The $c-$differential uniformity and boomerang uniformity of three classes of permutation polynomials over $\mathbb{F}_{2^n}$

Qian Liu [1,2] [*], Zhiwei Huang [1,2], Jianrui Xie [3], Ximeng Liu [1,2], Jian Zou [1,2]
1. College of Computer and Data Science, Fuzhou University, Fuzhou 350116, China
2. Key Laboratory of Information Security of Network Systems, Fuzhou University, Fuzhou 350116, China
3. Independent researcher, No. 2800 Chuangxin Avenue, Hefei 230088, China

Abstract

Permutation polynomials with low c-differential uniformity and boomerang uniformity have wide applications in cryptography. In this paper, by utilizing the Weil sums technique and solving some certain equations over $\mathbb{F}_{2^n}$, we determine the c-differential uniformity and boomerang uniformity of these permutation polynomials: (1) $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$, where $n = 2k+1$, $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$; (2) $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x+1)^{2^k+3})$, where $n = 2k+1$; (3) $f_3(x) = x^{-1} + \mathrm{Tr}_1^n((x^{-1}+1)^d + x^{-d})$, where n is even and d is a positive integer. The results show that the involutions $f_1(x)$ and $f_2(x)$ are APcN functions for $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$. Moreover, the boomerang uniformity of $f_1(x)$ and $f_2(x)$ can attain 2^n. Furthermore, we generalize some previous works and derive the upper bounds on the c-differential uniformity and boomerang uniformity of $f_3(x)$.

Keywords: C-differential uniformity, Boomerang uniformity, Permutation polynomial.
Mathematics Subject Classification 94A60, 11T06, 11T55

1 Introduction

Let q be a power of a prime p, $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{F}_q^*$ be its multiplicative group. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial if its associated polynomial $f : c \mapsto f(c)$ from $\mathbb{F}_q$ into itself is a bijection [18]. Moreover, f is called an involution if the compositional inverse of f is itself. Permutation polynomials over finite fields have been a hot topic of study for many years due to their significant applications in cryptography, design theory, coding theory, and other areas of mathematics and engineering. In particular, permutation polynomials with low differential uniformity, such as substitution boxes (S-boxes), which refer to vectorial Boolean functions, play an important role in block ciphers. The reader can see the recent book of [7] for more details concerning vectorial Boolean functions and their cryptographic properties.

Inspired by a practical differential attack on ciphers, multiplicative differential utilizing modular multiplication as a primitive operation was introduced by Borisov et al. [5] and was redefined by Ellingsen et al. [10]. They characterized the c-differential uniformity of some known PN functions and their inverses for the first time. Hasan et al. [11] focused on the (-1)-differential uniformity of

[*] e-mail: lqmova@foxmail.com

monomial functions and exhibited some PcN power maps over finite fields of odd characteristics. Bartoli and Calderini [2] applied the AGW criterion [1] and its generalization to the construction of PcN and APcN functions. Determining the c-differential uniformity of several classes of power functions, including PcN and APcN functions, Mesnager et al. [20] extended the work in [2, 10, 11], especially about the c-differential uniformity of some known APN functions with odd characteristics. While Zha and Hu [31] presented power functions with low c-differential uniformity such as $\mathrm{P}_{-1}\mathrm{N}$, Yan [30] obtained ternary power functions with low (-1)-differential uniformity such as $\mathrm{AP}_{-1}\mathrm{N}$. Through the cyclotomic technique, the switch method, and the AGW criteria, Wu and Li [29] constructed $\mathrm{P}_c\mathrm{N}$ and $\mathrm{AP}_c\mathrm{N}$ multinomial functions. To the best of our knowledge, there are only a few functions with low c-differential uniformity over finite fields with even characteristics for $c \neq 1$. Stănică [23] characterized the c-differential uniformity of the binary $(0, 1)$-swapped inverse function. By solving a two-equation system on two parameters, Tu et al. [26] gave the second class of APcN power functions over finite fields of even characteristic. Recently, Li et al. [16] constructed low c-differential uniformity functions in even and odd characteristics via generalizing Dillon's switching method, and generalized some results of [29].

Boomerang attack introduced by Wanger [27] is an important cryptanalysis technique against block ciphers. It can be regarded as an extension of classical differential attack [4]. In Eurocrypt 2018, Cid et al. [9] firstly proposed a new tool called the Boomerang Connectivity Table (BCT) to evaluate the resistance of block ciphers against boomerang attack. They also gave some relations between BCT and DDT (Differential Distribution Table). Boura and Canteaut [6] further studied the boomerang uniformity of differentially 4-uniform permutations of 4-bit S-boxes and also determined the boomerang uniformity of the inverse function and quadratic permutations. Later, Li et al. [15] provided an equivalent formula to compute the boomerang uniformity of a cryptographic function. Moreover, they proposed some 4-uniform BCT permutation polynomials over $\mathbb{F}_{2^n}$. Mesnager et al. [21] considered the boomerang uniformity of quadratic permutations by using the relation between BCT and DDT. Generally speaking, the functions with boomerang uniformity four offer the best resistance to boomerang attacks. Currently, only six classes of 4-uniform BCT permutations have been discovered. The readers can refer to [2, 13–15, 17, 21, 25] for more details. Recent trends towards generalized differential and boomerang uniformities can be found in [19] and the references therein.

In particular, Hasan et al. [12] characterized the c-differential uniformity and boomerang uniformity of two classes of permutation polynomials, which was studied in [3] and [24]. Motivated by their work, this paper aims to find more permutation polynomials over $\mathbb{F}_{2^n}$ with low c-differential uniformity and boomerang uniformity. In this paper, we determine the c-differential uniformity and boomerang uniformity of the following three classes of permutation polynomials:

(1) $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$, where $n = 2k + 1$, $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$;

(2) $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x + 1)^{2^k+3})$, where $n = 2k + 1$;

(3) $f_3(x) = x^{-1} + \mathrm{Tr}_1^n((x^{-1} + 1)^d + x^{-d})$, where n is even and d is a positive integer.

The reason for choosing these three classes of permutation polynomials is as follows:

(1) By using the Gold function, the function $G(x) = x + \mathrm{Tr}_1^n(\alpha x + x^{2^k+1})$ is an involution over $\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$, $\gcd(k, n) = 1$ [3]. Recently, the c-differential uniformity and boomerang uniformity of $G(x)$ have been determined by utilizing Weil sums technique in [12]. Motivated by their work, we consider the involution $f_1(x)$ by using Welch permutation polynomial $x^{2^{k+1}+1}+x^3+x$ over $\mathbb{F}_{2^{2k+1}}$ and calculate the c-differential uniformity and boomerang uniformity of $f_1(x)$ by using Weil sums technique. The result shows that $f_1(x)$ is an APcN function for $c \in \mathbb{F}_{2^n}\backslash\{0, 1\}$ with boomerang uniformity of 2^n.

(2) In [8], the authors showed that for any $h(x) \in \mathbb{F}_{2^n}[x]$, the function $f(x) = x + \mathrm{Tr}_1^n(h(x) + h(x+1))$ is a permutation polynomial over $\mathbb{F}_{2^n}$. Inspired by their work, let $h(x) = x^{2^k+3}$ be a Welch function over $\mathbb{F}_{2^{2k+1}}$, we consider the c-differential uniformity and boomerang uniformity of the involution $f_2(x)$ by using Weil sums technique. The result shows that $f_2(x)$ is also an APcN function for $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$ with boomerang uniformity of 2^n.

(3) Let n be even and $d \in \{2^n - 2, 2^{\frac{n}{2}} + 2^{\frac{n}{4}} + 1, 2^{t_1} + 1, 3(2^{t_2} + 1)\}$, where $1 \leq t_1 \leq \frac{n}{2} - 1$ and $2 \leq t_2 \leq \frac{n}{2} - 1$, the function $G(x) = x^{-1} + \mathrm{Tr}_1^n((x^{-1} + 1)^d + x^{-d})$ is a differentially 4-uniform permuation polynomial over $\mathbb{F}_{2^n}$ (see [24]). Recently, the upper bounds on the c-differential uniformity and boomerang uniformity of $G(x)$ for $d = 2^n - 2$ had been given in [12]. Motivated by their work, we propose the upper bounds on the c-differential uniformity and boomerang uniformity of $f_3(x)$ for any positive integer d.

The remainder of the paper is organized as follows. In Section 2, we introduce some preliminaries needed in the sequel. In Section 3, the c-differential uniformity of three classes of permutation polynomials over $\mathbb{F}_{2^n}$ is given. In Section 4, the boomerang uniformity of three classes of permutation polynomials over $\mathbb{F}_{2^n}$ is proposed. Finally, we give some concluding remarks in Section 5.

2 Preliminaries

For two positive integers m and n with $m \mid n$, we use $\mathrm{Tr}_m^n(\cdot)$ to denote the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, i.e.,

$$\mathrm{Tr}_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \ldots + x^{2^{(n/m-1)m}}.$$

For $m = 1$, the absolute trace function is defined by $\mathrm{Tr}_1^n(x) = \sum\limits_{i=0}^{n-1} x^{2^i}$.

Lemma 1. ([18]) *The trace function $\mathrm{Tr}_1^n(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ has the following properties:*
(1) $\mathrm{Tr}_1^n(ax + by) = a\mathrm{Tr}_1^n(x) + b\mathrm{Tr}_1^n(y)$ for all $x, y \in \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_2$.
(2) $\mathrm{Tr}_1^n(x^2) = \mathrm{Tr}_1^n(x)$ for all $x \in \mathbb{F}_{2^n}$.
(3) Let $m|n$, then $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(x))$ for all $x \in \mathbb{F}_{2^n}$.

Definition 1. ([7]) *For a Boolean function $f(x) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$, the Walsh transform of $f(x)$ at $\omega \in \mathbb{F}_{2^n}$ is defined as*

$$W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)}.$$

Definition 2. ([22]) *For any function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, its derivative with respect to $a \in \mathbb{F}_{p^n}$ is defined by*

$$D_a f(x) = f(x + a) - f(x).$$

Let $\Delta_f(a, b)$ be the cardinality of the solution set of $D_a f(x) = b$ for $a, b \in \mathbb{F}_{p^n}$, then the differential uniformity of $f(x)$ is

$$\Delta_f = \max_{a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}} \Delta_f(a, b).$$

Particularly, $f(x)$ is called a perfect nonlinear (PN) function if $\Delta_f = 1$ or an almost perfect nonlinear (APN) function if $\Delta_f = 2$.

Definition 3. ([10]) *For any function $f(x):\mathbb{F}_{p^n}\mapsto\mathbb{F}_{p^n}$, its c-derivative with respect to $a\in\mathbb{F}_{p^n}$ is defined by*

$$ {}_cD_af(x)=f(x+a)-cf(x), $$

where $c\in\mathbb{F}_{p^n}$. Correspondingly, let ${}_c\Delta_f(a,b)$ be the cardinality of the solution set of ${}_cD_af(x)=b$ for $a,b\in\mathbb{F}_{p^n}$, then

$$ {}_c\Delta_f=\max_{a,b\in\mathbb{F}_{p^n},a\neq0\ \text{if}\ c=1}{}_c\Delta_f(a,b) $$

defines the c-differential uniformity of $f(x)$.

Note that differential uniformity is an instance of c-differential uniformity when $c=1$. In particular, $f(x)$ is called a perfect c-nonlinear (PcN) function if ${}_c\Delta_f=1$ or an almost perfect c-nonlinear (APcN) function if ${}_c\Delta_f=2$.

