Bull. Math. Soc. Sci. Math. Roumanie
Tome 64 (112), No. 1, 2021, 75–87

Some generalized permutation polynomials over finite fields

by
Xiaoer Qin[(1)], Li Yan*[(2)]

Abstract

Constructing permutation polynomials is a hot topic in finite fields, and permutation polynomials have many applications in another areas. In this paper, we combine the AGW criterion and the piecewise method to construct several classes of permutation polynomials over $\mathbf{F}_{q^2}$, which generalize some known classes of permutation polynomials over $\mathbf{F}_{q^2}$.

Key Words: Permutation polynomials, AGW criterion, piecewise method, finite fields.
2010 Mathematics Subject Classification: Primary 11T06; Secondary 12E20.

1 Introduction

Let $\mathbf{F}_q$ denote the finite field with q elements. Functions from $\mathbf{F}_q$ to $\mathbf{F}_q$ are uniquely represented by polynomials in $\mathbf{F}_q[x]$ module $x^q - x$. A polynomial $f(x) \in \mathbf{F}_q[x]$ is called a *permutation polynomial* if f induces a bijection of $\mathbf{F}_q$. The study of permutation polynomials has a long history, which can be traced to Hermite[3] and Dickson[2]. In the books[6, 10], systematic treatments of permutation polynomials are introduced. In [5], Hou surveyed the recent achievements related to permutation polynomials, and showed the significant results and novel methods.

Recently, many classes of permutation polynomials of the forms $(x^q - x + \delta)^s + L(x)$ and $(x^q - x + \delta)^{s_1} + (x^q - x + \delta)^{s_2} + x$ were studied widely, the readers can refer to [4, 8, 11, 12, 13, 14, 16, 17]. Specially, Li et. al. [7] showed that a class of permutation polynomials of the form $(x^q - x + \delta)^{\frac{q^2-1}{3}+1} + x$ by using the piecewise method. Yuan and Zheng [15] further studied several classes of permutation polynomials of the forms similar to

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

where $d = 2, 3, 4, 6$. Furthermore, Zheng, Yuan and Pei [19] gave a class of generalized permutation polynomial having the form

$$f(x) := (ax^q + bx + c)^r \psi((ax^q + bx + c)^{\frac{q^2-1}{d}}) + ux^q + vx$$

over $\mathbf{F}_{q^2}$. In [19], the authors used twice the AGW criterion to explain their results. Firstly, by the AGW criterion, they showed that the permutation property of f by a bijection g between two smaller sets S and $\bar{S}$. Secondly, the authors used the AGW criterion again to show that g is a bijection if and only if h permutes U_n, where U_n is the set of n-th roots of unity in $\mathbf{F}_{q^2}$. Meanwhile, they built the relation between f and h.

Motivated by the piecewise method and the AGW criterion, we can construct a class of generalized permutation polynomials having the form

$$f(x)=\frac{1}{d}\sum_{i=0}^{d-1}X^{r_i}g_i(X^{\frac{q^2-1}{d}})\eta^i\prod_{j=0,j\neq i}^{d-1}(X^{(q^2-1)/d}-\eta^j)+ux^q+vx,$$

where $X:=ax^q+bx+c$ and η is a d-th root of unity. First we use the AGW criterion to transform the permutation property of f on $\mathbf{F}_{q^2}$ to a permutation on a subset S of $\mathbf{F}_{q^2}$. Then we divide S into d different sets, and use the piecewise method to say that g is bijective on S. By combining the piecewise method and the AGW criterion, we can generalize some results of [15, 19].

In [9], the authors proposed several classes of permutation polynomials over $\mathbf{F}_{2^{2m}}$ of the form $(\mathbf{Tr}_m^n(x)^k+\delta)^s+x$ and $(\mathbf{Tr}_m^n(x)^{k_1}+\delta)^{s_1}+(\mathbf{Tr}_m^n(x)^{k_2}+\delta)^{s_2}+x$ based on the AGW criterion. Zha and Hu [18] studied the permutation polynomials having the form $(x^q-x+\delta)^{i(q-1)+1}+x$. Wang and Wu [13] gave the permutation polynomials of the form $(x^{2^m}+x+\delta)^s+x$ over $\mathbf{F}_{2^{2m}}$, where the exponent s is of the form $s=i(2^m-1)+1$. In this paper, motivated by their constructions, by using twice the AGW criterion, we present two classes of permutation polynomials having the forms

$$\sum_{j=0}^{k}(x^q+ax+\delta)^{i_j(q-1)+1}+ax$$

and

$$\sum_{j=0}^{k}(x^q+ax+\delta)^{i_j(q+1)+1}+ax,$$

which generalize some known classes of permutation polynomials.

