AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 7(10): 17815–17828.
DOI: 10.3934/math.2022981
Received: 22 June 2022
Revised: 24 July 2022
Accepted: 28 July 2022
Published: 03 August 2022

Research article

Some specific classes of permutation polynomials over $\mathbf{F}_{q^3}$

Xiaoer Qin[1] **and Li Yan**[2,*]

[1] School of Mathematics and Big Data, Chongqing University of Education, Chongqing 400065, China

[2] School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China

* **Correspondence:** Email: yanl903@163.com.

Abstract: Constructing permutation polynomials is a hot topic in finite fields. Recently, huge kinds of permutation polynomials over $\mathbf{F}_{q^2}$ have been studied. In this paper, by using AGW criterion and piecewise method, we construct several classes of permutation polynomials over $\mathbf{F}_{q^3}$ of the forms similar to $(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{d}+1} + L(x)$, for $d = 2, 3, 4, 6$, where $L(x)$ is a linearized polynomial over $\mathbf{F}_q$.

Keywords: finite filed; permutation polynomial; AGW criterion; piecewise method
Mathematics Subject Classification: 11T06, 12E20

1. Introduction

Let $\mathbf{F}_q$ be the finite field of characteristic p with q elements ($q = p^n, n \in \mathbf{N}$), and $\mathbf{F}_q^*$ be the nonzero elements of $\mathbf{F}_q$. Let $\mathbf{F}_q[x]$ be the ring of polynomials over $\mathbf{F}_q$ in the indeterminate x. A polynomial $f(x) \in \mathbf{F}_q[x]$ is called a *permutation polynomial* if f induces a bijection from $\mathbf{F}_q$ to itself. Recently, several classes of permutation polynomials were studied, which can be referred to [5, 8, 11, 12, 20, 21]. More information about properties, constructions and applications of permutation polynomials may be found in the books [7, 9]. We refer the readers to [3, 14] for more details of the recent advances.

We found that the permutation polynomials of the form $(x^q + x + \delta)^s + x$ were studied wildly. During the research on Kloosterman sums, a class of permutation polynomials found in [4] motivated Yuan and Ding to study the permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$. Tu et al. [13] further proposed two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$ over $\mathbf{F}_{2^{2m}}$. Li et al. [6] presented a kind of permutation polynomials over $\mathbf{F}_{q^2}$ of the form

$$(x^q - x + \delta)^{\frac{q^2-1}{3}+1} + x.$$

Yuan and Zheng [19] studied the permutation polynomials over $\mathbf{F}_{q^2}$ having the form

$$(x^{p^k} + ax + \delta)^{\frac{q^2-1}{d}+1} - ax.$$

Recently, Zheng et al. [22] constructed large classes of permutation polynomials over $\mathbf{F}_{q^2}$, which have a more general form

$$(ax^q + bx + c)^r \phi((ax^q + bx + c)^{\frac{q^2-1}{d}}) + ux^q + vx,$$

where $a, b, c, u, v \in \mathbf{F}_{q^2}, r \in \mathrm{Z}^+, \phi(x) \in \mathbf{F}_{q^2}[x]$. We notice that these classes of permutation polynomials are in $\mathbf{F}_{q^2}$. Comparing to permutation polynomials over $\mathbf{F}_{q^2}$, there are few classes of permutation polynomials over $\mathbf{F}_{q^3}$ constructed recently. Ding et al. [2] presented six classes of permutation polynomials over $\mathbf{F}_{3^{3m}}$. Wang, Zhang, Bartoli and Wang [15] constructed several classes of permutation polynomials and complete permutation polynomials over $\mathbf{F}_{q^3}$. Motivated by recent constructions of permutation polynomials over $\mathbf{F}_{q^2}$ and $\mathbf{F}_{q^3}$, we can use AGW criterion and piecewise method to construct several classes of permutation polynomials over $\mathbf{F}_{q^3}$. In this paper, we will focus on constructing permutation polynomials over $\mathbf{F}_{q^3}$ having the similar forms to

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{d}+1} + L(x), d = 2, 3, 4, 6,$$

where $L(x)$ is a linearized polynomial over $\mathbf{F}_q$.

The remainder of this paper is organized as follows. In Section 2, we introduce three lemmas which are used in the following sequels. Subsequently, we give several classes of permutation polynomials of the forms similar to $(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{d}+1} + L(x)$ for $d = 2, 3, 4, 6$, in Section 3–6, respectively.

2. Preliminary

In this section, we will present some results that will be used in the sequels.

The following lemma was developed by Akbary, Ghioca and Wang [1, Lemma 1.1], which was called AGW criterion in [10]. By using AGW criterion, several classes of permutation polynomials were constructed, which could be seen in [16–19,22]. The lemma is listed as follows:

Lemma 2.1. [1] *Let A, S and $\bar{S}$ be finite sets with $\#S = \#\bar{S}$, and let $f : A \to A, h : S \to \bar{S}, \varphi : A \to S$, and $\psi : A \to \bar{S}$ be maps such that $\psi \circ f = h \circ \varphi$, i.e., the following diagram is commutative:*

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

If both ψ and φ are surjective, then the following statements are equivalent:
(i) f is bijective (a permutation of A); and
(ii) h is bijective from S to $\bar{S}$ and f is injective on $\varphi^{-1}(s)$ for each $s \in S$.

Lemma 2.2. *Let k, δ be in $\mathbf{F}_q$. Then we have*

$$\#Im(x^{q^2} + x^q + x + \delta) = \#Im(x^{q^2} + x^q + x + k\delta) = \#\mathbf{F}_q.$$

Proof. Let $\varphi(x) = x^{q^2} + x^q + x + \delta$, then we find that $\varphi(x)^q = \varphi(x)$. Thus for every $\alpha \in \mathbf{F}_{q^3}$, we have $\varphi(\alpha) \in \mathbf{F}_q$. Namely, $Im(\varphi(x)) \subseteq \mathbf{F}_q$. On the other hand, since $\#(Im\varphi(x)) \geq q^3/deg(\varphi(x)) = q^3/q^2 = q$, it follows that $Im(\varphi(x)) = \mathbf{F}_q$. Similarly, we can easily get that $Im(x^{q^2} + x^q + x + k\delta) = \mathbf{F}_q$. Therefore, $\#(Im(x^{q^2} + x^q + x + \delta)) = \#(Im(x^{q^2} + x^q + x + k\delta)) = \#\mathbf{F}_q$.

