# Bivariate functions with low $c$-differential uniformity

Yanan Wu[*], Pantelimon Stănică[†], Chunlei Li[‡], Nian Li[§], Xiangyong Zeng[¶]

**Abstract**

Starting with the multiplication of elements in $\mathbb{F}_q^2$ which is consistent with that over $\mathbb{F}_{q^2}$, where $q$ is a prime power, via some identification of the two environments, we investigate the $c$-differential uniformity for bivariate functions $F(x,y) = (G(x,y), H(x,y))$. By carefully choosing the functions $G(x,y)$ and $H(x,y)$, we present several constructions of bivariate functions with low $c$-differential uniformity, in particular, many P$c$N and AP$c$N functions can be produced from our constructions.

**Keywords:** Low $c$-differential uniformity, perfect and almost perfect $c$-nonlinearity, the bivariate function.

**Mathematics Subject Classification:** 11T06, 12E20, 94A60.

# 1 Introduction

The differential attack, introduced by Biham and Shamir in [5], is one of the most fundamental cryptanalytic approaches targeting symmetric-key primitives. The ability of a cryptographic function applied in the S-box to resist the differential attack is quantified

[*]Y. Wu is with the Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. Email: yanan.wu@aliyun.com

[†]P. Stănică (corresponding author) is with the Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943, USA. Email: pstanica@nps.edu

[‡]C. Li is with the Department of Informatics, University of Bergen, 5020 Bergen, Norway. Email: chunlei.li@uib.no

[§]N. Li is with Hubei Key Laboratory of Applied Mathematics, School of Cyber Science and Technology, Hubei University, Wuhan 430062, China. Email: nianli@hubu.edu.cn

[¶]X. Zeng is with Hubei Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

by the so-called differential uniformity [18]. In [7], the authors proposed a new type of differential by utilizing modular multiplication as a primitive operation which can be used to attack some known ciphers such as a variant of the IDEA cipher. Very recently, motivated by their work, Ellingsen et al. [11] introduced a new concept called multiplicative differential (and the corresponding $c$-differential uniformity) in the following way.

**Definition 1.1.** *Let $\mathbb{F}_{p^n}$ denote the finite field with $p^n$ elements, where $p$ is a prime and $n$ is a positive integer. For a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $c \in \mathbb{F}_{p^n}$, the (multiplicative) $c$-derivative of $F$ with respect to $a \in \mathbb{F}_{p^n}$ is defined as*

$$ {}_cD_aF(x) = F(x+a) - cF(x), $$

*for all $x \in \mathbb{F}_{p^n}$. For $b \in \mathbb{F}_{p^n}$, we define ${}_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n}, {}_cD_aF(x) = b\}$ and call ${}_c\Delta_F = \max\{{}_c\Delta_F \ (a,b) : a, b \in \mathbb{F}_{p^n}$, and $a \neq 0$ if $c = 1\}$, the $c$-differential uniformity of $F$. In this case, $F$ is said to be $(c, {}_c\Delta_F)$-uniform.*

Note that if $c = 0$ or $a = 0$, then ${}_cD_aF(x)$ is a shift of the function $F$ and if $c = 1$ and $a \neq 0$, then ${}_cD_aF(x)$ becomes the usual derivative. Therefore, the concept of $c$-differential uniformity can be seen as the generalization of that of the classical differential uniformity. Similarly to the classic case, $F$ is called a *perfect $c$-nonlinear* (P$c$N) function if ${}_c\Delta_F = 1$ and an *almost perfect $c$-nonlinear* (AP$c$N) function if ${}_c\Delta_F = 2$. Bartoli and Timpanella in [3] proposed the concept of $\beta$-planar functions, which is just the P$c$N function with respect to $c = \beta$.

Ellingsen et al. [11] investigated the $c$-differential uniformity of some well-known PN functions and the inverse function. Inspired by their work, this topic has been extensively studied in the past years. Researchers proposed several constructions of functions with low $c$-differential uniformity, such as the AGW criterion, cyclotomic method, the perturbing and swapping method, as well as the switching method [2, 12, 15, 17, 21, 22, 23, 25, 26, 27].

In [1], it was shown that the graph of a P$c$N function corresponds to a difference set in a quasigroup, hence providing the first application of the $c$-differential uniformity (recall that difference sets give rise to symmetric designs, used in the construction of optimal self complementary codes, among other applications). Moreover, it was suggested in [1] that the post-whitening keys in an even number of rounds (like in the higher-order differential cryptanalysis) will disappear, when the round keys are connected via some of the constants $c$ in the higher order $c$-derivatives, or if just *one* of the sequence of derivatives is the classical one. Further, in a very recent manuscript by Pal and Stănică [19] it was shown

that the boomerang uniformity for an odd APN function in odd characteristic equals its $c$-differential uniformity when $c = -1$, if the function is a permutation, otherwise it is the maximum of the $(-1)$-DDT entries, disregarding the first row/column. This indicates that our work may have implications in the classical differential uniformity area.

