Cryptogr. Commun. (2018) 10:567–578
DOI 10.1007/s12095-017-0234-9

New results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x^{p^m} + x$ over $\mathbb{F}_{p^{2m}}$

Zhengbang Zha[1,3] · Lei Hu[2,4] · Zhizheng Zhang[1]

Received: 16 July 2016 / Accepted: 15 June 2017 / Published online: 5 July 2017

Abstract Permutation polynomials over finite fields have significant applications in coding theory, cryptography, combinatorial designs and many other areas of mathematics and engineering. In this paper, we study the permutation behavior of polynomials with the form $(x^{p^m} - x + \delta)^s + x^{p^m} + x$ over the finite field $\mathbb{F}_{p^{2m}}$. By using the Akbary-Ghioca-Wang (AGW) criterion, we present several new classes of permutations over $\mathbb{F}_{p^{2m}}$ based on some bijections over the set $\{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$ or the subfield $\mathbb{F}_{p^m}$.

Keywords Finite field · Permutation polynomial · Trace function

Mathematics Subject Classification (2000) 05A05 · 11T06 · 11T55

1 Introduction

Let p be a prime, n be a positive integer and $\mathbb{F}_{p^n}$ be a finite field with p^n elements. A polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_{p^n}$ if it induces a

✉ Zhengbang Zha
zhazhengbang@163.com

Lei Hu
hu@is.ac.cn

Zhizheng Zhang
zhzhzhang-yang@163.com

[1] School of Mathematical Sciences, Luoyang Normal University, Luoyang 471934, China

[2] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

[3] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China

[4] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

bijection from $\mathbb{F}_{p^n}$ to itself. A linearized polynomial or p-polynomial [10, Definition 3.49] over $\mathbb{F}_{p^n}$ is defined by

$$L(x) = \sum_{i=0}^{n-1} a_i x^{p^i} \in \mathbb{F}_{p^n}[x].$$

It has a unique zero root in $\mathbb{F}_{p^n}$ if and only if $L(x)$ permutes $\mathbb{F}_{p^n}$, which means that the equation $L(x) + b = 0$ has a unique nonzero solution for any $b \in \mathbb{F}_{p^n} \setminus \{0\}$. PPs are an interesting subject of mathematics and engineering, and have significant applications in coding theory, cryptography, combinatorial designs and so on. For more details of the recent advances and contributions to the area, the reader is referred to [4, 7, 12, 20] and the references therein.

Helleseth and Zinoviev [6] first proposed PPs of the form

$$\left(\frac{1}{x^2 + x + \delta}\right)^{2^l} + x$$

for the goal of deriving new identities on Kloosterman sums over $\mathbb{F}_{2^n}$, where $\delta \in \mathbb{F}_{2^n}$ and $l = 0$ or 1. Yuan et al. [15, 16] further investigated the permutation behavior of the polynomials with the form

$$(x^{p^k} - x + \delta)^s + L(x) \tag{1}$$

over $\mathbb{F}_{p^n}$, where k, s are integers, $\delta \in \mathbb{F}_{p^n}$ and $L(x)$ is a linearized polynomial. Akbary et al. [1] proposed a criterion of PPs by the following lemma:

Lemma 1 [1] *(The AGW criterion) Let A, S and $\overline{S}$ be finite sets with $\sharp S = \sharp \overline{S}$, and let $f : A \to A$, $h : S \to \overline{S}$, $\lambda : A \to S$ and $\overline{\lambda} : A \to \overline{S}$ be maps such that $\overline{\lambda} \circ f = h \circ \lambda$. If both λ and $\overline{\lambda}$ are surjective, then the following statements are equivalent:*

(1) *f is a bijection (a permutation over A); and*
(2) *h is a bijection from S to $\overline{S}$ and f is injective on $\lambda^{-1}(t)$ for each $t \in S$.*

Yuan and Ding [17, 18] gave a unified treatment of some earlier constructions of PPs and get many new specific PPs by using the AGW criterion. Followed by Yuan and Ding's work, many researchers began to study PPs having the form as in (1). They obtained many important results and advances, which can be seen in [3, 9, 19, 21, 23] and the references therein.

Very recently, Tu et al. [13, 14] presented several classes of PPs over $\mathbb{F}_{p^{2m}}$ with the form (1), where $k = m$, s and m are integers satisfying $s \equiv 1 (\mathrm{mod}\ p^m + 1)$ or $s \equiv 1 (\mathrm{mod}\ p^m - 1)$. For this kind of exponents s, Zeng et al. [22] proposed several classes of PPs based on trace functions over $\mathbb{F}_{2^n}$. This motivated Zha and Hu [24] to construct PPs of the form (1) with new such exponents s.

As we know, both $x^{p^m} - x$ and $x^{p^m} + x$ are not permutations on $\mathbb{F}_{p^{2m}}$. In this paper, we further study the permutation behavior of polynomials with the form

$$(x^{p^m} - x + \delta)^s + x^{p^m} + x$$

over $\mathbb{F}_{p^{2m}}$. By using the AGW criterion, we find some new exponents s and present several new classes of PPs over $\mathbb{F}_{p^{2m}}$ based on some bijections over the set $\{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$ or the subfield $\mathbb{F}_{p^m}$.

The rest of this paper is organized as follows. In Section 2, some preliminaries needed later are presented. In Section 3, we propose three classes of PPs based on some bijections over the set $\{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$. In Section 4, by determining some bijections over the

subfield $\mathbb{F}_{p^m}$ we exhibit some new classes of PPs with exponents $s = ip^j(p^m + 1) + p^j$ or $ip^j(p^m + 1) + 2p^j$ for some integers i and j. Finally, we conclude the paper in Section 5.

