On inverses of some permutation polynomials over finite fields of characteristic three✩

Yanbin Zheng,a,b, Fu Wangb, Libo Wangc, Wenhong Weia,b,*

aSchool of Computer Science and Technology, Dongguan University of Technology, Dongguan, China
bGuangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, China
cCollege of Information Science and Technology, Jinan University, Guangzhou, China

Abstract
By using the piecewise method, Lagrange interpolation formula and Lucas’ theorem, we determine explicit expressions of the inverses of a class of reversed Dickson permutation polynomials and some classes of generalized cyclotomic mapping permutation polynomials over finite fields of characteristic three.

Keywords: Permutation polynomial, Inverse, Reversed Dickson polynomial, Cyclotomic mapping polynomial

2010 MSC: 11T06, 11T71

1. Introduction

For 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 \( f(x) \in \mathbb{F}_q[x] \) is called a permutation polynomial (PP) of \( \mathbb{F}_q \) if it induces a bijection from \( \mathbb{F}_q \) to itself. Hence for any PP \( f(x) \) of \( \mathbb{F}_q \), there exists a polynomial \( f^{-1}(x) \in \mathbb{F}_q[x] \) such that \( f^{-1}(f(x)) = x \) for each \( x \in \mathbb{F}_q \) or equivalently \( f^{-1}(f(x)) \equiv x \pmod{x^q-x} \), and \( f^{-1}(x) \) is unique in the sense of reduction modulo \( x^q-x \). Here \( f^{-1}(x) \) is defined as the composition inverse of \( f(x) \), and we simply call it the inverse of \( f(x) \) on \( \mathbb{F}_q \).

Recently, some classes of PPs are found; see for example [10, 13, 23, 24, 26] for PPs of the form \( x^r h(x^{q-1}) \) of \( \mathbb{F}_q^* \), [16, 27] for PPs of the form \( (x^q - x + c)^s + L(x) \) of \( \mathbb{F}_q^* \), [9, 23, 31] for PPs of the form \( (ax^q + bx + c)^s \phi((ax^q + bx + c)^r) + ux^q + vx \) of \( \mathbb{F}_q^* \), and [1, 4, 7] for PPs studied by using the Hasse-Weil bound and Hermite’s criterion.

The construction of PPs of finite fields is not an easy subject. However, the problem of determining the inverse of a PP seems to be an even more complicated problem. In fact, there are few known classes of PPs whose inverses have been obtained explicitly; see for example [8, 11, 17, 29] for PPs of the form \( x^r h(x^{q-1}/d) \), [20, 22] for linearized PPs, [19, 29] for generalized cyclotomic mapping PPs, [30] for general piecewise PPs, [2] for involutions over \( \mathbb{F}_2^n \), and [14, 15] for more general classes of PPs. The general results

✩The work was partially supported by the National NSF of China (61602125, 61862011, 61862012), the China Postdoctoral Science Foundation (2018M630341), the NSFC of Guangxi (2018GXNSFAA188116, 2018GXNSFAA138116), the Guangxi Science and Technology Plan Project (AD18280105), the research start-up grants of Dongguan University of Technology, and the Guangdong Provincial Science and Technology Plan Projects (2016A010101034, 2016A010108035).

*Corresponding author.

Email addresses: zhengyanbin@guet.edu.cn (Yanbin Zheng), wanglibo12b@emails.ucas.ac.cn (Libo Wang), 20171640dgut.edu.cn (Wenhong Wei)
in [14, 15] also contain some concrete classes, such as bilinear PPs in [21] and linearized PPs of the form \( L(x) + K(x) \) in [12]. For a brief summary of the results concerning the inverses of PPs, we refer the reader to [28] and the references therein.

In the study of permutation behavior of the reversed Dickson polynomial, Hou [6] proved the following Lemma 1. Since the reversed Dickson polynomial \( D_{3n+5}(1, x) = f(1 - x) - 1 \), Hou equivalently proved that \( D_{3n+5}(1, x) \) is a PP of \( \mathbb{F}_{3^n} \) for even \( n \).

**Lemma 1.** (see [6, Theorem 1.1]) Let \( n \) be a positive even integer. Then

\[
f(x) = (x - x^2 - x^3)x^{\frac{3n-1}{2}} - x^2
\]

is a PP of \( \mathbb{F}_{3^n} \).

The purpose of this paper is to find the inverse of \( f(x) \) in (1). The main idea of this paper is the combination of the piecewise method in [29] and some techniques in [28].

