Local method for compositional inverses of permutation polynomials

Pingzhi Yuan

School of Mathematical Sciences, South China Normal University, Guangzhou, P. R. China

ABSTRACT
In this paper, we provide a local method to find compositional inverses of all PPs, some new PPs and their compositional inverses are given.

1. Introduction

Let \( q \) be a prime power, \( \mathbb{F}_q \) be the finite field of order \( q \), and \( \mathbb{F}_q[x] \) be the ring of polynomials in a single indeterminate \( x \) over \( \mathbb{F}_q \). A polynomial \( f \in \mathbb{F}_q[x] \) is called a permutation polynomial (PP for short) of \( \mathbb{F}_q \) if it induces a bijective map from \( \mathbb{F}_q \) to itself.

Constructing PPs and explicitly determining the compositional inverse of a PP are useful because a PP and its inverse are required in many applications. For example, involutions are particularly useful (as a part of a block cipher) in devices with limited resources. However, it is difficult to determine whether a given polynomial over a finite field is a PP or not, and it is not easy to find the explicit compositional inverse of a random PP, except for several well-known classes of PPs, which have very nice structure. See [2–6, 8, 10–16, 19–23] for more details.

In [7, Problem 10], G. L. Mullen posed an open problem: how to compute the coefficients of the compositional inverse of a permutation polynomial efficiently? This problem is in general quite difficult. In addition to classical classes such as monomials, linearized polynomials, and Dickson polynomials, there are several more recent classes of permutation polynomials whose compositional inverses have been obtained in explicit or implicit forms, and we refer the interested reader to consult articles [2, 5, 8, 10, 11, 13–15, 17, 18, 22].

The main purpose of this paper is to provide a new method to find compositional inverses of all PPs. The idea is completely different from the ideas of references as before. The core idea comes from number theory and algebra, we use local information to explicitly determine the compositional inverse of a permutation polynomial. We can consider this as an algebraic framework for the computation of compositional inverses of permutation polynomials.

The rest of this paper is organized as follows. In Section 2, we present the local criterion for a polynomial to be a PP. In Section 3, we present some known PPs and their compositional inverses by applying the results in Section 2. In Section 4, we use the method developed in Section 2 to give necessary...
and sufficient conditions for two kinds of polynomials to be PPs, and we also give their compositional inverses.

We know that every map from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be viewed as a polynomial in the ring $\left(\mathbb{F}_q[x]/(x^q - x), +, \circ\right)$, where the two operations are the addition and the composition of two polynomials modulo $x^q - x$. For a polynomial, $f(x)$ is a PP over $\mathbb{F}_q$ if and only if $f(x)$ is an unit in the ring $\left(\mathbb{F}_q[x]/(x^q - x), +, \circ\right)$, and we use $f^{-1}(x)$ to denote the compositional inverse of $f(x)$. Hence we view the polynomials over $\mathbb{F}_q$ as elements in the ring $\left(\mathbb{F}_q[x]/(x^q - x), +, \circ\right)$ throughout the paper.

2. Local criterion for a polynomial to be a PP

To begin with, we give the following simple and useful result for a map to be a bijection. We have

**Lemma 2.1.** (Local criterion) Let $A$ and $S$ be finite sets and let $f : A \rightarrow A$ be a map. Then $f$ is a bijection if and only if for any surjection $\psi : A \rightarrow S$, $\varphi = \psi \circ f$ is a surjection and $f$ is injective on $\varphi^{-1}(s)$ for each $s \in S$.

$$
\begin{array}{ccc}
A & \xrightarrow{f} & A \\
\downarrow \varphi & & \downarrow \psi \\
S & & S
\end{array}
$$

**Proof.** The necessity is obvious.

Now we prove the sufficiency. If $f(a) = f(b)$ for some $a, b \in A$, then

$$
\varphi(f(a)) = \varphi(f(b)).
$$

That is $\varphi(a) = \varphi(b) = s, s \in S$. Hence

$$
a, b \in \varphi^{-1}(s).
$$

Since $f$ is injective on $\varphi^{-1}(s)$ for each $s \in S$ and $f(a) = f(b)$, we get $a = b$. Therefore $f$ is a bijection. □

In 2011, Akbrary, Ghioca and Wang [1] proposed a powerful method called the AGW criterion for constructing PPs.

