

Some new results on permutation polynomials over finite fields

Jingxue Ma^a, Tao Zhang^a, Tao Feng^{a,c} and Gennian Ge^{b,c,*}

^a School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, Zhejiang, China

^b School of Mathematical Sciences, Capital Normal University, Beijing, 100048, China

^c Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China

Abstract

Permutation polynomials over finite fields constitute an active research area and have applications in many areas of science and engineering. In this paper, four classes of monomial complete permutation polynomials and one class of trinomial complete permutation polynomials are presented, one of which confirms a conjecture proposed by Wu et al. (Sci. China Math., 2015, 58, pp. 2081-2094). Furthermore, we give two classes of permutation trinomial, and make some progress on a conjecture about the differential uniformity of power permutation polynomials proposed by Blondeau et al. (Int. J. Inf. Coding Theory, 2010, 1, pp. 149-170).

Keywords and phrases: Permutation polynomials, complete permutation polynomials, trace function, differential uniformity

Mathematics subject classifications: 11T06, 11T55, 05A05.

1 Introduction

Let \mathbb{F}_{p^n} be a finite field with p^n elements, where p is a prime and n is a positive integer. A polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is called a permutation polynomial (PP) if the associated mapping $f : c \mapsto f(c)$ from \mathbb{F}_{p^n} to itself is a bijection. PPs have been intensively studied in recent years due to their important applications in cryptography, coding theory and combinatorial design theory (see [7, 8, 15, 19, 20] and the references therein). For instance, Ding et al. [7] constructed a family of skew Hadamard difference sets via the Dickson PP of order five, which disproved the longstanding conjecture on skew Hadamard difference sets. Some recent progress on PPs can be found in [1, 5, 6, 9, 14, 11, 12, 13, 16, 25, 26, 27].

A polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ is called a complete permutation polynomial (CPP) if both $f(x)$ and $f(x) + x$ are permutations of \mathbb{F}_{p^n} . These polynomials were introduced by Niederreiter and Robinson in [18]. The simplest polynomials are monomials, and for a positive integer d and $\alpha \in \mathbb{F}_{p^n}^*$, the monomial αx^d over \mathbb{F}_{p^n} is a CPP if and only if $\gcd(d, p^n - 1) = 1$ and $\alpha x^d + x$ is a PP. We call such an integer d a CPP exponent over \mathbb{F}_{p^n} . Recently, Charpin and Kyureghyan [4] proved that $2^k + 2$ is a CPP exponent

*Corresponding author. Email address: majingxue@zju.edu.cn (J. Ma), tzh@zju.edu.cn (T. Zhang), tfeng@zju.edu.cn (T. Feng), gnge@zju.edu.cn (G. Ge)

over $\mathbb{F}_{2^{2k}}$ for odd k . In [22], a class of CPP exponents over \mathbb{F}_{2^n} of Niho type was given. Two new classes of CPP exponents and a multinomial CPPs were proposed in [24]. Further results about CPPs can be found in [21, 23, 28].

In this paper, we construct four classes of monomial CPPs, one class of trinomial CPPs and two classes of permutation trinomials as follows:

1. Let p be an odd prime, $r + 1 = p$ and $d = \frac{p^{rk}-1}{p^k-1} + 1$. Then $a^{-1}x^d$ is a CPP over $\mathbb{F}_{p^{rk}}$, where $a \in \mathbb{F}_{p^{rk}}^*$ such that $a^{p^k-1} = -1$.
2. Let $n = 6k$, where k is a positive integer with $\gcd(k, 3) = 1$. Then $d = 2^{4k-1} + 2^{2k-1}$ is a CPP exponent over \mathbb{F}_{2^n} . To be specific, $a^{-1}x^d$ is a CPP over \mathbb{F}_{2^n} , where $a \in \{\omega^{t(2^{2k}-1)} \mid 0 < t \leq 2^{2k} + 2^{4k}, 3 \nmid t\}$.
3. Let $n = 4k$. Then $d = (1 + 2^{2k-1})(1 + 2^{2k}) + 1$ is a CPP exponent over \mathbb{F}_{2^n} . To be specific, if a is a non-cubic element of $\mathbb{F}_{2^{2k}}^*$, then $a^{-1}x^d$ is a CPP over \mathbb{F}_{2^n} .
4. Let p be an odd prime and $n = 4k$. Then $d = \frac{p^{4k}-1}{2} + p^{2k}$ is a CPP exponent over \mathbb{F}_{p^n} . To be specific, $a^{-1}x^d$ is a CPP over \mathbb{F}_{p^n} , where $a \in \{\omega^{t(p^{2k}-1) + \frac{p^{2k}-1}{2}} : 0 \leq t \leq p^{2k}\}$.
5. For any odd prime p , $f(x) = -x + x^{\frac{p^{2m}+1}{2}} + x^{\frac{p^{2m}+1}{2}}p^m$ is a CPP over $\mathbb{F}_{p^{3m}}$.
6. Let $m > 1$ be an odd integer, and write $k = \frac{m+1}{2}$. Then for each $u \in \mathbb{F}_{2^m}^*$, $f(x) = x + u^{2^{k-1}-1}x^{2^{k-1}} + u^{2^{k-1}}x^{2^k+1}$ is a PP over \mathbb{F}_{2^m} .
7. Let $m > 1$ be an odd integer such that $m = 2k-1$. Then $f(x) = x + ux^{2^k-1} + u^{2^k}x^{2^m-2^{k+1}+2}$, $u \in \mathbb{F}_{2^m}^*$, is a PP over \mathbb{F}_{2^m} .

The first class is a conjecture made by Wu et al. [24], and our main technique is using the AGW Criterion [1]. By using the additive characters over the underlying finite fields [21], we give three other new classes (Class 2–Class 4) of monomial CPPs over finite fields. Classes 5, 6 and 7 are explicit constructions of PPs and CPPs through the study of the number of solutions of special equations [5, ?].

Functions with a low differential uniformity are interesting from the viewpoint of cryptography as they provide good resistance to differential attack. In [3], the authors considered the differential properties of power functions and proposed the following conjecture.

Conjecture 1. [3] *Let $n = 2m$ with m odd. Let $F_d : x \rightarrow x^d$ be the power PPs over \mathbb{F}_{2^n} defined by the following values of d :*

$$(1) \quad d = 2^m + 2^{(m+1)/2} + 1,$$

$$(2) \quad d = 2^{m+1} + 3.$$

Then, for these values of d , F_d is differentially 8-uniform and all values 0, 2, 4, 6, 8 appear in its differential spectrum.

To determine the exact value of differential uniformity is a difficult problem. In this paper, we make some progress towards Conjecture 1, and prove that the differential uniformities of these polynomials are at most 10.

This paper is organized as follows. In Section 2, we introduce some basic notations and related results. In Section 3, four classes of monomial CPPs are given. In Section 4, we give a class of trinomial CPPs. Two classes of PPs are presented in Section 5. Section 6 investigates the differential properties of monomial PPs. Section 7 concludes the paper.

2 Preliminaries

The following notations are fixed throughout this paper.

- Let p be a prime, n be an integer, and \mathbb{F}_{p^n} be the finite field of order p^n .
- Let $\text{Tr}_r^n : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^r}$ be the trace mapping defined by

$$\text{Tr}_r^n(x) = x + x^{p^r} + x^{p^{2r}} + \cdots + x^{p^{n-r}},$$

where $r|n$. For $r = 1$, we get the absolute trace function mapping onto the prime field \mathbb{F}_p , which is denoted by Tr_n .

- Let $N_r^n : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^r}$ be the norm mapping defined by

$$N_r^n(x) = xx^{p^r} x^{p^{2r}} \cdots x^{p^{n-r}},$$

where $r|n$. For $r = 1$, we get the absolute norm function mapping onto the prime field \mathbb{F}_p , which is denoted by N_n .

- Let $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ be a p -th root of unity, and $\chi_n(x) = \zeta_p^{\text{Tr}_n(x)}$ be the canonical additive character on \mathbb{F}_{p^n} .

We first recall a criterion for PPs which can be given by using additive characters over the underlying finite field.

Lemma 2.1. [17] *A mapping $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^n}$ is a PP if and only if for every $\alpha \in \mathbb{F}_{p^n}^*$,*

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(\alpha f(x)) = 0.$$

Let n, r, k be integers such that $n = rk$. For any $a \in \mathbb{F}_{p^n}$, let $a_i = a^{p^{ik}}$, where $0 \leq i \leq r-1$. Define

$$h_a(x) = x \prod_{i=0}^{r-1} (x + a_i).$$

Then we have the following lemma.