In [9], Carlet constructed new classes of APN functions by employing the bivariate function. This method was later used to construct other classes of APN functions and has turned to be effective to give rise to a new family of APN functions [8, 10, 16, 24, 28]. A natural problem is to investigate how the $c$-differential uniformity of the known APN bivariate functions behaves. The computational data shows that the $c$-differential properties of these APN functions are not good, in general. This motivates us to study low $c$-differential uniformity by virtue of bivariate functions $F(x, y) \in \mathbb{F}_q[x, y]$. By utilizing the 1-to-1 correspondence between $\mathbb{F}_q^2$ and $\mathbb{F}_{q^2}$, we firstly characterize the multiplication over $\mathbb{F}_q^2$ and then give a definition of the $c$-differential uniformity of $F(x, y)$, which is consistent with the $c$-differential uniformity in univariate form. This is somewhat different, in general, from the approach of [20], where the $c$-differential uniformity was taken as the maximum for each bivariate component. Based on the newly defined concept of the $c$-differential uniformity in this paper, we present an infinite class of bivariate functions and the upper bound of the $c$-differential uniformity is given for any $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$. By employing some well-known cryptographic functions, such as the Gold function and the inverse function, we propose some concrete examples and investigate the $c$-differential uniformity explicitly in any characteristic. Furthermore, we propose several classes of functions with low $c$-differential uniformity for any $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$. In addition, by fixing $c = (c_1, 0) \in \mathbb{F}_q \backslash \{1\} \times \{0\}$, we derive other five classes of bivariate functions with low $c$-differential uniformity. It is worth noting that many P$c$N and AP$c$N functions can be produced from our constructions.

Throughout this paper, we assume $q = p^m$ for a prime $p$ and a positive integer $m$, and we denote by $\mathbb{F}_q$, the finite field with $q$ elements. For $l \mid m$, we denote by $\mathrm{Tr}_l^m$, the relative trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^l}$, defined by $\mathrm{Tr}_l^m(x) = \sum_{i=0}^{m/l-1} x^{p^{li}}$.

# 2 Preliminaries

Let $\chi$ be the quadratic character of $\mathbb{F}_q$ when $q$ is odd, namely, for any $\alpha \in \mathbb{F}_q^*$, $\chi(\alpha) = 1$ if $\alpha$ is a square, $\chi(\alpha) = -1$ if $\alpha$ is not a square. We denote by $SQ$ and $NSQ$, the set of square elements and non-square elements in $\mathbb{F}_q^*$, respectively. Throughout this paper, we

select some $t \in \mathbb{F}_q$ which satisfies $\mathrm{Tr}_1^m(t) = 1$ when $q$ is even and $1 - 4t \in NSQ$ when $q$ is odd. Below we recall basic results on the factorization of low-degree polynomials over $t \in \mathbb{F}_q$.

**Lemma 2.1** ([4]). *Let $m$ be a positive integer, $p$ a prime number and $q = p^m$. Then:*

(1) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_q^*$ and $q$ even, has two solutions in $\mathbb{F}_q$ if and only if $\mathrm{Tr}_1^m\left(\frac{b}{a^2}\right) = 0$, and no solution, otherwise.*

(2) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_q$ and $q$ odd, has two (respectively, one) solutions in $\mathbb{F}_q$ if and only if the discriminant $a^2 - 4b \in SQ$ (respectively, $a^2 - 4b = 0$).*

The factorization of a quartic polynomial over a finite field $\mathbb{F}_{2^m}$ can be given in terms of the roots of a related cubic equation. Let $f(x) = x^4 + a_2x^2 + a_1x + a_0$ with $a_0a_1 \neq 0$ and $g(y) = y^3 + a_2y + a_1$ with the roots $r_1$, $r_2$, $r_3$. When the roots exist in $\mathbb{F}_{2^m}$, we set $w_i = a_0r_i^2/a_1^2$, $1 \leq i \leq 3$. If a polynomial $f$ is factored as a product of irreducible polynomials of degrees $a, b, c, \ldots$, we write that as $f = (a, b, c, \ldots,)$.