**Proposition 2.2.** (AGW criterion) Let $A$, $S$ and $\tilde{S}$ be finite sets with $|S| = |\tilde{S}|$, and let $f : A \rightarrow A$, $h : S \rightarrow \tilde{S}$, $\lambda : A \rightarrow S$, and $\tilde{\lambda} : A \rightarrow \tilde{S}$ be maps such that $\lambda \circ f = h \circ \lambda$. If both $\lambda$ and $\tilde{\lambda}$ are surjective, then the following statements are equivalent:

(i) $f$ is a bijective (a permutation of $A$); and

(ii) $h$ is a bijective from $S$ to $\tilde{S}$ and if $f$ is injective on $\lambda^{-1}(s)$ for each $s \in S$.

Obviously, the local criterion is a special case of the AGW criterion. Now we show that AGW criterion follows from Lemma 2.1 also, so the two criteria are equivalent.

**The proof of AGW criterion by Lemma 2.1:** Applying Lemma 2.1 to $\psi = \tilde{\lambda}$ and $\varphi = \tilde{\lambda} \circ f = h \circ \lambda$. Since $\lambda$ is a surjection and $\varphi S = \varphi \tilde{S}$, we have $\varphi = h \circ \lambda$ is a surjection if and only if $h$ is a bijection. On the other hand, if $h$ is a bijection, then we have

$$
\{\lambda^{-1}(s), s \in S\} = \{\varphi^{-1}(\tilde{s}), \tilde{s} \in \tilde{S}\}.
$$

Hence we have the result. □

**Remark:** We note that the heart of the AGW criterion lies in transforming the problem of constructing permutations of a finite set into finding bijections over a smaller set, while the core idea of the local criterion is to consider the polynomial locally. Hence the two ideas are different in essence.

We also have the following corollary.
Corollary 2.3. Let $A, S$, and $\tilde{S}$ be finite sets with $\sharp S = \sharp \tilde{S}$, and let $f : A \to A, h : S \to \tilde{S}, \lambda : A \to S$, and $\tilde{\lambda} : A \to \tilde{S}$ be maps such that $\lambda \circ f = h \circ \tilde{\lambda}$. If $\lambda$ is a surjection and $h$ is a bijection, then the following statements are equivalent:

(i) $f$ is a bijective (a permutation of $A$); and
(ii) $\lambda$ is a surjection and $f$ is injective on $\lambda^{-1}(s)$ for each $s \in S$.

We now prove the following general result on PP.

Theorem 2.4. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a PP if and only if for any maps $\psi_i$, $i = 1, \ldots, t, t \in \mathbb{N}$ (we also denote them as $\psi_i(x) \in \mathbb{F}_q[x]/(x^d - x)$) such that $F(\psi_1(x), \ldots, \psi_t(x)) = x$ for some polynomial $F(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t]$, there exists a polynomial $G(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t]$ satisfies $G(\psi_1(f(x)), \ldots, \psi_t(f(x))) = x$. Moreover, if $f(x)$ is a PP, then

$$f^{-1}(x) = G(\psi_1(x), \ldots, \psi_t(x)),$$

where $f^{-1}(x)$ denotes the compositional inverse of $f(x)$.

Proof. We first prove the necessity. Assume that $f(x)$ is a PP, let

$$\varphi_i(x) = \psi_i(f(x)), i = 1, \ldots, t,$$

then we have

$$\psi_i(x) = \varphi_i(f^{-1}(x)), i = 1, \ldots, t,$$

where $f^{-1}(x)$ denotes the compositional inverse of $f(x)$. Since $F(\psi_1(x), \ldots, \psi_t(x)) = x$, we get

$$F(\psi_1(f^{-1}(x)), \ldots, \varphi_t(f^{-1}(x))) = x.$$

It follows that

$$F(\psi_1(x), \ldots, \psi_t(x)) = f(x) \text{ and } f^{-1}(F(\psi_1(x), \ldots, \psi_t(x))) = x.$$

Let $G(x_1, \ldots, x_t) = f^{-1} \circ F(x_1, \ldots, x_t)$, then we have $G(\psi_1(x), \ldots, \psi_t(x)) = x$, that is

$$G(\psi_1(f(x)), \ldots, \psi_t(f(x))) = x.$$

Next, we prove the sufficiency. Since for any maps $\psi_i$, $i = 1, \ldots, t, t \in \mathbb{N}$ such that $F(\psi_1(x), \ldots, \psi_t(x)) = x$ for some polynomial $F(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t]$, there exists a polynomial $G(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t]$ satisfies $G(\psi_1(f(x)), \ldots, \psi_t(f(x))) = x$. Let

$$g(x) = G(\psi_1(x), \ldots, \psi_t(x)),$$

then $g \circ f(x) = x$, which implies that $g(x) = f^{-1}(x)$, i.e., $f(x)$ is a PP. We are done.