This paper is organized as follows: In Section 2, we combine the AGW criterion and the piecewise method to characterize a class of permutation polynomials having the form

$$\frac{1}{d}\sum_{i=0}^{d-1}(x^q+ax+\delta)^{r_i}g_i((x^q+ax+\delta)^{\frac{q^2-1}{d}})\eta^i\prod_{j=0,j\neq i}^{d-1}((x^q+ax+\delta)^{(q^2-1)/d}-\eta^j)+ux^q+vx,$$

which generalizes several results of [15]. Moreover, by using twice the AGW criterion, we show that two classes of permutation polynomials of the forms $\sum_{j=0}^{k}(x^q+ax+\delta)^{i_j(q-1)+1}+ax$ and $\sum_{j=0}^{k}(x^q+ax+\delta)^{i_j(q+1)+1}+ax$. In Section 3, by characterizing some special $g_i(x)$ in Theorem 2.1, we present some specific permutation polynomials over $\mathbf{F}_{q^2}$ and deduce some known permutation polynomials. Furthermore, motivated by the piecewise method and the idea of [19], we can give two more general forms of Theorem 2.1 in Section 4.

2 Constructing permutation polynomials by the AGW criterion and the piecewise method

In this section, let d be a positive integer, q satisfy $q\equiv 1(\mathrm{mod}\ d)$ and ξ be a primitive element of $\mathbf{F}_{q^2}$, then we make some denotations: $D_0=<\xi^d>$ and $D_i=\xi^iD_0$, for $1\leq i\leq d-1$.

The following lemma is called AGW criterion, many classes of permutation polynomials can be constructed by using the AGW criterion, some of them can be found in [9, 15, 19].

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);
(ii) h is bijective from S to $\bar{S}$ and f is injective on $\varphi^{-1}(s)$ for each $s \in S$.

The following result will be often used.

Lemma 2.2.[15] *Let $a, \delta \in \mathbf{F}_{q^2}$ satisfy $a^{q+1} = 1$ and $a\delta^q = \delta$. Then we have*

$$Im(x^q + ax + \delta) = Im(ax^q + x + \delta) = \{\xi^{-t}b | b \in \mathbf{F}_q\},$$

where t is the positive integer such that $a = \xi^{(q-1)t}$.

In what follows, we always assume that $a^{q+1} = 1$ and $a\delta^q = \delta$ for $a, \delta \in \mathbf{F}_{q^2}$. For convenience, we introduce the denotation $X := x^q + ax + \delta$.

Theorem 2.1. *Let $g_i(x) \in \mathbf{F}_{q^2}[x]$ for $0 \le i \le d-1$, $1 \ne u \in \mathbf{F}_q$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1} X^{r_i} g_i(X^{\frac{q^2-1}{d}})\eta^i \prod_{j=0, j\ne i}^{d-1} (X^{(q^2-1)/d} - \eta^j) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if

$$x^{r_i}(g_i(\eta^i) + a^{1-r_i} g_i(\eta^i)^q) + (1+u)x$$

is a bijection from D_i to $D_{\sigma(i)}$ for $0 \le i \le d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$.