Definition 4. ([15]) *For a given permutation $f(x):\mathbb{F}_{2^n}\mapsto\mathbb{F}_{2^n}$, the BCT of $f(x)$ is a $2^n\times2^n$ table, the value at the position $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of which is the number of solution pairs $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ of the following system*

$$ \begin{cases} f(x)+f(y)=b\\ f(x+a)+f(y+a)=b. \end{cases} $$

The boomerang uniformity of $f(x)$, denoted by $\mathcal{B}_f$, is given by

$$ \mathcal{B}_f=\max_{a\in\mathbb{F}_{2^n}^*,b\in\mathbb{F}_{2^n}^*}\mathcal{B}_f(a,b). $$

Lemma 2. ([18]) *The number $N(b)$ of solutions $(x_1,x_2,\ldots,x_n)\in\mathbb{F}_{2^n}^n$, for a fixed $b\in\mathbb{F}_{2^n}$, of the equation $f(x_1,x_2,\ldots,x_n)=b$ is*

$$ N(b) = \frac{1}{2^n}\sum_{x_1,x_2,\ldots,x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(f(x_1,x_2,\ldots,x_n)-b))}. $$

Similarly, the number $\hat{N}(b)$ of solutions $(x_1,x_2,\ldots,x_n)\in\mathbb{F}_{2^n}^n$, for a fixed $b=(b_1,b_2)\in\mathbb{F}_{2^n}^2$, of the system

$$ \begin{cases} f_1(x_1,x_2,\ldots,x_n)=b_1\\ f_2(x_1,x_2,\ldots,x_n)=b_2, \end{cases} $$

is

$$ \hat{N}(b) = \frac{1}{2^{2n}}\sum_{x_1,x_2,\ldots,x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(x_1,x_2,\ldots,x_n)-b_1))}\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\gamma(f_2(x_1,x_2,\ldots,x_n)-b_2))}. $$

3 The c-differential uniformity of three classes of permutation polynomials

In this section, we investigate the c-differential uniformity of the following three classes of permutation polynomials:

(1) $f_1(x)=x+\mathrm{Tr}_1^n(x^{2^{k+1}+1}+x^3+x+ux)$, where $n=2k+1$, $u\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$;

(2) $f_2(x)=x+\mathrm{Tr}_1^n(x^{2^k+3}+(x+1)^{2^k+3})$, where $n=2k+1$;

(3) $f_3(x)=x^{-1}+\mathrm{Tr}_1^n((x^{-1}+1)^d+x^{-d})$, where n is even and d is a positive integer.

3.1 The c-differential uniformity of the first class of permutation polynomials

Lemma 3. *For any two positive integers n, k with $n = 2k+1$, let $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$. Then $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$ is an involution over $\mathbb{F}_{2^n}$.*

Proof. Since $n = 2k+1$, we have $\mathrm{Tr}_1^n(1) = 1$. Let $y = x^{2^{k+1}+1} + x^3 + x + ux$, then

$$\begin{aligned} f_1(f_1(x)) &= f_1(x) + \mathrm{Tr}_1^n((x + \mathrm{Tr}_1^n(y))^{2^{k+1}+1} + (x + \mathrm{Tr}_1^n(y))^3 + (x + \mathrm{Tr}_1^n(y)) + u((x + \mathrm{Tr}_1^n(y)))) \\ &= f_1(x) + \mathrm{Tr}_1^n(y) + \mathrm{Tr}_1^n(\mathrm{Tr}_1^n(y)) + \mathrm{Tr}_1^n(y)\mathrm{Tr}_1^n(u) \\ &= x. \end{aligned}$$

Hence, $f_1(x)$ is an involution over $\mathbb{F}_{2^n}$. □

Lemma 4. *For any two positive integers n, k with $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, let $L_1(x) = x^{2^{-(k+1)}} + x^{2^{k+1}} + x^{2^{-1}} + x^2 \in \mathbb{F}_{2^n}[x]$. Then $L_1(x) = 0$ has two solutions $x = 0, 1$ in $\mathbb{F}_{2^n}$.*

Proof. Since $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, we have $\gcd(n, k-1) = \gcd(2k+1, k-1) = \gcd(3, k-1) = 1$ and $\gcd(n, k+1) = \gcd(2k+1, k+1) = \gcd(k, k+1) = \gcd(1, k) = 1$.

Raising 2^{3k+1}-th power on both sides of $L_1(x) = 0$ gives

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

Let $L_1'(x) = x^{2^{2k}} + x + x^{2^{k-1}} + x^{2^{k+1}}$. From [18], we know that the conventional associate of the linearized polynomial $L_1'(x)$ is $A_1(x) = x^{2k} + x^{k+1} + x^{k-1} + 1$ and $\gcd(L_1'(x), x^{2^n} + x)$ is the linearized associate of $\gcd(A_1(x), x^n + 1)$. Therefore, to prove the claim that $L_1'(x) = 0$ has two solutions $x = 0, 1$ in $\mathbb{F}_{2^n}$, it suffices to show that $\gcd(A_1(x), x^n + 1) = x + 1$, which follows from $A_1(x) = (x^{k+1} + 1)(x^{k-1} + 1)$ and $\gcd(n, k+1) = \gcd(n, k-1) = 1$. □

Theorem 1. *For any two positive integers n, k with $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, let $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$ and $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$. Then for $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we have*

$$\Delta_{f_1}(a, b) = \begin{cases} 2^n & \text{if } (a, b) = (1, 1) \\ 2^{n-1} & \text{if } (a, b) \neq (1, 1), f_1(a) \in \{b, b+1\} \\ 0 & \text{otherwise}, \end{cases}$$

and $\Delta_{f_1} = 2^n$.

Proof. Recall that $L_1(x) = x^{2^{-(k+1)}} + x^{2^{k+1}} + x^{2^{-1}} + x^2$. By Definition 2, we consider the equation $b = D_a f_1(x) = f_1(x+a) + f_1(x)$, which can be further written as

$$\mathrm{Tr}_1^n(xL_1(a)) = f_1(a) + b. \tag{1}$$

Since $L_1(1) = 0$ and $f_1(1) = 1$, Eq. (1) has 2^n solutions if $(a, b) = (1, 1)$ and no solution if $(a, b) \in \{(\zeta, \xi) \mid \zeta = 1, \xi \neq 1\}$. By Lemma 4, $L_1(a) \neq 0$ for $a \notin \{0, 1\}$, then Eq. (1) has 2^{n-1} solutions if $f_1(a) \in \{b, b+1\}$ and has no solution otherwise.

Clearly,

$$\Delta_{f_1} = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_{f_1}(a, b) = 2^n.$$

□

Example 1. *Take $n = 5$, $k = 2$ and $c = 1$. There are 16 different $u \in \mathbb{F}_{2^5}$ satisfying $\mathrm{Tr}_1^5(u) = 1$. We can select $u = \alpha^5$, where α is a root of the primitive polynomial $x^5 + x^2 + 1$. By computer, it can be verified that the differential uniformity of*

$$f_1(x) = x + \mathrm{Tr}_1^5(x^9 + x^3 + x + \alpha^5 x)$$

is 32.

Remark 1. *For any two positive integers n, k with $n = 2k + 1$, let $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$. Then $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$ is a PcN function for $c = 0$.*

Theorem 2. *For any two positive integers n, k with $n = 2k + 1$, let $g_1(x) = \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x)$ over $\mathbb{F}_{2^n}$. Then*

$$W_{g_1}(\alpha) = \begin{cases} 0 & if\ \mathrm{Tr}_1^n(\alpha) = 0 \\ (-1)^{\mathrm{Tr}_1^n(\theta^{2^{k+1}+1} + \theta^{2^{k+1}+2^k})} W_{g_1}(1) & if\ \mathrm{Tr}_1^n(\alpha) = 1, \end{cases}$$

where $\theta \in \mathbb{F}_{2^n}$ satisfying $L_1(\theta) = \alpha + 1$.

Proof. Recall that $L_1(x) = x^{2^{-(k+1)}} + x^{2^{k+1}} + x^{2^{-1}} + x^2$. Let $\theta \in \mathbb{F}_{2^n}$, then by Definition 1,

$$\begin{aligned} W_{g_1}(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n((x+\theta)^{2^{k+1}+1} + (x+\theta)^3 + (x+\theta) + \alpha(x+\theta))} \\ &= (-1)^{\mathrm{Tr}_1^n(\theta^{2^{k+1}+1} + \theta^3 + \theta + \alpha\theta)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + x(L_1(\theta) + \alpha))}. \end{aligned}$$

It is easy to see that $\mathrm{Tr}_1^n(L_1(\theta)) = 0$. So we choose a θ such that $L_1(\theta) = \alpha$ if $\mathrm{Tr}_1^n(\alpha) = 0$, then the sum arrives at $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x)}$, which is 0. Thus, $W_{g_1}(\alpha) = 0$.

If $\mathrm{Tr}_1^n(\alpha) = 1$, we choose a θ such that $L_1(\theta) = \alpha + 1$. The sum becomes $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3)} = W_{g_1}(1)$. That leads to

$$W_{g_1}(\alpha) = (-1)^{\mathrm{Tr}_1^n(\theta^{2^{k+1}+1} + \theta^{2^{k+1}+2^k})} W_{g_1}(1).$$

□

Remark 2. *In order to evaluate $W_{g_1}(\alpha)$, it suffices to calculate $W_{g_1}(1)$. Notice that the Walsh spectrum of the trace of the Welch permutation polynomial $g_1(x) = \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x)$ over $\mathbb{F}_{2^{2k+1}}$ had been given in [28], so we can obtain $W_{g_1}(1) \in \{\pm 2^{k+1}, \pm 2^{k+2}\}$.*

Theorem 3. *For any two positive integers n, k with $n = 2k + 1$ and $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$, let $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$. Then for any $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$, we have*

$${}_c\Delta_{f_1}(a, b) = \begin{cases} 0 & if\ A = 1\ and\ B = 1 \\ 1 & if\ B = 0 \\ 2 & if\ A = 0\ and\ B = 1, \end{cases}$$

where $A = \mathrm{Tr}_1^n((a + b)L_1(a)(1 + c)^{-1} + a^{2^{k+1}+1} + a^3 + a + ua)$ and $B = \mathrm{Tr}_1^n(L_1(a)(1 + c)^{-1})$. Moreover, $f_1(x)$ is an APcN function for $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$.

Proof. For sake of conciseness, let $h_1(x) = x^{2^{k+1}+1} + x^3 + x + ux$, then $f_1(x) = x + \mathrm{Tr}_1^n(h_1(x))$. By Definition 3, we consider the equation $b = cD_af_1(x) = f_1(x+a) + cf_1(x)$, which can be further written as

$$(1+c)f_1(x) + \mathrm{Tr}_1^n(ax^{2^{k+1}} + a^{2^{k+1}}x + ax^2 + a^2x) + f_1(a) + b = 0.$$

Recall that $L_1(x) = x^{2^{-(k+1)}} + x^{2^{k+1}} + x^{2^{-1}} + x^2$. Then by Definition 3 and Lemma 2, we have

$$\begin{aligned}
{}_c\Delta_{f_1}(a,b) &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta((1+c)f_1(x)+\mathrm{Tr}_1^n(xL_1(a))+f_1(a)+b))}\\
&= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_1(x))+\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_1(a))}\\
&= \frac{1}{2^n}(M_0+M_1),
\end{aligned}$$

where M_0 and M_1 are the sums corresponding to $\mathrm{Tr}_1^n(\beta)=0$ and $\mathrm{Tr}_1^n(\beta)=1$, respectively. Apparently,

$$\begin{aligned}
M_0 &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_1(x))}\\
&= 2^n + \sum_{\beta\in\mathbb{F}_{2^n}^*,\mathrm{Tr}_1^n(\beta)=0}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_1(x))}\\
&= 2^n.
\end{aligned}$$

The last equality above holds because $\beta(1+c)\neq 0$ and $f_1(x)$ is a permutation of $\mathbb{F}_{2^n}$, leading the inner sum to zero. Similarly,

$$\begin{aligned}
M_1 &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(1+c)(x+\mathrm{Tr}_1^n(h_1(x))))+\mathrm{Tr}_1^n(xL_1(a))}\\
&= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1}(-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta(1+c))\mathrm{Tr}_1^n(h_1(x))+\mathrm{Tr}_1^n(x(L_1(a)+\beta(1+c)))}\\
&= M_{1,1}+M_{1,0},
\end{aligned}$$

where $M_{1,1}$ and $M_{1,0}$ are the sums corresponding to $\mathrm{Tr}_1^n(\beta c) = 1$ (i.e. $\mathrm{Tr}_1^n(\beta(1+c) = 0)$ and $\mathrm{Tr}_1^n(\beta c) = 0$ (i.e. $\mathrm{Tr}_1^n(\beta(1+c) = 1)$, respectively.

$$\begin{aligned}
M_{1,1} &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=\mathrm{Tr}_1^n(\beta c)=1}(-1)^{\mathrm{Tr}_1^n(\beta(a+b))+\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(h_1(a))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(x(L_1(a)+\beta(1+c)))}\\
&= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=\mathrm{Tr}(\beta c)=1}(-1)^{\mathrm{Tr}(\beta(a+b)+h_1(a))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x(L_1(a)+\beta(1+c)))}.
\end{aligned}$$

Notice that the inner sum will have a contribution if and only if $\beta(1+c) = L_1(a)$. Therefore, we have

$$M_{1,1} = \begin{cases} 0 & if\ \ B=0\\ 2^n\cdot(-1)^A & if\ \ B=1,\end{cases}$$

where $A = \mathrm{Tr}_1^n((a+b)L_1(a)(1+c)^{-1} + h_1(a))$ and $B = \mathrm{Tr}_1^n(L_1(a)(1+c)^{-1})$.