The proof of Lemma 2.2 is completed.

We close this section with the following result that will be used frequently in the sequels.

Lemma 2.3. [7] *Let $L(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ be a linearized polynomial of $\mathbf{F}_{q^m}$ for $m \in Z^+$. Then $L(x)$ is a permutation polynomial of $\mathbf{F}_{q^m}$ if and only if*

$$\det\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{m-1} \\ a_{m-1}^q & a_0^q & a_1^q & \cdots & a_{m-2}^q \\ a_{m-2}^{q^2} & a_{m-1}^{q^2} & a_0^{q^2} & \cdots & a_{m-3}^{q^2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1^{q^{m-1}} & a_2^{q^{m-1}} & a_3^{q^{m-1}} & \cdots & a_0^{q^{m-1}} \end{pmatrix} \neq 0.$$

3. Permutation polynomials of the form $a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^{q^2} - cx^q - dx$

In this section, we suppose that $p \neq 3$ is an odd prime, ϵ is a primitive element of $\mathbf{F}_{q^3}$. Define $D_0 =< \epsilon^2 >$, which is the multiplicative group generated by ϵ^2, and $D_1 = \epsilon D_0$. Then we get that $\mathbf{F}_{q^3} = \{0\} \cup D_0 \cup D_1$. Furthermore, if $x \in D_i$, we have

$$x^{\frac{q^3-1}{2}} = \epsilon^{i\frac{q^3-1}{2}} = (-1)^i,$$

where $i = 0, 1$.

Since p is an odd prime, then $q \equiv 1 \pmod 2$. By Lemma 2.2, we know that

$$\#Im(x^{q^2} + x^q + x + \delta) = \#Im(x^{q^2} + x^q + x + k\delta) = \#\mathbf{F}_q.$$

In this case, $Im(x^{q^2} + x^q + x + \delta) = Im(x^{q^2} + x^q + x + k\delta) = \mathbf{F}_q$ is the disjoint union of 0 and $\frac{q-1}{2}$ elements from D_0 and $\frac{q-1}{2}$ elements from D_1.

By using Lemma 2.3, we give the first main result of this paper.

Theorem 3.1. *Let $p \neq 3$ be an odd prime and $a, b, c, d, \delta \in \mathbf{F}_q$. If b, c and d satisfy*

$$\det\begin{pmatrix} b & c & d \\ d & b & c \\ c & d & b \end{pmatrix} \neq 0,$$

then

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^{q^2} - cx^q - dx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a - (b + c + d), -(3a + b + c + d))$ belongs to one of $\{D_0 \times D_0, D_1 \times D_1\}$.

Proof. Let $f(x) = a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^{q^2} - cx^q - dx$, $\varphi(x) = x^{q^2} + x^q + x + \delta$, $\psi(x) = x^{q^2} + x^q + x - (b + c + d)\delta$ and $h(x) = x(3ax^{\frac{q^3-1}{2}} - (b + c + d))$. One has

$$\begin{aligned}\psi \circ f = \psi(f(x)) =& f(x)^{q^2} + f(x)^q + f(x) - (b + c + d)\delta \\ =& a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^q - cx - dx^{q^2} \\ &+a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx - cx^{q^2} - dx^q \\ &+a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^{q^2} - cx^q - dx - (b + c + d)\delta \\ =& 3a\varphi(x)^{\frac{q^3-1}{2}+1} - (b + c + d)\varphi(x) \\ =& h(\varphi(x)) = h \circ \varphi.\end{aligned}$$

By Lemma 2.3, it follows from

$$\det\begin{pmatrix} b & c & d \\ d & b & c \\ c & d & b \end{pmatrix} \neq 0,$$

that $bx^{q^2} + cx^q + dx$ is a permutation polynomial of $\mathbf{F}_{q^3}$. Clearly, $as^{\frac{q^3-1}{2}+1} - (bx^{q^2} + cx^q + dx)$ for every $s \in \mathbf{F}_{q^3}$ is also a permutation polynomial of $\mathbf{F}_{q^3}$. For $x \in \varphi^{-1}(s)$, it implies that $f(x) = as^{\frac{q^3-1}{2}+1} - (bx^{q^2} + cx^q + dx)$. Thus for every $s \in Im(\varphi)$, $f(x)$ is injective on $\varphi^{-1}(s)$. By Lemma 2.1, we know that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $h(x)$ is a bijection from $Im(\varphi)$ to $Im(\psi)$.

It is easy to check that

$$h(x) = \begin{cases} (3a - (b + c + d))x, & x \in D_0; \\ -(3a + (b + c + d))x, & x \in D_1. \end{cases}$$

Then we can infer that $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$ if and only if $(3a-(b+c+d), -(3a+b+c+d))$ belongs to one of $\{D_0 \times D_0, D_1 \times D_1\}$. Thus

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx^{q^2} - cx^q - dx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a - (b + c + d), -(3a + b + c + d))$ belongs to one of $\{D_0 \times D_0, D_1 \times D_1\}$.

The proof of Theorem 3.1 is completed.

Corollaries 3.2 and 3.3 are two explicit examples of Theorem 3.1, we omit their proofs, just list them in the following.

Corollary 3.2. *Let $p \neq 3$ be an odd prime, $\delta \in \mathbf{F}_q$ and let $a, b \in \mathbf{F}_q$ satisfy $3a - b \neq 0$ and $3a + b \neq 0$. Then we get that*

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - bx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a-b, -(3a+b))$ belongs to one of $\{D_0\times D_0, D_1\times D_1\}$.

Corollary 3.3. *Let $p \neq 3, 5$ be an odd prime, $\delta \in \mathbf{F}_q$ and $-5 \in D_0$. Then we get that*

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{2}+1} - x - x^q$$

is a permutation polynomial over $\mathbf{F}_{q^3}$.