The rest of the paper is organized as follows. Section 2 first gives a formula for the inverse of a class of piecewise PPs \( f(x) \), which converts the problem of determining the inverse of \( f(x) \) on \( \mathbb{F}_{q} \) to the problem of computing the inverse \( f_{-1}^e(x) \) of piece function \( f_s(x) \) when restricted to a subset \( C_s \) of \( \mathbb{F}_{q} \) for all \( s \). Then we present an expression of \( f_{-1}^e(x) \) in Theorem 2, which provides all the coefficients of \( f_{-1}^e(x) \) by computing the coefficients of \( x^{(q-3)/2} \) and \( x^{q-2} \) in \( f_s(x)^k \) (mod \( x^q - x \)) for \( 1 \leq k \leq (q - 3)/2 \). Applying these results in Section 2 to \( f(x) \) in (1), we reduce the coefficients of \( f^{-1}(x) \) into two classes of binomial coefficients in Section 3. Section 4 gives explicit values of these binomial coefficients by using a congruence of binomial coefficients and the Lucas’ theorem. In other words, we determine the inverse of \( f(x) \) as follows.

**Theorem 1.** The inverse of \( f(x) \) in Lemma 1 on \( \mathbb{F}_{3^n} \) is

\[
f^{-1}(x) = x^{3n-1}(x^{\frac{3n-1}{2}} + 1) + g(x)(x^{\frac{3n-1}{2}} - 1),
\]

where

\[
g(x) = \sum_{0 \leq j \leq k \leq n-1} a_{jk}(-1)^{j+k}x^{\frac{j}{2}+k}, \quad a_{jk} = \begin{cases} 1 & \text{if } j = k, \\ -1 & \text{if } j < k. \end{cases}
\]

Furthermore, the inverse of \( D_{3n+5}(1, x) \) on \( \mathbb{F}_{3^n} \) is \( D_{3n+5}^{-1}(1, x) = 1 - f^{-1}(x + 1) \).

In the last section, by an argument similar to the one used in Theorem 1, we also obtain explicit inverses of some generalized cyclotomic mapping PPs studied in [18].

2. The inverse of a class of piecewise PPs

The piecewise methods for constructing PPs and their inverses were summarized in [2, 5] and [29] respectively. Applying these methods, we can easily get the following result.

**Lemma 2.** Let \( q \) be odd and \( f_0(x), f_1(x) \in \mathbb{F}_{q}[x] \). Define

\[
f(x) = \frac{1}{2}f_0(x)(1 + x^{\frac{q-1}{2}}) + \frac{1}{2}f_1(x)(1 - x^{\frac{q-1}{2}}) \quad \text{with } f(0) = 0,
\]

\( C_0 = \{ e^2 : e \in \mathbb{F}_{q}^* \} \), and \( C_1 = \mathbb{F}_{q}^* \setminus C_0 \). Then \( f(x) \) is a PP of \( \mathbb{F}_{q} \) if and only if \( f_s \) is injective on \( C_s \) for \( s \in \{0, 1\} \), and \( f_0(C_0) \cap f_1(C_1) = \emptyset \). Assume \( f(x) \) is a PP of \( \mathbb{F}_{q} \), and \( f_s^{-1}(x) \in \mathbb{F}_{q}[x] \) satisfies that \( f_s^{-1}(f_s(c)) = c \) for any \( c \in C_s \) and \( s \in \{0, 1\} \).

(i) If \( f_s \) maps \( C_s \) into \( C_s \) for \( s \in \{0, 1\} \), then the inverse of \( f(x) \) on \( \mathbb{F}_{q} \) is

\[
f^{-1}(x) = \frac{1}{2}f_0^{-1}(x)(1 + x^{\frac{q-1}{2}}) + \frac{1}{2}f_1^{-1}(x)(1 - x^{\frac{q-1}{2}}),
\]

(2)
(ii) If $f_s$ maps $C_s$ into $C_t$ for $s \neq t \in \{0, 1\}$, then the inverse of $f(x)$ on $\mathbb{F}_q$ is
\[
f_s^{-1}(x) = \frac{1}{2} f_0^{-1}(x) (1 - x^{\frac{q+1}{2}}) + \frac{1}{2} f_1^{-1}(x) (1 + x^{\frac{q+1}{2}}).
\]

Lemma 2 converts the problem of determining $f_s^{-1}(x)$ into the problem of computing $f_s^{-1}(x)$, the inverse of piece function $f_s(x)$ when restricted to $C_s$. In Lemma 2, if $q = 3$ then $f(x) = f_s^{-1}(x) = \pm x$ in the sense of reduction modulo $x^3 - x$. We will give an expression of $f_s^{-1}(x)$ for $q > 3$ after the following lemma.