We also have the following alternative result.

Theorem 2.5. Let $q$ be a prime power and $f(x)$ be a polynomial over $\mathbb{F}_q$. Then $f(x)$ is a PP if and only if there exist nonempty finite subsets $S_i, i = 1, \ldots, t$ of $\mathbb{F}_q$ and maps $\psi_i : \mathbb{F}_q \rightarrow S_i, i = 1, \ldots, t$ such that $\psi_i \circ f = \psi_i$, $i = 1, \ldots, t$ and $x = F(\psi_1(x), \ldots, \psi_t(x))$, where $F(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t]$. Moreover, we have

$$f^{-1}(x) = F(\psi_1(x), \ldots, \psi_t(x)).$$
**Proof.** If there exist nonempty finite subsets $S_i, i = 1, \ldots, t$ of $\mathbb{F}_q$ and maps $\psi_i : \mathbb{F}_q \rightarrow S_i, i = 1, \ldots, t$ such that $\psi_i \circ f = \varphi_i, i = 1, \ldots, t$ and $x = F(\psi_1(x), \ldots, \psi_t(x))$, then the following diagram commutes.

\[ \begin{array}{ccc}
\mathbb{F}_q & \xrightarrow{f} & \mathbb{F}_q \\
\downarrow{(\psi_1, \ldots, \psi_t)} & & \downarrow{(\psi_1, \ldots, \psi_t)} \\
S_1 \times \cdots \times S_t & \xrightarrow{F(x_1, \ldots, x_t)} & S_1 \times \cdots \times S_t
\end{array} \]

Hence

\[ F(\psi_1(f(x)), \ldots, \psi_t(f(x))) = x, \]

which implies that

\[ f^{-1}(x) = F(\psi_1(x), \ldots, \psi_t(x)). \]

If $f(x)$ is a permutational polynomial over $\mathbb{F}_q$, we can take $S = \mathbb{F}_q, i = 1, \psi = f^{-1}(x), \varphi(x) = x$ and $F(x) = x$, then all conditions are satisfied, and we have $f^{-1}(x) = \psi(x). \square$

**Remark 2.6.** The results in this section can be viewed as some generalizations and refinements of the related results in [8, Theorem 2] and [18, Proposition 4.1].

### 3. Some old PPs and their compositional inverses

In this section, we give new proofs for some known PPs and their compositional inverses by applying the results in Section 2. To do this, we need to find out two polynomials $\psi_1(x)$ and $\psi_2(x)$ such that we can find a polynomial $G(x, y) \in \mathbb{F}_q[x, y]$ satisfying

\[ x = G(\psi_1(f(x)), \psi_2(f(x))). \]

Now applying Theorem 2.5, we get

\[ f^{-1}(x) = G(\psi_1(x), \psi_2(x)). \]

We give two examples below. The following result was discovered independently by several authors, we will give a new proof of Theorem 11 in [8] by applying Theorem 2.5.

**Lemma 3.1.** ([9, Theorem 2.3] [12, Theorem 1] [24, Lemma 2.1]) Let $q$ be a prime power and $f(x) = x^th(x^s) \in \mathbb{F}_q[x]$, where $s = \frac{q-1}{\ell}$ and $\ell$ is an integer. Then $f(x)$ permutes $\mathbb{F}_q$ if and only if

1. $\gcd(r, s) = 1$ and
2. $g(x) = x^t h(x)^s$ permutes $\mu_\ell$.

**Proposition 3.2.** [8, Theorem 11] Let $f(x) = x^th(x^s) \in \mathbb{F}_q[x]$ defined in Lemma 3.1 be a permutation over $\mathbb{F}_q$ and $g^{-1}(x)$ be the compositional inverse of $g(x) = x^t h(x)^s$ over $\mu_\ell$. Suppose $a$ and $b$ are two integers satisfying $a + br = 1$. Then the compositional inverse of $f(x)$ in $\mathbb{F}_q[x]$ is given by

\[ f^{-1}(x) = g^{-1}(x^a)x^bh(g^{-1}(x^a))^{-b}. \]

**Proof.** By the assumptions, we have the following commutative diagrams

\[ \begin{array}{ccc}
\mathbb{F}_q & \xrightarrow{f(x)} & \mathbb{F}_q \\
\downarrow{\varphi_i} & & \downarrow{\psi_i} \\
\mu_\ell & \xrightarrow{\mu_\ell} & \mathbb{F}_q
\end{array} \quad i = 1, 2, \]
where
\[ \psi_1(x) = g^{-1}(x'), \varphi_1(x) = x', \quad \psi_2(x) = f(x) = x'h(x'). \]
We have
\[ \varphi_1(x)^a \cdot \left( \frac{\psi_2(x)}{h(\varphi_1(x))} \right)^b = x, \]
it follows from Theorem 2.5 that
\[ f^{-1}(x) = \psi_1(x)^a \cdot \left( \frac{\psi_2(x)}{h(\psi_1(x))} \right)^b = (g^{-1}(x'))^a x^b \left( h(g^{-1}(x')) \right)^{-b}. \]
This completes the proof.