Example 3.4. For $q = 19$ and $\delta \in \mathbf{F}_{19}$, it is easy to check that $(2, -1) \in D_1 \times D_1$ by Magma, thus we can imply from Corollary 3.2 that $(x^{q^2} + x^q + x + \delta)^{2287} - x$ is a permutation polynomial over $\mathbf{F}_{19^3}$.

4. Permutation polynomials of the form $a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx^{q^2}+cx^q+dx$

In this section, we suppose $p\neq 3$ be an odd prime and $q^3\equiv 1 \pmod 3$. Let ϵ be a primitive element of $\mathbf{F}_{q^3}$, we define $D_0=<\epsilon^3>$ and $D_i=\epsilon^i D_0$ for $i=1,2$. Then $\mathbf{F}_{q^3}=\{0\}\cup D_0\cup D_1\cup D_2$. Let $\omega=\epsilon^{\frac{q^3-1}{3}}$, one has $\omega^2+\omega+1=0$.

It follows from $q^3\equiv 1 \pmod 3$ that $q\equiv 1 \pmod 3$ and $q^2+q+1\equiv 0 \pmod 3$, so $\mathbf{F}_q\subseteq\{0\}\cup D_0$.

We can get the following result, which is the second main result in this paper.

Theorem 4.1. *Let $p\neq 3$ be an odd prime, $q\equiv 1 \pmod 3$ and $a,b,c,d,\delta\in\mathbf{F}_q$. If $6a+b+c+d\neq 0$, $-3a+b+c+d\neq 0$ and*

$$\det\begin{pmatrix} b & c & d\\ d & b & c\\ c & d & b\end{pmatrix}\neq 0,$$

then we have

$$a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx^{q^2}+cx^q+dx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$.

Proof. Define

$$\begin{aligned}
f(x)=&a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx^{q^2}+cx^q+dx,\\
\varphi(x)=&x^{q^2}+x^q+x+\delta,\\
\psi(x)=&x^{q^2}+x^q+x+(b+c+d)\delta,\\
h(x)=&x(3ax^{\frac{q^3-1}{3}}+3ax^{\frac{2(q^3-1)}{3}}+b+c+d).
\end{aligned}$$

In the following, it is easy to check that

$$\begin{aligned}
\psi\circ f=&\psi(f(x))=f(x)^{q^2}+f(x)^q+f(x)+(b+c+d)\delta\\
=&a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx^q+cx+dx^{q^2}\\
&+a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx+cx^{q^2}+dx^q\\
&+a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{3}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{2(q^3-1)}{3}+1}+bx^{q^2}+cx^q+dx+(b+c+d)\delta\\
=&3a\varphi(x)^{\frac{q^3-1}{3}+1}+3a\varphi(x)^{\frac{2(q^3-1)}{3}+1}+(b+c+d)\varphi(x)\\
=&h(\varphi(x))=h\circ\varphi.
\end{aligned}$$

Since

$$\det\begin{pmatrix} b & c & d\\ d & b & c\\ c & d & b\end{pmatrix}\neq 0,$$

it follows from Lemma 2.3 that $bx^{q^2}+cx^q+dx$ is a permutation polynomial of $\mathbf{F}_{q^3}$. Thus $f(x)$ is injective on $\varphi^{-1}(s)$. By Lemma 2.1, $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$.

By Lemma 2.2, we get that $Im(\varphi) = Im(\psi) = \mathbf{F}_q$. Hence we need to prove that $h(x)$ is a bijection on $\mathbf{F}_q$. Since $x^{\frac{q^3-1}{3}} + x^{\frac{2(q^3-1)}{3}} = 2$ for $x \in D_0$ and $x^{\frac{q^3-1}{3}} + x^{\frac{2(q^3-1)}{3}} = -1$ for $x \in D_1 \cup D_2$, we get that

$$h(x) = \begin{cases} (6a + b + c + d)x, & x \in D_0; \\ (-3a + b + c + d)x, & x \in D_1; \\ (-3a + b + c + d)x, & x \in D_2. \end{cases}$$

Since $q \equiv 1 \pmod 3$, then $\mathbf{F}_q \subseteq D_0 \cup \{0\}$. It follows that $6a + b + c + d$ and $-3a + b + c + d$ are in D_0. Thus $h(x)$ is a bijection on $\mathbf{F}_q$.

Therefore, we can conclude that $a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{3}+1} + a(x^{q^2} + x^q + x + \delta)^{\frac{2(q^3-1)}{3}+1} + bx^{q^2} + cx^q + dx$ is a permutation polynomial over $\mathbf{F}_{q^3}$. This completes the proof of Theorem 4.1.

By Theorem 4.1, we can easily give the following results.

Corollary 4.2. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 3$ and $\delta \in \mathbf{F}_q$. Then we get that*

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{3}+1} + (x^{q^2} + x^q + x + \delta)^{\frac{2(q^3-1)}{3}+1} - 3x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$.

Corollary 4.3. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 3$ and $\delta \in \mathbf{F}_q$. Then we get that*

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{3}+1} + (x^{q^2} + x^q + x + \delta)^{\frac{2(q^3-1)}{3}3+1} + x^q + x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$.

5. Permutation polynomials of the form $a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{4}+1} + a(x^{q^2} + x^q + x + \delta)^{\frac{3(q^3-1)}{4}+1} + bx^{q^2} + cx^q + dx$

In this section, we suppose that $p \neq 3$ is an odd prime and $q^3 \equiv 1 \pmod 4$, ϵ is a primitive element of $\mathbf{F}_{q^3}$. Define $D_0 =< \epsilon^4 >$, which is the multiplicative group generated by ϵ^4, and $D_i = \epsilon^i D_0$ for $i = 1, 2, 3$. Then we get that $\mathbf{F}_{q^3} = \{0\} \cup D_0 \cup D_1 \cup D_2 \cup D_3$. Note that $x^{\frac{q^3-1}{4}} = \epsilon^{i\frac{q^3-1}{4}}$, for $x \in D_i$, where $i = 1, 2, 3$. Let $\omega = \epsilon^{\frac{q^3-1}{4}}$, then $\omega^2 + 1 = 0$.