2 Preliminaries

Throughout this paper, we always let p be an odd prime, and let j, s, m and n be positive integers. Denote the multiplicative group of $\mathbb{F}_{p^m}$ by $\mathbb{F}_{p^m}^*$. For each element δ in the finite field $\mathbb{F}_{p^{2m}}$, we denote δ^{p^m} by $\overline{\delta}$ in analogy with the usual complex conjugation. Obviously, $\delta + \overline{\delta} \in \mathbb{F}_{p^m}$ and $\delta\overline{\delta} \in \mathbb{F}_{p^m}$. Denote the p-adic order of an integer m by $v_p(m)$ and let $v_p(m) = n$ if $p^n | m$ and $p^{n+1} \nmid m$.

By the AGW criterion, we have the following propositions.

Proposition 1 *Let $\delta \in \mathbb{F}_{p^{2m}}$. The polynomial $f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$ induces a permutation on $\mathbb{F}_{p^{2m}}$ if and only if the polynomial*

$$h(t) = (-t + \overline{\delta})^s - (t + \delta)^s$$

is a bijection over the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$.

Proof Note that the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$ can be denoted as $\{x^{p^m} - x | x \in \mathbb{F}_{p^{2m}}\}$. Let $\lambda(x) = \overline{\lambda}(x) = x^{p^m} - x$ and $h(x) = (x + \delta)^{s \cdot p^m} - (x + \delta)^s$. It can be verified that the following diagram commutes

$$\begin{array}{ccc} \mathbb{F}_{p^{2m}} & \xrightarrow{f} & \mathbb{F}_{p^{2m}} \\ {\scriptstyle x^{p^m}-x}\downarrow & & \downarrow{\scriptstyle x^{p^m}-x} \\ S & \xrightarrow[h]{} & S. \end{array}$$

For each $t \in S$, we have that $\lambda^{-1}(t) = \{x \in \mathbb{F}_{p^{2m}} | x^{p^m} - x = t\}$ and $f(x) = (t+\delta)^s + t + 2x$ is injective on $\lambda^{-1}(t)$. Then by the AGW criterion, f permutes $\mathbb{F}_{p^{2m}}$ if and only if

$$h(t) = (t + \delta)^{s \cdot p^m} - (t + \delta)^s = (-t + \overline{\delta})^s - (t + \delta)^s$$

is a bijection over S. □

Remark 1 Let $\lambda \in \mathbb{F}_{p^m}^*$. We note that $t \in S$ if and only if $\lambda t \in S$, where S is defined in Proposition 1.

Proposition 2 *Let $\delta \in \mathbb{F}_{p^{2m}}$. The polynomial $f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$ if and only if the polynomial $g(x) = (x^{p^m} - x + \delta)^{s \cdot p^j} + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$ for any integer $j \geq 0$.*

Proof According to Proposition 1, the polynomials $f(x)$ and $g(x)$ permute $\mathbb{F}_{p^{2m}}$ if and only if $h(t) = (-t+\overline{\delta})^s - (t+\delta)^s$ and $h^{p^j}(t)$ permute S respectively. Moreover, the mapping $h(t)$ is a bijection on S if and only if $h^{p^j}(t)$ is a bijection on S. Hence the proof is completed. □

3 Three classes of PPs over $\mathbb{F}_{p^{2m}}$ derived from bijections over the set $\{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$

In this section, we present three classes of permutation polynomials over $\mathbb{F}_{p^{2m}}$ by applying Propositions 1 and 2.

Theorem 1 *Let $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} = 0$. Then*

$$f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$$

permutes $\mathbb{F}_{p^{2m}}$ if and only if s is odd and $\gcd(s, p^m - 1) = 1$.

Proof By Proposition 1, $f(x)$ permutes $\mathbb{F}_{p^{2m}}$ if and only if $h(t) = (-t + \overline{\delta})^s - (t + \delta)^s$ is a bijection on the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$. Since $\delta + \overline{\delta} = 0$, we get $(t+\delta)^{p^m} + t + \delta = 0$, which implies that $t + \delta = 0$ or $(t + \delta)^{2(p^m-1)} = 1$. It can be easily checked that

$$h(t) = (t + \delta)^s((-1)^s - 1).$$

If s is even, $h(t) = 0$ is not a bijection on S. If s is odd and $\gcd(s, p^m - 1) = i > 1$, then there exist two different values $t_1, t_2 \in S$ such that $t_1 + \delta = \beta(t_2 + \delta)$ and $h(t_1) = h(t_2)$, where $\beta \in \mathbb{F}_{p^m}$, $\beta^i = 1$ and $\beta \neq 1$. It follows that $h(t)$ is not a bijection on S. If s is odd and $\gcd(s, p^m - 1) = 1$, then $\gcd(s, 2(p^m - 1)) = 1$. It can be verified that $h(t) = 2(t+\delta)^s$ is an injection on S, which implies that $h(t)$ permutes S. Hence the proof is finished. □

Theorem 2 *Let k be an integer with $k < m$ and let $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} \neq 0$. Then*

$$f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$$

permutes $\mathbb{F}_{p^{2m}}$ in the following two cases:

(i) $s = p^j$ *or* $2p^j$*;*
(ii) $s = (p^k + 1) \cdot p^j$ *with* $\frac{m-k}{\gcd(m,k)}$ *is odd.*

Proof By Propositions 1 and 2, we just need to prove that $h(t) = (-t + \overline{\delta})^s - (t + \delta)^s$ is a bijection on the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$ in the case of $j = 0$.