**Lemma 3.** For an odd prime power, let $C_0 = \{e^2 : e \in \mathbb{F}_q^*\}$ and $C_1 = \mathbb{F}_q^* \setminus C_0$. Then
\[
\sum_{a \in C_x} a^k = \begin{cases}
-2^{-1} & \text{if } k = q - 1, \\
(-1)^{q+1} - 2^{-1} & \text{if } k = (q - 1)/2, \\
0 & \text{if } 0 \leq k \leq q - 2 \text{ and } k \neq (q - 1)/2.
\end{cases}
\]

**Proof.** Let $A = \sum_{a \in C_0} a^k$ and $\xi$ a prime element of $\mathbb{F}_q$. Obviously,
\[
(\xi^k + 1)A = \sum_{a \in C_0} a^k + \sum_{a \in C_1} a^k = \sum_{a \in \mathbb{F}_q} a^k = \begin{cases}
-1 & \text{if } k = q - 1, \\
0 & \text{if } k = 0, 1, \ldots, q - 2.
\end{cases}
\]

If $k = q - 1$, then $\xi^k = 1$ and $2A = -1$, so $A = -1/2$. If $k = (q - 1)/2$, then $a^k = -1$ for $a \in C_1$. Hence $A = (-1)(q - 1)/2 = 1/2$. If $0 \leq k \leq q - 2$ and $k \neq (q - 1)/2$, then $\xi^k \neq -1$ and $(\xi^k + 1)A = 0$. Thus $A = 0$. Then using (3) can complete the proof. \qed

**Theorem 2.** For an odd prime power $q > 3$, let $C_0 = \{e^2 : e \in \mathbb{F}_q^*\}$ and $C_1 = \mathbb{F}_q^* \setminus C_0$. For $s, t \in \{0, 1\}$, assume $f_s(x) \in \mathbb{F}_q[x]$ induces a bijection from $C_s$ to $C_t$, and
\[
f_s(x)^{q-1-i} \equiv \sum_{0 \leq k \leq q-1} b_{ik} x^k \pmod{x^q - x}
\]
for $(q + 1)/2 \leq i \leq q - 2$. Then the inverse of $f_s(x)$ when restricted to $C_s$ is
\[
f_s^{-1}(x) = \sum_{(q+1)/2 \leq i \leq q-2} (-1)^{q+i}(b_{i,(q-3)/2} + (-1)^s b_{i,q-2})x^{q-1-i} + (-1)^{i+1}
\]
in the sense of reduction modulo $x^{\frac{q+1}{2}} + (-1)^{i+1}$.

**Proof.** Let $f_s^{-1}(x) = \sum_{i=0}^{q-1} c_i x^i \in \mathbb{F}_q[x]$. Then by the Lagrange interpolation formula,
\[
f_s^{-1}(x) = \sum_{a \in C_s} a (1 - (x - f_s(a))^{q-1})
= \sum_{a \in C_s} a \left( - \sum_{1 \leq i \leq q-1} (-1)^i (-f_s(a))^{q-1-i} x^i \right)
= \sum_{1 \leq i \leq q-1} \left(- \sum_{a \in C_s} a f_s(a)^{q-1-i} \right) x^i.
\]
Hence $c_0 = 0$ and
\[
c_i = - \sum_{a \in C_s} a f_s(a)^{q-1-i}, \quad \text{where } 1 \leq i \leq q - 1.
\]
Then by (6) and Lemma 3
\[ c_i = -\sum_{a \in C_s} a \sum_{0 \leq k \leq q-1} b_{ik} a^k = -\sum_{0 \leq k \leq q-1} b_{ik} \sum_{a \in C_s} a^{k+1} \]
\[ = 2^{-1} (b_{i,q-2} + (-1)^q b_{i,(q-3)/2}). \] (7)

We next reduce the degree of \( f_s^{-1}(x) \). Since \( f_s(x) \) induces a bijection from \( C_s \) to \( C_t \), we have \( f_s(a) \in C_t \) and \( f_s(a)^{(q-1)/2} = (-1)^t \) for any \( a \in C_s \), and so
\[ f_s(a)^{q-1-i} = (-1)^t f_s(a)^{q-1-i}/f_s(a)^{q-1-y} = (-1)^t f_s(a)^{q-1-(i+y)}. \]
Substituting it into (7) yields
\[ c_i = (-1)^t c_{i+\frac{q+1}{2}}, \quad 1 \leq i \leq (q-1)/2. \] (8)