Lemma 2.2. [24] Let $n = rk$, and $d = \frac{p^{rk}-1}{p^k-1} + 1$. Then $x^d + ax \in \mathbb{F}_{p^n}[x]$ is a PP over \mathbb{F}_{p^n} if and only if $h_a(x) \in \mathbb{F}_{p^k}[x]$ is a PP over \mathbb{F}_{p^k} .

The following lemmas will also be needed in the following sections.

Lemma 2.3. [1](AGW Criterion) Let A, S and \overline{S} be finite sets with $\#S = \#\overline{S}$, and let $f : A \rightarrow A$, $h : S \rightarrow \overline{S}$, $\lambda : A \rightarrow S$, and $\overline{\lambda} : A \rightarrow \overline{S}$ 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 bijective;
2. h is bijective from S to \overline{S} and f is injective on $\lambda^{-1}(s)$ for each $s \in S$.

Lemma 2.4. [17] Let p be an odd prime, and let m, k be positive integers such that $\frac{m}{\gcd(m,k)}$ is odd. Then $x^{p^k} + x$ is a permutation on \mathbb{F}_{p^m} .

Lemma 2.5. [17] An irreducible polynomial over \mathbb{F}_q of degree n remains irreducible over \mathbb{F}_{q^k} if and only if $\gcd(k, n) = 1$.

3 Four classes of monomial CPPs

3.1 The first class of monomial CPPs

In this subsection, we will prove the conjecture of Wu et al. [24]. Before proving it, we establish the following useful lemma.

Lemma 3.1. Let p be an odd prime and k be a positive integer. Then $f(x) = x(x^2 - c)^{\frac{p-1}{2}}$ is a PP over \mathbb{F}_{p^k} , where c is a non-square element in \mathbb{F}_{p^k} .

Proof. We first show that $x = 0$ is the only solution to $f(x) = 0$. If $f(x) = 0$, then $x = 0$ or $(x^2 - c)^{\frac{p-1}{2}} = 0$. If $(x^2 - c)^{\frac{p-1}{2}} = 0$, then $c = x^2$, which leads to a contradiction since c is a non-square element. Therefore $f(x) = 0$ if and only if $x = 0$.

Next, we prove that $f(x) = a$ has a unique nonzero solution for each nonzero $a \in \mathbb{F}_{p^k}$. Let $\lambda(x) = x^2 - c$, $\overline{\lambda}(x) = x^2$ and $h(x) = (x + c)x^{p-1}$. Then it is easy to see that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{F}_{p^k}^* & \xrightarrow{\lambda} & \lambda(\mathbb{F}_{p^k}^*) \\ \downarrow f & & \downarrow h \\ \mathbb{F}_{p^k}^* & \xrightarrow{\overline{\lambda}} & \overline{\lambda}(\mathbb{F}_{p^k}^*). \end{array}$$

By Lemma 2.3, it suffices to prove that h is bijective and f is injective on $\lambda^{-1}(s)$ for each $s \in \lambda(\mathbb{F}_{p^k}^*)$. Since for each $s \in \lambda(\mathbb{F}_{p^k}^*)$, $\lambda^{-1}(s) = \{\pm(c + s)^{\frac{1}{2}}\}$, and $f((c + s)^{\frac{1}{2}}) \neq f(-(c + s)^{\frac{1}{2}})$, it implies that f is injective on $\lambda^{-1}(s)$ for each $s \in \lambda(\mathbb{F}_{p^k}^*)$.

In the following, we will verify that h is bijective. Since $\#\lambda(\mathbb{F}_{p^k}^*) = \#\overline{\lambda}(\mathbb{F}_{p^k}^*)$, we only need to show that h is injective. For any $b \in \overline{\lambda}(\mathbb{F}_{p^k}^*)$, b is a square element in $\mathbb{F}_{p^k}^*$. We assume

$$x^p + cx^{p-1} = b \quad (1)$$

has at least two distinct solutions. Setting $y = \frac{1}{x}$, the equation

$$y^p - \frac{c}{b}y - \frac{1}{b} = 0 \quad (2)$$

has at least two distinct solutions. Assume y_1, y_2 are two distinct solutions of Eq. (2). Then $y_1 - y_2$ is a root of $y^p - \frac{c}{b}y = 0$, and so must be a root of $y^{p-1} - \frac{c}{b} = 0$. It follows that $\frac{c}{b} = y_0^{p-1}$ for some $y_0 \in \mathbb{F}_{p^k}$, which is impossible since $\frac{c}{b}$ is a non-square element in \mathbb{F}_{p^k} . Hence Eq. (1) has at most one solution in $\lambda(\mathbb{F}_{p^k}^*)$. Therefore, $h(x)$ is bijective. This completes the proof. \square

Now we can prove the following result, which is a conjecture made by Wu et al. [24].

Theorem 3.2 ([24] Conjecture 4.20). *Let p be an odd prime, $r + 1 = p$ and $d = \frac{p^{rk}-1}{p^k-1} + 1$. Then $a^{-1}x^d$ is a CPP over $\mathbb{F}_{p^{rk}}$, where $a \in \mathbb{F}_{p^{rk}}^*$ such that $a^{p^k-1} = -1$.*

Proof. Since $\gcd(p^{rk} - 1, d) = 1$, the monomial x^d is a PP over $\mathbb{F}_{p^{rk}}$.

Note that $a^{p^k-1} = -1$. Then $a^{p^k} = -a$ and $(a^2)^{p^k-1} = 1$. By Lemma 2.2, to prove the conjecture we only need to show that $h_a(x) = x(x^2 - a^2)^{\frac{p-1}{2}}$ is a PP over \mathbb{F}_{p^k} for any k . Let $c = a^2 \in \mathbb{F}_{p^k}$. Then c is a non-square element in \mathbb{F}_{p^k} since $a \notin \mathbb{F}_{p^k}$. Hence the result follows from Lemma 3.1. \square

3.2 The second class of CPPs

In this subsection, let $p = 2$ and $n = 6k$ for some integer k satisfying $\gcd(k, 3) = 1$, and ω be a fixed primitive element of $\mathbb{F}_{2^{6k}}$. We will show that $d = 2^{4k-1} + 2^{2k-1}$ is a CPP exponent over $\mathbb{F}_{2^{6k}}$. We define the following set

$$S := \{\omega^{t(2^{2k}-1)} \mid 0 < t \leq 2^{2k} + 2^{4k}, 3 \nmid t\}. \quad (3)$$

Lemma 3.3. *For each $a \in S$, $\text{Tr}_{2k}^{6k}(a) \neq 1$.*

Proof. If $a \in S \cap \mathbb{F}_{2^{2k}}$, then $\text{Tr}_{2k}^{6k}(a) = a \neq 1$. So we assume that $a \in S \setminus \mathbb{F}_{2^{2k}}$ below.

Since $3 \mid (2^{2k} - 1)$, there exists $b \in \mathbb{F}_{2^{6k}} \setminus \mathbb{F}_{2^{2k}}$ such that $b^3 = a$. We observe that $N_{2k}^{6k}(a) = 1$ by the definition of S , so $\eta := N_{2k}^{6k}(b) \in \mathbb{F}_4^*$. Here, $\eta \neq 1$, again by the definition of S .

Let $B(x) = x^3 + B_1x^2 + B_2x + B_3 \in \mathbb{F}_{2^{2k}}[x]$ be the minimal polynomial of b over $\mathbb{F}_{2^{2k}}$. Then $B(x)$ is irreducible over $\mathbb{F}_{2^{2k}}$, $B_1 = \text{Tr}_{2k}^{6k}(b)$ and $B_3 = \eta$. We can directly verify that

$$\text{Tr}_{2k}^{6k}(a) = \text{Tr}_{2k}^{6k}(b^3) = B_1^3 + B_1B_2 + B_3. \quad (4)$$

If $B_1 = 0$, then $\text{Tr}_{2k}^{6k}(a) = B_3 = \eta \neq 1$, and the claim follows. We assume that $B_1 \neq 0$ below. Assume to the contrary that $\text{Tr}_{2k}^{6k}(a) = 1$. Then Eq. (4) gives that $B_2 = \frac{B_1^3 + \eta^2}{B_1}$, and we have

$$\begin{aligned} B(x) &= x^3 + B_1x^2 + B_2x + B_3 \\ &= x^3 + B_1x^2 + \frac{B_1^3 + \eta^2}{B_1}x + B_3 \\ &= (\eta x + B_1)(\eta^2x^2 + B_1x + \frac{\eta}{B_1}), \end{aligned}$$

contradicting to the fact that $B(x)$ is irreducible over $\mathbb{F}_{2^{2k}}$. This completes the proof. \square

Lemma 3.4. *Fix an integer k with $\gcd(k, 3) = 1$. Suppose $n = 6k$ and $d = 2^{4k-1} + 2^{2k-1}$. If $v \in S$, then*

$$\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + vx) = 0.$$

Proof. Let a be a primitive element of \mathbb{F}_8 with $a^3 + a + 1 = 0$. Since $\gcd(k, 3) = 1$, we have $\mathbb{F}_{2^{6k}} = \mathbb{F}_{2^{2k}}(a)$. For any $x \in \mathbb{F}_{2^{6k}}$, it can be expressed as

$$x = x_0 + x_1a + x_2a^2,$$

where $x_0, x_1, x_2 \in \mathbb{F}_{2^{2k}}$.