Since $q^3 \equiv 1 \pmod 4$, we get that $q \equiv 1 \pmod 4$, then $q^2 + q + 1 \equiv 3 \pmod 4$. By Lemma 2.2, we know that

$$\#Im(x^{q^2} + x^q + x + \delta) = \#Im(x^{q^2} + x^q + x + k\delta) = \#\mathbf{F}_q.$$

It follows that $\mathbf{F}_q$ is a disjoint union of 0 and $\frac{q-1}{4}$ elements from D_0 and $\frac{q-1}{4}$ elements from D_1 and $\frac{q-1}{4}$ elements from D_2 and $\frac{q-1}{4}$ elements from D_3.

We present the third main result of this paper in the following.

Theorem 5.1. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 4$ and $\delta \in \mathbf{F}_q$. Let $a \in \mathbf{F}_q^*, b, c, d \in \mathbf{F}_q$ satisfy $6a + b + c + d \neq 0, b + c + d \neq 0$, $-6a + b + c + d \neq 0$ and*

$$\det\begin{pmatrix} b & c & d \\ d & b & c \\ c & d & b \end{pmatrix} \neq 0.$$

Then

$$a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1}+bx^{q^2}+cx^q+dx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ *if and only if* $(6a+b+c+d, b+c+d, -6a+b+c+d)$ *belongs to one of* $\{D_0\times D_0\times D_0, D_0\times D_2\times D_0, D_1\times D_1\times D_1, D_1\times D_3\times D_1, D_2\times D_2\times D_2, D_2\times D_0\times D_2, D_3\times D_3\times D_3, D_3\times D_1\times D_3\}$.

Proof. Let

$$\begin{aligned}
f(x) =& a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1}+bx^{q^2}+cx^q+dx,\\
\varphi(x) =& x^{q^2}+x^q+x+\delta,\\
\psi(x) =& x^{q^2}+x^q+x+(b+c+d)\delta,\\
h(x) =& x(3ax^{\frac{q^3-1}{4}}+3ax^{\frac{3(q^3-1)}{4}}+b+c+d).
\end{aligned}$$

It is easy to check that

$$\begin{aligned}
\psi\circ f =& \psi(f(x)) = f(x)^{q^2}+f(x)^q+f(x)+(b+c+d)\delta\\
=& a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1}+bx^q+cx+dx^{q^2}\\
&+a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1}+bx+cx^{q^2}+dx^q\\
&+a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}+a(x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1}+bx^{q^2}+cx^q+dx+(b+c+d)\delta\\
=& 3a\varphi(x)^{\frac{q^3-1}{4}+1}+3a\varphi(x)^{\frac{3(q^3-1)}{4}+1}+(b+c+d)\varphi(x)\\
=& h(\varphi(x)) = h\circ\varphi.
\end{aligned}$$

Since

$$\det\begin{pmatrix} b & c & d\\ d & b & c\\ c & d & b\end{pmatrix}\neq 0,$$

it follows from Lemma 2.3 that $bx^{q^2}+cx^q+dx$ is a permutation polynomial over $\mathbf{F}_{q^3}$. Therefore, we can easily get that for every $s\in Im(\varphi)$, $f(x)$ is injective on $\varphi^{-1}(s)$. By Lemma 2.1, $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$.

Note that

$$x^{\frac{q^3-1}{4}}+x^{\frac{3(q^3-1)}{4}}=\begin{cases}2, & x\in D_0;\\ 0, & x\in D_1;\\ -2, & x\in D_2;\\ 0, & x\in D_3.\end{cases}$$

Then $h(x)$ can be rewritten as

$$h(x)=\begin{cases}(6a+b+c+d)x, & x\in D_0;\\ (b+c+d)x, & x\in D_1;\\ (-6a+b+c+d)x, & x\in D_2;\\ (b+c+d)x, & x\in D_3.\end{cases}$$

In the following, we focus on proving that $h(x)$ is a bijection from $Im(\varphi)$ to $Im(\psi)$ if and only if $(6a+b+c+d, b+c+d, -6a+b+c+d)$ belongs to one of $\{D_0 \times D_0 \times D_0, D_0 \times D_2 \times D_0, D_1 \times D_1 \times D_1, D_1 \times D_3 \times D_1, D_2 \times D_2 \times D_2, D_2 \times D_0 \times D_2, D_3 \times D_3 \times D_3, D_3 \times D_1 \times D_3\}$.

Now we first prove the sufficiency part. Assume that $h(x)$ is a bijection. We consider the following cases:

(1) $6a+b+c+d \in D_0$. Clearly, we have $(6a+b+c+d)x \in D_0$ for $x \in D_0$, then it implies that $(b+c+d)x \notin D_0$ for $x \in D_1 \cup D_3$. It tells us that $b+c+d \notin D_1 \cup D_3$. If $b+c+d \in D_0$, then $(b+c+d)x \in D_1$ and $(b+c+d)x \in D_3$ for $x \in D_1$ and $x \in D_3$, respectively. Since $h(x)$ is a bijection, we can get that $(-6a+b+c+d)x \in D_2$ for $x \in D_2$, thus $-6a+b+c+d \in D_0$. On the other hand, if $b+c+d \in D_2$, then $(b+c+d)x \in D_3$ for $x \in D_1$ and $(b+c+d)x \in D_1$ for $x \in D_3$. It follows from $h(x)$ being a bijection that $(-6a+b+c+d)x \in D_2$ for $x \in D_2$, one has $-6a+b+c+d \in D_0$.

(2) $6a+b+c+d \in D_1$. In this case, we can imply that $b+c+d \notin D_0 \cup D_2$. If $b+c+d \in D_1$, by $h(x)$ being a bijection, we can get that $-6a+b+c+d \in D_1$. Similarly, if $b+c+d \in D_3$, then it follows from $h(x)$ being a bijection that $-6a+b+c+d \in D_1$.