Recall that $g_1(x) = \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x)$, then

$$M_{1,0} \;=\; \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1, \mathrm{Tr}_1^n(\beta c)=0} (-1)^{\mathrm{Tr}_1^n(\beta(f_1(a)+b))} W_{g_1}(\alpha),$$

where $\alpha = L_1(a) + \beta(1+c) + u$. It is easy to see that $\mathrm{Tr}_1^n(\alpha) = \mathrm{Tr}_1^n(\beta(1+c)+u) = 0$. Therefore, we get $M_{1,0} = 0$ from Theorem 2. The proof of the distribution of ${}_c\Delta_{f_1}(a,b)$ for $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$ is completed.

By Definition 3,

$${}_c\Delta_{f_1} = \max_{a\in\mathbb{F}_{2^n}, b\in\mathbb{F}_{2^n}} {}_c\Delta_{f_1}(a,b) = 2.$$

Thus, $f_1(x)$ is an APcN function for $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$. □

Example 2. *Take $n = 9$, $k = 4$ and $c \in \mathbb{F}_{2^9}\backslash\{0,1\}$. There are 256 different $u \in \mathbb{F}_{2^9}$ satisfying $\mathrm{Tr}_1^9(u) = 1$, and we can select $u = \alpha^9$, where α is a root of the primitive polynomial $x^9 + x^4 + 1$. By computer, it can be verified that the c-differential uniformity of*

$$f_1(x) = x + \mathrm{Tr}_1^9(x^{33} + x^3 + x + \alpha^9 x)$$

is 2 for $c \in \mathbb{F}_{2^9}\backslash\{0,1\}$.

3.2 The c-differential uniformity of the second class of permutation polynomials

Lemma 5. *For any two positive integers n, k with $n = 2k+1$, $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x+1)^{2^k+3})$ is an involution over $\mathbb{F}_{2^n}$.*

Proof. Note that $f_2(x) = 1 + x + \mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3 + x)$. Since $n = 2k+1$, we have $\mathrm{Tr}_1^n(1) = 1$. Then it is easy to calculate that $f_2(f_2(x)) = x$. Hence, $f_2(x)$ is an involution over $\mathbb{F}_{2^n}$. □

Lemma 6. *For any two positive integers n, k with $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, let $L_2(x) = x^{2^{1-k}} + x^{2^{k-1}} + x^{2^k} + x^{2^{-k}} + x^2 + x^{2^{-1}} \in \mathbb{F}_{2^n}[x]$. Then $L_2(x) = 0$ has two solutions $x = 0, 1$ in $\mathbb{F}_{2^n}$.*

Proof. Since $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, we have $\gcd(n, k-1) = \gcd(2k+1, k-1) = \gcd(3, k-1) = 1$ and $\gcd(n,k) = \gcd(2k+1, k) = \gcd(1,k) = 1$.

Raising 2^k-th power on both sides of $L_2(x) = 0$ leads to

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

Let $L_2'(x) = x^2 + x^{2^{2k-1}} + x^{2^{2k}} + x + x^{2^{k+1}} + x^{2^{k-1}}$. From [18], we know that the conventional associate of the linearized polynomial $L_2'(x)$ is $A_2(x) = 1 + x + x^{k-1} + x^{k+1} + x^{2k-1} + x^{2k}$ and $\gcd(L_2'(x), x^{2^n}+x)$ is the linearized associate of $\gcd(A_2(x), x^n+1)$. Therefore, $A_2(x) = (x+1)(x^k+1)(x^{k-1}+1)$ and $\gcd(n,1) = \gcd(n,k) = \gcd(n,k-1) = 1$ give $\gcd(A_2(x), x^n+1) = x+1$, which is sufficient for the claim that $L_2'(x) = 0$ has two solutions $x = 0, 1$ in $\mathbb{F}_{2^n}$. □

Theorem 4. *For any two positive integers n, k with $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, let $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x+1)^{2^k+3})$. Then for $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we have*

$$\Delta_{f_2}(a,b) = \begin{cases} 2^n & \text{if } (a,b) = (1,1) \\ 2^{n-1} & \text{if } (a,b) \neq (1,1), f_2(a) \in \{b, b+1\} \\ 0 & \text{otherwise,} \end{cases}$$

and $\Delta_{f_2} = 2^n$.

Proof. Recall that $f_2(x) = 1 + x + \mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3 + x)$ and $L_2(x) = x^{2^{1-k}} + x^{2^{k-1}} + x^{2^k} + x^{2^{-k}} + x^2 + x^{2^{-1}}$. Then by Definition 2, we consider the equation $b = D_a f_2(x) = f_2(x+a) + f_2(x)$, which can be further written as

$$\mathrm{Tr}_1^n(xL_2(a)) = 1 + f_2(a) + b. \tag{2}$$

Since $L_2(1) = 0$ and $f_2(1) = 1$, Eq. (2) has 2^n solutions if $(a, b) = (1, 1)$ and no solution if $(a, b) \in \{(\zeta, \xi) \mid \zeta = 1, \xi \neq 1\}$. By Lemma 6, $L_2(a) \neq 0$ for $a \notin \{0, 1\}$, then Eq. (2) has 2^{n-1} solutions if $f_1(a) \in \{b, b+1\}$ and has no solution otherwise.

Clearly,

$$\Delta_{f_2} = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \Delta_{f_2}(a, b) = 2^n.$$

□

Example 3. *Take $n = 7$, $k = 3$ and $c = 1$. By computer, it can be verified that the differential uniformity of*

$$f_2(x) = x + \mathrm{Tr}_1^7(x^{11} + (x+1)^{11})$$

is 128.

Remark 3. *For any two positive integers n, k with $n = 2k+1$, $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x+1)^{2^k+3})$ is a PcN function for $c = 0$.*

Theorem 5. *For any two positive integers n, k with $n = 2k+1$, let $g_2(x) = \mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3)$ over $\mathbb{F}_{2^n}$. Then*

$$W_{g_2}(\alpha) = \begin{cases} 0 & if\ \mathrm{Tr}_1^n(\alpha) = 0 \\ (-1)^{\mathrm{Tr}_1^n(\beta^{2^{k+2}+1} + \beta^{2^k+1} + \beta^{2^{k+1}+2^k} + \beta\delta)} W_{g_2}(\delta) & if\ \mathrm{Tr}_1^n(\alpha) = 1, \end{cases}$$

where $\beta, \delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\delta) = 1$ and $\alpha = L_2(\beta) + \delta$.

Proof. Recall that $L_2(x) = x^{2^{1-k}} + x^{2^{k-1}} + x^{2^k} + x^{2^{-k}} + x^2 + x^{2^{-1}}$. Let $\beta \in \mathbb{F}_{2^n}$, then by Definition 1,

$$\begin{aligned} W_{g_2}(\alpha) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n((x+\beta)^{2^k+2} + (x+\beta)^{2^k+1} + (x+\beta)^3 + \alpha(x+\beta))} \\ &= (-1)^{\mathrm{Tr}_1^n(\beta^{2^k+2} + \beta^{2^k+1} + \beta^3 + \alpha\beta)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3 + x(L_2(\beta) + \alpha))}. \end{aligned}$$

It is easy to see that $\mathrm{Tr}_1^n(L_2(\beta)) = 0$. So we choose a β such that $L_2(\beta) = \alpha$ if $\mathrm{Tr}_1^n(\alpha) = 0$, then the sum becomes $\sum\limits_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3)} = 0$. Therefore, we have $W_{g_2}(\alpha) = 0$.

If $\mathrm{Tr}_1^n(\alpha) = 1$, we choose a β such that $L_2(\beta) = \alpha + \delta$, where $\mathrm{Tr}_1^n(\delta) = 1$. The sum turns out to be $\sum\limits_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3 + \delta x)} = W_{g_2}(\delta)$. It results in

$$W_{g_2}(\alpha) = (-1)^{\mathrm{Tr}_1^n(\beta^{2^{k+2}+1} + \beta^{2^k+1} + \beta^{2^{k+1}+2^k} + \beta\delta)} W_{g_2}(\delta).$$

□

Theorem 6. *For any two positive integers n, k with $n = 2k+1$, let $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3} + (x+1)^{2^k+3})$. Then for any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$, we have*

$$
{}_c\Delta_{f_2}(a,b) = \begin{cases} 0 & if\ \ A = 1 \ and\ B = 1 \\ 1 & if\ \ B = 0 \\ 2 & if\ \ A = 0 \ and\ B = 1, \end{cases}
$$

where $A = \mathrm{Tr}_1^n((a+b)L_2(a)(1+c)^{-1} + a^{2^k+2} + a^{2^k+1} + a^3 + a)$
and $B = \mathrm{Tr}_1^n(L_2(a)(1+c)^{-1})$. Moreover, $f_2(x)$ is an APcN function for $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$.