Next, we give another proof of the following result.

**Proposition 3.3.** [17, Theorem 3.1] Let \( q \) be a prime power, and \( S, \bar{S} \) subsets of \( \mathbb{F}_q^* \) with \( \sharp S = \sharp \bar{S} \). Let \( f : \mathbb{F}_q^* \to \mathbb{F}_q^*, g : S \to \bar{S}, \lambda : \mathbb{F}_q^* \to S, \) and \( \bar{\lambda} : \mathbb{F}_q^* \to \bar{S} \) be maps such that both \( \lambda \) and \( \bar{\lambda} \) are surjective maps and \( \bar{\lambda} \circ f = g \circ \lambda \).

Let \( f_1(x) \) and \( f(x) = f_1(x)h(\lambda(x)) \) be PPs over \( \mathbb{F}_q^* \), and let \( f_1^{-1}(x), f^{-1}(x) \) and \( g^{-1}(x) \) be the compositional inverses of \( f_1(x), f(x) \) and \( g(x) \), respectively. Then we have
\[ f^{-1}(x) = f_1^{-1} \left( \frac{x}{h(g^{-1}(\bar{\lambda}(x)))} \right). \]

**Proof.** By the assumptions of the theorem, we have
\[
\begin{array}{ccc}
\mathbb{F}_q & \xleftarrow{f} & \mathbb{F}_q \\
\psi_i & \downarrow & \psi_i \\
S & \xrightarrow{\bar{\psi}_i} & S \\
\end{array}
\]

where
\[ \psi_1(x) = g^{-1}(\bar{\lambda}), \varphi_1(x) = \lambda, \quad \psi_2(x) = x, \varphi_2(x) = f(x). \]
It is easy to check that
\[ x = f_1^{-1} \left( \frac{\varphi_2(x)}{h(\varphi_1(x))} \right), \]
by Theorem 2.5, we have
\[ f^{-1}(x) = f_1^{-1} \left( \frac{x}{h(g^{-1}(\bar{\lambda}(x)))} \right). \]
And we are done.

**Remark 3.4.** We can also obtain the compositional inverses of many known PPs by the method above. We stop to do this here.

4. Some new PPs and their compositional inverses

For more applications of the results in Section 2, we will present some new PPs and their compositional inverses in this section.
Let $d > 1$ be a positive integer, $q$ a prime power with $q \equiv 1 \pmod{d}$ and $\omega$ a $d$-th primitive root of unity over $\mathbb{F}_q$. For $0 \leq i \leq d - 1$, let

$$A_i(x) = x^{d^i-1} + \omega^i x^{d^{i-1}} + \cdots + \omega^{i(d-1)} x.$$ 

Most results in the following two lemmas are proved in [18], for completeness and self-contained, we present the full proof here. We have

**Lemma 4.1.** Let the notations be as above and let $g(x) \in \mathbb{F}_q[x]$ be a polynomial, then we have

(i) $A_i^q(x) = \omega^i A_i(x)$, $0 \leq i \leq d - 1$.

(ii) For any positive integer $m$ and integers $i, j$ with $0 \leq i, j \leq d - 1$, we have

$$A_j(x) \circ A_i^m(x) = \begin{cases} d\omega^{-j}A_i^m(x), & \text{if } j \equiv im \pmod{d}, \\ 0, & \text{otherwise}. \end{cases}$$

(iii) For any positive integer $j$ with $1 \leq j \leq d - 1$, we have

$$A_j(x) \circ g(A_0(x)) = 0.$$

**Proof.** For (i), we have

$$(A_i(x))^q = x + \omega^i x^{q^{d-1}} + \cdots + \omega^{i(d-1)} x^q = \omega^i A_i(x).$$