(3) $6a+b+c+d \in D_2$. In this case, we first get that $b+c+d \notin D_1 \cup D_3$. If $b+c+d \in D_2$, since $h(x)$ is a bijection, we can get that $-6a+b+c+d \in D_2$. If $b+c+d \in D_0$, it follows that $-6a+b+c+d \in D_2$.

(4) $6a+b+c+d \in D_3$. In this case, it is easy to imply that $b+c+d \notin D_0 \cup D_2$. If $b+c+d \in D_1$, then we can get that $-6a+b+c+d \in D_3$. If $b+c+d \in D_3$, it follows from $h(x)$ being a bijection that $-6a+b+c+d \in D_3$.

Conversely, we can easily check the necessity part is true.

Thus we can conclude that $a(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1} + a(x^{q^2}+x^q+x+\delta)^{3\frac{q^3-1}{4}+1} + bx^{q^2}+cx^q+dx$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(6a+b+c+d, b+c+d, -6a+b+c+d)$ belongs to one of $\{D_0 \times D_0 \times D_0, D_0 \times D_2 \times D_0, D_1 \times D_1 \times D_1, D_1 \times D_3 \times D_1, D_2 \times D_2 \times D_2, D_2 \times D_0 \times D_2, D_3 \times D_3 \times D_3, D_3 \times D_1 \times D_3\}$.

By Theorem 5.1, we can get the following results.

Corollary 5.2. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 4$ and $\delta \in \mathbf{F}_q$. Then*

$$(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1} + (x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1} - x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(-1, 5, 7)$ belongs to one of $\{D_0 \times D_0 \times D_0, D_0 \times D_2 \times D_2, D_2 \times D_0 \times D_2, D_2 \times D_2 \times D_0\}$.

Corollary 5.3. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 4$ and $\delta \in \mathbf{F}_q$. Then*

$$(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1} + (x^{q^2}+x^q+x+\delta)^{\frac{3(q^3-1)}{4}+1} + x^q + x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(-1, 2)$ belongs to one of $\{D_0 \times D_0, D_0 \times D_2, D_2 \times D_3\}$.

Example 5.4. For $q = 29$ and $\delta \in \mathbf{F}_q$, we can check that $(-1, 5, 7) \in D_2 \times D_2 \times D_0$ by Magma, it follows from Corollary 5.2 that $(x^{q^2}+x^q+x+\delta)^{6098} + (x^{q^2}+x^q+x+\delta)^{18292} - x$ is a permutation polynomial over $\mathbf{F}_{29^3}$.

In what follows, we will give the fourth main result in this paper.

Theorem 5.5. *Let $p \neq 3, 5$ be an odd prime, $q \equiv 1 \pmod 4$ and $\delta \in \mathbf{F}_q$. Then*

$$(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1} - x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ *if and only if* $(2, -4, 3\omega-1, -3\omega-1)$ *belongs to one of* $\{D_0\times D_0\times D_0\times D_0, D_0\times D_0\times D_2\times D_2, D_1\times D_2\times D_1\times D_0, D_1\times D_2\times D_2\times D_3, D_1\times D_0\times D_3\times D_0, D_1\times D_0\times D_2\times D_1, D_2\times D_2\times D_0\times D_0, D_2\times D_2\times D_2\times D_2, D_3\times D_2\times D_0\times D_3, D_3\times D_2\times D_2\times D_2, D_3\times D_0\times D_3\times D_2, D_3\times D_0\times D_0\times D_1\}$.

Proof. Let $(x^{q^2}+x^q+x+\delta)^{\frac{q^3-1}{4}+1}-x$, $\varphi(x) = x^{q^2}+x^q+x+\delta$, $\psi(x) = x^{q^2}+x^q+x-\delta$ and $h(x) = x(3x^{\frac{q^3-1}{4}}-1)$. Then we can easily check that

$$\psi \circ f = h \circ \varphi.$$

Namely, the diagram is commutative. Furthermore, it is easy to get that for every $s \in Im(\varphi)$, $f(x)$ is injective on $\varphi^{-1}(s)$. Thus it follows from Lemma 2.1 that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$.

By Lemma 2.2, we know that $Im(\varphi) = Im(\psi) = \mathbf{F}_q$. For $x \in \mathbf{F}_q$, we can rewrite $h(x)$ as:

$$h(x) = \begin{cases} 2x, & x \in D_0; \\ (3\omega-1)x, & x \in D_1; \\ -4x, & x \in D_2; \\ (-3\omega-1)x, & x \in D_3. \end{cases}$$

Since $p \neq 3, 5$ is an odd prime, we get that $(3\omega-1)(-3\omega-1) \neq 0$. We claim that $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$ if and only if $(2, -4, 3\omega-1, -3\omega-1)$ belongs to one of $\{D_0\times D_0\times D_0\times D_0, D_0\times D_0\times D_2\times D_2, D_1\times D_2\times D_1\times D_0, D_1\times D_2\times D_2\times D_3, D_1\times D_0\times D_3\times D_0, D_1\times D_0\times D_2\times D_1, D_2\times D_2\times D_0\times D_0, D_2\times D_2\times D_2\times D_2, D_3\times D_2\times D_0\times D_3, D_3\times D_2\times D_2\times D_2, D_3\times D_0\times D_3\times D_2, D_3\times D_0\times D_0\times D_1\}$.

First we assume $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$. Since $q \equiv 1 \pmod 4$, it tells us that $-1 \in D_0$ or $-1 \in D_2$. We consider the following cases:

(1) $2 \in D_0$. Then we get that $-4 \in D_0$ or $-4 \in D_2$. For $x \in D_0$, we have $2x \in D_0$, it follows from $h(x)$ being a bijection that $-4x \notin D_0$ for $x \in D_2$, hence $-4 \in D_0$ and $-4x \in D_2$ for $x \in D_2$. Furthermore, since $2x \in D_0$ for $x \in D_0$ and $-4x \in D_2$ for $x \in D_2$, then $(3\omega-1)x \notin D_0 \cup D_2$ for $x \in D_1$, thus $3\omega-1 \in D_0$ or $3\omega-1 \in D_2$. If $3\omega-1 \in D_0$, by $h(x)$ being a bijection, one has $-3\omega-1 \in D_0$. If $3\omega-1 \in D_2$, then it implies that $-3\omega-1 \in D_2$.