Proof. Firstly, we introduce some denotations $S = Im(\varphi)$, $\bar{S} = Im(\psi)$, $\varphi(x) = x^q + ax + \delta$, $\psi(x) = ax^q + x + (1+u)\delta$ and

$$g(x) = \sum_{i=0}^{d-1} \Big(x^{r_i}(g_i(x^{(q^2-1)/d}) + a^{1-r_i} g_i(x^{(q^2-1)/d})^q)\eta^i \prod_{j=0, j\ne i}^{d-1} (x^{(q^2-1)/d} - \eta^j) \Big) + (1+u)x.$$

It is easy to check that

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

Namely, the following diagram is commutative.

$$\begin{array}{ccc} \mathbf{F}_{q^2} & \xrightarrow{f} & \mathbf{F}_{q^2} \\ \downarrow\varphi & & \downarrow\psi \\ S & \xrightarrow{g} & \bar{S} \end{array}$$

Since $f(x)$ can be rewritten as

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1}\Big(X^{r_i}g_i(X^{\frac{q^2-1}{d}})\eta^i\prod_{j=0,j\neq i}^{d-1}(X^{(q^2-1)/d}-\eta^j)\Big) + uX - (u-1)ax - u\delta,$$

thus we can easily get that $f(x)$ is injective on $\varphi^{-1}(s)$ for every $s \in Im(\varphi)$. By Lemma 2.1, in order to prove that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^2}$, we only need to prove that $g(x)$ is a bijection from S to $\bar{S}$. It follows from Lemma 2.2 that $S = \bar{S} \subseteq \mathbf{F}_{q^2}$. Since $\mathbf{F}_{q^2} = \{0\} \cup_{i=0}^{d-1} D_i$, it implies that $S = \{0\} \cup_{i=0}^{d-1} (D_i \cap S)$. For $x \in D_i$, one has

$$g(x) = x^{r_i}(g_i(\eta^i) + a^{1-r_i}g_i(\eta^i)^q) + (1+u)x.$$

Thus $g(x)$ is a bijection of S if and only if $x^{r_i}(g_i(\eta^i) + a^{1-r_i}g_i(\eta^i)^q) + (1+u)x$ is a bijection from D_i to $D_{\sigma(i)}$ for $0 \leq i \leq d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$. It follows from Lemma 2.1 that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $x^{r_i}(g_i(\eta^i) + a^{1-r_i}g_i(\eta^i)^q) + (1+u)x$ is a bijection from D_i to $D_{\sigma(i)}$. The proof of Theorem 2.1 is completed. □

Recently, Zha and Hu [18] studied the permutation polynomials having the form $(x^q - x + \delta)^{i(q-1)+1} + x$. Wang and Wu [13] characterized the permutation polynomials of the form $(x^{2^m} + x + \delta)^{i(2^m-1)} + x$ over $\mathbf{F}_{2^{2m}}$, In what follows, we construct a class of permutation polynomials of the form

$$\sum_{j=0}^{k}(x^q + ax + \delta)^{i_j(q-1)+1} + ax,$$

where $i_0, ..., i_k$ are different positive integers.

Theorem 2.2. *Let $i_0, ..., i_k$ be different positive integers and $h(x) := 1 + \sum_{j=0}^{k}(x^{i_j} + x^{-i_j}) \in \mathbf{F}_q[x]$. If $h(x)$ has no roots in μ_{q+1}, where μ_{q+1} is the set of $q+1$-th roots of unity. Then*

$$f(x) = \sum_{j=0}^{k}(x^q + ax + \delta)^{i_j(q-1)+1} + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

Proof. Let

$$\varphi(x) = x^q + ax + \delta, \psi(x) = ax^q + x + \delta,$$

$$g(x) = x\big(1 + \sum_{j=0}^{k}(x^{i_j(q-1)} + x^{-i_j(q-1)})\big)$$

and

$$l(x) = xh(x)^{q-1}.$$

It is easy to check that

$$\psi \circ f = g \circ \varphi$$

and

$$x^{q-1} \circ g = l \circ x^{q-1}.$$

Namely, the following diagrams are commutative.

$$\begin{array}{ccc} \mathbf{F}_{q^2} & \xrightarrow{f} & \mathbf{F}_{q^2} \\ \downarrow\varphi & & \downarrow\psi \\ S & \xrightarrow{g} & S \\ \downarrow x^{q-1} & & \downarrow x^{q-1} \\ T & \xrightarrow{l} & T \end{array},$$

where $S = \{\xi^{-t}b | b \in \mathbf{F}_q\}$ and $T = \{\xi^{-t(q-1)}\}$, where t is the positive integer such that $a = \xi^{(q-1)t}$. We can immediately deduce that $T \subseteq \mu_{q+1}$. Since $h(x)$ has no roots in μ_{q+1} and $h(x)$ is a self-reciprocal polynomial, we can easily check that