(i) If $s = 1$, $h(t) = -2t + \overline{\delta} - \delta$ is an affine permutation of S. If $s = 2$, $h(t) = -2(\overline{\delta} + \delta)t + \overline{\delta}^2 - \delta^2$ is also an affine permutation of S since $\delta + \overline{\delta} \neq 0$.

(ii) If $s = p^k + 1$, then $h(t) = -(\overline{\delta}+\delta)t^{p^k} - (\overline{\delta}+\delta)^{p^k}t + \overline{\delta}^{p^k+1} - \delta^{p^k+1}$. Since $\delta + \overline{\delta} \neq 0$, $h(t)$ is a bijection on S if and only if

$$h_1(t) = h((\overline{\delta} + \delta)t) = -(\overline{\delta} + \delta)^{p^k+1}(t^{p^k} + t) + \overline{\delta}^{p^k+1} - \delta^{p^k+1}$$

is a bijection on S. Assume $t_1, t_2 \in S$ with $t_1 \neq t_2$ and $h_1(t_1) = h_1(t_2)$. It leads to $(t_1 - t_2)^{p^m} + (t_1 - t_2) = 0$ and $(t_1 - t_2)^{p^k} + (t_1 - t_2) = 0$. Let $u = t_1 - t_2$. Then we have $u \neq 0$ and

$$u^{p^m-1} = u^{p^k-1} = -1,$$

which implies that $u^{p^{m-k}-1} = 1$, i.e., $u \in \mathbb{F}^*_{p^{m-k}}$. We note that $u^{p^k-1} = -1$ has a solution u in $\mathbb{F}^*_{p^{m-k}}$ if and only if $\frac{m-k}{\gcd(k,m-k)}$ is even. Since $\gcd(k, m-k) = \gcd(m, k)$

and $\frac{m-k}{\gcd(m,k)}$ is odd, there is no solution of $u^{p^k-1} = -1$ over $\mathbb{F}^*_{p^{m-k}}$. Therefore, $h_1(t)$ and $h(t)$ are bijections on S.

□

Lemma 2 [5] *Let a, b be integers and $l = \gcd(a, b)$. Let $a' = a/l$ and $b' = b/l$. Then*

$$\gcd(p^a + 1, p^b - 1) = \begin{cases} p^l + 1, & \text{for odd } a' \text{ and even } b', \\ 2, & \text{otherwise.} \end{cases}$$

Theorem 3 *Let k be an integer and $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} \neq 0$. Then*

$$f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$$

permutes $\mathbb{F}_{p^{2m}}$ in the following cases:

(i) $p = 3$, $s = \frac{(3^k+1)\cdot 3^j}{2}$ *or* $\frac{(3^{2m}+3^{k+1}+2)\cdot 3^j}{2}$, *where* $\gcd(k, 2m) = 1$;
(ii) $s = \frac{(p^k+1)\cdot p^j}{2}$ *or* $\frac{(p^{2m}+p^{k+1}+p-1)\cdot p^j}{2}$, *where* $v_2(k) \geq v_2(2m)$.

Proof Let $S_1 = \{z \in \mathbb{F}_{p^{2m}} | z+\overline{z} = \delta+\overline{\delta}\}$ and ρ be a mapping from S_1 to S with $\rho(z) = z-\delta$. It is clear that ρ is a one to one mapping. According to Proposition 1, we need to prove that $h(t) = (-t + \overline{\delta})^s - (t + \delta)^s$ is a bijection on the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$, which is equivalent that

$$h \circ \rho(z) = (-1)^s(z - \delta - \overline{\delta})^s - z^s (:= h_1(z))$$

is a one to one mapping from $S_1 = \{z \in \mathbb{F}_{p^{2m}} | z + \overline{z} = \delta + \overline{\delta}\}$ to S. Note that $|S_1| = |S|$. It is sufficient to show that for any $\gamma \in S$, there is at most one solution $z \in S_1$ of equation

$$h_1(z) = \gamma. \tag{2}$$

Let $u = \frac{\overline{\delta}+\delta}{4}$ and $z = \eta + \frac{u^2}{\eta} + 2u$, where $\eta \in \mathbb{F}^*_{p^{2m}}$ satisfying $\overline{\eta} + \eta = 0$ or $\overline{\eta}\eta + u^2 = 0$. Then $z = \frac{(\eta+u)^2}{\eta}$ and $z - \delta - \overline{\delta} = \eta + \frac{u^2}{\eta} - 2u = \frac{(\eta-u)^2}{\eta}$. Equation (2) can be written as

$$h_1\left(\eta + \frac{u^2}{\eta} + 2u\right) = \frac{(-1)^s(\eta - u)^{2s} - (\eta + u)^{2s}}{\eta^s} = \gamma. \tag{3}$$

By Proposition 2, we only consider the following exponents s in the case of $j = 0$.