(2) $2 \in D_1$. Since $-1 \in D_0$ or $-1 \in D_2$, thus $-4 \in D_2$ or $-4 \in D_0$. For the first case, if $-4 \in D_2$, then $2x \in D_1$ for $x \in D_0$ and $-4x \in D_0$ for $x \in D_2$. Since $h(x)$ is a bijection, we know that $3\omega-1 \in D_1$ or $3\omega-1 \in D_2$. If $3\omega-1 \in D_1$, it follows that $-3\omega-1 \in D_0$. If $3\omega-1 \in D_2$, one has that $-3\omega-1 \in D_3$. For the second case, if $-4 \in D_0$, then $2x \in D_1$ for $x \in D_0$ and $-4x \in D_2$ for $x \in D_2$. Since $h(x)$ is a bijection, we know that $3\omega-1 \in D_3$ or $3\omega-1 \in D_2$. If $3\omega-1 \in D_3$, it follows that $-3\omega-1 \in D_0$. If $3\omega-1 \in D_2$, we know that $-3\omega-1 \in D_1$.

(3) $2 \in D_2$. Since $2 \in D_2$, then we get that $-4 \in D_0$ or $-4 \in D_2$. For $x \in D_0$, we have $2x \in D_2$, it follows from $h(x)$ being a bijection that $-4x \notin D_2$ for $x \in D_2$, hence $-4 \in D_2$ and $-4x \in D_0$ for $x \in D_2$. Furthermore, since $2x \in D_2$ for $x \in D_0$ and $-4x \in D_0$ for $x \in D_2$, then $(3\omega-1)x \notin D_0 \cup D_2$ for $x \in D_1$, thus $3\omega-1 \in D_0$ or $3\omega-1 \in D_2$. If $3\omega-1 \in D_0$, it implies that $-3\omega-1 \in D_0$. If $3\omega-1 \in D_2$, we have $-3\omega-1 \in D_2$.

(4) $2 \in D_3$. Since $-1 \in D_0$ or $-1 \in D_2$, thus $-4 \in D_2$ or $-4 \in D_0$. For the first case, if $-4 \in D_2$, then $2x \in D_3$ for $x \in D_0$ and $-4x \in D_0$ for $x \in D_2$. Since $h(x)$ is a bijection, we know that $3\omega-1 \in D_0$ or $3\omega-1 \in D_1$. If $3\omega-1 \in D_0$, it follows that $-3\omega-1 \in D_3$. If $3\omega-1 \in D_1$, we get that $-3\omega-1 \in D_2$. For the second case, if $-4 \in D_0$, then $2x \in D_3$ for $x \in D_0$ and $-4x \in D_2$ for $x \in D_2$. Since $h(x)$ is

a bijection, one has $3\omega - 1 \in D_3$ or $3\omega - 1 \in D_0$. If $3\omega - 1 \in D_3$, it follows that $-3\omega - 1 \in D_2$. If $3\omega - 1 \in D_0$, it implies that $-3\omega - 1 \in D_1$.

The sufficiency part is proved.

For the necessity part, if $(2, -4, 3\omega - 1, -3\omega - 1)$ belongs to one of $\{D_0 \times D_0 \times D_0 \times D_0, D_0 \times D_0 \times D_2 \times D_2, D_1 \times D_2 \times D_1 \times D_0, D_1 \times D_2 \times D_2 \times D_3, D_1 \times D_0 \times D_3 \times D_0, D_1 \times D_0 \times D_2 \times D_1, D_2 \times D_2 \times D_0 \times D_0, D_2 \times D_2 \times D_2 \times D_2, D_3 \times D_2 \times D_0 \times D_3, D_3 \times D_2 \times D_2 \times D_2, D_3 \times D_0 \times D_3 \times D_2, D_3 \times D_0 \times D_0 \times D_1\}$, we easily check that $h(x)$ is a bijection from $Im(\varphi)$ to $Im(\psi)$. Thus the claim is true.

Therefore, we get that

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{4}+1} - x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(2, -4, 3\omega - 1, -3\omega - 1)$ belongs to one of $\{D_0 \times D_0 \times D_0 \times D_0, D_0 \times D_0 \times D_2 \times D_2, D_1 \times D_2 \times D_1 \times D_0, D_1 \times D_2 \times D_2 \times D_3, D_1 \times D_0 \times D_3 \times D_0, D_1 \times D_0 \times D_2 \times D_1, D_2 \times D_2 \times D_0 \times D_0, D_2 \times D_2 \times D_2 \times D_2, D_3 \times D_2 \times D_0 \times D_3, D_3 \times D_2 \times D_2 \times D_2, D_3 \times D_0 \times D_3 \times D_2, D_3 \times D_0 \times D_0 \times D_1\}$.

The proof of Theorem 5.5 is completed.

Similarly, we have

Theorem 5.6. *Let $p \neq 3, 5$ be an odd prime, $q \equiv 1 \pmod 4$ and $\delta \in \mathbf{F}_q$. Then*

$$(x^{q^2} + x^q + x + \delta)^{\frac{3(q^3-1)}{4}+1} - x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(2, -4, -3\omega - 1, 3\omega - 1)$ belongs to one of $\{D_0 \times D_0 \times D_0 \times D_0, D_0 \times D_0 \times D_2 \times D_2, D_1 \times D_2 \times D_1 \times D_0, D_1 \times D_2 \times D_2 \times D_3, D_1 \times D_0 \times D_3 \times D_0, D_1 \times D_0 \times D_2 \times D_1, D_2 \times D_2 \times D_0 \times D_0, D_2 \times D_2 \times D_2 \times D_2, D_3 \times D_2 \times D_0 \times D_3, D_3 \times D_2 \times D_2 \times D_2, D_3 \times D_0 \times D_3 \times D_2, D_3 \times D_0 \times D_0 \times D_1\}$.