$$l(x) = xh(x)^{q-1} = x\frac{h(x)^q}{h(x)} = x\frac{h(1/x)}{h(x)} = x,$$

for $x \in T$. Thus l is bijective on T. Furthermore, we can infer that g is injective on the set $\{s \in S | s^{q-1} = t^{'}, t^{'} \in T\}$. Therefore, by the AGW criterion, it implies that g is a bijection on S. We can also immediately check that f is injective on the set $\{x \in \mathbf{F}_{q^2} | \varphi(x) = s, s \in S\}$. By using the AGW criterion again, we can conclude that $f(x)$ is a permutation polynomial of $\mathbf{F}_{q^2}$. □

Specially, we can get the following result.

Corollary 2.1. *Let q be the power of a prime satisfying $(3, q+1) = 1$, and i be a positive integer. Then*

$$f(x) = (x^q + ax + \delta)^{i(q-1)+1} + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

Proof. In Theorem 2.2, by taking $k = 0$, one has $h(x) = 1 + x^i + x^{-i}$. Since $(3, q+1) = 1$, it follows that $h(x)$ has no roots in μ_{q+1}. Then by using Theorem 2.2, we can get Corollary 2.1 immediately. □

Similarly, we can also get the following result.

Theorem 2.3. *Let $i_0, ..., i_k$ be positive integers. Then*

$$f(x) := \sum_{j=0}^{k} (x^q + ax + \delta)^{i_j(q+1)+1} + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if

$$l(x) := x\big(1 + \sum_{j=0}^{k} 2x^{i_j}\big)^2$$

is a bijection on T, where $T := \{\xi^{-t(q+1)}b^2 | b \in \mathbf{F}_q\}$, where t is the positive integer such that $a = \xi^{(q-1)t}$.

Proof. First we introduce the following denotations.

$$\varphi(x) = x^q + ax + \delta, \psi(x) = ax^q + x + \delta,$$

$$g(x) = x\big(1 + \sum_{j=0}^{k} (2x^{i_j(q+1)})\big)$$

and

$$l(x) = xh(x)^2,$$

where $h(x) = 1 + \sum_{j=0}^{k} 2x^{i_j}$. It is easy to check that

$$\psi \circ f = g \circ \varphi$$

and

$$x^{q+1} \circ g = l \circ x^{q+1}.$$

Namely, the following diagrams are commutative.

$$\begin{array}{ccc} \mathbf{F}_{q^2} & \xrightarrow{f} & \mathbf{F}_{q^2} \\ \downarrow\varphi & & \downarrow\psi \\ S & \xrightarrow{g} & S \\ \downarrow x^{q+1} & & \downarrow x^{q+1} \\ T & \xrightarrow{l} & T \end{array},$$

where $S = \{\xi^{-t}b | b \in \mathbf{F}_q\}$. It is trivial to check that $T \subseteq \mathbf{F}_q$, thus $l(x) = xh(x)^2 = xh(x)^{q+1}$ for $x \in T$. Then we can easily check that g is injective on the set $\{s \in S | s^{q+1} = t', t' \in T\}$, it follows from Lemma 2.1 that l is bijective on T is equivalent to g is bijective on S. Furthermore, by using the AGW criterion again and checking that f is injective on the set $\{x \in \mathbf{F}_{q^2} | \varphi(x) = s, s \in S\}$, we can get that $f(x)$ is a permutation polynomial of $\mathbf{F}_{q^2}$ if and only if g is a bijection on S. Therefore, $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $l(x)$ is a bijection of T. □

In Theorem 2.3, T is a subset of $\mathbf{F}_q$ and $l(x)$ is surjective on T. Thus if $l(x)$ is a permutation polynomial of $\mathbf{F}_q$, then $l(x)$ is a bijection of T. Based on this fact, we can get some permutation polynomials of $\mathbf{F}_{q^2}$ from some known permutation polynomials of $\mathbf{F}_q$.