This proves (i). Now we prove (ii), repeating the procedure in (i), we get

$$(A_i(x))^q = \omega^i A_i(x).$$

Hence

$$(A_i^m(x))^q = \left(A_i(x)^q\right)^m = \omega^{im} A_i^m(x).$$

Therefore

$$A_j(x) \circ A_i^m(x) = A_i^m(x) \sum_{t=0}^{d-1} \omega^{(j+i(d-1)-t)m} = A_i^m(x)\omega^{im(d-1)} \sum_{t=0}^{d-1} \omega^{(j-im)t} = \begin{cases} d\omega^{-j}A_i^m(x), & \text{if } j \equiv im \pmod{d}, \\ 0, & \text{otherwise}. \end{cases}$$

(iii) Let $g(x) = b_0 + b_1 x + \cdots + b_t x^t, b_i \in \mathbb{F}_q, 0 \leq i \leq t$, since $A_j(x)$ is a $q$-polynomial and $b_i \in \mathbb{F}_q, 0 \leq i \leq t$, by (ii), we have

$$A_j(x) \circ g(A_0(x)) = A_j(b_0) + \sum_{i=1}^{t} A_j(x) \circ A_i^0(x) = A_j(b_0) = b_0(1 + \omega^j + \cdots + \omega^{j(d-1)}) = 0.$$ 

\[ \square \]

**Lemma 4.2.** Let the notations be as in Lemma 4.1, and let

$$B_i = \{A_i(x), x \in \mathbb{F}_q^d\}, \ 0 \leq i \leq d - 1.$$ 

Then $B_i = \{0\} \cup y_i \mathbb{F}_q^*$, where $y_i$ is a fixed nonzero element of $B_i, 1 \leq i \leq d - 1$ and $B_0 = \mathbb{F}_q$.

**Proof.** Obviously, $0 \in B_i$ and $B_0 = \mathbb{F}_q$. For any elements $y_1, y_2 \in B_i$ with $y_1 y_2 \neq 0$, by Lemma 4.1 (i), we have

$$y_i^q = \omega^i y_i, \ j = 1, 2.$$

Hence $(y_1/y_2)^q = y_1/y_2$, which implies that $y_1/y_2 \in \mathbb{F}_q^*$, and the assertion follows. 

\[ \square \]
Theorem 4.3. Let $d > 1$ be a positive integer, $q$ a prime power with $q \equiv 1 \pmod{d}$ and $\omega$ a $d$-th primitive root of unity over $\mathbb{F}_q$. Let

$$A_i(x) = x^{d^i-1} + \omega x^{d^{i-2}} + \cdots + \omega^{(d-1)x}, \ 0 \leq i \leq d - 1.$$ 

Let $m_1, \ldots, m_{d-1}$ be positive integers and $u_1, \ldots, u_{d-1} \in \mathbb{F}_q^*$, and let $g(x) \in \mathbb{F}_q[x]$ be a polynomial. Then the polynomial

$$f(x) = g(A_0(x)) + \sum_{i=1}^{d-1} u_i A_i^{m_i}(x),$$

is a PP over $\mathbb{F}_q^d$ if and only if $\{0\} \cup \{im_i, 1 \leq i \leq d-1\}$ is a complete residue modulo $d$, $u_1 \cdots u_{d-1} \in \mathbb{F}_q^*$, $\gcd(m_1 \cdot \cdots \cdot m_{d-1}, q-1) = 1$ and $g(x)$ is a PP over $\mathbb{F}_q$. Furthermore, if $f(x)$ is a PP over $\mathbb{F}_q^d$, $r_i$ are positive integers with $m_ir_i \equiv 1 \pmod{d(q-1)}(1 \leq i \leq d - 1)$ and $g^{-1}(x)$ is the compositional inverse of $g(x)$, then

$$f^{-1}(x) = \frac{1}{d} \left( g^{-1}(A_0(x)/d) + \sum_{i=1}^{d-1} \omega^i (du_i \omega^{-j})^{-r_i} A_j(x)^{r_i} \right).$$

Proof. We first prove the necessity. Suppose that there is a positive integer $j, 1 \leq j \leq d - 1$ such that $j \not\equiv im_i \pmod{d}$ for any $i \in \{1, \ldots, d-1\}$. By Lemma 4.1(ii) and (iii), we have

$$A_j(x) \circ (u_i A_i^{m_i}(x)) = 0, \quad 1 \leq i \leq d - 1, \quad A_j(x) \circ g(A_0(x)) = 0,$$