**Lemma 2.2** ([14]). *Let $f(x) = x^4 + a_2x^2 + a_1x + a_0 \in \mathbb{F}_{2^m}[x]$ with $a_0a_1 \neq 0$. The factorization of $f(x)$ over $\mathbb{F}_{2^m}$ is characterized as follows:*

(1) $f = (1,1,1,1) \Leftrightarrow g = (1,1,1)$ *and* $\mathrm{Tr}_1^m(w_1) = \mathrm{Tr}_1^m(w_2) = \mathrm{Tr}_1^m(w_3) = 0$;

(2) $f = (2,2) \Leftrightarrow g = (1,1,1)$ *and* $\mathrm{Tr}_1^m(w_1) = 0, \mathrm{Tr}_1^m(w_2) = \mathrm{Tr}_1^m(w_3) = 1$;

(3) $f = (1,3) \Leftrightarrow g = (3)$;

(4) $f = (1,1,2) \Leftrightarrow g = (1,2)$ *and* $\mathrm{Tr}_1^m(w_1) = 0$;

(5) $f = (4) \Leftrightarrow g = (1,2)$ *and* $\mathrm{Tr}_1^n(w_1) = 1$.

With the natural 1-to-1 correspondence between $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$ with respect to some primitive element in $\mathbb{F}_{q^2}$, below we consider the multiplication between elements in $\mathbb{F}_q^2$, which induces a multiplicative isomorphism between $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$. Based on the multiplication operation, the $c$-differential uniformity of a bivariate function can be investigated in terms of a system of two bivariate equations.

According to Lemma 2.1, one can verify that

$$tc_2^2 + (1 - c_1)c_2 + (1 - c_1)^2 \neq 0, \tag{2.1}$$

for any $(c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1,0)\}$. Besides, it can be easily checked that the quadratic polynomial $f(x) = x^2 + x + t$ is irreducible over $\mathbb{F}_q$. Let $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ be a root of $f(x)$, then we can extend $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$ based on the basis $\{1, \beta\}$. Also, $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$ are in 1-to-1 correspondence under the mapping

$$\varphi(x, y) = z = x + \beta y;\ z \in \mathbb{F}_{q^2},\ x,\ y \in \mathbb{F}_q. \tag{2.2}$$

From (2.2), $x,\ y \in \mathbb{F}_q$ can be expressed by $z \in \mathbb{F}_{q^2}$ as

$$x = \frac{\overline{\beta} z - \beta \overline{z}}{\overline{\beta} - \beta},\ y = \frac{z - \overline{z}}{\beta - \overline{\beta}}, \tag{2.3}$$

where $\overline{z}$ is the Galois conjugate of $z$, i.e., $\overline{z} = z^q$. Therefore,

$$\varphi^{-1}(z) = \varphi^{-1}(x + \beta y) = (x, y) = \left( \frac{\overline{\beta} z - \beta \overline{z}}{\overline{\beta} - \beta}, \frac{z - \overline{z}}{\beta - \overline{\beta}} \right).$$

For any $z_1 = \varphi(x_1, y_1)$, $z_2 = \varphi(x_2, y_2)$, we have

$$\begin{aligned} \varphi^{-1}(z_1 \cdot z_2) &= \varphi^{-1}\left((x_1 + \beta y_1)(x_2 + \beta y_2)\right) \\ &= \varphi^{-1}(x_1 x_2 + \beta(x_1 y_2 + x_2 y_1) + \beta^2 (y_1 y_2)) \\ &= \varphi^{-1}(x_1 x_2 - t y_1 y_2 + \beta(x_1 y_2 + x_2 y_1 - y_1 y_2)) \\ &= (x_1 x_2 - t y_1 y_2, x_1 y_2 + x_2 y_1 - y_1 y_2)\,. \end{aligned}$$

To be consistent with the multiplication over $\mathbb{F}_{q^2}$, we can define the multiplication over $\mathbb{F}_q^2$ as

$$(x_1, y_1) \cdot (x_2, y_2) = \varphi^{-1}\left(\varphi(x_1, y_1) \cdot \varphi(x_2, y_2)\right) = (x_1 x_2 - t y_1 y_2, x_1 y_2 + x_2 y_1 - y_1 y_2).$$

Let $F(x, y) = (G(x, y), H(x, y))$ be a bivariate function from $\mathbb{F}_q^2$ to itself, where both $H(x, y)$ and $G(x, y)$ are bivariate functions from $\mathbb{F}_q^2$ to $\mathbb{F}_q$. Based on the multiplicative definition over $\mathbb{F}_q^2$ as above, we next give a proper definition of the $c$-differential uniformity of $F(x, y)$.