(i) Since $\gcd(k, 2m) = 1$, both $\frac{3^k+1}{2}$ and $\frac{3^{2m}+3^{k+1}+2}{2}$ are even. If $s = \frac{3^k+1}{2}$, (3) turns to be

$$\begin{aligned} h_1(\eta + \frac{u^2}{\eta} + 2u) &= \frac{(\eta - u)^{3^k+1} - (\eta + u)^{3^k+1}}{\eta^{(3^k+1)/2}} = \frac{-2u\eta^{3^k} - 2u^{3^k}\eta}{\eta^{(3^k+1)/2}} \\ &= -2u(\eta^{\frac{3^k-1}{2}} + (\frac{u^2}{\eta})^{\frac{3^k-1}{2}}) = \gamma. \end{aligned} \tag{4}$$

Assume $\theta = \eta^{\frac{3^k-1}{2}}$. Equation (4) turns to

$$-2u\left(\theta + \frac{u^{3^k-1}}{\theta}\right) = \gamma.$$

Since $\delta + \overline{\delta} \neq 0$ and $\eta \in \mathbb{F}^*_{3^{2m}}$, we obtain $u \neq 0$ and $\theta \neq 0$. The above equation implies that

$$\theta^2 + \frac{\gamma}{2u}\theta + u^{3^k-1} = 0,$$

which has at most two solutions θ_1 and θ_2 with $\theta_1\theta_2 = u^{3^k-1}$. Note that

$$\gcd\left(\frac{3^k-1}{2}, 3^{2m}-1\right) = \frac{3^{\gcd(k,2m)}-1}{2} = 1.$$

Both θ_1 and θ_2 lead to one solution η_1 and η_2 respectively, where $\eta_1 = \frac{u^2}{\eta_2}$. It is obvious that η_1 and η_2 give the same value z. Therefore, (2) has at most one solution of z.

If $s = \frac{3^{2m}+3^{k+1}+2}{2}$, (3) leads to

$$\begin{aligned} h_1(\eta + \frac{u^2}{\eta} + 2u) &= \frac{(\eta-u)^{3^{k+1}+3} - (\eta+u)^{3^{k+1}+3}}{\eta^{(3^{2m}+3^{k+1}+2)/2}} = \frac{-2u^3\eta^{3^{k+1}} - 2u^{3^{k+1}}\eta^3}{\eta^{(3^{2m}+3^{k+1}+2)/2}} \\ &= -2u^3\left(\eta^{\frac{3^{2m}+3^{k+1}-4}{2}} + \left(\frac{u^2}{\eta}\right)^{\frac{3^{2m}+3^{k+1}-4}{2}}\right) = \gamma \end{aligned} \tag{5}$$

since $\eta, u \in \mathbb{F}^*_{3^{2m}}$. Note that $\gcd(\frac{3^{2m}+3^{k+1}-4}{2}, 3^{2m}-1) = \gcd(\frac{3^{k+1}-3}{2}, 3^{2m}-1) = 1$. Similarly, we can show that (2) has at most one solution of z.

(ii) Since $v_2(k) \geq v_2(2m)$, we get k is even and $p^k \equiv 1 \pmod 4$, which means that $\frac{p^k+1}{2}$ and $\frac{p^{2m}+p^{k+1}+p-1}{2}$ are both odd. If $s = \frac{p^k+1}{2}$, (3) turns to be

$$\begin{aligned} h_1\left(\eta + \frac{u^2}{\eta} + 2u\right) &= \frac{-(\eta-u)^{p^k+1} - (\eta+u)^{p^k+1}}{\eta^{(p^k+1)/2}} \\ &= -2\left(\eta^{\frac{p^k+1}{2}} + \left(\frac{u^2}{\eta}\right)^{\frac{p^k+1}{2}}\right) = \gamma. \end{aligned} \tag{6}$$

From the known condition $v_2(k) \geq v_2(2m)$, we can deduce that $\frac{k}{\gcd(2m,k)}$ is even or both $\frac{k}{\gcd(2m,k)}$ and $\frac{2m}{\gcd(2m,k)}$ are odd. Then by Lemma 2, we obtain

$$\gcd\left(\frac{p^k+1}{2}, p^{2m}-1\right) = \frac{\gcd(p^k+1, p^{2m}-1)}{2} = 1,$$

which implies that (2) has at most one solution of z.

If $s = \frac{p^{2m}+p^{k+1}+p-1}{2}$, (3) leads to

$$\begin{aligned} h_1\left(\eta + \frac{u^2}{\eta} + 2u\right) &= \frac{-(\eta-u)^{p^{k+1}+p} - (\eta+u)^{p^{k+1}+p}}{\eta^{(p^{2m}+p^{k+1}+p-1)/2}} \\ &= -2\left(\eta^{\frac{p^{2m}+p^{k+1}+p-1}{2}} + \left(\frac{u^2}{\eta}\right)^{\frac{p^{2m}+p^{k+1}+p-1}{2}}\right) = \gamma \end{aligned} \tag{7}$$

since $\eta, u \in \mathbb{F}^*_{p^{2m}}$. It can be checked that

$$\gcd\left(\frac{p^{2m}+p^{k+1}+p-1}{2}, p^{2m}-1\right) = \gcd\left(\frac{p^{k+1}+p}{2}, p^{2m}-1\right) = 1.$$

This implies that (2) has at most one solution of z.

□

Remark 2 It is clear that the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$ can be denoted as the following simpler way

$$S = \{t \in \mathbb{F}_{p^{2m}} | t = a^{p^m} - a, a \in \mathbb{F}_{p^{2m}}\}.$$

4 Some classes of PPs over $\mathbb{F}_{p^{2m}}$ with exponents $s = ip^j(p^m+1)+p^j$ or $ip^j(p^m+1)+2p^j$

In this section, we present some new classes of permutation polynomials $f(x) = (x^{p^m} - x + \delta)^s + x + x^{p^m}$ over $\mathbb{F}_{p^{2m}}$ with exponents $s = ip^j(p^m+1)+p^j$ or $ip^j(p^m+1)+2p^j$, where $\delta \in \mathbb{F}_{p^{2m}}$. By Proposition 2, we just need to prove the case of $j = 0$ in the sequel. Firstly, we give some lemmas needed later.