hence $A_j(x)$ of $\{x\}$ = 0 and $f(x)$ is not a PP over $\mathbb{F}_q^d$. On the other hand, if $u_i = 0$ for some $i, 1 \leq i \leq d-1$, then it is trivial that $\{0\} \cup \{tm_i, 1 \leq t \leq d-1, t \neq i\}$ is not a complete residue modulo $d$, so $f(x)$ is not a PP over $\mathbb{F}_q^d$. As for $g(x)$, by (ii) and a direct computation we have

$$A_0(x) \circ (f(x)) = dg(A_0(x)).$$

It follows from Lemma 2.1 that $f(x)$ is a PP only if $dg(A_0(x))$ is a surjective map from $\mathbb{F}_q$ to $\mathbb{F}_q$, which implies that $g(x)$ is a PP over $\mathbb{F}_q$ since $A_0(\mathbb{F}_q^d) = B_0 = \mathbb{F}_q$.

Now we assume that $u_1 \cdots u_{d-1} \in \mathbb{F}_q^*$, $\{0\} \cup \{im_i, 1 \leq i \leq d-1\}$ is a complete residue modulo $d$ and $g(x)$ is a PP over $\mathbb{F}_q$. Then

$$A_j(x) \circ f(x) = du_i \omega^{-j} A_i^{m_i}(x), \quad im_i \equiv j \pmod{d}, \ 1 \leq j \leq d - 1,$$

so we have the following commutative diagram

$$\begin{array}{ccc}
\mathbb{F}_q^d & \xrightarrow{f} & \mathbb{F}_q^d \\
A_i(x) \downarrow & & A_i(x) \downarrow \\
B_i \xrightarrow{du_i \omega^{-j} x^{m_i}} & & B_j
\end{array}$$

for each $j, 1 \leq j \leq d - 1$, where $i$ is the integer with $im_i \equiv j \pmod{d}$, $B_i = \{A_i(x), x \in \mathbb{F}_q^d\}, 1 \leq i \leq d - 1$. By Lemma 4.2, the map

$$h_{ij} : B_i \rightarrow B_j, \ a \mapsto du_i \omega^{-j} a^{m_i},$$

is bijective if and only if $\gcd(m_i, q-1) = 1$. If $\gcd(m_i, q-1) = 1$, then the compositional inverse of $du_i \omega^{-j} x^{m_i}$ is $(du_i \omega^{-j})^{-r_i} x^{r_i}$, where $m_ir_i \equiv 1 \pmod{d(q-1)}$. Hence we have the following commutative diagrams

$$\begin{array}{ccc}
\mathbb{F}_q^d & \xrightarrow{f(x)} & \mathbb{F}_q^d \\
\psi_i & & \psi_i \\
B_i \downarrow & & B_i \downarrow
\end{array}$$

for $i = 0, 1, \ldots, d - 1$, where $\psi_i$ is the identity map.
where \( \varphi_i(x) = A_i(x), i = 0, 1, \ldots, d - 1, \) \( \psi_0(x) = g^{-1}(A_0(x)/d) \) and \( \psi_i(x) = (du_i\omega^{-i})^{-r_i}A_j^{r_i}(x), i = 1, \ldots, d - 1. \)

Note that

\[
x = \frac{1}{d} \sum_{i=0}^{d-1} \omega^i A_i(x) = \frac{1}{d} \sum_{i=0}^{d-1} \omega^i \varphi_i(x),
\]

by Theorem 2.5, we have

\[
f^{-1}(x) = \frac{1}{d} \left( g^{-1}(A_0(x)/d) + \sum_{i=1}^{d-1} \omega^i (du_i\omega^{-i})^{-r_i}A_j^{r_i}(x) \right).
\]

This completes the proof.

A polynomial \( f(x) \in \mathbb{F}_q[x] \) is called a complete permutation polynomial (CPP) if both \( f(x) \) and \( f(x) + x \) are permutation polynomials of \( \mathbb{F}_q. \) By applying the above theorem, we have

**Corollary 4.4.** Let the notations be as in Theorem 4.3, then

\[
f(x) = g(A_0(x)) + \sum_{i=0}^{d-1} u_i A_i(x)
\]

is a CPP over \( \mathbb{F}_{q^d} \) if and only if \( \prod_{i=1}^{d-1} u_i(1 + du_i\omega^{-i}) \neq 0 \) and both \( g(x) \) and \( dg(x) + x \) are PPs over \( \mathbb{F}_q. \)

**Proof.** We have

\[
\mathbb{F}_{q^d} \xrightarrow{f(x)+x} \mathbb{F}_{q^d} \quad 1 \leq i \leq d - 1
\]

\[
A_i(x) \xrightarrow{B_i} \mathbb{F}_{q^d} \quad \text{and}
\]

\[
\mathbb{F}_{q^d} \xrightarrow{f(x)+x} \mathbb{F}_{q^d} \quad \text{if and only if} \quad \prod_{i=1}^{d-1} u_i(1 + du_i\omega^{-i}) \neq 0 \quad \text{and both} \quad g(x) \quad \text{and} \quad dg(x) + x \quad \text{are PPs over} \quad \mathbb{F}_q. \quad \text{We are done.}
\]

Theorem 4.3 extends Theorem 6.1 in [18] greatly. We also have the following result, which improves Theorem 6.2 in [18].