In particular, if \( q > 3 \) then
\[ c_{(q-1)/2} = (-1)^t c_{q-1} = \sum_{a \in C_s} a = 0, \] (9)
where the last identity follows from Lemma 3. Therefore,
\[ f_s^{-1}(x) \equiv \sum_{1 \leq i \leq (q-3)/2} \left( c_i x^i + c_{i+\frac{q+1}{2}} x^{i+\frac{q+1}{2}} \right) \]
\[ \equiv \sum_{1 \leq i \leq (q-3)/2} \left( c_i + (-1)^t c_{i+\frac{q+1}{2}} \right) x^i \pmod{x^{\frac{q-1}{2}} + (-1)^t x^{t+1}} \] (9)
\[ = \sum_{1 \leq i \leq (q-3)/2} 2(-1)^t c_{i+\frac{q+1}{2}} x^i \]
\[ = \sum_{(q+1)/2 \leq i \leq q-2} 2(-1)^t c_i x^{i-\frac{q+1}{2}}. \]
Substituting (7) into the formula above, we complete the proof. \( \square \)

3. The inverse of \( f(x) \) in Lemma 1

In this section, we will employ the results in Section 2 to compute the inverse of the PP \( f(x) \) in Lemma 1. First, let \( n > 0 \) be even, \( C_0 = \{ e^2 : e \in \mathbb{F}_3^n \} \) and \( C_1 = \mathbb{F}_3^n \setminus C_0 \). Then \( x^{(3^n-1)/2} = 1 \) if \( x \in C_0 \), and \( x^{(3^n-1)/2} = -1 \) if \( x \in C_1 \). Therefore,
\[ f(x) = (x - x^2 - x^3)x^{\frac{3n-1}{2}} - x + x^2 \]
can be written as
\[ f(x) = \begin{cases} 
0 & \text{if } x = 0, \\
f_0(x) = -x^3 & \text{if } x \in C_0, \\
f_1(x) = x(x+1)^2 & \text{if } x \in C_1.
\end{cases} \]

Lemma 1 stated that \( f(x) \) is a PP of \( \mathbb{F}_{3^n} \). It means that \( f_0(x) \) (resp. \( f_1(x) \)) induces an injection on \( C_0 \) (resp. \( C_1 \)), and \( f_0(C_0) \cap f_1(C_1) = \emptyset \). Since \( n \) is even, \( 3^n \equiv 1 \pmod{4} \), and so \(-1 \in C_0 \). Hence \( f_0(x) \) (resp. \( f_1(x) \)) induces a permutation on \( C_0 \) (resp. \( C_1 \)).

Since \( (x^3)^{\frac{3n-1}{2}} = x^{3n} = x \) for any \( x \in C_0 \), the inverse of \( f_0(x) \) on \( C_0 \) is
\[ f_0^{-1}(x) = -x^{3n-1}. \] (10)
We next apply Theorem 2 to determine the inverse of $f_1(x)$ on $C_1$. Denote $q = 3^n$, $u = (q - 3)/2$, $v = q - 2$ and $w_i = q - 1 - i$, where $(q + 1)/2 \leq i \leq q - 2$. Then

$$f_1(x)^{w_i} = x^{w_i}(x + 1)^{2w_i} = \sum_{0 \leq j \leq 2w_i} \binom{2w_i}{j} x^{w_i+j}. \quad (11)$$

The degree of $f_1(x)^{w_i}$ is $3w_i$, and $3 \leq 3w_i < q - 1 + u$, as shown in Figure 1. Hence the coefficient of $x^u$ in (11) equals the coefficient of $x^u$ in (14), i.e., $b_{iu} = \binom{2w_i}{u-w_i}$. Similarly, $b_{iv} = \binom{2w_i}{v-w_i}$. If $3w_i < u$, i.e., $i > (5q - 3)/6$, then $b_{iu} = 0$. If $3w_i < v$, i.e., $i \geq 2q/3$, then $b_{iv} = 0$. Hence we only need to consider the binomial coefficients

$$b_{iu} = \binom{2q - 2 - 2i}{i - \frac{q+1}{2}} \text{ for } (q + 1)/2 \leq i \leq (5q - 3)/6,$$

$$b_{iv} = \binom{2q - 2 - 2i}{i - 1} \text{ for } (q + 1)/2 \leq i < 2q/3.$$

Employing the following Lemma 4 and \(\binom{-m}{n} = (-1)^n \binom{m+n-1}{n} \) for $m, n > 0$, we have

$$b_{iv} \equiv \binom{-2 - 2i}{i - 1} \equiv (-1)^{i-1} \binom{3i}{i-1} \pmod{3}, \quad (12)$$

where $(q + 1)/2 \leq i < 2q/3$. Similarly, if $(q + 1)/2 \leq i \leq (5q - 3)/6$, then

$$b_{iu} \equiv \binom{-2 - 2i}{i - \frac{q+1}{2}} \equiv (-1)^{i-\frac{q+1}{2}} \binom{3i - \frac{q+1}{2}}{i - \frac{q+1}{2}} \pmod{3}. \quad (13)$$

**Lemma 4.** \[24, Lemma 9\] Let $q$ be a prime $p$ power, and let $r, k$ be integers with $0 \leq k < q$. Then

$$\binom{q+r}{k} \equiv \binom{r}{k} \pmod{p},$$

where $\binom{r}{k} = r(r - 1) \cdots (r - k + 1)/k!$.