Since $\gcd(k, 3) = 1$, we first consider the case $k \equiv 1 \pmod{3}$, in which $a^{2^{2k}} = a^4$. The first step is to compute a direct representation of $\text{Tr}_n(x^d)$ as a function of x_0, x_1 and x_2 . Note that $\text{Tr}_{2k}^{6k}(a) = \text{Tr}_{2k}^{6k}(a^2) = 0$ and $\text{Tr}_{2k}^{6k}(1) = 1$. A routine computation shows that

$$\text{Tr}_{6k}(x^d) = \text{Tr}_{2k}(x_0 + x_1 + x_2 + x_1x_2).$$

Next, putting

$$v = v_0 + v_1a + v_2a^2$$

with $v_0, v_1, v_2 \in \mathbb{F}_{2^{2k}}$, we find that

$$\text{Tr}_{6k}(vx) = \text{Tr}_{2k}(v_0x_0 + v_1x_2 + v_2x_1).$$

Consequently,

$$\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + vx) = \sum_{x_1, x_2 \in \mathbb{F}_{2^{2k}}} \chi_{2k}(x_1 + x_2 + x_1x_2 + v_1x_2 + v_2x_1) \sum_{x_0 \in \mathbb{F}_{2^{2k}}} \chi_{2k}(x_0 + v_0x_0).$$

From Lemma 3.3 we get $v_0 \neq 1$. Therefore, $\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + vx) = 0$.

For the remaining case $k \equiv 2 \pmod{3}$, a similar discussion leads to $\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + vx) = 0$. \square

Theorem 3.5. *Let $n = 6k$, where k is a positive integer with $\gcd(k, 3) = 1$. Then $d = 2^{4k-1} + 2^{2k-1}$ is a CPP exponent over \mathbb{F}_{2^n} . To be specific, if $a \in S$ with S defined as in (3), then $a^{-1}x^d$ is a CPP over \mathbb{F}_{2^n} .*

Proof. Since $\gcd(d, 2^{6k} - 1) = 1$, we have x^d is a PP over $\mathbb{F}_{2^{6k}}$. In what follows we prove that $x^d + ax$ is also a PP over $\mathbb{F}_{2^{6k}}$. We only need to prove that for each $\alpha \in \mathbb{F}_{2^{6k}}^*$,

$$\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d + ax)) = 0,$$

where $a \in S$. Since $\gcd(d, 2^{6k} - 1) = 1$, each nonzero $\alpha \in \mathbb{F}_{2^{6k}}$ can be written as $\alpha = \beta^d$ for a unique $\beta \in \mathbb{F}_{2^{6k}}^*$, and we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d + ax)) &= \sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}((\beta x)^d + \beta^{d-1}a\beta x) \\ &= \sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + \beta^{d-1}ax) \\ &= \sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(x^d + \beta^{2^{4k-1}+2^{2k-1}-1}ax). \end{aligned}$$

Since $\beta^{2^{4k-1}+2^{2k-1}-1}a \in S$, it follows from Lemma 3.4 that for each $\alpha \in \mathbb{F}_{2^{6k}}^*$, we have

$$\sum_{x \in \mathbb{F}_{2^{6k}}} \chi_{6k}(\alpha(x^d + ax)) = 0.$$

This completes the proof. □

3.3 The third class of monomial CPPs

In this subsection, let $p = 2$ and $n = 4k$. We will use an analysis similar to that of the previous subsection to show that $d = (1 + 2^{2k-1})(1 + 2^{2k}) + 1$ is a CPP exponent over $\mathbb{F}_{2^{4k}}$.

Lemma 3.6. *If v is a non-cubic element of $\mathbb{F}_{2^{2k}}^*$, then*

$$\sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1} + vx) = 0.$$

Proof. Using polar coordinate representation, every nonzero element x of $\mathbb{F}_{2^{4k}}$ can be uniquely represented as $x = yz$ with $y \in U$ and $z \in \mathbb{F}_{2^{2k}}^*$, where $U = \{\lambda \in \mathbb{F}_{2^{4k}} \mid \lambda^{2^{2k}+1} = 1\}$. Then

$$\sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1} + vx) = 1 + \sum_{x \in \mathbb{F}_{2^{4k}}^*} \chi_{4k}(x^{(1+2^{2k-1})(1+2^{2k})+1} + vx)$$

$$\begin{aligned}
&= 1 + \sum_{y \in U} \sum_{z \in \mathbb{F}_{2^{2k}}^*} \chi_{4k}((yz)^{(1+2^{2k-1})(1+2^{2k})+1} + vyz) \\
&= -2^{2k} + \sum_{y \in U} \sum_{z \in \mathbb{F}_{2^{2k}}} \chi_{4k}(yz^4 + vyz) \\
&= -2^{2k} + \sum_{y \in U} \sum_{z \in \mathbb{F}_{2^{2k}}} \chi_{2k}(\text{Tr}_{2k}^{4k}(yz^4 + vyz)) \\
&= -2^{2k} + \sum_{y \in U} \sum_{z \in \mathbb{F}_{2^{2k}}} \chi_{2k}((y + y^{2^{2k}})z^4 + (y + y^{2^{2k}})vz) \\
&= -2^{2k} + \sum_{y \in U} \sum_{z \in \mathbb{F}_{2^{2k}}} \chi_{2k}(z^4(y + y^{2^{2k}} + y^4v^4 + y^{2^{2k+2}}v^4)) \\
&= (N(v) - 1)2^{2k},
\end{aligned}$$

where $N(v)$ denotes the number of y 's in U such that $y + y^{2^{2k}} + y^4v^4 + y^{2^{2k+2}}v^4 = 0$, which is equivalent to

$$y + y^{-1} + y^4v^4 + y^{-4}v^4 = 0,$$

that is,

$$(y + y^{-1})[1 + v^4(y + y^{-1})^3] = 0.$$

Since v is a non-cubic element of $\mathbb{F}_{2^{2k}}^*$, we get $1 + v^4(y + y^{-1})^3 \neq 0$. Hence $y = 1$ is the unique root. Thus $N(v) = 1$, and this completes the proof. \square

Theorem 3.7. *Let $n = 4k$. Then $d = (1 + 2^{2k-1})(1 + 2^{2k}) + 1$ is a CPP exponent over \mathbb{F}_{2^n} . To be specific, if a is a non-cubic element of $\mathbb{F}_{2^{2k}}^*$, then $a^{-1}x^d$ is a CPP over \mathbb{F}_{2^n} .*

Proof. It can be verified that $\gcd(d, 2^{4k} - 1) = 1$. Thus, it suffices to prove that $x^d + ax$ is a PP for a non-cubic $a \in \mathbb{F}_{2^{2k}}^*$. Since each nonzero $\alpha \in \mathbb{F}_{2^{4k}}$ can be written as $\alpha = \beta^d$ for a unique $\beta \in \mathbb{F}_{2^{4k}}^*$, we have

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(\alpha(x^d + ax)) &= \sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}((\beta x)^d + \beta^{d-1}a\beta x) \\
&= \sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(x^d + \beta^{d-1}ax) \\
&= \sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(x^d + \beta^{(1+2^{2k-1})(1+2^{2k})}ax).
\end{aligned}$$

Note that $\beta^{(1+2^{2k-1})(1+2^{2k})}a$ is also a non-cubic element of $\mathbb{F}_{2^{2k}}^*$. For each $\alpha \in \mathbb{F}_{2^{4k}}^*$, we have

$$\sum_{x \in \mathbb{F}_{2^{4k}}} \chi_{4k}(\alpha(x^d + ax)) = 0,$$

by Lemma 3.6. This completes the proof. \square

3.4 The fourth class of monomial CPPs

In this subsection, we study the fourth class of monomial CPPs, where p is an odd prime, $n = 4k$ and $d = \frac{p^{4k}-1}{2} + p^{2k}$. Let ω be a fixed primitive element of \mathbb{F}_{p^n} . Denote the conjugate of x over \mathbb{F}_{p^n} by \bar{x} , i.e. $\bar{x} = x^{p^{2k}}$. We also define the set S as follows:

$$S := \{\omega^{t(p^{2k}-1) + \frac{p^{2k}-1}{2}} : 0 \leq t \leq p^{2k}\}. \quad (5)$$

We first recall two lemmas.