Proof. For simplicity, let $h_2(x) = x^{2^k+2} + x^{2^k+1} + x^3 + x$, then $f_2(x) = 1 + x + \mathrm{Tr}_1^n(h_2(x))$. By Definition 3, we consider the equation $b = cD_a f_2(x) = f_2(x+a) + cf_2(x)$, leading to

$$
(1+c)f_2(x) + f_2(a) + 1 + \mathrm{Tr}_1^n(a^2x^{2^k} + a^{2^k}x^2 + ax^{2^k} + a^{2^k}x + ax^2 + a^2x) + b = 0.
$$

Recall that $L_2(x) = x^{2^{1-k}} + x^{2^{k-1}} + x^{2^k} + x^{2^{-k}} + x^2 + x^{2^{-1}}$. Then, by Definition 3 and Lemma 2, we have

$$
\begin{aligned}
{}_c\Delta_{f_2}(a,b) &= \frac{1}{2^n} \sum_{\beta \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b+1))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_2(x)) + \mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_2(a))} \\
&= \frac{1}{2^n}(M_0 + M_1),
\end{aligned}
$$

where M_0 and M_1 are the sums corresponding to $\mathrm{Tr}_1^n(\beta) = 0$ and $\mathrm{Tr}_1^n(\beta) = 1$, respectively. Obviously,

$$
\begin{aligned}
M_0 &= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b+1))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_2(x))} \\
&= 2^n + \sum_{\beta \in \mathbb{F}_{2^n}^*, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b+1))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+c)f_2(x))} \\
&= 2^n.
\end{aligned}
$$

The last equality above holds because $\beta(1+c) \neq 0$ and $f_2(x)$ is a permutation of $\mathbb{F}_{2^n}$, making the inner sum zero. Similarly,

$$
\begin{aligned}
M_1 &= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b+1))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+c)(1+x+\mathrm{Tr}_1^n(h_2(x)))) + \mathrm{Tr}_1^n(xL_2(a))} \\
&= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b+c))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+c))\mathrm{Tr}_1^n(h_2(x)) + \mathrm{Tr}_1^n(x(L_2(a)+\beta(1+c)))} \\
&= M_{1,1} + M_{1,0},
\end{aligned}
$$

where $M_{1,1}$ and $M_{1,0}$ are the sums corresponding to $\mathrm{Tr}_1^n(\beta c) = 1$ (i.e. $\mathrm{Tr}_1^n(\beta(1+c)) = 0$) and $\mathrm{Tr}_1^n(\beta c) = 0$ (i.e. $\mathrm{Tr}_1^n(\beta(1+c)) = 1$). We easily obtain

$$
\begin{aligned}
M_{1,1} &= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=\mathrm{Tr}_1^n(\beta c)=1} (-1)^{\mathrm{Tr}_1^n(\beta(a+b)+\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(h_2(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x(L_2(a)+\beta(1+c)))} \\
&= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=\mathrm{Tr}_1^n(\beta c)=1} (-1)^{\mathrm{Tr}_1^n(\beta(a+b)+h_2(a))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(x(L_2(a)+\beta(1+c)))}.
\end{aligned}
$$

Notice that the inner sum will have a contribution if and only if $\beta(1+c) = L_2(a)$. Therefore, we have

$$M_{1,1} = \begin{cases} 0 & if\ B = 0 \\ 2^n \cdot (-1)^A & if\ B = 1, \end{cases}$$

where $A = \mathrm{Tr}_1^n((a+b)(1+c)^{-1}L_2(a) + h_2(a))$ and $B = \mathrm{Tr}_1^n((1+c)^{-1}L_2(a))$.

Similarly, recall that $g_2(x) = \mathrm{Tr}_1^n(x^{2^k+2} + x^{2^k+1} + x^3)$, then

$$M_{1,0} \;=\; \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1, \mathrm{Tr}_1^n(\beta c)=0} (-1)^{\mathrm{Tr}_1^n(\beta(f_2(a)+b))} W_{g_2}(\alpha),$$

where $\alpha = L_2(a) + \beta(1+c) + 1$. It is easy to see that $\mathrm{Tr}_1^n(\alpha) = \mathrm{Tr}_1^n(\beta(1+c)+1) = 0$. Thus, we get $M_{1,0} = 0$ from Theorem 5.

The second conclusion follows Definition 3, where

$${}_c\Delta_{f_2} = \max_{a\in\mathbb{F}_{2^n}, b\in\mathbb{F}_{2^n}} {}_c\Delta_{f_2}(a,b) = 2.$$

Thus, $f_2(x)$ is an APcN function for $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$. □

Example 4. *Take $n = 9$, $k = 4$ and $c \in \mathbb{F}_{2^9}\backslash\{0,1\}$. By computer, it can be verified that the c-differential uniformity of*

$$f_2(x) = x + \mathrm{Tr}_1^9(x^{19} + (x+1)^{19})$$

is 2 for $c \in \mathbb{F}_{2^9}\backslash\{0,1\}$.

3.3 The c-differential uniformity of the third class of permutation polynomials

Lemma 7. ([10]) *Let n be a positive integer and $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$. For any $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, the distribution of solutions of $(x+a)^{-1} + cx^{-1} = b$ is described as Table 1:*

Table 1
Distribution of solutions of $(x+a)^{-1} + cx^{-1} = b$ with conditions on (a,b,c)

Conditions on (a,b,c)	Solution set Ω	Card(Ω)
$ab = 1$, $\mathrm{Tr}_1^n(c^{-1}) = 0$	$\{0$, two roots from $x^2 + acx + a^2c = 0\}$	3
$ab = c$, $\mathrm{Tr}_1^n(c) = 0$	$\{a$, two roots from $x^2 + ac^{-1}x + a^2 = 0\}$	3
$ab \notin \{1, c, 1+c\}$, $\mathrm{Tr}_1^n(\frac{abc}{a^2b^2+c^2+1}) = 0$	$\{$two roots from $x^2 + \frac{ab+c+1}{b}x + \frac{ac}{b} = 0\}$	2
$b = 0$	$\{\frac{ac}{1+c}\}$	1
$a = 0$, $b \neq 0$	$\{b^{-1}(1+c)\}$	1
$ab = 1$, $\mathrm{Tr}_1^n(c^{-1}) = 1$	$\{0\}$	1
$ab = c$, $\mathrm{Tr}_1^n(c) = 1$	$\{a\}$	1
$ab = 1+c$	$\{(\frac{ac}{b})^{2^{n-1}}\}$	1
otherwise	$\{\varnothing\}$	0

Theorem 7. *Let n be even and d be a positive integer. Let $f_3(x) = x^{-1} + \mathrm{Tr}_1^n((x^{-1}+1)^d + x^{-d})$ be a map from $\mathbb{F}_{2^n}$ to itself. Then for any $c \in \mathbb{F}_{2^n}$, we have:*
(1) If $c = 0$, then $f_3(x)$ is a PcN function;
(2) If $c = 1$ and $d \in \{2^n-2, 2^{\frac{n}{2}}+2^{\frac{n}{4}}+1, 2^{t_1}+1, 3(2^{t_2}+1)\}$, where $1 \le t_1 \le \frac{n}{2}-1$ and $2 \le t_2 \le \frac{n}{2}-1$, then $\Delta_{f_3} = 4$;
(3) If $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$ and $\mathrm{Tr}_1^n(c) = \mathrm{Tr}_1^n(c^{-1}) = 1$, then ${}_c\Delta_{f_3} \le 8$;
(4) If $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$, $\mathrm{Tr}_1^n(c) = 0$ or $\mathrm{Tr}_1^n(c^{-1}) = 0$, then ${}_c\Delta_{f_3} \le 9$.

Proof. For convenience, let $h_3(x) = (x^{-1}+1)^d + x^{-d}$, then $f_3(x) = x^{-1} + \mathrm{Tr}_1^n(h_3(x))$.

By Definition 3, we consider the following equation for determining ${}_c\Delta_{f_2}(a,b)$ where $a, b \in \mathbb{F}_{2^n}$

$$(x+a)^{-1} + \mathrm{Tr}_1^n(h_3(x+a)) + cx^{-1} + c\mathrm{Tr}_1^n(h_3(x)) = b, \tag{3}$$

For $c = 0$ with $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ or $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$ with $a = 0, b \in \mathbb{F}_{2^n}$, Eq. (3) has exactly one solution since $f_3(x+a)$ or $f_3(x)$ is a permutation polynomial. Thus, $f_3(x)$ is a PcN function.

For $c = 1$ and $d \in \{2^n-2, 2^{\frac{n}{2}}+2^{\frac{n}{4}}+1, 2^{t_1}+1, 3(2^{t_2}+1)\}$ with $1 \le t_1 \le \frac{n}{2}-1$ and $2 \le t_2 \le \frac{n}{2}-1$, $\Delta_{f_3} = 4$ [24].

For $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$ with $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, let $A = \mathrm{Tr}_1^n(h_3(x+a))$, $B = \mathrm{Tr}_1^n(h_3(x))$, then Eq. (3) is denoted as

$$(x+a)^{-1} + cx^{-1} = A + cB + b. \tag{4}$$

Before starting our discussion with the division of (A,B) in Eq. (4), we underline a trivial fact that $x = 0$ (resp. $x = a$) is not a solution to Eq. (4) when $(A,B) = (\times, 1)$ (resp. $(A,B) = (1,\times)$) simply because $\mathrm{Tr}_1^n(1) = 0$.

Case I: $(A,B) = (0,0)$. By Lemma 7, Eq. (4) has three solutions if $ab = 1$, $\mathrm{Tr}_1^n(c^{-1}) = 0$, $\mathrm{Tr}_1^n(h_3(a)) = 0$ (i.e. $A = 0$), or $ab = c$, $\mathrm{Tr}_1^n(c) = 0$, $\mathrm{Tr}_1^n(h_3(a)) = 0$ (i.e. $B = 0$). Otherwise, the cardinality of its solution set is two at maximum.

Case II: $(A,B) = (1,1)$. By Lemma 7, Eq. (4) has only two solutions if $a(b+c+1) = 1$, $\mathrm{Tr}_1^n(c^{-1}) = 0$, or $a(b+c+1) = c$, $\mathrm{Tr}_1^n(c) = 0$. Note that $x = 0$ and $x = a$ in Table 1 are excluded since they arouse contradictions in the value of $\mathrm{Tr}_1^n(1)$ as stated above. In the rest of (a,b,c), Eq. (4) has two solutions at maximum.

Case III: $(A,B) = (0,1)$. Similarly, only when $a(b+c) = c$, $\mathrm{Tr}_1^n(c) = 0$ and $\mathrm{Tr}_1^n((h_3(a)) = 1$ (i.e. $B = 1$) does Eq. (4) have three solutions by Lemma 7. Else, it has two solutions at maximum.

Case IV: $(A,B) = (1,0)$. When $a(b+1) = 1$, $\mathrm{Tr}_1^n(c^{-1}) = 0$ and $\mathrm{Tr}_1^n(h_3(a)) = 1$ (i.e. $A = 1$), there are three solutions to Eq. (4) while there are at most two solutions in other cases of (a,b,c) according to Lemma 7.

Table 2
Conditions on (a,b,c) for the maximum cardinality of the solution set of Eq. (4)

	ab	$a(b+c)$	$a(b+1)$	$\mathrm{Tr}_1^n(c^{-1})$	$\mathrm{Tr}_1^n(c)$	$\mathrm{Tr}_1^n(h_3(a))$
Case I	1	×	×	0	×	0
	c	×	×	×	0	0
Case II	×	×	×	×	×	×
Case III	×	c	×	×	0	1
Case IV	×	×	1	0	×	1

In Table 2, mutual exclusion emerges between the conditions on $\mathrm{Tr}_1^n(h_3(a))$ in Case I and in Case III/IV and between the conditions on $a(b+c)=c$ in Case III and $a(b+1)=1$ in Case IV because $a(b+c)=c$ together with $a(b+1)=1$ yields $c=1$. Hence, we can at most obtain three solutions in only one of Case I/III/IV and two in the left three cases, which is $3+2\times 3=9$. Table 3 illustrates the distribution of the maximum cardinality of the solution set of Eq. (3).

Table 3
Distribution of the maximum cardinality of the solution set of Eq. (3)

Conditions on (a,b,c)	Case I	Case II	Case III	Case IV	$\max(\mathrm{Card}(\Omega_1))$
$ab=1$, $\mathrm{Tr}_1^n(c^{-1})=0$, $\mathrm{Tr}_1^n(h_3(a))=0$	3	2	2	2	9
$ab=c$, $\mathrm{Tr}_1^n(c)=0$, $\mathrm{Tr}_1^n(h_3(a))=0$	3	2	2	2	9
$a(b+c)=c$, $\mathrm{Tr}_1^n(c^{-1})=0$, $\mathrm{Tr}_1^n(h_3(a))=1$	2	2	3	2	9
$a(b+1)=1$, $\mathrm{Tr}_1^n(c^{-1})=0$, $\mathrm{Tr}_1^n(h_3(a))=1$	2	2	2	3	9
otherwise	2	2	2	2	8

* Ω_1 represents the solution set of Eq. (3).

□

To end this subsection, we show in Table 4 the possible maximum values of $c\Delta_{f_3}$ with $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$ over $\mathbb{F}_{2^n}$ for some small n.