Lemma 3 [14] *For an odd prime p and a positive integer m, if $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} = 0$, then the polynomial $f(x) = (x^{p^m} - x + \delta)^{i(p^m+1)+1} + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$, where the integer i satisfies $0 < i < p^m - 1$ and $\gcd(1+2i, p^m-1) = 1$.*

Lemma 4 *Let i be an integer and $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial $f(x) = (x^{p^m} - x + \delta)^{i(p^m+1)+1} + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$ if and only if the polynomial $g(x) = (x^{p^m} - x + \delta)^{i(p^m+1)+2} + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$.*

Proof According to Proposition 1, the polynomial $f(x)$ permutes $\mathbb{F}_{p^{2m}}$ if and only if

$$\begin{aligned} h_1(t) &= (-t+\overline{\delta})^{i(p^m+1)+1} - (t+\delta)^{i(p^m+1)+1} \\ &= (-t+\overline{\delta})^i (t+\delta)^i (-t+\overline{\delta} - (t+\delta)) \\ &= (-t^2 + (\overline{\delta}-\delta)t + \overline{\delta}\delta)^i (-2t + \overline{\delta} - \delta) \end{aligned} \tag{8}$$

is a bijection over the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$. Similarly, the polynomial $g(x)$ permutes $\mathbb{F}_{p^{2m}}$ if and only if

$$\begin{aligned} h_2(t) &= (-t+\overline{\delta})^{i(p^m+1)+2} - (t+\delta)^{i(p^m+1)+2} \\ &= (-t+\overline{\delta})^i (t+\delta)^i ((-t+\overline{\delta})^2 - (t+\delta)^2) \\ &= (-t^2 + (\overline{\delta}-\delta)t + \overline{\delta}\delta)^i (-2t + \overline{\delta} - \delta)(\overline{\delta} + \delta). \end{aligned} \tag{9}$$

is a bijection on S. Since $\delta + \overline{\delta} \neq 0$, the mappings of (8) and (9) are linear equivalent. This completes the proof. □

Lemma 5 *Let i be an integer and $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial $f(x) = (x^{p^m} - x + \delta)^{i(p^m+1)+1} + x^{p^m} + x$ permutes $\mathbb{F}_{p^{2m}}$ if the polynomial*

$$h'(\lambda) = \lambda(\lambda^2 - c^2)^i \tag{10}$$

permutes $\mathbb{F}_{p^m}$ for any $c \in \mathbb{F}^*_{p^{2m}}$ with $c + c^{p^m} = 0$.

Proof As stated in Lemma 4, the polynomial $f(x)$ permutes $\mathbb{F}_{p^{2m}}$ if and only if

$$h_1(t) = (-t^2 + (\overline{\delta} - \delta)t + \overline{\delta}\delta)^i(-2t + \overline{\delta} - \delta)$$

is a bijection on the set $S = \{t \in \mathbb{F}_{p^{2m}} | t^{p^m} + t = 0\}$.

If $\delta = \overline{\delta}$, then $h_1(t) = -2t(-t^2 + \delta^2)^i$. Assume $\theta \in S$ with $\theta \neq 0$. The mapping $\Phi : z \longmapsto \theta z$ from $\mathbb{F}_{p^m}$ to S is a bijection. Let $t = \theta z$ for $z \in \mathbb{F}_{p^m}$. The mapping $h_1(t)$ can be rewritten as

$$h_1(\theta z) = -2\theta z(-\theta^2 z^2 + \delta^2)^i = (-1)^{i+1}2\theta^{1+2i} z(z^2 - \theta^{-2}\delta^2)^i.$$

Note that $h_1(t)$ is a bijection over S if and only if the mapping

$$h'_1(z) = z(z^2 - \theta^{-2}\delta^2)^i$$

is a bijection on $\mathbb{F}_{p^m}$. Since $\delta + \overline{\delta} \neq 0$, we have $\delta \neq 0$. Then $\theta^{-1}\delta \neq 0$ and $\theta^{-1}\delta + (\theta^{-1}\delta)^{p^m} = 0$.

If $\delta \neq \overline{\delta}$, the mapping $\Phi_1 : z \longmapsto (\delta - \overline{\delta})z$ from $\mathbb{F}_{p^m}$ to S is a bijection. Let $t = (\delta - \overline{\delta})z$ for $z \in \mathbb{F}_{p^m}$. The mapping $h_1(t)$ turns to be

$$h_1((\delta - \overline{\delta})z) = (\delta - \overline{\delta})(-1)^{i+1}((\delta - \overline{\delta})^2 z^2 + (\delta - \overline{\delta})^2 z - \overline{\delta}\delta)^i(2z + 1).$$

Since $\delta + \overline{\delta} \neq 0$, $h_1(t)$ is a bijection on S if and only if the mapping

$$h'_2(z) = \left(z^2 + z - \frac{\overline{\delta}\delta}{(\delta - \overline{\delta})^2}\right)^i (2z + 1)$$

permutes $\mathbb{F}_{p^m}$. Let $\lambda = 2z + 1$. Then $\lambda \in \mathbb{F}_{p^m}$ and $h'_2(z)$ is affine equivalent to the following mapping

$$h''(\lambda) = \lambda\left(\frac{\lambda^2 - 1}{4} - \frac{\overline{\delta}\delta}{(\delta - \overline{\delta})^2}\right)^i = \left(\frac{1}{4}\right)^i \lambda\left(\lambda^2 - \left(\frac{\delta + \overline{\delta}}{\delta - \overline{\delta}}\right)^2\right)^i$$

over $\mathbb{F}_{p^m}$. It can be easily check that $\frac{\delta+\overline{\delta}}{\delta-\overline{\delta}} \neq 0$ and $\frac{\delta+\overline{\delta}}{\delta-\overline{\delta}} + (\frac{\delta+\overline{\delta}}{\delta-\overline{\delta}})^{p^m} = 0$.