Lemma 3.8. [10] Let p be an odd prime and $d|p^n - 1$. Let s be the least positive integer such that $d|p^s + 1$. For each $0 \leq j < d$, define the set

$$C_j := \{\omega^{di+j} \in \mathbb{F}_{p^n}^* | 0 \leq i < \frac{p^n - 1}{d}\}.$$

1. In the case d is an even integer, and both $(p^s + 1)/d$ and $d/2s$ are odd integers, we have

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(ax^d) = \begin{cases} p^n; & \text{if } a = 0, \\ (-1)^{\frac{n}{2s}+1} (d-1)p^{\frac{n}{2}}; & \text{if } a \in C_{\frac{d}{2}}, \\ (-1)^{\frac{n}{2s}} p^{\frac{n}{2}}; & \text{if } a \notin C_{\frac{d}{2}}. \end{cases}$$

2. In all the other cases, we get

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(ax^d) = \begin{cases} p^n; & \text{if } a = 0, \\ (-1)^{\frac{n}{2s}+1} (d-1)p^{\frac{n}{2}}; & \text{if } a \in C_0, \\ (-1)^{\frac{n}{2s}} p^{\frac{n}{2}}; & \text{if } a \notin C_0. \end{cases}$$

Lemma 3.9. [10] Let d be an integer with $\gcd(d, p^n - 1) = 1$. Suppose that there exists an integer i such that $0 \leq i < n$ and $(d - p^i)|(p^n - 1)$. Choose an integer N such that $(d - p^i)N \equiv 0 \pmod{p^n - 1}$. Then

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + ax) = \frac{1}{N} \sum_{j=0}^{N-1} \sum_{y \in \mathbb{F}_{p^n}} \chi_n(y^N (a\omega^j + \omega^{dj p^{-i}})).$$

As a preparation, we have the following lemmas.

Lemma 3.10. *If $a \in S$ with S defined as in (5), then $\frac{a+1}{a-1} = \omega^{2s}$ for some integer s .*

Proof. Assume to the contrary that $\frac{a+1}{a-1} = \omega^{2s+1}$ for some integer s . Since $a\bar{a} = -1$, we have

$$\frac{a+1}{a-1} = \frac{a - a\bar{a}}{a + a\bar{a}} = \frac{1 - \bar{a}}{1 + \bar{a}} = \left(\frac{1-a}{1+a}\right)^{p^{2k}} = -\omega^{-(2s+1)p^{2k}}.$$

It follows that

$$\omega^{(2s+1)(p^{2k}+1)} = -1 = \omega^{(p^{2k}+1)\frac{p^{2k}-1}{2}},$$

which is a contradiction. So we have $\frac{a+1}{a-1} = \omega^{2s}$ for some integer s . □

Lemma 3.11. *Let p be an odd prime, $n = 4k$ and $d = \frac{p^{4k}-1}{2} + p^{2k}$. If $a \in S$ with S defined as in (5), then $\sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + ax) = 0$.*

Proof. By Lemma 3.9, we have

$$\begin{aligned} 2 \sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + ax) &= \sum_{y \in \mathbb{F}_{p^n}} \chi_n(y^2(a+1)) + \sum_{y \in \mathbb{F}_{p^n}} \chi_n(y^2(a\omega + \omega^{dp^{2k}})) \\ &= \sum_{y \in \mathbb{F}_{p^n}} \chi_n(y^2(a+1)) + \sum_{y \in \mathbb{F}_{p^n}} \chi_n(y^2((a-1)\omega)). \end{aligned}$$

From Lemma 3.10, $a-1, a+1 \in C_0$ or $a-1, a+1 \in C_1$. Then a direct application of Lemma 3.8 shows $\sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + ax) = 0$. \square

We now have the following theorem.

Theorem 3.12. *Let p be an odd prime and $n = 4k$. Then $d = \frac{p^{4k}-1}{2} + p^{2k}$ is a CPP exponent over \mathbb{F}_{p^n} . To be specific, if $a \in S$ with S defined as in (5), then $a^{-1}x^d$ is a CPP over \mathbb{F}_{p^n} .*

Proof. Since $\gcd(d, p^n - 1) = 1$, for each $a \in S$, the monomial $a^{-1}x^d$ is a PP over \mathbb{F}_{p^n} . To finish the proof, it suffices to prove that $x^d + ax$ permutes \mathbb{F}_{p^n} .

The fact $\gcd(d, p^n - 1) = 1$ shows that each nonzero element $\alpha \in \mathbb{F}_{p^n}$ can be represented as $\alpha = \beta^d$ for a unique $\beta \in \mathbb{F}_{p^n}^*$. Then

$$\begin{aligned} \sum_{x \in \mathbb{F}_{p^n}} \chi_n(\alpha(x^d + ax)) &= \sum_{x \in \mathbb{F}_{p^n}} \chi_n((\beta x)^d + \beta^{d-1}a\beta x) \\ &= \sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + \beta^{d-1}ax) \\ &= \sum_{x \in \mathbb{F}_{p^n}} \chi_n(x^d + \beta^{(\frac{p^{2k}+1}{2}+1)(p^{2k}-1)}ax). \end{aligned}$$

Since $\beta^{(\frac{p^{2k}+1}{2}+1)(p^{2k}-1)}a \in S$, it follows from Lemma 3.11 that for each $\alpha \in \mathbb{F}_{p^n}^*$, we have

$$\sum_{x \in \mathbb{F}_{p^n}} \chi_n(\alpha(x^d + ax)) = 0.$$

This completes the proof. \square

4 A class of trinomial CPPs

In this section, we consider a class of trinomial polynomials and show that they are CPPs.

Theorem 4.1. *For any odd prime p , $f(x) = -x + x^{\frac{p^{2m}+1}{2}} + x^{\frac{p^{2m}+1}{2}}p^m$ is a CPP over $\mathbb{F}_{p^{3m}}$.*

Proof. Note that

$$f(x) + x = x^{\frac{p^{2m}+1}{2}} + x^{\frac{p^{3m}+p^m}{2}} = g(x^{\frac{p^{2m}+1}{2}})$$

with $g(x) = x + x^{p^m}$. It follows that $f(x) + x$ is a PP over $\mathbb{F}_{p^{3m}}$ if and only if $g(x)$ is so, since $\gcd(\frac{p^{2m}+1}{2}, p^{3m} - 1) = 1$. By Lemma 2.4, $g(x)$ is a PP over $\mathbb{F}_{p^{3m}}$, so $f(x) + x$ is a PP.

In the following, we show that $f(x)$ is a PP over $\mathbb{F}_{p^{3m}}$. Write $h(x) := x + x^{p^m} - x^{1+p^m-p^{2m}}$, so that $f(x) = h(x^{\frac{p^{2m}+1}{2}})$. Since $\gcd(\frac{p^{2m}+1}{2}, p^{3m} - 1) = 1$, $f(x)$ is a PP over $\mathbb{F}_{p^{3m}}$ if and only if $h(x)$ is a PP over $\mathbb{F}_{p^{3m}}$. Note that $h(0) = 0$ and for $x \neq 0$,

$$h(x) = \frac{x^{1+p^{2m}} + x^{p^m+p^{2m}} - x^{1+p^m}}{x^{p^{2m}}}.$$

We first prove that $h(x) = 0$ if and only if $x = 0$. Suppose to the contrary that $h(x) = 0$ for some $x \neq 0$, that is,

$$x^{1+p^{2m}} + x^{p^m+p^{2m}} - x^{1+p^m} = 0.$$

Raising the above equation to the p^m -th power and the p^{2m} -th power respectively, we obtain

$$x^{1+p^m} + x^{1+p^{2m}} - x^{p^m+p^{2m}} = 0,$$

$$x^{p^m+p^{2m}} + x^{1+p^m} - x^{1+p^{2m}} = 0.$$

Adding the above two equations together, we deduce that $2x^{1+p^m} = 0$. So $x = 0$, contradicting to the assumption that $x \in \mathbb{F}_{p^{3m}}^*$. Thus $h(x) = 0$ if and only if $x = 0$.