Table 4
Some possible maximum values of ${}_c\Delta_{f_3}$ over $\mathbb{F}_{2^n}$

n	$f(x)$	Conditions on $(\mathrm{Tr}_1^n(c),\mathrm{Tr}_1^n(c^{-1}))$	${}_c\Delta_{f_3}$
8	$x^{-1}+\mathrm{Tr}_1^8((x^{-1}+1)^{254}+x^{-254})$	$\in\{(0,0),(0,1),(1,0)\}$	8
		$(1,1)$	7
8	$x^{-1}+\mathrm{Tr}_1^8((x^{-1}+1)^{21}+x^{21})$	$\in\{(0,0),(0,1),(1,0)\}$	8
		$(1,1)$	5
6	$x^{-1}+\mathrm{Tr}_1^6((x^{-1}+1)^{5}+x^{5})$	$\in\{(0,0),(0,1),(1,0)\}$	3
		$(1,1)$	2
6	$x^{-1}+\mathrm{Tr}_1^6((x^{-1}+1)^{15}+x^{15})$	$\in\{(0,0),(0,1),(1,0)\}$	7
		$(1,1)$	6

4 The boomerang uniformity of three classes of permutation polynomials

In this section, we study the boomerang uniformity of the following three families of permutation polynomials:

(1) $f_1(x)=x+\mathrm{Tr}_1^n(x^{2^{k+1}+1}+x^3+x+ux)$, where $n=2k+1$ with $k\not\equiv 1 \pmod 3$ and $u\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$;

(2) $f_2(x)=x+\mathrm{Tr}_1^n(x^{2^k+3}+(x+1)^{2^k+3})$, where $n=2k+1$ and $k\not\equiv 1 \pmod 3$;

(3) $f_3(x)=x^{-1}+\mathrm{Tr}_1^n((x^{-1}+1)^d+x^{-d})$, where n is even and d is a positive integer.

4.1 The boomerang uniformity of the first class of permutation polynomials

Theorem 8. *For any two positive integers n, k with $n = 2k+1$ and $k \not\equiv 1 \pmod 3$, let $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u) = 1$ and $f_1(x) = x + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + x^3 + x + ux)$. Then for any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, we have*

$$\mathcal{B}_{f_1}(a,b) = \begin{cases} 2^n & if\ \mathrm{Tr}_1^n(L_1(a)b) = 0 \\ 0 & if\ \mathrm{Tr}_1^n(L_1(a)b) = 1, \end{cases}$$

and $\mathcal{B}_{f_1} = 2^n$.

Proof. Recall that $L_1(x) = x^{2^{-(k+1)}} + x^{2^{k+1}} + x^{2^{-1}} + x^2$. The following system is derived from Definition 4:

$$\begin{cases} x + y + \mathrm{Tr}_1^n(u(x+y)) + \mathrm{Tr}_1^n(x^{2^{k+1}+1} + y^{2^{k+1}+1}) + \mathrm{Tr}_1^n(x^3 + y^3) + \mathrm{Tr}_1^n(x+y) = b \\ x + y + \mathrm{Tr}_1^n(u(x+y)) + \mathrm{Tr}_1^n((x+a)^{2^{k+1}+1} + (y+a)^{2^{k+1}+1}) \\ \quad + \mathrm{Tr}_1^n((x+a)^3 + (y+a)^3) + \mathrm{Tr}_1^n(x+y) = b. \end{cases} \tag{5}$$

Adding the two equations of the system (5) gives

$$\mathrm{Tr}_1^n((x+y)^{2^{k+1}}a + (x+y)a^{2^{k+1}}) + \mathrm{Tr}_1^n((x+y)^2 a + (x+y)a^2) = 0.$$

Then the system (5) is equivalent to

$$\begin{cases} x + y + \mathrm{Tr}_1^n(u(x+y) + (x+y)^{2^{k+1}+1} + x^{2^{k+1}}y + xy^{2^{k+1}}) \\ \quad + \mathrm{Tr}_1^n((x+y)^3 + x^2y + xy^2) + \mathrm{Tr}_1^n(x+y) = b \\ \mathrm{Tr}_1^n((x+y)^{2^{k+1}}a + (x+y)a^{2^{k+1}}) + \mathrm{Tr}_1^n((x+y)^2 a + (x+y)a^2) = 0. \end{cases} \tag{6}$$

Let $y = x + z$, the system (6) turns out to be

$$\begin{cases} z + \mathrm{Tr}_1^n(uz + z^{2^{k+1}+1} + z^3 + z) + \mathrm{Tr}_1^n(x^{2^{k+1}}z + xz^{2^{k+1}} + x^2 z + xz^2) = b \\ \mathrm{Tr}_1^n(z^{2^{k+1}}a + za^{2^{k+1}} + z^2 a + za^2) = 0, \end{cases}$$

which can be further reduced to

$$\begin{cases} f_1(z) + \mathrm{Tr}_1^n(xL_1(z)) = b \\ \mathrm{Tr}_1^n(aL_1(z)) = 0. \end{cases} \tag{7}$$

By Lemma 2, the cardinality of the solution set for $(x, z) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the system (7) is given by:

$$\begin{aligned} \mathcal{B}_{f_1}(a,b) &= \frac{1}{2^{2n}} \sum_{x,z \in \mathbb{F}_{2^n}} \sum_{\beta \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(f_1(z)+b)) + \mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_1(z))} \sum_{\gamma \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\gamma)\mathrm{Tr}_1^n(aL_1(z))} \\ &= \frac{1}{2^{2n}} \sum_{\beta,\gamma \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z)) + \mathrm{Tr}_1^n(\gamma)\mathrm{Tr}_1^n(aL_1(z))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_1(z))} \\ &= \frac{1}{2^{2n}}(S_{0,0} + S_{0,1} + S_{1,0} + S_{1,1}), \end{aligned}$$

where $S_{0,0}$, $S_{0,1}$, $S_{1,0}$, and $S_{1,1}$ are a partition of the sum with the following correspondence of $\mathrm{Tr}_1^n(\beta)$ and $\mathrm{Tr}_1^n(\gamma)$. Specifically, for $\zeta, \xi \in \{0,1\}$, $S_{\zeta,\xi}$ denotes the part of the sum when $\mathrm{Tr}_1^n(\beta) = \zeta$ and $\mathrm{Tr}_1^n(\gamma) = \xi$. Hence, we have

$$\begin{aligned} S_{0,0} &= 2^n \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\gamma)=0} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z))} \\ &= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z))}. \end{aligned}$$

Similarly,

$$\begin{aligned} S_{0,1} &= 2^n \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\gamma)=1} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z)) + \mathrm{Tr}_1^n(aL_1(z))} \\ &= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(z(L_1(a)+\beta))}. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} S_{1,0} &= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(xL_1(z))} \\ &= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}\backslash\{0,1\}} (-1)^{Tr_1^n(\beta f_1(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(xL_1(z))} \\ &+ 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta b)} (1 + (-1)^{\mathrm{Tr}_1^n(\beta(1+\mathrm{Tr}_1^n(1+u)))}) \\ &= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta b)} (1 + (-1)^{\mathrm{Tr}_1^n(\beta(1+\mathrm{Tr}_1^n(1+u)))}) \\ &= 0, \end{aligned}$$

where the third equality holds since $L_1(z) \neq 0$ for $z \in \mathbb{F}_{2^n}\backslash\{0,1\}$ from Lemma 4. Similarly,

$$\begin{aligned} S_{1,1} &= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=1} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z)) + \mathrm{Tr}_1^n(aL_1(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(xL_1(z))} \\ &= 0. \end{aligned}$$

Thus, we have

$$\begin{aligned} \mathcal{B}_{f_1}(a,b) &= \frac{1}{2^{2n}} (S_{0,0} + S_{0,1} + S_{1,0} + S_{1,1}) \\ &= \frac{1}{2} \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} (\sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z))} + \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(z(L_1(a)+\beta))}) \\ &= \frac{1}{2} (2^n + \sum_{\beta\in\mathbb{F}_{2^n}^*, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_1(z))} \\ &+ \sum_{\beta\in\mathbb{F}_{2^n}, \mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(z(L_1(a)+\beta))}) \\ &= 2^{n-1} + 2^{n-1}(-1)^{\mathrm{Tr}_1^n(L_1(a)b)} \\ &= \begin{cases} 2^n & if \ \mathrm{Tr}_1^n(L_1(a)b) = 0 \\ 0 & if \ \mathrm{Tr}_1^n(L_1(a)b) = 1, \end{cases} \end{aligned}$$

where the fourth equality holds since $f_1(z)$ is a permutation of $\mathbb{F}_{2^n}$ and the inner sum will contribute if and only if $\beta = L_1(a)$. Then by Definition 4,

$$\mathcal{B}_{f_1} = \max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}^*} \mathcal{B}_{f_1}(a,b) = 2^n.$$

□

Example 5. *Take $n=5$ and $k=2$. There are 16 different $u \in \mathbb{F}_{2^5}$ satisfying $\mathrm{Tr}_1^5(u)=1$. We can select $u=\alpha^5$, where α is a root of the primitive polynomial x^5+x^2+1. By computer, it can be verified that the boomerang uniformity of*

$$f_1(x) = x + \mathrm{Tr}_1^5(x^9+x^3+x+\alpha^5 x)$$

is 32.

4.2 The boomerang uniformity of the second class of permutation polynomials

Theorem 9. *For any two positive integers n, k with $n=2k+1$ and $k \not\equiv 1 \pmod 3$, let $f_2(x) = x + \mathrm{Tr}_1^n(x^{2^k+3}+(x+1)^{2^k+3})$. Then for any $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$, we have*

$$\mathcal{B}_{f_2}(a,b) = \begin{cases} 2^n & if\ \mathrm{Tr}_1^n(L_2(a)b)=0 \\ 0 & if\ \mathrm{Tr}_1^n(L_2(a)b)=1, \end{cases}$$

and $\mathcal{B}_{f_2} = 2^n$.

Proof. Recall that $f_2(x) = 1+x+\mathrm{Tr}_1^n(x^{2^k+2}+x^{2^k+1}+x^3+x)$ and $L_2(x) = x^{2^{1-k}}+x^{2^{k-1}}+x^{2^{-k}}+x^{2^k}+x^{2^{-1}}+x^2$. We derive the following system from Definition 4:

$$\begin{cases} x+y+\mathrm{Tr}_1^n(x^{2^k+2}+y^{2^k+2})+\mathrm{Tr}_1^n(x^{2^k+1}+y^{2^k+1})+\mathrm{Tr}_1^n(x^3+y^3)+\mathrm{Tr}_1^n(x+y)=b \\ x+y+\mathrm{Tr}_1^n((x+a)^{2^k+2}+(y+a)^{2^k+2})+\mathrm{Tr}_1^n((x+a)^{2^k+1}+(y+a)^{2^k+1}) \\ \quad +\mathrm{Tr}_1^n((x+a)^3+(y+a)^3)+\mathrm{Tr}_1^n(x+y)=b. \end{cases} \tag{8}$$

An equation addition within the system (8) brings

$$\mathrm{Tr}_1^n((x+y)^{2^k}a^2+(x+y)^2a^{2^k})+\mathrm{Tr}_1^n((x+y)^{2^k}a+(x+y)a^{2^k})+\mathrm{Tr}_1^n(a(x+y)^2+a^2(x+y))=0.$$

Then the system (8) is equivalent to

$$\begin{cases} x+y+\mathrm{Tr}_1^n((x+y)^{2^k+2}+x^{2^k}y^2+x^2y^{2^k})+\mathrm{Tr}_1^n((x+y)^{2^k+1}+x^{2^k}y+xy^{2^k}) \\ \quad +\mathrm{Tr}_1^n((x+y)^3+x^2y+xy^2)+\mathrm{Tr}_1^n(x+y)=b \\ \mathrm{Tr}_1^n(a^2(x+y)^{2^k}+a^{2^k}(x+y)^2)+\mathrm{Tr}_1^n(a(x+y)^{2^k}+a^{2^k}(x+y))+\mathrm{Tr}_1^n(a(x+y)^2+a^2(x+y))=0. \end{cases} \tag{9}$$