By Lemma 2, Theorem 2, (10), (12) and (13), the inverse of $f(x)$ in Lemma 1 on $\mathbb{F}_{3^n}$ is

$$f^{-1}(x) = x^{3^n-1}(x^{\frac{3^n-1}{3}} + 1) + f_1^{-1}(x)(x^{\frac{3^n-1}{3}} - 1), \quad (14)$$

where

$$f_1^{-1}(x) = \sum_{(3^n+1)/2 \leq i \leq (5\cdot 3^n - 3)/6} (-1)^{i-\frac{3^n+1}{2}} \binom{3i - \frac{3^n+1}{2}}{i - \frac{3^n+1}{2}} x^{i - \frac{3^n-1}{3}}$$

$$+ \sum_{(3^n+1)/2 \leq i \leq 2\cdot 3^n/3} (-1)^i \binom{3i}{i-1} x^{i - \frac{3^n-1}{3}} \quad (15)$$

in the sense of reduction modulo $x^{\frac{3^n-1}{3}} + 1$. 

---

**Figure 1:** The range of $3w_i$.
4. Explicit values of binomial coefficients

This section will give the explicit values of binomial coefficients in \( \binom{3i}{i-1} \).

**Theorem 3.** Let \( n \geq 1 \) and \((3^n - 1)/2 < i < 3^n\). Then \( \binom{3i}{i-1} \equiv 0 \pmod{3} \).

**Proof.** If \( 1 \leq i < 3^n \), then we can write \( i = i_0 + i_1 3 + i_2 3^2 + \cdots + i_{n-1} 3^{n-1} \), where \( i_t = 0, 1, 2 \) for \( 0 \leq t \leq n - 1 \). Then

\[
3i = 0 + i_0 3 + i_1 3^2 + \cdots + i_{n-1} 3^{n-1} + i_{n-1} 3^n,
\]

\[
i - 1 = i_0 - 1 + i_1 3 + i_2 3^2 + \cdots + i_{n-1} 3^{n-1}.
\]

By the Lucas’ theorem, if \( i_0 = 0 \) then \( \binom{3i}{i-1} \equiv \binom{0}{0} \equiv 0 \pmod{3} \), and if \( i_0 = 1, 2 \) then

\[
\binom{3i}{i-1} \equiv \binom{0}{i_0 - 1} \binom{i_0}{i_1} \cdots \binom{i_{n-2}}{i_{n-1}} \binom{i_{n-1}}{0} \pmod{3}.
\]

Hence \( \binom{3i}{i-1} \not\equiv 0 \pmod{3} \) if and only if one of the following conditions holds:

1. \( i_0 = 1, i_0 \geq i_1, i_1 \geq i_2, \ldots, i_{n-1} \geq 0; \)
2. \( i_0 = 1 \) and \( 1 \geq i_1 \geq i_2 \geq \cdots \geq i_{n-2} \geq i_{n-1} \geq 0; \)
3. \( i = 1, 1 + 3, 1 + 3 + 3^2, \ldots, 1 + 3 + 3^2 + \cdots + 3^{n-1}; \)
4. \( i = (3^k - 1)/2, \) where \( k = 1, 2, \ldots, n. \)

Hence \( \binom{3i}{i-1} \equiv 0 \pmod{3} \) if \((3^n - 1)/2 < i < 3^n\).

It is easy to obtain the following 3-adic expansion:

\[
(5 \cdot 3^n - 3)/6 - (3^n + 1)/2 = 2 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^{n-2}.
\]

Thus, when \((3^n + 1)/2 \leq i \leq (5 \cdot 3^n - 3)/6\), we can write

\[
i = (3^n + 1)/2 + i_0 + i_1 \cdot 3 + i_2 \cdot 3^2 + \cdots + i_{n-2} \cdot 3^{n-2},
\]

where \( i_t = 0, 1, 2 \) for \( 0 \leq t \leq n - 2 \). Then by an argument similar to the one used in Theorems 11 and 12, we obtain the following two results.