Corollary 2.2. *Let $i_0, ..., i_k$ be positive integers. If*

$$l(x) := x\big(1 + \sum_{j=0}^{k} 2x^{i_j}\big)^2$$

is a permutation polynomial of $\mathbf{F}_q$, then

$$f(x) := \sum_{j=0}^{k} (x^q + ax + \delta)^{i_j(q+1)+1} + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

By the proof of Theorem 2.3, we can get a more general result than Theorem 2.3 in the following.

Theorem 2.4. *Let $i_0, ..., i_k$ be positive integers and $f_j(x) \in \mathbf{F}_q[x]$ for $0 \le j \le k$. Then*

$$f(x) := (x^q + ax + \delta) \sum_{j=0}^{k} f_j((x^q + ax + \delta)^{i_j(q+1)}) + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if

$$l(x) := x\big(1 + \sum_{j=0}^{k} 2f_j(x^{i_j})\big)^2$$

is a bijection of T, where $T := \{\xi^{-t(q+1)}b^2 | b \in \mathbf{F}_q\}$, where t is the positive integer such that $a = \xi^{(q-1)t}$.

Proof. The proof of Theorem 2.4 is similar to that of Theorem 2.3, we omit it here. □

3 Special permutation polynomials

In this section, we will show some special cases of Theorem 2.1. In what follows, we also assume that $a, \delta \in \mathbf{F}_{q^2}$ satisfy $a^{q+1} = 1, a\delta^q = \delta$ and use the denotation $X := x^q + ax + \delta$. First, by taking $g_i(x)$ as a constant in Theorem 2.1, we can get some special permutation polynomials.

Theorem 3.1. *Let $c_i \in \mathbf{F}_{q^2}$ for $0 \le i \le d-1$, $1 \ne u \in \mathbf{F}_q$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\Big(\sum_{i=0}^{d-1} c_i X^{r_i}\eta^i \prod_{j=0, j\ne i}^{d-1}(X^{(q^2-1)/d} - \eta^j)\Big) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $x^{r_i}(c_i + a^{1-r_i}c_i^q) + (1+u)x$ is a bijection from D_i to $D_{\sigma(i)}$ for $0 \le i \le d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$.

Proof. Taking $g_i(x) = c_i$ in Theorem 2.1, we can get Theorem 3.1 immediately. □

If $c_i + a^{1-r_i}c_i^q = 0$ for $0 \le i \le d-1$ in Theorem 3.1, we can get the following result.

Corollary 3.1. *Let $c_i \in \mathbf{F}_{q^2}$ for $0 \le i \le d-1$, $u \in \mathbf{F}_q$, let $r_0, r_1, ..., r_{d-1}$ be integers and η be a d-th root of unity. If $c_0, c_1, ..., c_{d-1}$ satisfy $c_i + a^{1-r_i}c_i^q = 0$ for $0 \le i \le d-1$ and $u \notin \{1, -1\}$. Then*

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1}\Big(c_i X^{r_i}\eta^i \prod_{j=0, j\ne i}^{d-1}(X^{(q^2-1)/d} - \eta^j)\Big) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

Corollary 3.2. *Let $c_i \in \mathbf{F}_{q^2}$ and $r_0, r_1, ..., r_{d-1}$ be integers with $c_i + a^{1-r_i}c_i^q \in D_0$ for $0 \le i \le d-1$. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1}\Big(c_i X^{r_i}\eta^i \prod_{j=0, j\ne i}^{d-1}(X^{(q^2-1)/d} - \eta^j)\Big) + ax - x^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $\gcd(r_i, (q^2-1)/d) = 1$ for $0 \le i \le d-1$.

Proof. By Theorem 3.1, it follows from $c_i + a^{1-r_i}c_i^q \in D_0$ that $f(x)$ is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $x^{r_i}(c_i + a^{1-r_i}c_i^q)$ is a bijection from D_i to D_i for $0 \le i \le d-1$. Since $x^{r_i}(c_i + a^{1-r_i}c_i^q)$ is bijective on D_i if and only if $\gcd(r_i, (q^2-1)/d) = 1$. Thus Corollary 3.2 is true. □

Next, picking $g_i(x) = x$ in Theorem 2.1, we can get the following result.