Taking $y=x+z$, the system (9) becomes

$$\begin{cases} z+\mathrm{Tr}_1^n(z^{2^k+2}+z^{2^k+1}+z^3+z)+\mathrm{Tr}_1^n(x^{2^k}z^2+x^2z^{2^k}+x^{2^k}z+xz^{2^k}+x^2z+xz^2)=b \\ \mathrm{Tr}_1^n(a^2z^{2^k}+a^{2^k}z^2+az^{2^k}+a^{2^k}z+az^2+a^2z)=0, \end{cases}$$

which can be written as

$$\begin{cases} 1+f_2(z)+\mathrm{Tr}_1^n(xL_2(z))=b \\ \mathrm{Tr}_1^n(aL_2(z))=0. \end{cases} \tag{10}$$

By Lemma 2, the cardinality of the solution set for $(x,z) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the system (10) is given by:

$$\begin{aligned}
\mathcal{B}_{f_2}(a,b) &= \frac{1}{2^{2n}} \sum_{x,z\in\mathbb{F}_{2^n}} \sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+f_2(z)+b))+\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_2(z))} \sum_{\gamma\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\gamma)\mathrm{Tr}_1^n(aL_2(z))}\\
&= \frac{1}{2^{2n}} \sum_{\beta,\gamma\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta(1+b))} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))+\mathrm{Tr}_1^n(\gamma)\mathrm{Tr}_1^n(aL_2(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta)\mathrm{Tr}_1^n(xL_2(z))}\\
&= \frac{1}{2^{2n}}(S_{0,0}+S_{0,1}+S_{1,0}+S_{1,1}),
\end{aligned}$$

where $S_{0,0}$, $S_{0,1}$, $S_{1,0}$, and $S_{1,1}$ are a partition of the sum with the following correspondence of $\mathrm{Tr}_1^n(\beta)$ and $\mathrm{Tr}_1^n(\gamma)$. Specifically, for $\zeta,\xi \in \{0,1\}$, $S_{\zeta,\xi}$ denotes the part of the sum when $\mathrm{Tr}_1^n(\beta)=\zeta$ and $\mathrm{Tr}_1^n(\gamma)=\xi$. Hence, we have

$$\begin{aligned}
S_{0,0} &= 2^n \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\gamma)=0} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))}\\
&= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
S_{0,1} &= 2^n \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\gamma)=1} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))+\mathrm{Tr}_1^n(aL_2(z))}\\
&= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0} (-1)^{\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(z(L_2(a)+\beta))}.
\end{aligned}$$

Furthermore, we have

$$\begin{aligned}
S_{1,0} &= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1} (-1)^{1+\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(xL_2(z))}\\
&= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1} (-1)^{1+\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}\backslash\{0,1\}} (-1)^{Tr_1^n(\beta f_2(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(xL_2(z))}\\
&\quad +2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1} (-1)^{1+\mathrm{Tr}_1^n(\beta b)}((-1)^{Tr_1^n(\beta f_2(0))}+(-1)^{Tr_1^n(\beta f_2(1))})\\
&= 2^{2n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1} (-1)^{1+\mathrm{Tr}_1^n(\beta b)}((-1)^{\mathrm{Tr}_1^n(\beta)}+1)\\
&= 0,
\end{aligned}$$

where $f_2(0)=1$, $f_2(1)=0$, and the third identity holds since $L_2(z)\neq 0$ for $z\in\mathbb{F}_{2^n}\backslash\{0,1\}$ from Lemma 6. Similarly,

$$\begin{aligned}
S_{1,1} &= 2^{n-1} \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=1} (-1)^{1+\mathrm{Tr}_1^n(\beta b)} \sum_{z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\beta f_2(z))+\mathrm{Tr}_1^n(aL_2(z))} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(xL_2(z))}\\
&= 0.
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\mathcal{B}_{f_2}(a,b) &= \frac{1}{2^{2n}}(S_{0,0}+S_{0,1}+S_{1,0}+S_{1,1}) \\
&= \frac{1}{2}\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0}(-1)^{\mathrm{Tr}_1^n(\beta b)}(\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta f_2(z))}+\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(z(L_2(a)+\beta))}) \\
&= \frac{1}{2}(2^n+\sum_{\beta\in\mathbb{F}_{2^n}^*,\mathrm{Tr}_1^n(\beta)=0}(-1)^{\mathrm{Tr}_1^n(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(\beta f_2(z))} \\
&+ \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}_1^n(\beta)=0}(-1)^{\mathrm{Tr}_1^n(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_1^n(z(L_2(a)+\beta))}) \\
&= 2^{n-1}+2^{n-1}(-1)^{\mathrm{Tr}_1^n(L_2(a)b)} \\
&= \begin{cases} 2^n & if\ \mathrm{Tr}_1^n(L_2(a)b)=0 \\ 0 & if\ \mathrm{Tr}_1^n(L_2(a)b)=1, \end{cases}
\end{aligned}$$

where the fourth equality holds since $f_2(z)$ is a permutation of $\mathbb{F}_{2^n}$ and the inner sum will contribute if and only if $\beta = L_2(a)$. Then by Definition 4,

$$\mathcal{B}_{f_2} = \max_{a\in\mathbb{F}_{2^n}^*,b\in\mathbb{F}_{2^n}^*}\mathcal{B}_{f_2}(a,b) = 2^n.$$

□

Example 6. *Take $n = 7$ and $k = 3$. By computer, it can be verified that the boomerang uniformity of*

$$f_2(x) = x + Tr_1^7(x^{11} + (x+1)^{11})$$

is 128.

4.3 The boomerang uniformity of the third classes of permutation polynomials

Lemma 8. ([6]) *Let n be even and $f(x) = x^{-1}$ be a map from $\mathbb{F}_{2^n}$ to itself. For any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, the distribution of solutions of the system (11) is listed in Table 5, in which $\omega \in \mathbb{F}_4\backslash\mathbb{F}_2$ is a primitive third root of unity and $\mathbb{F}_4 =< \omega >= \{0,1,\omega,\omega^2\}$.*

$$\begin{cases} x^{-1}+y^{-1}=b \\ (x+a)^{-1}+(y+a)^{-1}=b \end{cases} \tag{11}$$

Theorem 10. *Let n be even and d be an integer. Let $f_3(x) = x^{-1} + \mathrm{Tr}_1^n((x^{-1}+1)^d + x^{-d})$ be a map from $\mathbb{F}_{2^n}$ to itself. Then $\mathcal{B}_{f_3} \leq 12$.*

Proof. Recall that $\omega \in \mathbb{F}_4\backslash\mathbb{F}_2$ and $\mathbb{F}_4 = \{0,1,\omega,\omega^2\}$. By Definition 4, we consider the following system to compute $\mathcal{B}_{f_3}(a,b)$ for any $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$:

$$\begin{cases} x^{-1}+y^{-1}=b+A \\ (x+a)^{-1}+(y+a)^{-1}=b+B, \end{cases} \tag{12}$$

where $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, $A = \mathrm{Tr}_1^n(x^{-d}+y^{-d}+(x^{-1}+1)^d+(y^{-1}+1)^d)$, $B = \mathrm{Tr}_1^n((x+a)^{-d}+(y+a)^{-d}+((x+a)^{-1}+1)^d+((y+a)^{-1}+1)^d)$.

Table 5
Distribution of solutions of the system (11) with conditions on (a, b)

ab	$\mathrm{Tr}_1^n(\frac{1}{ab})$	Solution set Ω_1 $(n \equiv 2 \pmod 4)$	Solution set Ω_2 $(n \equiv 0 \pmod 4)$
1	$\times$	$\{(0, a),\ (a, 0),\ (a\omega, a\omega^2),\ (a\omega^2, a\omega)\}$	Ω_1
ω	$\times$	$\{(0, a\omega^2),\ (a\omega^2, 0),\ (a, a\omega),\ (a\omega, a)\}$	$\Omega_1 \cup \{(x_2, x_2 + a), (x_2 + a, x_2)\}$
ω^2	$\times$	$\{(0, a\omega),\ (a\omega, 0),\ (a, a\omega^2),\ (a\omega^2, a)\}$	$\Omega_1 \cup \{(x_3, x_3 + a), (x_3 + a, x_3)\}$
$\notin \mathbb{F}_4^*$	0	$\{(x_1, x_1 + a), (x_1 + a, x_1)\}$	Ω_1
$\notin \mathbb{F}_4^*$	1	$\{\varnothing\}$	$\{\varnothing\}$

* x_2 and $x_2 + a$ are roots of $x_2^2 + ax_2 + a^2\omega^2 = 0$.
* x_3 and $x_3 + a$ are roots of $x_3^2 + ax_3 + a^2\omega = 0$.
* x_1 and $x_1 + a$ are roots of $x_1^2 + ax_1 + ab^{-1} = 0$.

Evidently, any element in $\{(x, y)|x = y\}$ is not the solution to the system (12) for they lead to $b = 0$. Hence, we discuss below the solutions within $\{(x, y)|x \neq y\}$ concerning various (A, B).

Case I: $A = B$. Knowing that $ab = a(b+1)$ will result in a contradiction with $a \in \mathbb{F}_{2^n}^*$, we first look at $(ab, a(b+1)) \in \Gamma = \{(\zeta, \xi) \mid \zeta, \xi \in \mathbb{F}_4^*, \zeta \neq \xi\}$. For instance, if $(ab, a(b+1)) = (1, \omega)$, we have $(a, b) = (\omega^2, \omega)$. Then by Lemma 8, we handily get four solutions $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$ for $(A, B) = (0, 0)$ and another four solutions $\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}$ for $(A, B) = (1, 1)$ when $n \equiv 2 \pmod 4$ and two more when $n \equiv 0 \pmod 4$. Table 6 simply gives all solutions of the system (12) derived from Table 5 regarding $(ab, a(b + 1)) \in \Gamma$ and $A = B$.

Table 6
Solutions of the system (12) for $(ab, a(b + 1)) \in \Gamma$ and $A = B$

ab	$a(b+1)$	a	b	$A = B = 0$	$A = B = 1$
1	ω	ω^2	ω	$\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$	$\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}^{+2}$
1	ω^2	ω	ω^2	$\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$	$\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}^{+2}$
ω	1	ω^2	ω^2	$\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}^{+2}$	$\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}$
ω	ω^2	1	ω	$\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}^{+2}$	$\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}^{+2}$
ω^2	1	ω	ω	$\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}^{+2}$	$\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}$
ω^2	ω	1	ω^2	$\{(0, \omega), (\omega, 0), (\omega^2, 1), (1, \omega^2)\}^{+2}$	$\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}^{+2}$

* $^{+2}$ implies two more solutions when $n \equiv 0 \pmod 4$.

Secondly, for the rest of $(ab, a(b + 1))$, which is $\{(\zeta, \xi) \mid \zeta, \xi \in \mathbb{F}_{2^n}, \zeta \neq \xi\} \backslash \Gamma$, we rephrase it as the situation that at least one of ab and $a(b + 1)$ is not in $\mathbb{F}_4^*$. For instance, if $ab = 1$ and $a(b+1) \notin \mathbb{F}_4^*$, we again easily obtain by Lemma 8 four solutions $\{(0, a), (a, 0), (a\omega, a\omega^2), (a\omega^2, a\omega)\}$ for $(A, B) = (0, 0)$ and two more solutions for $(A, B) = (1, 1)$ if and only if $\mathrm{Tr}_1^n(a^{-1}(b + 1)^{-1}) = 0$.

To sum up Case I, we conclude in Table 7 the distribution of solutions of the system (12) for $A = B$. Notice that for any element of $\{(x, y) \mid x, y \in \mathbb{F}_4, x \neq y\}$ we always have $A = B = 0$. Therefore, these solutions for $A = B = 1$ in Table 6 have been excluded in Table 7.