Next, we prove that $h(x) = a$ has at most one nonzero solution for each $a \in \mathbb{F}_{p^{3m}}^*$, that is

$$x^{1+p^{2m}} + x^{p^m+p^{2m}} - x^{1+p^m} = ax^{p^{2m}} \quad (6)$$

has at most one nonzero solution for each $a \in \mathbb{F}_{p^{3m}}^*$. Raising both sides of Eq. (6) to the power of p^m and p^{2m} respectively, we get

$$x^{1+p^m} + x^{1+p^{2m}} - x^{p^m+p^{2m}} = a^{p^m} x,$$

$$x^{p^m+p^{2m}} + x^{1+p^m} - x^{1+p^{2m}} = a^{p^{2m}} x^{p^m}.$$

Adding the above two equations together, we obtain

$$2x^{1+p^m} = a^{p^m} x + a^{p^{2m}} x^{p^m}. \quad (7)$$

Because $x \neq 0$, we have $2x^{p^m} = a^{p^m} + a^{p^{2m}} x^{p^m-1}$. Setting $y = \frac{1}{x}$, we get

$$y^{p^m} + a^{p^{2m}-p^m} y - 2a^{-p^m} = 0. \quad (8)$$

If Eq. (8) has at least two distinct nonzero solutions y_1, y_2 in $\mathbb{F}_{p^{3m}}$ we get $y_1 - y_2 \in \mathbb{F}_{p^{3m}}$ is a root of $y^{p^m} + a^{p^{2m}-p^m} y = 0$, and so a root of $y^{p^m-1} + a^{p^{2m}-p^m} = 0$, contradicting to the fact that $y^{p^m-1} + a^{p^{2m}-p^m} = 0$ has no solution in $\mathbb{F}_{p^{3m}}^*$. Therefore, Eq. (8) has at most one nonzero solution in $\mathbb{F}_{p^{3m}}$. Hence $h(x) = a$ has at most one nonzero solution for each nonzero $a \in \mathbb{F}_{p^{3m}}$.

To sum up, we have shown that $h(x)$ is a PP, and thus $f(x)$ is a PP. The proof is now complete. \square

5 Two classes of trinomial PPs

It looks difficult to give a simple characterization of trinomial PPs over finite fields. In [5], the authors use different tricks including the multivariate method introduced by Dobbertin [?, 8] to construct several classes of trinomial PPs. In this section, we construct two classes of trinomial PPs over \mathbb{F}_{2^m} by similar techniques.

Theorem 5.1. *Let $m > 1$ be an odd integer, and write $k = \frac{m+1}{2}$. Then for each $u \in \mathbb{F}_{2^m}^*$, $f(x) = x + u^{2^{k-1}-1}x^{2^k-1} + u^{2^{k-1}}x^{2^k+1}$ is a PP over \mathbb{F}_{2^m} .*

Proof. Since $\gcd(2, 2^m - 1) = 1$, we need only to show that $h(x) = (f(x))^2 = x^2 + u^{2^k-2}x^{2^{k+1}-2} + u^{2^k}x^{2^{k+1}+2}$ is a PP over \mathbb{F}_{2^m} . Let $\bar{u} = u^{2^k}$ and $y = x^{2^k}$.

First, we prove that $h(x) = 0$ if and only if $x = 0$. Clearly, if $x = 0$, then $h(x) = 0$. Conversely, if there exists some $x \in \mathbb{F}_{2^m}^*$ such that

$$u^2x^4 + \bar{u}y^2 + \bar{u}u^2x^4y^2 = 0, \quad (9)$$

raising both sides of Eq. (9) to the 2^k -th power gives us

$$\bar{u}^2y^4 + u^2x^4 + \bar{u}^2u^2x^4y^4 = 0.$$

Since $\gcd(2, 2^m - 1) = 1$, we have

$$\bar{u}y^2 + ux^2 + \bar{u}ux^2y^2 = 0. \quad (10)$$

Adding Eq. (9) and Eq. (10) together, we obtain

$$u^2x^4 + ux^2 + \bar{u}u^2x^4y^2 + \bar{u}ux^2y^2 = 0, \quad (11)$$

which can be factorized as $ux^2(1 + ux^2)^{1+2^k} = 0$. It follows that $x^2 = \frac{1}{u}$, i.e., $x = \frac{1}{u^{2^{m-1}}}$. But $h(\frac{1}{u^{2^{m-1}}}) = \frac{1}{u} \neq 0$, which is a contradiction. Hence $h(x) = 0$ if and only if $x = 0$.

Next, if $h(x)$ is not a PP, then there exist $x \in \mathbb{F}_{2^m}^*$ and $a \in \mathbb{F}_{2^m}^*$ such that $h(x) = h(x + ax)$. Let $b = a^{2^k}$. It is clear that $a, b \neq 0, 1$. Since $h(x) = h(x + ax)$, we have

$$\frac{u^2x^4 + \bar{u}y^2 + \bar{u}u^2y^2x^4}{u^2x^2} = \frac{u^2(a^4 + 1)x^4 + \bar{u}(b + 1)^2y^2 + \bar{u}u^2(b + 1)^2y^2(a + 1)^4x^4}{u^2(a + 1)^2x^2},$$

which simplifies to

$$A_1x^2y^2 + A_2y^2 + A_3x^2 = 0, \quad (12)$$

with $A_1 = (a^2b^2 + a^2 + b^2 + b)u\bar{u}$, $A_2 = (b^2 + b)\bar{u}$, and $A_3 = (b + a^2)u$.

We claim that $A_1A_2A_3 \neq 0$. If $A_1 = 0$, we get $(b + 1)^2a^2 = b(b + 1)$. Thus $a^2 = \frac{b}{b+1}$. Raising both sides to the 2^k -th power, we get $b^2 = \frac{a^2}{a^2+1}$. Then $b^2 = b$, which leads to $b = 0$ or 1 , a contradiction. So $A_1 \neq 0$. A similar discussion shows that $A_2, A_3 \neq 0$.

Raising both sides of Eq. (12) to the 2^k -th power, we have

$$A_1^{2^k}x^4y^2 + A_3^{2^k}y^2 + A_2^{2^k}x^4 = 0. \quad (13)$$

By Eq. (12) and Eq. (13), cancelling y^2 , we get

$$B_1x^4 + B_2x^2 + B_3 = 0, \quad (14)$$

where $B_1 = A_3A_1^{2k} + A_1A_2^{2k} = (b^3(a+1)^4)\bar{u}u^3 \neq 0$, $B_2 = A_2^{2k+1} \neq 0$, $B_3 = A_3^{2k+1} \neq 0$.

Substituting $x^2 = \frac{B_2}{B_1}\gamma$ into Eq. (14), we obtain

$$\gamma^2 + \gamma + D = 0, \quad (15)$$

where $D = \frac{B_1B_3}{B_2^2} = D_1 + D_1^{2k}$ and $D_1 = \frac{A_1A_3^{2k+1}}{A_2^{2k+2}} = \frac{A_1B_3}{A_2B_2}$. We also have

$$\begin{aligned} \text{Tr}_m(D_1) &= \text{Tr}_m\left(\frac{A_1}{A_2}\left(\frac{A_3}{A_2}\right)^{2k+1}\right) \\ &= \text{Tr}_m\left(\left(1 + a^2 + \frac{a^2}{b}\right)\frac{(a^2+b)(a+b)^2}{a^2(a+1)^2b(b+1)}\right) \\ &= \text{Tr}_m\left(\frac{(a^2+b)(a+b)^2}{a^2(a+1)^2b(b+1)} + \frac{(a^2+b)(a+b)^2}{(a+1)^2b(b+1)} + \frac{(a^2+b)(a+b)^2}{(a+1)^2b^2(b+1)}\right) \\ &= \text{Tr}_m\left(\frac{a^2}{(a+1)^2b(b+1)} + \frac{1}{(a+1)^2} + \frac{b^2}{a^2(a+1)^2(b+1)} + \frac{a^4}{(a+1)^2b(b+1)} + \frac{a^2}{(a+1)^2} + \right. \\ &\quad \left. \frac{b^2}{(a+1)^2(b+1)} + \frac{a^4}{(a+1)^2b^2(b+1)} + \frac{a^2}{b(a+1)^2} + \frac{b}{(a+1)^2(b+1)}\right) \\ &= \text{Tr}_m\left(\frac{a^2}{(a+1)^2b(b+1)} + \frac{a^2}{b(a+1)^2} + \frac{b}{(a+1)^2(b+1)}\right) + \text{Tr}_m\left(\frac{1}{(a+1)^2} + \frac{a^2}{(a+1)^2}\right) \\ &\quad + \text{Tr}_m\left(\frac{b^2}{a^2(a+1)^2(b+1)} + \frac{a^4}{(a+1)^2b(b+1)} + \frac{b^2}{(a+1)^2(b+1)} + \frac{a^4}{(a+1)^2b^2(b+1)}\right) \\ &= 1. \end{aligned}$$