If the polynomial $h'(\lambda) = \lambda(\lambda^2 - c^2)^i$ permutes $\mathbb{F}_{p^m}$ for any $c \in \mathbb{F}^*_{p^{2m}}$ with $c + c^{p^m} = 0$, then $h'_1(z)$ and $h''(\lambda)$ are both permutations on $\mathbb{F}_{p^m}$. Hence the proof is finished. □

Lemma 6 [14] *For $a, b \in \mathbb{F}_{p^m}$, the equation $x^p - ax + b = 0$ has the unique solution in $\mathbb{F}_{p^m}$ if and only if $a = 0$ or a is not a $(p-1)$ power in $\mathbb{F}^*_{p^m}$.*

Lemma 7 [11] *Let p be an odd prime and k be a positive integer. Then $f(x) = x(x^2 - t)^{\frac{p-1}{2}}$ is a permutation polynomial over $\mathbb{F}_{p^k}$, where t is a non-square element in $\mathbb{F}_{p^k}$.*

Lemma 8 *Let $c \in \mathbb{F}^*_{p^{2m}}$ with $c + c^{p^m} = 0$. Then $c^2 \in \mathbb{F}_{p^m}$ and c^2 is not a square in $\mathbb{F}_{p^m}$.*

Proof Since $c \in \mathbb{F}^*_{p^{2m}}$ with $c + c^{p^m} = 0$, we get $c^{p^m-1} = -1$, which implies that $c^{2p^m-2} = 1$. It follows that $c^{2p^m} = c^2$, i.e., $c^2 \in \mathbb{F}_{p^m}$.

If c^2 is a square in $\mathbb{F}_{p^m}$, then we have $c \in \mathbb{F}_{p^m}$. From $c + c^{p^m} = 0$ we get $c = 0$, which is a contradiction. □

With the above preparations, we have the following results by determining the permutation behavior of the polynomial in (10).

Theorem 4 *Let $\delta \in \mathbb{F}_{p^{2m}}$. The polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{(\frac{p-1}{2} \cdot p^m + \frac{p+1}{2}) \cdot p^j} + x^{p^m} + x$$

permutes $\mathbb{F}_{p^{2m}}$.

Proof The exponent $s = \frac{p-1}{2} \cdot p^m + \frac{p+1}{2} = \frac{p-1}{2}(p^m + 1) + 1$ implies $i = \frac{p-1}{2}$. Since $\gcd(1 + 2i, p^m - 1) = 1$, if $\delta + \overline{\delta} = 0$, we get that $f(x)$ is a permutation over $\mathbb{F}_{p^{2m}}$ by Lemma 3. Below we consider the case of $\delta + \overline{\delta} \neq 0$.

For any $c \in \mathbb{F}^*_{p^{2m}}$ with $c + c^{p^m} = 0$, from Lemma 8 we have that $c^2 \in \mathbb{F}_{p^m}$ and c^2 is not a square in $\mathbb{F}_{p^m}$. By Lemma 7, we get that $h'(\lambda) = \lambda(\lambda^2 - c^2)^{\frac{p-1}{2}}$ is a permutation polynomial over $\mathbb{F}_{p^m}$. Then the desired conclusion of this theorem follows from Lemma 5. □

According to Lemma 4 and Theorem 4, we get the following corollary directly.

Corollary 1 *Let $\delta \in \mathbb{F}_{p^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial*

$$f(x) = (x^{p^m} - x + \delta)^{(\frac{p-1}{2} \cdot p^m + \frac{p+3}{2}) \cdot p^j} + x^{p^m} + x$$

permutes $\mathbb{F}_{p^{2m}}$.

Theorem 5 *Let $\delta \in \mathbb{F}_{3^{2m}}$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{\frac{(3^{2m} + 2 \cdot 3^m + 3) \cdot 3^j}{2}} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

Proof The exponent

$$s = \frac{3^{2m} + 2 \cdot 3^m + 3}{2} = \frac{3^m + 1}{2}(3^m + 1) + 1$$

implies $i = \frac{3^m+1}{2}$. Since $\gcd(1 + 2i, 3^m - 1) = 1$, by Lemma 3 we get that $f(x)$ is a permutation over $\mathbb{F}_{3^{2m}}$ if $\delta + \overline{\delta} = 0$. Next we consider the case of $\delta + \overline{\delta} \neq 0$.