**Theorem 4.** Let \( n \geq 1 \) and \((3^n + 1)/2 \leq i \leq (5 \cdot 3^n - 3)/6\). Then the following statements are equivalent:

- (i) \( \binom{3i - 3^{n-1}}{i - 3^{n-1}} \not\equiv 0 \pmod{3} \);
- (ii) \( 2 \geq i_0 \geq i_1 \geq \cdots \geq i_{n-2} \geq 0, \) where \( i_0, i_1, \ldots, i_{n-2} \) are defined by \( 16 \);
- (iii) \( i = \frac{3^j + 1}{2} + \frac{3^{j+1} - 1}{2} + \frac{3^{j+2} - 1}{2}, \) where \( 0 \leq j \leq k \leq n - 1. \)

**Theorem 5.** Let \( i = \frac{3^n + 1}{2} + \frac{3^{j+1} - 1}{2} + \frac{3^{j+2} - 1}{2}, \) where \( 0 \leq j \leq k \leq n - 1. \) Then

\[
\binom{3i - 3^{n-1}}{i - 3^{n-1}} \equiv \begin{cases} 
1 & \text{if } j = k, \\
-1 & \text{if } j < k.
\end{cases} \pmod{3}.
\]
Proof. Since $3^m = (1 + 2)^m = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m} 2^m$, we have $(-1)^{\frac{1}{3} \cdot \frac{m-1}{3}} = (-1)^m$, and so $(-1)^{\frac{1}{3} \cdot \frac{m+1}{3}} = (-1)^{\frac{1}{3} \cdot \frac{m-1}{3} + \frac{2}{3}} = (-1)^{j+k}$. Substituting it into Theorem 5 can complete the proof. \qed

According to Theorems 4 and 6 we can write (15) as the following for $m$:

$$f^{-1}_1(x) = \sum_{0 \leq j \leq k \leq n-1} x^{3^k} - \sum_{0 \leq j < k \leq n-1} (-1)^{j+k+1} x^{\frac{3^k+3^j}{2}}$$

$$= \sum_{0 \leq j \leq k \leq n-1} a_{jk} (-1)^{j+k} x^{\frac{3^k+3^j}{2}},$$

where

$$a_{jk} = \begin{cases} 1 & \text{if } j = k, \\ -1 & \text{if } j < k. \end{cases}$$

Substituting (17) into (14), we complete the proof of Theorem 1.

5. Slight generalization

In this section, we also let $C_0 = \{ e^2 : e \in \mathbb{F}_{3^n} \}$ and $C_1 = \mathbb{F}_{3^n}^* \setminus C_0$. Let $\eta$ be the quadratic character. By an argument similar to that used in Theorem 1, we deduce the inverses of some generalized PPs studied in [18].

Lemma 5. (see [7], Theorem 4.7) Let $\alpha, \beta, \gamma, \theta \in \mathbb{F}_{3^n}^*$ with $n \geq 1$, and let

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ \alpha(x^3 + \gamma x^2 + \gamma^2 x) & \text{if } x \in C_0, \\ \beta(x^3 + \theta x^2 + \theta^2 x) & \text{if } x \in C_1. \end{cases}$$

Then $f(x)$ is a PP of $\mathbb{F}_{3^n}$ if and only if $\eta(\gamma) = -1$, $\eta(\theta) = 1$ and $\eta(\alpha) = \eta(\beta)$.

Lemma 5 is a special case of Lemma 5 for $n$ is even, $\gamma = 0$ and $\alpha = -\beta = \theta = -1$. The following result gives the inverse of $f(x)$ in Lemma 5.

Theorem 7. If $f(x)$ in (19) is a PP of $\mathbb{F}_{3^n}$, and $\eta(\alpha) = (-1)^m$ with $m \in \{0, 1\}$, then

$$f^{-1}(x) = -u(x) (1 + (-1)^m x^{3^n-1}/2) + v(x) (1 + (-1)^{m+1} x^{3^n-1}/2),$$

where

$$u(x) = \sum_{0 \leq j \leq k \leq n-1} a_{jk} \gamma^{(-1)^m} x^{\frac{3^k+3^j}{2}},$$

$$v(x) = \sum_{0 \leq j \leq k \leq n-1} a_{jk} \theta^{(-1)^m} x^{\frac{3^k+3^j}{2}},$$