Raising both sides of Eq. (15) to the 2^i -th power, $0 \leq i \leq d-1$, and then summing them up, we get

$$\gamma^{2^k} = \gamma + \sum_{i=0}^{k-1} (D_1 + D_1^{2^k})^{2^i} = \gamma + D_1 + \text{Tr}_m(D_1) = \gamma + D_1 + 1. \quad (16)$$

It follows that

$$\gamma^{2^k+1} = D_1\gamma + D. \quad (17)$$

Combining Eqs. (12), (16) and (17), we obtain

$$C_1\gamma + C_2 = 0, \quad (18)$$

where $C_1 = A_1A_2^{2k+2} \neq 0$ and $C_2 = A_2^2B_1 \neq 0$. Thus $\gamma = \frac{C_2}{C_1}$. Then from Eq. (15), we get

$$B_1A_2^2 + A_1A_2B_2 = A_1^2B_3,$$

which leads to

$$b^2(b^2 + a^4) = a^4(b^4 + a^2).$$

Note that $\gcd(2, 2^m - 1) = 1$ whence

$$a^2b^2 + b^2 + a^2b + a^3 = 0.$$

Raising both sides of the above equation to the 2^k -th power, we get

$$a^4b^2 + a^4 + a^2b^2 + b^3 = 0.$$

It follows that

$$b^2(a^4 + b) = a^2(a^2 + b^2) = (a^3 + a^2b)(a + b) = b^2(1 + a^2)(a + b).$$

Then

$$b = \frac{a^3 + a^2 + 1}{a},$$

and raising both sides of the above equation to the 2^k -th power, we deduce that

$$a^8 + a^7 + a^6 + a^5 + a^4 + a^2 + 1 = 0.$$

Since $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$ is irreducible over \mathbb{F}_2 , by Lemma 2.5, $x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$ is irreducible over \mathbb{F}_{2^m} . Hence $a \notin \mathbb{F}_{2^m}^*$, which is a contradiction. This completes the proof. \square

Theorem 5.2. *Let $m > 1$ be an odd integer such that $m = 2k - 1$. Then $f(x) = x + ux^{2^k-1} + u^{2^k}x^{2^m-2^{k+1}+2}$, $u \in \mathbb{F}_{2^m}^*$, is a PP over \mathbb{F}_{2^m} .*

Proof. We first prove that $f(x) = 0$ if and only if $x = 0$. Let $\bar{u} = u^{2^k}$ and $y = x^{2^k}$. Clearly, if $x = 0$ then $f(x) = 0$. Conversely, suppose there exists some $x \in \mathbb{F}_{2^m}^*$ such that

$$x^2y^2 + uy^3 + \bar{u}x^4 = 0. \tag{19}$$

Raising both sides of the above equation to the 2^k -th power, we get

$$x^4y^2 + u^2y^4 + \bar{u}x^6 = 0. \tag{20}$$

Multiplying both sides of Eq. (19) by x^2 , we obtain

$$x^4y^2 + ux^2y^3 + \bar{u}x^6 = 0. \tag{21}$$

Adding Eq. (20) and Eq. (21) together, we have

$$ux^2y^3 + u^2y^4 = 0.$$

It follows that $x^2 = uy$. So we have $x = u^{2^{k-1}+1}$, which leads to a contradiction since $f(u^{2^{k-1}+1}) = u^{2^{k-1}+1} \neq 0$. Thus $f(x) = 0$ if and only if $x = 0$.

Next, let $\bar{a} = a^{2^k}$. We will show that $f(x) = a$ has a unique nonzero solution for each nonzero $a \in \mathbb{F}_{2^m}$. That is, for the equation

$$x^2y^2 + uy^3 + \bar{u}x^4 + axy^2 = 0, \quad (22)$$

there exists a unique solution $x \in \mathbb{F}_{2^m}^*$. Raising both sides of Eq. (22) to the 2^k -th power and multiplying Eq. (22) by x^2 , we get

$$x^4y^2 + \bar{u}x^6 + u^2y^4 + \bar{a}x^4y = 0, \quad (23)$$

and

$$x^4y^2 + ux^2y^3 + \bar{u}x^6 + ax^3y^2 = 0. \quad (24)$$

Summing Eq. (23) and Eq. (24), and dividing by y , we have

$$u^2y^3 + ux^2y^2 + \bar{a}x^4 + ax^3y = 0. \quad (25)$$

Computing Eq. (22)· u +Eq. (25), and dividing by x , we obtain

$$(\bar{a} + u\bar{u})x^3 + ax^2y + auy^2 = 0. \quad (26)$$

Raising both sides of Eq. (26) to the 2^k -th power, and then adding \bar{a} ·Eq. (22), we have

$$(\bar{a} + \bar{u}u^2 + \bar{a}u)y + a\bar{a}x = 0. \quad (27)$$

Solving Eqs. (26) and (27), we get

$$x = \frac{a^3\bar{a}^2}{b\bar{b}}, \quad (28)$$

Here, $b = a^2 + \bar{u}u^2 + \bar{a}u$ and $\bar{b} = b^{2^k}$, which can be directly verified to be nonzero. This completes the proof. \square

6 Differential properties of power functions

In this section, we consider the differential uniformity of monomial PPs. We first recall the basic definitions.

Definition 6.1. *Let F be a function from \mathbb{F}_{2^n} to \mathbb{F}_{2^m} . For any $a \in \mathbb{F}_{2^n}$, the derivative of F with respect to a is the function $D_a(F)$ from \mathbb{F}_{2^n} into \mathbb{F}_{2^m} defined by*

$$D_a(F(x)) = F(x+a) + F(x), \quad x \in \mathbb{F}_{2^n}.$$

The resistance to differential cryptanalysis is related to the following quantities.

Definition 6.2. Let F be a function from \mathbb{F}_{2^n} into \mathbb{F}_{2^n} . For any a and b in \mathbb{F}_{2^n} , we denote

$$\delta(a, b) = \#\{x \in \mathbb{F}_{2^n} \mid D_a(F(x)) = b\}.$$

Then the differential uniformity of F is

$$\delta(F) = \max_{a \neq 0, b \in \mathbb{F}_{2^n}} \delta(a, b).$$

Remark 6.1. In the case $F(x) = x^d$ is a monomial, for any nonzero $a \in \mathbb{F}_{2^n}$, the equation $(x+a)^d + x^d = b$ can be rewritten as $a^d \left(\left(\frac{x}{a} + 1 \right)^d + \left(\frac{x}{a} \right)^d \right) = b$. This implies that $\delta(a, b) = \delta(1, b/a^d)$. Therefore, for a monomial function, the differential properties are determined by the values $\delta(1, b), b \in \mathbb{F}_{2^n}$. From now on, we denote the quantity $\delta(1, b)$ by $\delta(b)$ for monomial functions.

The following two lemmas can be found in [2], which will be used later.

Lemma 6.1. [2] For a positive integer m and $a, b \in \mathbb{F}_{2^m}, a \neq 0$, the quadratic equation $x^2 + ax + b = 0$ has solutions in \mathbb{F}_{2^m} if and only if $\text{Tr}_m\left(\frac{b}{a^2}\right) = 0$.

Lemma 6.2. [2] For a positive integer m and $a \in \mathbb{F}_{2^m}^*$, the cubic equation $x^3 + x + a = 0$ has

- (1) a unique solution in \mathbb{F}_{2^m} if and only if $\text{Tr}_m(a^{-1} + 1) = 1$;
- (2) three distinct solutions in \mathbb{F}_{2^m} if and only if $p_m(a) = 0$, where the polynomial $p_m(x)$ is recursively defined by the equations $p_1(x) = p_2(x) = x$, $p_k(x) = p_{k-1}(x) + x^{2^{k-3}} p_{k-2}(x)$ for $k \geq 3$;
- (3) no solution in \mathbb{F}_{2^m} , otherwise.

