] B. Wu, The compositional inverses of linearized permutation binomials over finite fields, arXiv:1311.2154v1, <https://arxiv.org/abs/1311.2154>, 2013.
- [33] B. Wu, Z. Liu, The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2, *Finite Fields Appl.* 24 (2013) 136–147.
- [34] B. Wu, Z. Liu, Linearized polynomials over finite fields revisited, *Finite Fields Appl.* 22 (2013) 79–100.
- [35] Z. Zha, L. Hu, Z. Zhang, Permutation polynomials of the form  $x + \gamma \text{Tr}_q^{q^n}(h(x))$ , *Finite Fields Appl.* 60 (2019) 101573.
- [36] D. Zheng, M. Yuan, N. Li, L. Hu, X. Zeng, Constructions of involutions over finite fields, *IEEE Trans. Inf. Theory* 65 (12) (2019) 7876–7883, doi:[10.1109/TIT.2019.2919511](https://doi.org/10.1109/TIT.2019.2919511).
- [37] Y. Zheng, F. Wang, L. Wang, W. Wei, On inverses of some permutation polynomials over finite fields of characteristic three, *Finite Fields Appl.* 66 (2020) 101670, doi:[10.1016/j.ffa.2020.101670](https://doi.org/10.1016/j.ffa.2020.101670).
- [38] Y. Zheng, Q. Wang, W. Wei, On inverses of permutation polynomials of small degree over finite fields, *IEEE Trans. Inf. Theory* 66 (2) (2020) 914–922, doi:[10.1109/TIT.2019.2939113](https://doi.org/10.1109/TIT.2019.2939113).
- [39] Y. Zheng, Y. Yu, Y. Zhang, D. Pei, Piecewise constructions of inverses of cyclotomic mapping permutation polynomials, *Finite Fields Appl.* 40 (2016) 1–9.
- [40] Y. Zheng, P. Yuan, D. Pei, Piecewise constructions of inverses of some permutation polynomials, *Finite Fields Appl.* 36 (2015) 151–169.