Theorem 3.2. *Let $1 \ne u \in \mathbf{F}_q$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\Big(\sum_{i=0}^{d-1} X^{\frac{q^2-1}{d}+r_i}\eta^i \prod_{j=0, j\ne i}^{d-1}(X^{(q^2-1)/d} - \eta^j)\Big) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ *if and only if* $x^{r_i}(1+a^{1-r_i})\eta^i+(1+u)x$ *is a bijection from* D_i *to* $D_{\sigma(i)}$ *for* $0 \le i \le d-1$, *where* σ *is a permutation on the set* $\{0,1,...,d-1\}$.

Specially, for $d=2$, we have the following result.

Corollary 3.3. *Let* r *be an integer and* q *be the power of an odd prime. If* $u \in \mathbf{F}_q$ *and* $u \neq -1$. *Then*

$$f(x) = X^{\frac{q^2-1}{2}+r} - ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ *if and only if* $x^r(1+a^{1-r})+(u-1)x$ *is a bijection from* D_0 *to* $D_i (i=0$ *or* $1)$, *and* $-x^r(1+a^{1-r})+(u-1)x$ *is a bijection from* D_1 *to* $D_j (j=0$ *or* $1)$, *where* $\{i,j\}=\{0,1\}$.

For $r=1$ in Corollary 3.3, we can get the result of [15].

Corollary 3.4. **[15]** *Let* $p \neq 3$ *and* $q=p^m$ *for a positive integer* m. *Then*

$$f(x) = X^{\frac{q^2-1}{2}+1} - ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

Proof. For $r=1$ in Corollary 3.3, it implies that $f(x)$ permutes $\mathbf{F}_{q^2}$ if and only if x is a bijection on D_0 and $-3x$ is a bijection on D_1. It is easy to check that x is a bijection on D_0 and $-3x$ is a bijection on D_1. Thus Corollary 3.4. is true. □

For $d=3$, we have the following result.

Corollary 3.5. *Let* r_1, r_2, r_3 *be integers and* $q \equiv 1 (\mathrm{mod}\ 3)$. *Let* η *be a* 3*-rd root of unity. If* $u \in \mathbf{F}_q$ *and* $u \neq -1$. *Then*

$$f(x) = X^{\frac{q^2-1}{3}+r_1}(1+X^{\frac{q^2-1}{3}}+X^{2\frac{q^2-1}{3}}) + X^{\frac{q^2-1}{3}+r_2}(1+\eta^2 X^{\frac{q^2-1}{3}}+\eta X^{2\frac{q^2-1}{3}})$$

$$+X^{\frac{q^2-1}{3}+r_3}(1+\eta X^{\frac{q^2-1}{3}}+\eta^2 X^{2\frac{q^2-1}{3}}) - ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ *if and only if* $x^{r_i}(1+a^{1-r_i})\eta^i+(u-1)x$ *is a bijection from* D_i *to* $D_{\sigma(i)}$ *for* $0 \le i \le 2$, *where* σ *is a permutation on the set* $\{0,1,2\}$.

In what follows, as a special case of Corollary 3.5, by taking $r_1=r_2=r_3=1$, we can get a result of [15].

Corollary 3.6. **[15]** *Let* $p \neq 7$. *Then*

$$f(x) = X^{\frac{q^2-1}{3}+1} - ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ *if and only if* $(2\eta-1, 2\eta^2-1) \in D_0 \times D_0$ *or* $D_1 \times D_2$.

In the following, we consider the case of $g_i(x) = \sum_{i=0}^{d-1} x^i$. For $1 \le i \le d-1$, one has $\sum_{i=0}^{d-1} \eta^i = 0$, where η is a d-th root of unity. If we take g_i to be $\sum_{i=0}^{d-1} x^i$ for $0 \le i \le d-1$, then we can get the following result.

Theorem 3.3. *Let $r_0, r_1, ..., r_{d-1}$ be integers and η be a d-th root of unity. If $u \neq 1 \in \mathbf{F}_q$ and $u+1 \in D_0$, then*

$$f(x) = \frac{1}{d}\Big(\sum_{i=0}^{d-1} X^{r_i} \sum_{k=0}^{d-1} (X^{k\frac{q^2-1}{d}})\eta^i \prod_{j=0, j\neq i}^{d-1} (X^{(q^2-1)/d} - \eta^j)\Big) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $d(1+a^{1-r_0})x^{r_0} + (u+1)x$ is a bijection of D_0.