and $a_{jk}$ is the same as in (18).
Proof. Let $\tau, \lambda \in \mathbb{F}_3^*$, $s \in \{0, 1\}$ and $f_s(x) = \tau(x^{3^s} + \lambda x^2 + \lambda^2 x) = \tau x(x - \lambda)^2$. If $f(x)$ in (19) is a PP of $\mathbb{F}_3^n$ and $\eta(\tau) = (-1)^{m}$ with $m \in \{0, 1\}$, then $f_s(x)$ induces a bijection from $C_s$ to $C_t$, where $s, t \in \{0, 1\}$. Clearly, $s = t$ if $m = 0$, and $s \neq t$ if $m = 1$. Hence $s + t + m \equiv 0 \pmod{2}$. Let $w_i = 3^n - 1 - i$, where $(3^n + 1)/2 \leq i \leq 3^n - 2$. Then
\[
f_s(x)^{w_i} = (\tau x)^{w_i} (x - \lambda)^{2w_i} = \sum_{0 \leq j \leq 2w_i} \tau^{w_i} (-\lambda)^{2w_i-j} \binom{2w_i}{j} x^{w_i+j}. \tag{22}
\]
By an argument similar to that used in the previous sections, we have
\[
f_s^{-1}(x) = (-1)^{s+t} \left( \sum_{0 \leq k \leq n-1} \tau^{3^k x^3 \lambda^3 x \lambda^{-3}} \right) = (\sum_{0 \leq j \leq k \leq n-1} a_{jk} \lambda^j x^k) \tag{23}
\]
Substituting it into Lemma 2, we complete the proof. □

Lemma 6. (see [18, Theorem 4.2]) Let $\alpha, \beta, \theta \in \mathbb{F}_3^*$ with $n \geq 1$, and let
\[
f(x) = \begin{cases} 0 & \text{if } x = 0, \\ \alpha x^t & \text{if } x \in C_0, \\ \beta x^t + \theta x^2 + \theta^2 x & \text{if } x \in C_1. \end{cases} \tag{24}
\]
Then $f(x)$ is a PP of $\mathbb{F}_3^n$ if and only if $(t, \frac{3^n-1}{2}) = 1$, $\eta(\theta) = 1$ and $\eta(\alpha) = \eta(\beta)$.

Theorem 8. If $f(x)$ in (23) is a PP of $\mathbb{F}_3^n$ and $\eta(\alpha) = (-1)^m$ with $m \in \{0, 1\}$, then $f^{-1}(x) = -u(x)((1 + (-1)^m x^{(3^n-1)/2}) - v(x)(1 + (-1)^{m+1} x^{(3^n-1)/2})$, where $v(x)$ is defined by (21), $u(x) = (\alpha^{-1} x)^s$, and $s$ is the inverse of $t$ modulo $(3^n-1)/2$.

Lemma 7. (see [18, Corollary 4.5]) Let $n, t$ be positive integers. Let $\alpha, \beta, \gamma \in \mathbb{F}_3^n$ and
\[
f(x) = \begin{cases} 0 & \text{if } x = 0, \\ \alpha x^3 + \gamma x^2 + \gamma^2 x & \text{if } x \in C_0, \\ \beta x^t & \text{if } x \in C_1. \end{cases} \tag{24}
\]
Then $f(x)$ is a PP of $\mathbb{F}_3^n$ if and only if $(t, \frac{3^n-1}{2}) = 1$, $\eta(\gamma) = -1$ and $\eta(\alpha) = \eta(\beta)(-1)^{t+1}$.

Theorem 9. If $f(x)$ in (24) is a PP of $\mathbb{F}_3^n$ and $\eta(\alpha) = (-1)^m$ with $m \in \{0, 1\}$, then $f^{-1}(x) = -u(x)((1 + (-1)^m x^{(3^n-1)/2}) - v(x)(1 + (-1)^{m+1} x^{(3^n-1)/2})$, where $u(x)$ is defined by (20), $v(x) = (\beta^{-1} x)^r$, $r$ and $s$ are integers such that 1 $\leq s < (3^n - 1)/2$ and st + r(3^n - 1)/2 = 1.

When $n = 1$, it is easy to verify that $f(x) \equiv f^{-1}(x) \equiv \pm x \pmod{x^3 - x}$ in all results of this section. Hence Theorems 7, 8 and 9 are all true for $n = 1$. If $\gamma = \theta = 0$, then Lemmas 5, 8 and 7 are the special cases of [18, Corollary 2.3], and their inverses are given in [19, 29].
References

[1] D. Bartoli. On a conjecture about a class of permutation trinomials. *Finite Fields Appl.*, 52:30–50, 2018.

[2] X. Cao, L. Hu, and Z. Zha. Constructing permutation polynomials from piecewise permutations. *Finite Fields Appl.*, 26:162–174, 2014.

[3] P. Charpin, S. Mesnager, and S. Sarkar. Involutions over the Galois Field $\mathbb{F}_{2^n}$. *IEEE Trans. Inform. Theory*, 62(4):2266–2276, 2016.

[4] W.-S. Chou and X.-D. Hou. On a conjecture of Fernando, Hou and Lappano concerning permutation polynomials over finite fields. *Finite Fields Appl.*, 56:58–92, 2019.