As a preparation, we have the following lemma.

Lemma 6.3. Let $n = 2m$ with m odd, $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and $y \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$. Then the number of solutions of the equation $x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0$ is 0 or 4. Moreover, if x_0 is a solution, then the other three solutions are given by $x_0 + 1$, x_1 and $x_1 + 1$, where x_1 satisfies $x_1^2 + x_1 = x_0^2 + x_0 + 1 + y^2$.

Proof. If x_0 is a solution of equation $x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0$, then $x_0 + 1$ is also a solution. So we have

$$x^4 + y^2(x^2 + x + 1) + x + 1 + b = (x^2 + x + x_0^2 + x_0)(x^2 + x + x_0^2 + x_0 + 1 + y^2).$$

Since $\text{Tr}_n(x_0^2 + x_0 + 1 + y^2) = 0$, by Lemma 6.1 the equation $x^2 + x + x_0^2 + x_0 + 1 + y^2 = 0$ also has 2 solutions and these two solutions are different from x_0 and $x_0 + 1$. Hence the number of solutions of the equation $x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0$ is 0 or 4. The second part is obvious. \square

We now state our result.

Theorem 6.4. Let $n = 2m$ with m odd and $d = 2^{m+1} + 3$. Then $F_d : x \rightarrow x^d$ is a permutation over \mathbb{F}_{2^n} with $\delta(F_d) \leq 10$. Moreover, for $b \in \mathbb{F}_{2^m}$, we have $\delta(b) \in \{0, 4\}$.

Proof. It can be verified that $\gcd(d, 2^n - 1) = 1$, so F_d is a permutation. For each $x \in \mathbb{F}_{2^n}$, let $\bar{x} := x^{2^m}$. It is clear that $x + \bar{x} \in \mathbb{F}_{2^m}$ and $x\bar{x} \in \mathbb{F}_{2^m}$. We can then verify that

$$D_1(F_d(x)) = (x + 1)^d + x^d = (\bar{x}^2 + x)(x^2 + x + 1) + 1 = (\bar{x}x)^2 + ((\bar{x} + x)^2 + 1)(x + 1).$$

Then it suffices to show that for any $b \in \mathbb{F}_{2^n}$, the equation $D_1(F_d(x)) = b$ has at most 10 solutions.

Assume that

$$(\bar{x}x)^2 + ((\bar{x} + x)^2 + 1)(x + 1) = b. \quad (29)$$

Raising both sides of Eq. (29) to the 2^m -th power, we get

$$(\bar{x}x)^2 + ((\bar{x} + x)^2 + 1)(\bar{x} + 1) = \bar{b}. \quad (30)$$

Adding Eq. (29) and Eq. (30) together, we have

$$((\bar{x} + x)^2 + 1)(\bar{x} + x) = b + \bar{b}. \quad (31)$$

Setting $y := \bar{x} + x \in \mathbb{F}_{2^m}$ and $a := b + \bar{b} \in \mathbb{F}_{2^m}$, we obtain

$$y^3 + y + a = 0. \quad (32)$$

Replacing $\bar{x} = y + x$ into Eq. (29), we have

$$x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0. \quad (33)$$

Therefore, x is a solution of Eq. (29) if and only if it is a solution to following equations

$$\begin{cases} x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0, \\ y^3 + y + a = 0, \\ \bar{x} + x = y. \end{cases} \quad (34)$$

Hence $\delta(F_d) \leq 12$. Below, we consider the two cases where $a = 0$ and $a \neq 0$.

Case 1: $a = 0$

It is easy to see that $b \in \mathbb{F}_{2^m}$ and 0, 1 are solutions of Eq. (32). We consider these two cases separately.

(1) If $y = 0$, then $x \in \mathbb{F}_{2^m}$. Thus Eq. (34) will become $x^4 + x + 1 = b$, which has either 0 solution or 2 solutions. And it has 2 solutions if and only if $\text{Tr}_m(b) = 1$.

(2) If $y = 1$, then Eq. (34) becomes

$$\begin{cases} x^4 + x^2 + b = 0, \\ \bar{x} + x = 1. \end{cases} \quad (35)$$

Since $\gcd(2, 2^n - 1) = 1$, equation $x^4 + x^2 + b = 0$ is equivalent to $x^2 + x + b^{2^{m-1}} = 0$. Clearly it has 2 solutions by Lemma 6.1. Since $1 = \bar{x} + x = \sum_{i=0}^{m-1} (x^2 + x)^{2^i} = \text{Tr}_m(b^{2^{m-1}})$ we get that Eq. (35) has 2 solutions if and only if $\text{Tr}_m(b) = 1$.

Note that, for both cases, Eq. (34) has two solutions if and only if $\text{Tr}_m(b) = 1$. Therefore, $\delta(b) \in \{0, 4\}$.

Case 2: $a \neq 0$

In this case it is obvious that $b \notin \mathbb{F}_{2^m}$ and $y \notin \mathbb{F}_2$.

By Lemma 6.2, Eq. (32) has 0, 1 or 3 solutions. We consider these cases separately.

- (1) If Eq. (32) has no solution, then $\delta(b) = 0$.
- (2) If Eq. (32) has one solution, say y_0 , then by Lemma 6.3, Eq. (33) has 0 or 4 solutions given by $x_{11}, x_{11} + 1, x_{21}$ and $x_{21} + 1$. However, we need $x_{i1} + \overline{x_{i1}} = y_0$ holds for $i = 1, 2$. Thus $\delta(b) \in \{0, 2, 4\}$.
- (3) If Eq. (32) has three solutions, denoted by y_1, y_2 and y_3 . Then we have $y_1 + y_2 + y_3 = 0$. For each y_i , $1 \leq i \leq 3$, by Lemma 6.3, there are 0 or 4 solutions for Eq. (33). So the total number of solutions for x is 0, 4, 8 or 12.
 - (i) If the number of solutions for x is 0, 4 or 8, then the number of solutions to Eq. (34) is at most 8. Thus $\delta(b) \in \{0, 2, 4, 6, 8\}$.
 - (ii) If the number of solutions for x is 12, that is, for each y_i , $1 \leq i \leq 3$, there are 4 solutions of Eq. (33). Let the 12 solutions be $\{x_{ij}, x_{ij} + 1 | i = 1, 2, 3; j = 1, 2\}$, with y_i corresponding to $x_{i1}, x_{i1} + 1, x_{i2}$ and $x_{i2} + 1$. If $x_{i1}, x_{i1} + 1, x_{i2}$ and $x_{i2} + 1$ are exactly the solutions of Eqs. (34), we can easily get

$$\begin{cases} x_{i1} + x_{i2} + (x_{i1} + x_{i2})^2 = 1 + y_i^2, \\ x_{i1} + x_{i2} \in \mathbb{F}_{2^m}, \end{cases} \quad (36)$$

which means that the equation $t^2 + t + 1 + y_i^2 = 0$ has 2 solutions over \mathbb{F}_{2^m} . By Lemma 6.1, we have $\text{Tr}_m(1 + y_i^2) = 0$ so that $\text{Tr}_m(y_i) = 1$. Therefore, if $\delta(b) = 12$, then $\text{Tr}_m(y_1) = \text{Tr}_m(y_2) = \text{Tr}_m(y_3) = 1$. However, $1 = \text{Tr}_m(y_1) + \text{Tr}_m(y_2) + \text{Tr}_m(y_3) = \text{Tr}_m(y_1 + y_2 + y_3) = 0$, which is a contradiction. So $\delta(b) \leq 10$.

Thus we obtain $\delta(F_d) \leq 10$. □

Remark 6.2. For $d = 2^m + 2^{(m+1)/2} + 1$, we can obtain $\delta(F_d) \leq 10$ in a similar way. In fact, with $m = 2r - 1$ and $a := b + \overline{b}$, Eq. (34) now take the following form

$$\begin{cases} x^4 + (ay + 1)x^2 + ayx + (y^2 + 1)\overline{b}^{2^r} + b\overline{b} = 0, \\ (y + 1)x^{2^r} + x^2 + yx + y + 1 + b = 0, \\ y^3 + (a + 1)y^2 + a^{2^r}y + a^{2^r} = 0, \\ \overline{x} + x = y. \end{cases} \quad (37)$$

Hence $\delta(F_d) \leq 12$. If $b \in \mathbb{F}_{2^m}$, we can easily get $\delta(b) \in \{0, 4\}$. If $\delta(b) = 12$ for some $b \in \mathbb{F}_{2^m} \setminus \mathbb{F}_{2^r}$, we have $\text{Tr}_m(ay_i) = 1$, and $1 = \text{Tr}_m(ay_1) + \text{Tr}_m(ay_2) + \text{Tr}_m(ay_3) = \text{Tr}_m(a(a + 1)) = 0$, which is a contradiction.