Proof. Since $\sum_{i=0}^{d-1} \eta^i = 0$ for $1 \le i \le d-1$, it follows from Theorem 2.1 that $f(x)$ is a permutation polynomial of $\mathbf{F}_{q^2}$ if and only if $(u+1)x$ is a bijection on D_i for $1 \le i \le d-1$ and $d(1+a^{1-r_0})x^{r_0} + (u+1)x$ is a bijection of D_0. Thus Theorem 3.3 is true.

□

Now we can choose $g_i(x)$ in different ways. If we take $g_0(x) = c$ with c satisfying $c + a^{1-r_0}c^q = 0$, and $g_i(x) = \sum_{i=0}^{d-1} x^i$ for $1 \le i \le d-1$, then we have

Corollary 3.7. *Let $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\Big(cX^{r_0}\eta^i \prod_{j=1}^{d-1} (X^{(q^2-1)/d} - \eta^j) + \sum_{i=1}^{d-1} X^{r_i} \sum_{k=0}^{d-1} (X^{k\frac{q^2-1}{d}})\eta^i \prod_{j=0, j\neq i}^{d-1} (X^{(q^2-1)/d} - \eta^j)\Big) + ax$$

is a permutation polynomial over $\mathbf{F}_{q^2}$.

Finally, let $g_i(x)$ belong to $\mathbf{F}_q[x]$, then we deduce the following result directly from Theorem 2.1.

Theorem 3.4. *Let $g_i(x) \in \mathbf{F}_q[x]$ for $0 \le i \le d-1$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. If $u \in \mathbf{F}_q$ and $u \neq -1$. Then*

$$f(x) = \frac{1}{d}\Big(\sum_{i=0}^{d-1} X^{r_i} g_i(X^{\frac{q^2-1}{d}})\eta^i \prod_{j=0, j\neq i}^{d-1} (X^{(q^2-1)/d} - \eta^j)\Big) + ax + ux^q$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $g_i(\eta^i)(1+a^{1-r_i})x^{r_i} + (u+1)x$ is a bijection from D_i to $D_{\sigma(i)}$ for $0 \le i \le d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$.

4 Generalized forms of Theorem 2.1

In this section, we assume that $q \equiv 1 (\mathrm{mod}\ d)$, a, b, c, u, v are in $\mathbf{F}_{q^2}$ and satisfy $a^{q+1} = b^{q+1}$, $ac^q = b^q c$. Let $A = bu - av$, $B = au^q - bv^q$, $C = (u^{q+1} - v^{q+1})c$ and $X = ax^q + bx + c$. In the following, we can generalize Theorem 2.1 and get the following results.

Theorem 4.1. *Let $g_i(x) \in \mathbf{F}_{q^2}[x]$ for $0 \le i \le d-1$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1} X^{r_i} g_i(X^{\frac{q^2-1}{d}})\eta^i \prod_{j=0, j\neq i}^{d-1} (X^{(q^2-1)/d} - \eta^j) + ux^q + vx$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $x^{r_i}(Bg_i(\eta^i) + A^{1-r_i}B^{qr}g_i(\eta^i)^q) + (u^{q+1} - v^{q+1})x$ is a bijection from D_i to $D_{\sigma(i)}$ for $0 \le i \le d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$.

Proof. The proof of Theorem 4.1 is similar to that of Theorem 2.1. Some details can also be referred to [19]. Here we omit it. □

Remark. We notice that if $r_0 = r_1 = ... = r_{d-1} = r$ and $g_0(x) = g_1(x) = ... = g_{d-1}(x) = \psi(x)$, then Theorem 4.1 becomes Theorem 1 in [19].

Furthermore, we get a more general form of Theorem 4.1.