**Theorem 4.5.** Let \( n > 1 \) be a positive integer, \( q \) a prime power and \( g(x) \in \mathbb{F}_q[x]. \) Then the polynomial

\[
f(x) = x^q - x + g(\text{Tr}(x)),
\]

where \( \text{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}} \) is a PP over \( \mathbb{F}_{q^n} \) if and only if \( \gcd(n, q) = 1 \) and \( g(x) \) is a PP over \( \mathbb{F}_q. \) Moreover, if \( f(x) \) is a PP over \( \mathbb{F}_{q^n} \) and \( g^{-1}(x) \) is the compositional inverse of \( g(x), \) then

\[
f^{-1}(x) = \frac{1}{n} \left( g^{-1}(\text{Tr}(x)/n) - \frac{(n + 1)}{2} \text{Tr}(x) + \sum_{i=1}^{n-1} ix^i \right).
\]
Proof. By the assumptions, we have the following diagram

\[
\begin{array}{ccc}
\mathbb{F}_{q^n} & \overset{f}{\longrightarrow} & \mathbb{F}_{q^n} \\
\downarrow & & \downarrow \\
\mathbb{F}_q & \overset{Tr(x)}{\longrightarrow} & \mathbb{F}_q \\
\end{array}
\]

Hence \( f(x) \) is a PP over \( \mathbb{F}_{q^n} \) only if \( \gcd(n, q) = 1 \) and \( g(x) \) is a PP over \( \mathbb{F}_q \). Moreover we have the following commutative diagrams

\[
\begin{array}{ccc}
\mathbb{F}_{q^n} & \overset{f(x)}{\longrightarrow} & \mathbb{F}_{q^n} \\
\downarrow & & \downarrow \\
\mathbb{F}_{q^n} & \overset{\varphi_i}{\longrightarrow} & \mathbb{F}_{q^n} \\
\end{array}
\]

where \( \varphi_1(x) = Tr(x) \), \( \psi_1(x) = g^{-1}(Tr(x)/n) \), \( \varphi_2(x) = x \) and \( \psi_2(x) = f(x) = x^q - x + g(Tr(x)) \).

Note that \( \varphi_2(x) - g(\psi_1(x)) = x^q - x \) and

\[
\sum_{i=1}^{n-1} i(x^q - x)^q = n x^{q^n} - Tr(x) = nx - \varphi_1(x).
\]

It follows that

\[
x = \frac{1}{n} \left( \varphi_1(x) + \sum_{i=1}^{n-1} i(\psi_2(x) - g(\varphi_1(x)))^q \right).
\]

Therefore the polynomial \( f(x) \) is a PP over \( \mathbb{F}_{q^n} \) if and only if \( \gcd(n, q) = 1 \) and \( g(x) \) is a PP over \( \mathbb{F}_q \). By Theorem 2.5, we have

\[
f^{-1}(x) = \frac{1}{n} \left( \psi_1(x) + \sum_{i=1}^{n-1} i(\psi_2(x) - g(\psi_1(x)))^q \right)
\]

\[
= \frac{1}{n} \left( g^{-1}(Tr(x)/n) + \sum_{i=1}^{n-1} i(x - Tr(x)/n)^q \right)
\]

\[
= \frac{1}{n} \left( g^{-1}(Tr(x)/n) - \frac{(n + 1)}{2} Tr(x) + \sum_{i=1}^{n-1} ix^q \right)
\]

This completes the proof. \( \square \)