6. Permutation polynomials of the form $a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx$

In this section, let $p \neq 3$ be an odd prime and $q^3 \equiv 1 \pmod 6$. We assume ϵ is a primitive element of $\mathbf{F}_{q^3}$ and define $D_0 =< \epsilon^6 >$, which is the multiplicative group generated by ϵ^6, and $D_i = \epsilon^i D_0$ for $i = 1, 2, 3, 4, 5$. Then we get that $\mathbf{F}_{q^3} = \{0\} \cup D_0 \cup D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5$. Furthermore, if $x \in D_i$, we notice that $x^{\frac{q^3-1}{6}} = \epsilon^{i\frac{q^3-1}{6}}$. For simplicity, we define $\omega = \epsilon^{\frac{q^3-1}{6}}$, which satisfies $\omega^2 - \omega + 1 = 0$.

Since $q^3 \equiv 1 \pmod 6$, we know that $q \equiv 1 \pmod 6$, then $q^2 + q + 1 \equiv 3 \pmod 6$ and $q \equiv 1 \pmod 2$. By Lemma 2.2, we know that

$$\#Im(x^{q^2} + x^q + x + \delta) = \#Im(x^{q^2} + x^q + x + k\delta) = \#\mathbf{F}_q,$$

and $\mathbf{F}_q$ is a disjoint union of 0 and $\frac{q-1}{2}$ elements from D_0 and $\frac{q-1}{2}$ elements from D_3.

In what follows, we can get the permutation polynomials of the form $a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx$, which is the fifth main result in this paper.

Theorem 6.1. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 6$ and $\delta \in \mathbf{F}_q$, and let $a, b \in \mathbf{F}_q$ such that $3a + b \neq 0$ and $-3a + b \neq 0$. Then*

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a + b, -3a + b)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

Proof. Let $f(x) = a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx$, $\varphi(x) = x^{q^2} + x^q + x + \delta$, $\psi(x) = x^{q^2} + x^q + x + b\delta$ and $h(x) = x(3ax^{\frac{q^3-1}{6}} + b)$. It is easy to check that

$$\begin{aligned}\psi \circ f = \psi(f(x)) =& f(x)^{q^2} + f(x)^q + f(x) + b\delta\\ =& a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx^{q^2}\\ &+ a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx^q\\ &+ a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx + b\delta\\ =& 3a\varphi(x)^{\frac{q^3-1}{6}+1} + b\varphi(x)\\ =& h(\varphi(x)) = h \circ \varphi.\end{aligned}$$

Furthermore, we can easily check that for every $s \in Im(\varphi)$, $f(x)$ is injective on $\varphi^{-1}(s)$. Then it follows from Lemma 2.1 that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$.

Since $Im(\varphi) = Im(\psi) = \mathbf{F}_q$ is a disjoint union of 0 and $\frac{q-1}{2}$ elements from D_0 and $\frac{q-1}{2}$ elements from D_3, we get that

$$h(x) = \begin{cases}(3a+b)x, & x \in D_0;\\ (-3a+b)x, & x \in D_3.\end{cases}$$

Next we prove that $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$ if and only if $(3a+b, -3a+b)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

Firstly, we give the proof of the sufficiency part. Suppose $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$. If $3a + b \in D_0$, then we have $(3a + b)D_0 = D_0$. Hence $(-3a + b)D_3 = D_3$, it tells us that $-3a + b \in D_0$. On the other hand, if $3a + b \in D_3$, then $(3a + b)D_0 = D_3$ and $(-3a + b)D_3 = D_0$, thus it follows that $-3a + b \in D_3$.

Now we prove the necessity part. If $(3a + b, -3a + b) \in D_0 \times D_0$ or $D_3 \times D_3$, it is easy to check that $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$. Therefore, $h(x)$ is bijective from $Im(\varphi)$ to $Im(\psi)$ if and only if $(3a + b, -3a + b)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

We can conclude that

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + bx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a+b, -3a+b)$ belongs to one of $\{D_0\times D_0, D_3\times D_3\}$.

The proof of Theorem 6.1 is completed.

Corollary 6.2. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 6$ and $\delta \in \mathbf{F}_q$. Then*

$$(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} - x$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(2, -4)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

Proof. Taking $a = 1, b = -1$ in Theorem 6.1, it follows from Theorem 6.1 that $(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} - x$ is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(2, -4)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

Example 6.3. For $q = 19$ and $\delta \in \mathbf{F}_{19}$, we can find that $(2, -4) \in D_3 \times D_3$ by Magma, by Corollary 6.2, it follows that $(x^{q^2} + x^q + x + \delta)^{1144} - x$ is a permutation polynomial over $\mathbf{F}_{19^3}$.

Similarly, we have

Theorem 6.4. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 6$ and $\delta \in \mathbf{F}_q$, and let $a, b \in \mathbf{F}_q$ such that $3a + b \neq 0$ and $-3a + b \neq 0$. Then*

$$a(x^{q^2} + x^q + x + \delta)^{\frac{5(q^3-1)}{6}+1} + bx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a+b, -3a+b)$ belongs to one of $\{D_0\times D_0, D_3\times D_3\}$.

Proof. The proof of Theorem 6.4 is similar to that of Theorem 6.1, here we omit it.

Furthermore, we get a permutation polynomial having a more general form.

Theorem 6.5. *Let $p \neq 3$ be an odd prime, $q \equiv 1 \pmod 6$ and $\delta \in \mathbf{F}_q$, and let $a, b, c \in \mathbf{F}_q$ such that $3a + 3b + c \neq 0$ and $-3a - 3b + c \neq 0$. Then*

$$a(x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{6}+1} + b(x^{q^2} + x^q + x + \delta)^{\frac{5(q^3-1)}{6}+1} + cx$$

is a permutation polynomial over $\mathbf{F}_{q^3}$ if and only if $(3a + 3b + c, -3a - 3b + c)$ belongs to one of $\{D_0 \times D_0, D_3 \times D_3\}$.