[5] N. Fernando and X.-D. Hou. A piecewise construction of permutation polynomials over finite fields. *Finite Fields Appl.*, 18(6):1184–1194, 2012.

[6] X.-D. Hou. Two classes of permutation polynomials over finite fields. *J. Comb. Theory Ser. A*, 118:448–454, 2011.

[7] X.-D. Hou. Applications of the Hasse-Weil bound to permutation polynomials. *Finite Fields Appl.*, 54:113–132, 2018.

[8] K. Li, L. Qu, and Q. Wang. Compositional inverses of permutation polynomials of the form $x^r h(x^s)$ over finite fields. *Cryptogr. Commun.*, 11:279–298, 2019.

[9] L. Li, S. Wang, C. Li, and X. Zeng. Permutation polynomials $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ over $\mathbb{F}_p^n$. *Finite Fields Appl.*, 51:31–61, 2018.

[10] N. Li. On two conjectures about permutation trinomials over $\mathbb{F}_{3^{2k}}$. *Finite Fields Appl.*, 47:1–10, 2017.

[11] A. Muratović-Ribić. A note on the coefficients of inverse polynomials. *Finite Fields Appl.*, 13:977–980, 2007.

[12] L. Reis. Nilpotent linearized polynomials over finite fields and applications. *Finite Fields Appl.*, 50:279–292, 2018.

[13] Z. Tu and X. Zeng. Two classes of permutation trinomials with Niho exponents. *Finite Fields Appl.*, 53:99–112, 2018.

[14] A. Tuxanidy and Q. Wang. On the inverses of some classes of permutations of finite fields. *Finite Fields Appl.*, 28:244–281, 2014.

[15] A. Tuxanidy and Q. Wang. Compositional inverses and complete mappings over finite fields. *Discrete Appl. Math.*, 217:318–329, 2017.

[16] L. Wang and B. Wu. General constructions of permutation polynomials of the form $(x^{2^m} + x + \delta)^{(2m-1)+1} + x$ over $\mathbb{F}_{2^{2m}}$. *Finite Fields Appl.*, 52:137–155, 2018.

[17] Q. Wang. On inverse permutation polynomials. *Finite Fields Appl.*, 15:207–213, 2009.

[18] Q. Wang. Cyclotomy and permutation polynomials of large indices. *Finite Fields Appl.*, 22:57–69, 2013.
[19] Q. Wang. A note on inverses of cyclotomic mapping permutation polynomials over finite fields. *Finite Fields Appl.*, 45:422–427, 2017.

[20] B. Wu. The compositional inverses of linearized permutation binomials over finite fields. *arXiv:1311.2154*, 2013.

[21] B. Wu and Z. Liu. The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2. *Finite Fields Appl.*, 24:136–147, 2013.

[22] B. Wu and Z. Liu. Linearized polynomials over finite fields revisited. *Finite Fields Appl.*, 22:79–100, 2013.

[23] D. Wu, P. Yuan, C. Ding, and Y. Ma. Permutation trinomials over $\mathbb{F}_{2^n}$. *Finite Fields Appl.*, 46:38–56, 2017.

[24] G. Xu, X. Cao, and J. Ping. Some permutation pentanomials over finite fields with even characteristic. *Finite Fields Appl.*, 49:212–226, 2018.

[25] X. Xu, X. Feng, and X. Zeng. Complete permutation polynomials with the form $(x^{p^m} - x + \delta)^s + ax^{p^m} + bx$ over $\mathbb{F}_{p^n}$. *Finite Fields Appl.*, 57:309–343, 2019.

[26] Z. Zha, L. Hu, and S. Fan. Further results on permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, 45:43–52, 2017.

[27] D. Zheng, M. Yuan, and L. Yu. Two types of permutation polynomials with special forms. *Finite Fields Appl.*, 56:1–16, 2019.

[28] Y. Zheng, Q. Wang, and W. Wei. On inverses of permutation polynomials of small degree over finite fields. *arXiv:1812.06768*, 2018.

[29] Y. Zheng, Y. Yu, Y. Zhang, and D. Pei. Piecewise constructions of inverses of cyclotomic mapping permutation polynomials. *Finite Fields Appl.*, 40:1–9, 2016.

[30] Y. Zheng, P. Yuan, and D. Pei. Piecewise constructions of inverses of some permutation polynomials. *Finite Fields Appl.*, 36:151–169, 2015.

[31] Y. Zheng, P. Yuan, and D. Pei. Large classes of permutation polynomials over $\mathbb{F}_{q^2}$. *Des. Codes Cryptogr.*, 81:505–521, 2016.