Hence we have the following result.

Theorem 6.5. *Let $n = 2m$ with m odd and $d = 2^m + 2^{(m+1)/2} + 1$. Then $F_d : x \rightarrow x^d$ is a permutation over \mathbb{F}_{2^n} with $\delta(F_d) \leq 10$. Moreover, for $b \in \mathbb{F}_{2^m}$, we have $\delta(b) \in \{0, 4\}$.*

Remark 6.3. *Here we give a concrete example to illustrate the idea of the proof. Let w be a primitive element of \mathbb{F}_{2^n} , $n = 10$, $d = 67$, $b = w^{27}$ and $a = b + \bar{b}$. Then Eq. (32) and Eq. (33) become $y^3 + y + a = 0$ and $x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0$ respectively.*

Solutions of $y^3 + y + a = 0$	$\text{Tr}_m(y_i)$	Solutions of $x^4 + y^2(x^2 + x + 1) + x + 1 + b = 0$	Solutions of $D_1(F_d(x)) = b$
$y_1 = w^{330}$	1	$\{w^{672}, w^{1019}; w^{619}, w^{975}\}$	$w^{226}, w^{633},$
$y_2 = w^{363}$	1	$\{w^{226}, w^{633}; w^{586}, w^{903}\}$	$w^{586}, w^{903},$
$y_3 = w^{924}$	0	$\{w^{129}, w^{340}; w^{774}, w^{883}\}$	w^{129}, w^{340}

In the above table, for a fixed element b , we obtain 3 solutions of Eq. (32), denoted by y_1 , y_2 and y_3 . For each y_i , by Eq. (33) we get 4 solutions. We need to determine whether they are satisfying $x + \bar{x} = y_i$. Since $\text{Tr}_m(y_3) = 0$, there are at least 2 solutions which are not satisfying $x + \bar{x} = y_3$ (in the above example, w^{774} and w^{883} are not). However, for each y_i , $i = 1, 2$, we can not determine whether the 4 solutions are satisfying $x + \bar{x} = y_i$ since $\text{Tr}_m(y_1) = \text{Tr}_m(y_2) = 1$ (in the above example, the four solutions corresponding to y_1 are not, while the four solutions corresponding to y_2 are). Therefore, in our proof we only can get $\delta(b) \leq 10$, but in fact $\delta(b) = 6$ for this example. Thus, we need to find more detailed conditions to characterize the solutions of the equation.

7 Conclusion

Permutation and CPPs have important applications in cryptography. This paper demonstrates some new results on permutation and CPPs. First, by using the AGW Criterion, we proved a conjecture proposed by Wu et al. [24]. Then we give three other new classes of monomial CPPs over finite fields and the main tool is additive characters over the underlying finite fields. Moreover, a class of trinomial CPPs and two classes of trinomial PPs are also presented in this paper. Finally, for $d = 2^{m+1} + 3$ or $2^m + 2^{\frac{m+1}{2}} + 1$, Blondeau et al. [3] conjectured that x^d is differentially 8-uniform over \mathbb{F}_{2^n} , where $n = 2m$. We make some progress towards this conjecture and prove that the differential uniformity of x^d is at most 10. It seems not easy to exclude the possibility that $\delta(b) = 10$ for some $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. We look forward to seeing further progress on this conjecture.

Acknowledgements

The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper. The research of T. Feng was supported by Fundamental Research Fund for the Central Universities of China, the National Natural Science Foundation of China under Grant No. 11201418 and Grant No. 11422112, and the Research Fund for Doctoral Programs from the Ministry of Education of China under Grant

20120101120089. The research of G. Ge was supported by the National Natural Science Foundation of China under Grant Nos. 11431003 and 61571310.

References

- [1] A. AKBARY, D. GHIOCA, AND Q. WANG, *On constructing permutations of finite fields*, Finite Fields Appl., 17 (2011), pp. 51–67.
- [2] E. R. BERLEKAMP, H. RUMSEY, AND G. SOLOMON, *On the solution of algebraic equations over finite fields*, Inform. Control, 10 (1967), pp. 553–564.
- [3] C. BLONDEAU, A. CANTEAUT, AND P. CHARPIN, *Differential properties of power functions*, Int. J. Inf. Coding Theory, 1 (2010), pp. 149–170.
- [4] P. CHARPIN AND G. M. KYUREGHYAN, *Cubic monomial bent functions: a subclass of \mathcal{M}* , SIAM J. Discrete Math., 22 (2008), pp. 650–665.
- [5] C. DING, L. QU, Q. WANG, J. YUAN, AND P. YUAN, *Permutation trinomials over finite fields with even characteristic*, SIAM J. Discrete Math., 29 (2015), pp. 79–92.
- [6] C. DING, Q. XIANG, J. YUAN, AND P. YUAN, *Explicit classes of permutation polynomials of \mathbb{F}_{3^m}* , Sci. China Ser. A, 52 (2009), pp. 639–647.
- [7] C. DING AND J. YUAN, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A, 113 (2006), pp. 1526–1535.
- [8] H. DOBBERTIN, *Kasami power functions, permutation polynomials and cyclic difference sets*, in Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), vol. 542 of NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Kluwer Acad. Publ., Dordrecht, 1999, pp. 133–158.
- [9] N. FERNANDO AND X. HOU, *A piecewise construction of permutation polynomials over finite fields*, Finite Fields Appl., 18 (2012), pp. 1184–1194.
- [10] T. HELLESETH, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math., 16 (1976), pp. 209–232.
- [11] H. D. L. HOLLMANN AND Q. XIANG, *A class of permutation polynomials of \mathbb{F}_{2^m} related to Dickson polynomials*, Finite Fields Appl., 11 (2005), pp. 111–122.
- [12] X. HOU, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A, 118 (2011), pp. 448–454.
- [13] ———, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl., 18 (2012), pp. 492–521.

- [14] ———, *Permutation polynomials over finite fields—a survey of recent advances*, *Finite Fields Appl.*, 32 (2015), pp. 82–119.
- [15] Y. LAIGLE-CHAPUY, *Permutation polynomials and applications to coding theory*, *Finite Fields Appl.*, 13 (2007), pp. 58–70.
- [16] N. LI, T. HELLESETH, AND X. TANG, *Further results on a class of permutation polynomials over finite fields*, *Finite Fields Appl.*, 22 (2013), pp. 16–23.
- [17] R. LIDL AND H. NIEDERREITER, *Finite fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.
- [18] H. NIEDERREITER AND K. H. ROBINSON, *Complete mappings of finite fields*, *J. Austral. Math. Soc. Ser. A*, 33 (1982), pp. 197–212.
- [19] L. QU, Y. TAN, C. H. TAN, AND C. LI, *Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method*, *IEEE Trans. Inform. Theory*, 59 (2013), pp. 4675–4686.
- [20] J. SUN AND O. Y. TAKESHITA, *Interleavers for turbo codes using permutation polynomials over integer rings*, *IEEE Trans. Inform. Theory*, 51 (2005), pp. 101–119.
- [21] Z. TU, X. ZENG, AND L. HU, *Several classes of complete permutation polynomials*, *Finite Fields Appl.*, 25 (2014), pp. 182–193.
- [22] Z. TU, X. ZENG, L. HU, AND C. LI, *A class of binomial permutation polynomials*. arXiv:1310.0337.
- [23] G. WU, N. LI, T. HELLESETH, AND Y. ZHANG, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two*, *Finite Fields Appl.*, 28 (2014), pp. 148–165.
- [24] G. WU, N. LI, T. HELLESETH, AND Y. ZHANG, *Some classes of complete permutation polynomials over \mathbb{F}_q* , *Sci. China Math.*, 58 (2015), pp. 2081–2094.
- [25] J. YUAN AND C. DING, *Four classes of permutation polynomials of \mathbb{F}_{2^m}* , *Finite Fields Appl.*, 13 (2007), pp. 869–876.
- [26] J. YUAN, C. DING, H. WANG, AND J. PIEPRZYK, *Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$* , *Finite Fields Appl.*, 14 (2008), pp. 482–493.
- [27] Z. ZHA AND L. HU, *Two classes of permutation polynomials over finite fields*, *Finite Fields Appl.*, 18 (2012), pp. 781–790.
- [28] M. E. ZIEVE, *Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares*. arXiv:1312.1325.