5. Concluding remarks

If it is difficult to find enough surjections \( \varphi_i, \psi_i \), \( 1 \leq i \leq t \) such that the following diagrams commute

\[
\begin{array}{ccc}
\mathbb{F}_q & \overset{f(x)}{\longrightarrow} & \mathbb{F}_q \\
\downarrow & & \downarrow \\
\mathbb{F}_q & \overset{\varphi_i}{\longrightarrow} & \mathbb{F}_q \\
\end{array}
\]

and there exists a polynomial \( F(x_1, \ldots, x_t) \in \mathbb{F}_q[x_1, \ldots, x_t] \) with

\[
F(\varphi_1(x), \ldots, \varphi_t(x)) = x.
\]
We can use the dual diagrams of the related diagrams

\[
\begin{array}{c}
A \\
\downarrow \psi \\
S_i \\
\downarrow h_i^{-1}
\end{array} \quad \quad \quad
\begin{array}{c}
A \\
\downarrow \psi \\
S_i \\
\downarrow h_i^{-1}
\end{array}
\]

as we did in [17]. In [17], we obtained the compositional inverses of some PPs by using one diagram and its dual diagram. Now we can make use of a new local method to find the compositional inverses of some specified PPs. We believe that more PPs and their compositional inverses will be found or constructed by using the method of this paper. We will continue the work in the further paper.

**Acknowledgments**

We are very grateful to the anonymous referee for detailed comments and suggestions that have been a great help in improving the quality of this paper.

**Funding**

This work is supported by the National Natural Science Foundation of China (grant no. 12171163).

**References**

[1] Akbary, A., Ghioca, D., Wang, Q. (2001). On constructing permutations of finite fields. *Finite Fields Appl.* 17:51–67.

[2] Coullter, R. S., Henderson, M. (2002). The compositional inverse of a class of permutation polynomials over a finite field. *Bull. Austral. Math. Soc.* 65:521–526.

[3] Ding, C., Yuan, J. (2006). A family of skew Hadamard difference sets. *J. Comb. Theory, Ser. A* 113:1526–1535.

[4] Laigle-Chapuy, Y. (2007). Permutation polynomials and applications to coding theory. *Finite Fields Appl.* 13:58–70.

[5] Li, K., Qu, L., Wang, Q. (2019). Compositional inverses of permutation polynomials of the form \( x^rh(x^i) \) over finite fields. *Cryptogr. Commun.* 11:279–298.

[6] Lidl, R., Niederreiter, H. (1997). *Finite Fields*. Cambridge: Cambridge University Press.

[7] Mullen, G. L. (1991). Permutation polynomials over finite fields. In: *Finite Fields, Coding Theory, and Advances in Communication and Computing*. Las Vegas, NY: CRC Press, pp. 131–151.

[8] Niu, T., Li, K., Qu, L., Wang, Q. (2021). Finding compositional inverses of permutations from the AGW criterion. *IEEE Trans. Inf. Theory* 67:4975–4985.

[9] Park, Y. H., Lee, J. B. (2001). Permutation polynomials and group permutation polynomials. *Bull. Austral. Math. Soc.* 63:67–74.

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

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

[12] Wang, Q. (2007). Cyclotomic mapping permutation polynomials over finite fields. In: *Sequences, Subsequences, Consequences*. Berlin, Germany: Springer, pp. 119–128.

[13] Wang, Q. (2017). A note on inverses of cyclotomic mapping permutation polynomials over finite fields. *Finite Fields Appl.* 45:422–427.

[14] Wu, B. (2014). The compositional inverse of a class of linearized permutation polynomials over \( \mathbb{F}_{2^n} \), \( n \) odd. *Finite Fields Appl.* 29:34–48.

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

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

[17] Yuan, P. (2022). Compositional inverses of AGW-PPs. *Adv. Math. Commun.* 16(4):1185–1195.

[18] Yuan, P. (2022). Permutation polynomials and their compositional inverses. arXiv:2206.04252. Algebra Colloq. (to appear)

[19] Yuan, P., Ding, C. (2011). Permutation polynomials over finite fields from a powerful lemma. *Finite Fields Appl.* 17:560–574.
[20] Yuan, P., Ding, C. (2014). Further results on permutation polynomials over finite fields. *Finite Fields Appl.* 27:88–103.

[21] Zheng, D., Yuan, M., Li, N., Hu, L., Zeng, X. (2019). Constructions of involutions over finite fields. *IEEE Trans. Inf. Theory* 65:7876–7883.

[22] Zheng, Y., Yu, Y. (2018). On inverse of permutation polynomials of small degree over finite fields, II. arXiv:1812.11812.

[23] Zheng, Y., Wang, Q., Wei, W. (2020). On inverses of permutation polynomials of small degree over finite fields. *IEEE Trans. Inf. Theory* 66:914–922.

[24] Zieve, M. (2009). On some permutation polynomials over $\mathbb{F}_q$ of the form $x^rh(x^{(q-1)/d})$. *Proc. Amer. Math. Soc.* 137:2209–2216.