Case II: $A \neq B$, or equally $A = B + 1$. Notice that a solution (x_0, y_0) to the system (12) for $(A, B) = (0, 1)$ mirrors another solution $(x_0 + a, y_0 + a)$ to the system (12) for $(A, B) = (1, 0)$. Thus, to be succinct, we only discuss the situation of $(A, B) = (0, 1)$ as follows.

We first examine four obvious solutions. Consider $(x, y) \in \{(0, b^{-1}), (b^{-1}, 0)\}$, for example, then

Table 7
Distribution of solutions of the system (12) for $A = B$ with conditions on (a, b)

ab	$a(b+1)$	$\mathrm{Tr}_1^n(\frac{1}{ab})$	$\mathrm{Tr}_1^n(\frac{1}{a(b+1)})$	Solution set Ω	$\mathrm{Card}(\Omega)$
1	1	$\times$	$\times$	$\{\varnothing\}$	0
1	ω	$\times$	$\times$	$\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}^{+2}$	4/6
1	ω^2	$\times$	$\times$	$\{(0,\omega),(\omega,0),(\omega^2,1),(1,\omega^2)\}^{+2}$	4/6
1	$\notin \mathbb{F}_4^*$	$\times$	0	$\{(0,a),(a,0),(a\omega,a\omega^2),(a\omega^2,a\omega),+2\}$	6
1	$\notin \mathbb{F}_4^*$	$\times$	1	$\{(0,a),(a,0),(a\omega,a\omega^2),(a\omega^2,a\omega)\}$	4
ω	1	$\times$	$\times$	$\{(0,\omega),(\omega,0),(\omega^2,1),(1,\omega^2)\}^{+2}$	4/6
ω	ω	$\times$	$\times$	$\{\varnothing\}$	0
ω	ω^2	$\times$	$\times$	$\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}^{+4}$	4/8
ω	$\notin \mathbb{F}_4^*$	$\times$	0	$\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),\ (a\omega,a),+2\}^{+2}$	6/8
ω	$\notin \mathbb{F}_4^*$	$\times$	1	$\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}^{+2}$	4/6
ω^2	1	$\times$	$\times$	$\{(0,\omega^2),(\omega^2,0),(\omega,1),(1,\omega)\}^{+2}$	4/6
ω^2	ω	$\times$	$\times$	$\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}^{+4}$	4/8
ω^2	ω^2	$\times$	$\times$	$\{\varnothing\}$	0
ω^2	$\notin \mathbb{F}_4^*$	$\times$	0	$\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a),+2\}^{+2}$	6/8
ω^2	$\notin \mathbb{F}_4^*$	$\times$	1	$\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}^{+2}$	4/6
$\notin \mathbb{F}_4^*$	1	0	$\times$	$\{(0,a),(a,0),(a\omega,a\omega^2),(a\omega^2,a\omega),+2\}$	6
$\notin \mathbb{F}_4^*$	ω	0	$\times$	$\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a),+2\}^{+2}$	6/8
$\notin \mathbb{F}_4^*$	ω^2	0	$\times$	$\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a),+2\}^{+2}$	6/8
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	0	0	$+4$	4
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	0	1	$+2$	2
$\notin \mathbb{F}_4^*$	1	1	$\times$	$\{(0,a),(a,0),(a\omega,a\omega^2),(a\omega^2,a\omega)\}$	4
$\notin \mathbb{F}_4^*$	ω	1	$\times$	$\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}^{+2}$	4/6
$\notin \mathbb{F}_4^*$	ω^2	1	$\times$	$\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}^{+2}$	4/6
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	1	0	$+2$	2
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	1	1	$\{\varnothing\}$	0

* $+2$ and $+4$ respectively imply two and four (more) solutions implicitly given by quadratic equations.
* ${}^{+2}$ and ${}^{+4}$ respectively imply two and four more solutions when $n \equiv 0 \pmod 4$.

we have $a(b+1)(ab+1) = 1$, which further infers $ab \neq 1$, $a \neq 1$, and $b \neq 1$. The second is because $a = 1$ will lead to $(b+1)(b+1) = 1$ and then $b = 0$ against $b \in \mathbb{F}_{2^n}^*$. When considering another pair $(x, y) \in \{(a, (a^{-1} + b)^{-1}), ((a^{-1} + b)^{-1}, a)\}$, we have $ab(ab + a + 1) = 1$, implying $ab \neq 1$, $a \neq 1$, and $b \neq 1$. Particularly, under $ab(ab + a + 1) = 1$, we can deduce any two of $ab = 1$, $a = 1$, and $b = 1$ from the other one, then $(x, y) \in \{(1, 0), (0, 1)\}$ arrives at a paradox $(1 = 0)$ in the second equation of the system (12).

Now we turn to $\{(x, y) \mid x, y \in \mathbb{F}_{2^n} \backslash \{0, a\}\}$. The system (12) can be reduced to

$$\begin{cases} x + y = bxy \\ (x + y)(a(x + y) + a^2) = xy(x + a)(y + a). \end{cases} \tag{13}$$

Multiplying b^2 on both sides of the second part of the system (13) and replacing xy by $b^{-1}(x + y)$

reaches

$$\begin{cases} x+y=bxy \\ (ab^2+ab+1)(x+y)=a^2b^2+a^2b. \end{cases} \tag{14}$$

If $ab^2+ab+1=0$, then $a^2b^2+a^2b\neq 0$ always holds since otherwise $b=1$ and $ab^2+ab+1=1\neq 0$. Therefore, the system (14) has no solution.

If $ab^2+ab+1\neq 0$, we let $\theta=a^2b(b+1)(ab^2+ab+1)^{-1}$ and combine $x+y=bxy$ to get the following quadratic equation:

$$x^2+\theta x+\frac{\theta}{b}=0. \tag{15}$$

It is well known that Eq. (15) has two solutions if and only if $\mathrm{Tr}_1^n(\theta^{-1}b^{-1})=0$, which can be denoted by $x=x_0$ and $x=x_0+\theta$ ($y=x_0+\theta$ and $y=x_0$ respectively).

As in Case I, we also analyze the solution set by considering if $ab\in\mathbb{F}_4^*$ or $a(b+1)\in\mathbb{F}_4^*$.

If $ab\in\mathbb{F}_4^*$ or $a(b+1)\in\mathbb{F}_4^*$, it is easy to verify that $a(b+1)(ab+1)\neq 1$, $ab(ab+a+1)\neq 1$, and $ab^2+ab+1\neq 0$ always hold. Thus, none of $\{(0,b^{-1}),(b^{-1},0),(a,(a^{-1}+b)^{-1}),((a^{-1}+b)^{-1},a)\}$ is a solution and we can at most obtain two solutions from Eq. (15) if and only if the corresponding trace function $\mathrm{Tr}_1^n(\theta^{-1}b^{-1})=0$. Specifically, for $ab\in\{1,\omega,\omega^2\}$, we have $\theta^{-1}b^{-1}=(a+1)^{-1},(a+1)(a+\omega)^{-1},(a+1)(a+\omega^2)^{-1}$, respectively, while for $a(b+1)\in\{1,\omega,\omega^2\}$, we have $\theta^{-1}b^{-1}=(a^2+1)^{-1},\omega(a+1)(a^2+\omega^2)^{-1},(a+1)\omega^{-1}(a^2+\omega)^{-1}$, respectively.

If both $ab\notin\mathbb{F}_4^*$ and $a(b+1)\notin\mathbb{F}_4^*$, notice that $a(b+1)(ab+1)\neq ab(ab+a+1)$ otherwise $a=0$ contradicts $a\in\mathbb{F}_{2^n}^*$, then we may have either $\{(0,b^{-1}),(b^{-1},0)\}$ or $\{(a,(a^{-1}+b)^{-1}),((a^{-1}+b)^{-1},a)\}$ as possible solutions. Since either $a(b+1)(ab+1)=1$ or $ab(ab+a+1)=1$ is not incompatible with $ab^2+ab+1\neq 0$, it is still likely to find two more solutions from Eq. (15).

We summarize the solution set of the system (12) for $A\neq B$ (including $(A,B)=(0,1)$ as what has been discussed above and the mirroring situation $(A,B)=(1,0)$) in Table 8 and finally conclude in Table 9 the maximum cardinality of its solution set under different (a,b), namely $\mathcal{B}_{f_3}(a,b)$.

□

To end this subsection, for some small n, we give some possible maximum values of $\mathcal{B}_{f_3}$ over $\mathbb{F}_{2^n}$ with even n in Table 10.

5 Concluding remarks

This paper mainly concentrates on the c-differential uniformity and boomerang uniformity of three classes of permutation polynomials over $\mathbb{F}_{2^n}$. On the one hand, by using the Weil sums technique to determine the number of solutions of some certain equations, we obtain two families of involutions $f_1(x)$ and $f_2(x)$, which are APcN functions for $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$. Moreover, the boomerang uniformity of $f_1(x)$ and $f_2(x)$ can attain 2^n. On the other hand, we present some upper bounds on the c-differential uniformity and boomerang uniformity of $f_3(x)$ by calculating the solutions of some certain equations. It is a continuation and generalization of some previous works in [12, 24]. We summarize all the known permutation polynomials over $\mathbb{F}_{2^n}$ with low c-differential uniformity and boomerang uniformity in Table 11 and Table 12, respectively. Finding more permutation polynomials with low c-differential uniformity and boomerang uniformity over finite fields with even characteristics would be interesting.

Table 8
Distribution of solutions of the system (12) for $A \neq B$ with conditions on (a, b)

ab	$a(b+1)$	$a(b+1)(ab+1)$	$ab(ab+a+1)$	$\mathrm{Tr}_1^n(\frac{1}{\theta b})$	Solution set Ω	$\mathrm{Card}(\Omega)$
1	$\times$	$\times$	$\times$	0	$+4$	4
ω	$\times$	$\times$	$\times$	0	$+4$	4
ω^2	$\times$	$\times$	$\times$	0	$+4$	4
$\times$	1	$\times$	$\times$	0	$+4$	4
$\times$	ω	$\times$	$\times$	0	$+4$	4
$\times$	ω^2	$\times$	$\times$	0	$+4$	4
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	1	$\times$	0	$\Lambda + 4$	8
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	$\times$	1	0	$\Pi + 4$	8
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	$\neq 1$	$\neq 1$	0	$+4$	4
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	1	$\times$	1	Λ	4
$\notin \mathbb{F}_4^*$	$\notin \mathbb{F}_4^*$	$\times$	1	1	Π	4

* $+4$ implies four (more) solutions implicitly given by quadratic equations.
* $\Lambda = \{(0, b^{-1}), (b^{-1}, 0), (a, a + b^{-1}), (a + b^{-1}, a)\}$.
* $\Pi = \{(a, (a^{-1} + b)^{-1}), ((a^{-1} + b)^{-1}, a), (0, a + (a^{-1} + b)^{-1}), (a + (a^{-1} + b)^{-1}, 0)\}$.
* $\Omega = \{\varnothing\}$ for any other (a, b) unlisted and thus $\mathrm{Card}(\Omega) = 0$.

Table 9
Maximum cardinality of the system (12) with conditions on (a, b)

ab	$a(b+1)$	$\max(\mathrm{Card}(\Omega))$ for $A = B$	$\max(\mathrm{Card}(\Omega))$ for $A \neq B$	$\max(\mathcal{B}_{f_3}(a, b))$
1	$\times$	6	4	10
$\times$	1	6	4	10
$\in \mathbb{F}_4 \backslash \mathbb{F}_2$	$\times$	$6\ (n \equiv 2 \pmod 4)$	4	$10\ (n \equiv 2 \pmod 4)$
$\in \mathbb{F}_4 \backslash \mathbb{F}_2$	$\times$	$8\ (n \equiv 0 \pmod 4)$	4	$12\ (n \equiv 0 \pmod 4)$
$\times$	$\in \mathbb{F}_4 \backslash \mathbb{F}_2$	$6\ (n \equiv 2 \pmod 4)$	4	$10\ (n \equiv 2 \pmod 4)$
$\times$	$\in \mathbb{F}_4 \backslash \mathbb{F}_2$	$8\ (n \equiv 0 \pmod 4)$	4	$12\ (n \equiv 0 \pmod 4)$
$\notin \mathbb{F}_4$	$\notin \mathbb{F}_4$	4	8	12

Acknowledgements

The authors are grateful to anonymous reviewers and the editor for their detailed comments and suggestions, which significantly improved this paper's presentation and quality. Q. Liu was supported by the Educational Research Project of Young and Middle-aged Teachers of Fujian Province under Grant JAT200033 and the Talent Fund Project of Fuzhou University under Grant GXRC-20002. X. Liu was supported by the National Natural Science Foundation of China under Grant 62072109. J. Zou was supported by the National Natural Science Foundation of China under Grant 61902073.