Proof. The proof of Theorem 6.5 is similar to that of Theorem 6.1, here we only give that $h(x) = x(3ax^{\frac{q^3-1}{6}} + 3bx^{5\frac{q^3-1}{6}} + c)$, and $h(x)$ can be rewritten as

$$h(x) = \begin{cases} (3a + 3b + c)x, & x \in D_0; \\ (-3a - 3b + c)x, & x \in D_3. \end{cases}$$

We omit the other details of the proof.

7. Conclusions

In this paper, motivated by some constructions of permutation polynomials over $\mathbf{F}_{q^2}$, we used AGW criterion and piecewise method to construct several classes of permutation polynomials over $\mathbf{F}_{q^3}$ of the forms $(x^{q^2} + x^q + x + \delta)\phi((x^{q^2} + x^q + x + \delta)^{\frac{q^3-1}{d}}) + L(x)$, for $d = 2, 3, 4, 6$, where $L(x)$ is a linearized polynomial over $\mathbf{F}_q$, which enrich the permutation polynomials over $\mathbf{F}_{q^3}$.

Acknowledgments

The Authors express their gratitude to the anonymous reviewers for carefully examining this paper and providing a number of valuable comments and suggestions. This research was supported by the National Science Foundation of China (No. 11926344) and by Science and Technology Research Program of Chongqing Municipal Education Commission (No. KJQN201900506).

Conflict of interest

We declare that we have no conflict of interest.

References

1. A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.*, **17** (2011), 51–67. https://doi.org/10.1016/j.ffa.2010.10.002

2. C. S. Ding, Q. Xiang, J. Yuan, P. Z. Yuan, Explicit classes of permutation polynomials of $F_{3^{3m}}$, *Sci. China Ser. A: Math.*, **52** (2009), 639–647. https://doi.org/10.1007/s11425-008-0142-8

3. X. D. Hou, Permutation polynomials over finite fields–A survey of recent advances, *Finite Fields Appl.*, **32** (2015), 82–119. https://doi.org/10.1016/j.ffa.2014.10.001

4. T. Helleseth, V. Zinoviev, New Kloosterman sums identities over $\mathbf{F}_{2^m}$ for all m, *Finite Fields Appl.*, **9** (2003), 187–193. https://doi.org/10.1016/S1071-5797(02)00028-X

5. K. Q. Li, L. J. 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. https://doi.org/10.1007/s12095-018-0292-7

6. N. Li, T. Helleseth, X. H. Tang, Further results on a class of permutation polynomials over finite fields, *Finite Fields Appl.*, **22** (2013), 16–23. https://doi.org/10.1016/j.ffa.2013.02.004

7. R. Lidl, H. Niederreiter, *Finite fields*, 2 Eds, Cambridge: Cambridge University Press, 1997.

8. Q. Liu, Y. J. Sun, W. G. Zhang, Some classes of permutation polynomials over finite fields with odd characteristic, *AAECC*, **29** (2018), 409–431. https://doi.org/10.1007/s00200-018-0350-6

9. G. L. Mullen, D. Panario, *Handbook of finite fields*, Chapman and Hall/CRC, 2013. https://doi.org/10.1201/b15006

10. G. L. Mullen, Q. Wang, Permutation polynomials in one variable, In: *Handbook of finite fields*, Chapman and Hall/CRC, 2013, 215–229.

11. X. E. Qin, S. F. Hong, Constructing permutation polynomials over finite fields, *Bull. Aust. Math. Soc.*, **89** (2014), 420–430. https://doi.org/10.1017/S0004972713000646

12. X. E. Qin, G. Y. Qian, S. F. Hong, New results on permutation polynomials over finite fields, *Int. J. Number Theory*, **11** (2015), 437–449. https://doi.org/10.1142/S1793042115500220

13. Z. R. Tu, X. Y. Zeng, Y. P. Jiang, Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$, *Finite Fields Appl.*, **31** (2015), 12–24. https://doi.org/10.1016/j.ffa.2014.09.005

14. Q. Wang, Polynomials over finite fields: An index approach, In: *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*, 2019, 319–348. https://doi.org/10.1515/9783110642094-015

15. Y. P. Wang, W. G. Zhang, D. Bartoli, Q. Wang, Permutation polynomials and complete permutation polynomials over $\mathbf{F}_{q^3}$, 2018, arXiv: 1806.05712v1.

16. P. Z. Yuan, C. S. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.*, **17** (2011), 560–574. https://doi.org/10.1016/j.ffa.2011.04.001

17. P. Z. Yuan, C. S. Ding, Further results on permutation polynomials over finite fields, *Finite Fields Appl.*, **27** (2014), 88–103. https://doi.org/10.1016/j.ffa.2014.01.006

18. P. Z. Yuan, C. S. Ding, Permutation polynomials of the form $L(x) + S_a^{2k} + S_b^{2k}$ over $\mathbf{F}_{q^{3k}}$, *Finite Fields Appl.*, **29** (2014), 106–117. https://doi.org/10.1016/j.ffa.2014.04.004

19. P. Z. Yuan, Y. B. Zheng, Permutation polynomials from piecewise functions, *Finite Fields Appl.*, **35** (2015), 215–230. https://doi.org/10.1016/j.ffa.2015.05.001

20. Z. B. Zha, L. Hu, Z. Z. Zhang, New results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x^{p^m} + x$ over $\mathbf{F}_{p^{2m}}$, *Cryptogr. Commun.*, **10** (2018), 567–578. https://doi.org/10.1007/s12095-017-0234-9

21. D. B. Zheng, Z. Chen, More classes of permutation polynomial of the form $(x^{p^m} - x + \delta)^s + L(x)$, *AAECC*, **28** (2017), 215–223. https://doi.org/10.1007/s00200-016-0305-8

22. Y. B. Zheng, P. Z. Yuan, D. Y. Pei, Large classes of permutation polynomials over $\mathbf{F}_{q^2}$, *Des. Codes Cryptogr.*, **81** (2016), 505–521. https://doi.org/10.1007/s10623-015-0172-5

AIMS Press