By Lemma 5, we need to prove that $h'(\lambda)$ permutes $\mathbb{F}_{3^m}$. It is sufficient to prove that for any $\gamma \in \mathbb{F}_{3^m}$, the equation

$$\lambda(\lambda^2 - c^2)^{\frac{3^m+1}{2}} = \gamma \tag{11}$$

has at most one solution for any $c \in \mathbb{F}^*_{3^{2m}}$ with $c + c^{3^m} = 0$. Squaring both sides of (11) gives

$$\lambda^2(\lambda^2 - c^2)^2 = \gamma^2.$$

The above equation leads to

$$\lambda^3 - c^2\lambda = \gamma$$

or

$$\lambda^3 - c^2\lambda = -\gamma.$$

It follows from Lemma 8 that $c^2 \in \mathbb{F}_{3^m}$ and c^2 is not a square in $\mathbb{F}_{3^m}$. By Lemma 6 the above two equations have one solution λ_1 and λ_2 respectively, where $\lambda_1 = -\lambda_2$. If $\gamma = 0$, we get $\lambda_1 = \lambda_2 = 0$. If $\gamma \neq 0$, it can be verified that λ_1 and λ_2 are not the solutions of (11) simultaneously. That is to say, there is at most one solution λ of (11). The proof is completed. □

A direct consequence of Lemma 4 and Theorem 5 is the following.

Corollary 2 *Let $\delta \in \mathbb{F}_{3^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{\frac{(3^{2m}+2\cdot 3^m+5)\cdot 3^j}{2}} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

Theorem 6 *Let $\delta \in \mathbb{F}_{3^{2m}}$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{(2\cdot 3^{2m-1}-3^{m-1})\cdot 3^j} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

Proof The exponent

$$s = 2 \cdot 3^{2m-1} - 3^{m-1} = (2 \cdot 3^{m-1} - 1)(3^m + 1) + 1$$

implies $i = 2 \cdot 3^{m-1} - 1$. Since $\gcd(1 + 2i, 3^m - 1) = \gcd(3^m + 3^{m-1} - 1, 3^m - 1) = 1$, by Lemma 3 we have that $f(x)$ is a permutation over $\mathbb{F}_{3^{2m}}$ if $\delta + \overline{\delta} = 0$.

Now we discuss the case of $\delta + \overline{\delta} \neq 0$. By Lemma 5, it suffices to prove that for each $\gamma \in \mathbb{F}_{3^m}$, the equation

$$\lambda(\lambda^2 - c^2)^{2\cdot 3^{m-1}-1} = \gamma \tag{12}$$

has a unique solution for any $c \in \mathbb{F}^*_{3^{2m}}$ with $c + c^{3^m} = 0$. According to Lemma 8, $c^2 \in \mathbb{F}_{p^m}$ and c^2 is not a square in $\mathbb{F}_{p^m}$. If $\gamma = 0$, then $\lambda = 0$ is the unique solution of (12) since c^2 is not a square in $\mathbb{F}_{3^m}$. If $\gamma \neq 0$, then $\lambda \neq 0$ and $\lambda^2 - c^2 \neq 0$. Raising both sides of (12) to the third powers gives

$$\lambda^3(\lambda^2 - c^2)^{-1} = \gamma^3,$$

which implies that

$$\left(\frac{1}{\lambda}\right)^3 - c^{-2}\frac{1}{\lambda} = -\gamma^{-3}c^{-2}. \tag{13}$$

According to Lemma 6, there is exactly one solution λ of (13). We complete the proof. □

An immediate consequence of Lemma 4 and Theorem 6 is the following result.

Corollary 3 *Let $\delta \in \mathbb{F}_{3^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{(2\cdot 3^{2m-1}-3^{m-1}+1)\cdot 3^j} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

Theorem 7 *Let $\delta \in \mathbb{F}_{3^{2m}}$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{\frac{(3^{2m}-2\cdot 3^m+3)\cdot 3^j}{6}} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

Proof The exponent

$$s = \frac{3^{2m} - 2 \cdot 3^m + 3}{6} = \frac{3^m - 3}{6}(3^m + 1) + 1$$

implies $i = \frac{3^m-3}{6}$. Since $\gcd(1+2i, 3^m - 1) = \gcd(3^m, 3^m - 1) = 1$, as stated before, $f(x)$ is a permutation over $\mathbb{F}_{3^{2m}}$ if $\delta + \overline{\delta} = 0$.

Assume $\delta + \overline{\delta} \neq 0$. By Lemma 5, for any $\gamma \in \mathbb{F}_{3^m}$ we need to show that the equation

$$\lambda(\lambda^2 - c^2)^{\frac{3^m-3}{6}} = \gamma \tag{14}$$

has at most one solution for any $c \in \mathbb{F}^*_{3^{2m}}$ with $c + c^{3^m} = 0$. By Lemma 8 we have that $c^2 \in \mathbb{F}_{3^m}$ is not a square in $\mathbb{F}_{3^m}$. Similarly as the proof of Theorem 6, there is a unique solution of (14) when $\gamma = 0$. Next we suppose $\gamma \neq 0$. It leads to $\lambda \neq 0$. Taking the sixth powers on both sides of (14), we obtain

$$\lambda^6(\lambda^2 - c^2)^{-2} = \gamma^6. \tag{15}$$

We can deduced that

$$\lambda^3 = \gamma^3 c^2 - \gamma^3 \lambda^2$$

or

$$\lambda^3 = -\gamma^3 c^2 + \gamma^3 \lambda^2,$$

which implies that

$$\left(\frac{1}{\lambda}\right)^3 - c^{-2}\left(\frac{1}{\lambda}\right) = \gamma^{-3}c^{-2} \tag{16}$$

or

$$\left(\frac{1}{\lambda}\right)^3 - c^{-2}\left(\frac{1}{\lambda}\right) = -\gamma^{-3}c^{-2}. \tag{17}$$

Then by Lemma 6, we get that (16) and (17) have one solution λ_1 and λ_2 respectively, where $\lambda_1 = -\lambda_2 \neq 0$. It can be verified that λ_1 and λ_2 are not the solutions of (14) simultaneously. That is to say, there is at most one solution λ of (14). The proof is finished. □

Similarly, we can deduce the following result by Lemma 4 and Theorem 7.