Table 10
Some possible maximum values of $\mathcal{B}_{f_3}$ over $\mathbb{F}_{2^n}$

n	$f(x)$	$\mathcal{B}_{f_3}$
8	$x^{-1} + \mathrm{Tr}_1^8((x^{-1}+1)^{254} + x^{-254})$	10
8	$x^{-1} + \mathrm{Tr}_1^8((x^{-1}+1)^{21} + x^{21})$	6
6	$x^{-1} + \mathrm{Tr}_1^6((x^{-1}+1)^{5} + x^{5})$	4
6	$x^{-1} + \mathrm{Tr}_1^6((x^{-1}+1)^{15} + x^{15})$	8

References

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

[2] Bartoli. D., Calderini. M.: On construction and (non) existence of c-(almost) perfect nonlinear functions. Finite Fields and Their Applications. 72, 101835 (2021).

[3] Beierle. C., Leander. G.: 4-uniform permutations with null nonlinearity. Cryptography and Communications. 12, 1133-1141 (2020).

[4] Biham. E., Shamir. A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology. 4, 3-72 (1991).

[5] Borisov. N., Chew. M., Johnson. R., Wagner. D.: Multiplicative differentials. In: J. Daemen and V. Rijmen (Eds.) FSE 2002, LNCS 2365, Springer, Heidelberg, 17-33 (2002).

[6] Boura. C., Canteaut. A.: On the boomerang uniformity of cryptographic S-boxes. IACR Transactions on Symmetric Cryptology. 3, 290-310 (2018).

[7] Carlet. C.: Boolean functions for cryptography and coding theory, Cambridge University Press, Cambridge (2020).

[8] Charpin. P., Kyureghyan. G.: When does $G(x) + \gamma Tr(H(x))$ permute $\mathbb{F}_{p^n}$. Finite Fields and Their Applications. 15, 615-632 (2009).

[9] Cid. C., Huang. T., Peyrin. T. Sasaki. Y., Song. L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen J., Rijmen V. (Eds.) Advances in Cryptology-EUROCRYPT 2018, LNCS 10821, Springer, Heidelberg, 683-714 (2018).

[10] Ellingsen. P., Felke. P., Riera. C., Stănică. P., Tkachenko. A.: C-differentials, multiplicative uniformity and (almost) perfect$c$-nonlinearity. IEEE Transactions on Information Theory. 66(9), 5781-5789 (2020).

[11] Hasan. S., Pal. M., Riera. C., Stănică. P.: On the c-differential uniformity of certain maps over finite fields. Designs, Codes and Cryptography. 89, 221-239 (2021).

[12] Hasan. S., Pal, M., Stănică. P.: The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials. IEEE Transactions on Information Theory. 68, 679-691 (2021).

[13] Li. N., Hu. Z., Xiong. M., Zeng. X.: A note on "Cryptographically strong permutations from the butterfly structure". Designs, Codes and Cryptography, 90, 265-276 (2022).

[14] Li. K., Li. C., Helleseth. T., Qu. L.: Cryptographically strong permutations from the butterfly structure. Designs, Codes and Cryptography, 89, 737-761 (2021).

[15] Li. K., Qu. L., Sun. B., Li., C.: New results about the boomerang uniformity of permutation polynomials. IEEE Transactions on Information Theory. 65, 7542-7553 (2019).

[16] Li. C., Riera. C., Stănică. P.: Low c-differentially uniform functions via an extension of Dillon's switching method. https://arxiv.org/abs/2204.08760v1 (2022).

[17] Li. N., Xiong. M., Zeng. X.: On permutation quadrinomials and 4-uniform BCT. IEEE Transactions on Information Theory. 99, 4845-4855 (2021).

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

[19] Mesnager. S., Mandal. B., Msahli. M.: Survey on recent trends towards generalized differential and boomerang uniformities. Cryptography and Communications. https://doi.org/10.1007/s12095-021-00551-6 (2021).

[20] Mesnager. S., Riera. C., Stănică. P., Yan. H., Zhou. Z.: Investigations on c-(almost) perfect nonlinear functions. IEEE Transactions on Information Theory. 67, 6916-6925 (2021).

[21] Mesnager. S., Tang. C., Xiong. M.: On the boomerang uniformity of quadratic permutations. Designs, Codes and Cryptography. 88, 2233-2246 (2020).

[22] Nyberg. K.: Differentially uniform mappings for cryptography. In: T. Helleseth (Eds.) Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer, Heidelberg, 55-64 (1993).

[23] Stănică. P.: Low c-differential and c-boomerang uniformity of the swapped inverse function. Discrete Mathematics. 344, 112543 (2021).

[24] Tan. Y., Qu. L., Tan. C., Li. C.: New families of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$. In: T. Helleseth and J. Jedwab (Eds.) SETA 2012, LNCS 7280, Springer, Heidelberg, 25-39 (2012).

[25] Tu. Z., Li. N., Zeng. X., Zhou. J.: A class of quadrinomial permutations with boomerang uniformity four. IEEE Transactions on Information Theory. 66, 3753-3765 (2020).

[26] Tu. Z., Zeng. X., Jiang. Y., Tang. X.: A class of APcN power functions over finite fields of even characteristic. https://arxiv.org/abs/2107.06464v1 (2021).

[27] Wagner. D.: The boomerang attack. In: L. Knudsen (Eds.) FSE'99, LNCS 1636, Springer, Heidelberg, 156-170 (1999).

[28] Wang. Y., Kadir. W., Li. C., Xia. Y.: On cryptographic properties of the Welch permutation and a related conjecture. In: SETA 2020, LNCS 1636, Springer, Heidelberg, 156-170 (2020).

[29] Wu. Y., Li. N., Zeng. X.: New PcN and APcN functions over finite fields. Designs, Codes and Cryptography. 89, 2637-2651 (2021).

[30] Yan. H.: On (-1)-differential uniformity of ternary APN power functions. Cryptography and Communications. 14, 357-369 (2022).

[31] Zha. Z., Hu. L.: Some classes of power functions with low c-differential uniformity over finite fields. Designs, Codes and Cryptography. 89, 1193-1210 (2021).

Table 11
Known permutation polynomials over $\mathbb{F}_{2^n}$ with low c-differential uniformity

$f(x)$	Conditions	${}_c\Delta_f$	Reference
$x^{2^n-2}+x^{2^n-1}+(x+1)^{2^n-1}$	$n \geq 2$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	≤ 4	[23]
$x+\mathrm{Tr}_1^n(\alpha x+x^{2^k+1})$	$n \geq 3$ is odd and $\gcd(k,n)=1$, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\alpha)=1$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	2	[12]
	$n \geq 3$ is odd and $\gcd(k,n)=1$, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\alpha)=1$, $c=0$	1	[12]
	$n \geq 3$ is odd and $\gcd(k,n)=1$, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\alpha)=1$, $c=1$	2^n	[12]
$x^{-1}+\mathrm{Tr}_1^n(\frac{x^2}{x+1})$	all n, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$, $\mathrm{Tr}_1^n(c)=\mathrm{Tr}_1^n(c^{-1})=1$	≤ 8	[12]
	all n, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$, $\mathrm{Tr}_1^n(c)=\mathrm{Tr}_1^n(c^{-1})=0$ or $\mathrm{Tr}(c)+\mathrm{Tr}(c^{-1})=1$	≤ 9	[12]
	all n, $c=0$	1	[12]
$x+\mathrm{Tr}_1^n(x^{2^{k+1}+1}+x^3+x+ux)$	$n=2k+1$, $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	2	Theorem 3
	$n=2k+1$, $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$, $c=0$	1	Remark 1
	$n=2k+1$ with $k \not\equiv 1 \pmod 3$, $u \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$, $c=1$	2^n	Theorem 1
$x+\mathrm{Tr}_1^n(x^{2^k+3}+(x+1)^{2^k+3})$	$n=2k+1$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	2	Theorem 6
	$n=2k+1$, $c=0$	1	Remark 3
	$n=2k+1$ with $k \not\equiv 1 \pmod 3$, $c=1$	2^n	Theorem 4
$x^{-1}+\mathrm{Tr}_1^n((x^{-1}+1)^d+x^{-d})$	n even, any positive d, $\mathrm{Tr}_1^n(c)=\mathrm{Tr}_1^n(c^{-1})=1$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	≤ 8	Theorem 7
	n even, any positive d, $\mathrm{Tr}_1^n(c)=\mathrm{Tr}_1^n(c^{-1})=0$ or $\mathrm{Tr}(c)+\mathrm{Tr}(c^{-1})=1$, $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$	≤ 9	Theorem 7
	n even, any positive d, $c=0$	1	Theorem 7
	n even, $d \in \{2^n-2, 2^{\frac{n}{2}}+2^{\frac{n}{4}}+1, 2^{t_1}+1, 3(2^{t_2}+1)\}$, $1 \leq t_1 \leq \frac{n}{2}-1$, $2 \leq t_2 \leq \frac{n}{2}-1$, $c=1$	4	[24]

Table 12
Known permutation polynomials over $\mathbb{F}_{2^n}$ with low boomerang uniformity

$f(x)$	Conditions	$\mathcal{B}_f$	Reference
$\alpha x^{2^k+1}+\alpha^{2^m}x^{2^{-m}+2^{m+k}}$	$n=3m$, $m\equiv 2 \pmod 4$, $\gcd(n,k)=2$, $3\mid(m+k)$, $ord(\alpha)=2^n-1$	4	[6]
All quadratic permutation	$\Delta_f=4$	≤ 12	[6]
$x^{2^m+2}+\gamma x$	$n=2m$ and m odd, $ord(\gamma^{2^m-1})=3$	4	[15]
$x^{2^{m+1}+2^m}+c_1x^{2^{m+1}+1}+c_2x^{2^m+2}+c_3x^3$	$n=2m$, m odd, $(c_1,c_2,c_3)\in\Gamma$, the condition of Γ see [25]	4	[25]
$c_0x^{2^m(2^k+1)}+c_1x^{2^{k+m}+1}+c_2x^{2^m+2^k}+c_3x^{2^k+1}$	$n=2m$, odd m and k, $\gcd(m,k)=1$, $(c_0,c_1,c_2,c_3)\in\Gamma$, else see [17]	4	[17]
$x+\mathrm{Tr}_1^n(\alpha x+x^{2^k+1})$	$n\geq 3$ is odd, $\alpha\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\alpha)=1$, $\gcd(k,n)=1$	2^n	[12]
$x^{-1}+\mathrm{Tr}_1^n(\frac{x^2}{x+1})$	n even	≤ 12	[12]
$x+\mathrm{Tr}_1^n(x^{2^{k+1}+1}+x^3+x+ux)$	$n=2k+1$ with $k\neq 1 \pmod 3$, $u\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(u)=1$	2^n	Theorem 8
$x+\mathrm{Tr}_1^n(x^{2^k+3}+(x+1)^{2^k+3})$	$n=2k+1$ with $k\neq 1 \pmod 3$	2^n	Theorem 9
$x^{-1}+\mathrm{Tr}_1^n((x^{-1}+1)^d+x^{-d})$	n even, any positive d	≤ 12	Theorem 10