Theorem 4.2. *Let $g_i(x) \in \mathbf{F}_{q^2}[x]$ for $0 \le i \le d-1$, $\theta(x) \in \mathbf{F}_q[x]$ and $r_0, r_1, ..., r_{d-1}$ be integers. Let η be a d-th root of unity. Then*

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1} \Big(\sum_{j=0}^{d-1} X^{r_j} g_j(X^{\frac{q^2-1}{d}})\eta^{-ji}\Big)\theta(X^{(q^2-1)/d})^i + ux^q + vx$$

is a permutation polynomial over $\mathbf{F}_{q^2}$ if and only if $x^{r_i}(Bg_i(\eta^i) + A^{1-r_i}B^{qr}g_i(\eta^i)^q) + (u^{q+1} - v^{q+1})x$ is a bijection from D_i to $D_{\sigma(i)}$ for $0 \le i \le d-1$, where σ is a permutation on the set $\{0, 1, ..., d-1\}$, and $\theta(x^{\frac{q^2-1}{d}}) = \eta^i$ for $x \in D_i$.

Proof. In Theorem 4.2, we notice that $\theta(x)$ is a piecewise function on $\mathbf{F}_{q^2}$. The other proof of Theorem 4.2 is similar to that of Theorem 4.1. □

Acknowledgement. The authors thank the anonymous reviewer for his/her valuable suggestions and detailed comments which significantly improved both the quality and the presentation of this paper. Qin was Supported by National Science Foundation of China (Grant No.11926344) and the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJQN201901402) ; Yan was Supported by the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJQN201900506).

References

[1] A. Akbary, D. Ghioca, Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.*, **17**, 51-67 (2011).

[2] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.*, **11**, 65-120 (1896/97).

[3] C. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris*, **57**, 750-757 (1863).

[4] R. Gupta, R. K. Sharma, Further results on permutation polynomials of the form $x^{p^m} - x + \delta)^s + x$ over $\mathbf{F}_{p^{2m}}$, *Finite Fields Appl.*, **50**, 196-208 (2018).

[5] X. Hou, Permutation polynomials over finite fields-A survey of recent advances, *Finite Fields Appl.*, **32**, 82-119 (2015).

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

[7] N. Li, T. Helleseth, X. Tang, Further results on a class of permutation polynomials over finite fields, *Finite Fields Appl.*, **22**, 16-23 (2013).

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

[9] Z. Li, M. Wang, J. Wu, S. Zhu, Some new forms of permutation polynomials based on the AGW criterion, *Finite Fields Appl.*, **61**, 101584 (2020).

[10] G. L. Mullen, D. Panario, *Handbook of finite fields*, CRC Press, (2013).

[11] Z. Tu, X. Zeng, C. Li, T. Helleseth, Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $\mathbf{F}_{p^{2m}}$ of odd characteristic, *Finite Fields Appl.*, **34**, 20-35 (2015).

[12] L. Wang, B. Wu, Z. Liu, Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbf{F}_{p^{2m}}$, *Finite Fields Appl.*, **44**, 92-112 (2017).

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

[14] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, *Finite Fields Appl.*, **14**, 482-493 (2008).

[15] P. Yuan, Y. Zheng, Permutation polynomials from piecewise functions, *Finite Fields Appl.*, **35**, 215-230 (2015).

[16] P. Yuan, Permutation Polynomials from two piecewise functions, 2019 Ninth International Workshop on Signal Design and its Applications in Communications, (2020).

[17] X. Zeng, X. Zhu, N. Li , X. Liu, Permutation polynomials over $\mathbf{F}_{2^{2m}}$ of the form $(x^{2^i} + x + \delta)^{s_1} + (x^{2^i} + x + \delta)^{s_2} + x$, *Finite Fields Appl.*, **47**, 256-268 (2017).

[18] Z. Zha, L. Hu, Some classes of permutation polynomials of the form $(x^{p^m}-x+\delta)^s+x$ over $\mathbf{F}_{p^{2m}}$, *Finite Fields Appl.*, **40**, 150-162 (2016).

[19] Y. Zheng , P. Yuan, D. Pei, Large classes of permutation polynomials over $\mathbf{F}_{q^2}$, *Des. Codes Cryptogr.*, **81**, 505-521 (2016).

Received: 13.07.2020
Revised: 16.11.2020
Accepted: 31.01. 2021

(1) School of Mathematics and Statistics
Yangtze Normal University, Chongqing 408100, P.R. China
E-mail: qincn328@sina.com

* Corresponding author
(2) School of Mathematical Sciences
Chongqing Normal University, Chongqing 401331, P.R. China
E-mail: yanl930@163.com