Corollary 4 *Let $\delta \in \mathbb{F}_{3^{2m}}$ with $\delta + \overline{\delta} \neq 0$. The polynomial*

$$f(x) = (x^{3^m} - x + \delta)^{\frac{(3^{2m}-2\cdot 3^m+9)\cdot 3^j}{6}} + x^{3^m} + x$$

permutes $\mathbb{F}_{3^{2m}}$.

5 Conclusion

In this paper, we continued the work in [9, 14, 16, 19, 24] and proposed several new classes of permutation polynomials $f(x) = (x^{p^m} - x + \delta)^s + x^{p^m} + x$ over $\mathbb{F}_{p^{2m}}$ for some $\delta \in \mathbb{F}_{p^{2m}}$ by using the AGW criterion. Note that the AGW criterion can be used to investigate the

permutation behavior of more explicit polynomials of the form $(x^{p^m}+ax+\delta)^s+bx^{p^m}+cx$ over $\mathbb{F}_{p^{2m}}$, where s is an integer and $a, b, c, \delta \in \mathbb{F}_{p^{2m}}$.

Acknowledgements The authors would like to thank the anonymous reviewers for their valuable comments and helpful suggestions which improved both the quality and presentation of this paper. The work of this paper was supported by the National Natural Science Foundation of China (Grants 11571005, 61472417 and 11371184), and the Program for Science and Technology Innovation Talents in Universities of Henan Province under Grant 16HASTIT039.

References

1. Akbary, A., Ghioca, D., Wang, Q.: On constructing permutations of finite fields. Finite Fields Appl. **17**(1), 51–67 (2011)
2. Berlekamp, E.-R., Rumsey, H., Solomon, G.: On the solution of algebraic equations over finite fields. Inf. Control **10**(6), 553–564 (1967)
3. Cepak, N., Charpin, P., Pasalic, E.: Permutations via linear translators. Finite Fields Appl. **45**, 19–42 (2017)
4. Charpin, P., Kyureghyan, G.: When does $G(x)+\gamma \mathrm{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$. Finite Fields Appl. **15**(5), 615–632 (2009)
5. Choi, S.-T., Hong, S., No, J.-S., Chung, H.: Differential spectrum of some power functions in odd prime characteristic. Finite Fields Appl. **21**, 11–29 (2013)
6. Helleseth, T., Zinoviev, V.: New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m. Finite Fields Appl. **9**(2), 187–193 (2003)
7. Hou, X.: Permutation polynomials over finite fields—a survey of recent advances. Finite Fields Appl. **32**, 82–119 (2015)
8. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inf. Theory **36**(3), 686–692 (1990)
9. Li, N., Helleseth, T., Tang, X.: Further results on a class of permutation polynomials over finite fields. Finite Fields Appl. **22**, 16–23 (2013)
10. Lidl, R., Niederreiter, H.: Finite Fields, 2nd edn. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
11. Ma, J., Zhang, T., Feng T., Ge, G.: Some new results on permutation polynomilas over finite fields. Des. Codes Cryptogr. **83**(2), 425–443 (2017)
12. Mullen, G.-L., Panario, D.: Handbook of Finite Fields. Taylor & Francis, Boca Raton (2013)
13. Tu, Z., Zeng, X., Jiang, Y.: Two classes of permutation polynomials having the form $(x^{2^m}+x+\delta)^s+x$. Finite Fields Appl. **31**, 12–24 (2015)
14. Tu, Z., Zeng, X., Li, C., Helleseth, T.: Permutation polynomials of the form $(x^{p^m}-x+\delta)^s+L(x)$. Finite Fields Appl. **34**, 20–35 (2015)
15. Yuan, J., Ding, C.: Four classes of permutation polynomials of $\mathbb{F}_{2^m}$. Finite Fields Appl. **13**(4), 869–876 (2007)
16. Yuan, J., Ding, C., Wang, H., Pieprzyk, J.: Permutation polynomials of the form $(x^p-x+\delta)^s+L(x)$. Finite Fields Appl. **14**(2), 482–493 (2008)
17. Yuan, P., Ding, C.: Permutation polynomials over finite fields from a powerful lemma. Finite Fields Appl. **17**(6), 560–574 (2011)
18. Yuan, P., Ding, C.: Further results on permutation polynomials over finite fields. Finite Fields Appl. **27**, 88–103 (2014)
19. Yuan, P., Zheng, Y.: Permutation polynomials from piecewise functions. Finite Fields Appl. **35**, 215–230 (2015)
20. Zeng, X., Hu, L., Jiang, W., Yue, Q., Cao, X.: The weight distribution of a class of p-ary cyclic codes. Finite Fields Appl. **16**(1), 56–73 (2010)
21. Zeng, X., Zhu, X., Hu, L.: Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over $\mathbb{F}_{2^n}$. Appl. Algebra Eng. Commun. Comput. **21**(2), 145–150 (2010)
22. Zeng, X., Tian, S., Tu, Z.: Permutation polynomials from trace functions over finite fields. Finite Fields Appl. **35**, 36–51 (2015)
23. Zha, Z., Hu, L.: Two classes of permutation polynomials over finite fields. Finite Fields Appl. **18**(4), 781–790 (2012)
24. Zha, Z., Hu, L.: Some classes of permutation polynomials of the form $(x^{p^m}-x+\delta)^s+x$ over $\mathbb{F}_{p^{2m}}$. Finite Fields Appl. **40**, 150–162 (2016)