**Definition 2.3.** *Let $F(x, y) = (G(x, y), H(x, y))$ be a bivariate function from $\mathbb{F}_q^2$ to $\mathbb{F}_q^2$, where $H(x, y)$ and $G(x, y)$ are bivariate functions from $\mathbb{F}_q^2$ to $\mathbb{F}_q$. The c-differential equation $D_{c,a}F(x, y) = b$ with $a = (a_1, a_2)$, $b = (b_1, b_2)$, $c = (c_1, c_2) \in \mathbb{F}_q^2$ is given in the following system of equations*

$$\begin{cases} G(x + a_1, y + a_2) - c_1 G(x, y) + t c_2 H(x, y) &= b_1, \\ H(x + a_1, y + a_2) - (c_1 - c_2) H(x, y) - c_2 G(x, y) &= b_2. \end{cases} \tag{2.4}$$

*We define the c-Differential Distribution Table (DDT) entry at* $(a, b)$ *as*

$$ {}_c\Delta_F(a,b) = \#\left\{(x,y) \in \mathbb{F}_q^2 \,:\, D_{c,a}F(x,y) = b\right\} $$

*and the c-differential uniformity of* $F$ *as* ${}_c\Delta_F = \max\left\{{}_c\Delta_F(a,b) \,:\, a,b \in \mathbb{F}_q^2, \text{ and } a \neq (0,0) \text{ if } c = (1,0)\right\}$ *(we say that* $F$ *is* $(c,\ {}_c\Delta_F)$*-uniform).*

It should be noted that the 1-to-1 correspondence between the univariate and bivariate representations of $F(x, y)$ is given by

$$ F(z) = H\left(\frac{\overline{\beta}z - \beta\overline{z}}{\overline{\beta} - \beta}, \frac{z - \overline{z}}{\beta - \overline{\beta}}\right) + \beta\, G\left(\frac{\overline{\beta}z - \beta\overline{z}}{\overline{\beta} - \beta}, \frac{z - \overline{z}}{\beta - \overline{\beta}}\right). \tag{2.5} $$

To prove our results, we need the following lemmas.

**Lemma 2.4** ([6])**.** *Let* $m$, $k$ *be two positive integers with* $\gcd(m, k) = d$. *Let* $p$ *be a prime,* $q = p^m$ *and* $r = [\mathbb{F}_q : \mathbb{F}_{p^{\gcd(m,k)}}]$ *be the degree of the extension. Then the polynomial* $f(x) = x^{p^k+1} + ax + b$ *has exactly* 0, 1, 2 *or* $p^d + 1$ *roots in* $\mathbb{F}_q$, *when* $a$, $b$ *run through* $\mathbb{F}_q^*$. *In particular, the number of* $b \in \mathbb{F}_q^*$ *such that* $x^{p^k+1} + x + b = 0$ *has exactly* $p^d + 1$ *solutions in* $\mathbb{F}_q$ *is* $\frac{p^{(r-1)d} - p^{\epsilon d}}{p^{2d}-1}$, *where* $\epsilon = 0$ *if* $r$ *is odd and* $\epsilon = 1$, *otherwise.*

**Remark 2.5.** *Note that if* $r = 2$ *in Lemma* 2.4, *then* $\frac{p^{(r-1)d} - p^{\epsilon d}}{p^{2d}-1} = 0$ *and therefore, there is no* $a \in \mathbb{F}_q^*$ *such that* $x^{p^k+1} + x + a = 0$ *has* $p^d + 1$ *solutions in* $\mathbb{F}_q$.

The $c$-differential uniformity of the inverse function $f(x) = x^{-1}$ and Gold function $f(x) = x^{p^k+1}$ has been completely described. Below, we recall the results which can be used to simplify our proof of the main results in our paper.

**Lemma 2.6** ([12]))**.** *Let* $q = 2^m$, $m \geq 2$, $c \in \mathbb{F}_q$ *and* $F : \mathbb{F}_q \to \mathbb{F}_q$ *be the inverse function defined by* $F(x) = x^{q-2}$. *We have:*

(1) *If* $c = 0$, *then* $F$ *is* $PcN$ *(this is equivalent to* $F$ *being a permutation).*

(2) *If* $c = 1$, *the differential uniformity of* $F$ *is* 2, *when* $m$ *is even, and* 4, *when* $m$ *is odd.*

(3) *If* $c \neq 0$ *and* $\mathrm{Tr}_1^m(c) = \mathrm{Tr}_1^m(1/c) = 1$, *the c-differential uniformity of* $F$ *is* 2 *(and hence* $F$ *is APcN).*

(4) *If* $c \neq 0$ *and* $\mathrm{Tr}_1^m(1/c) = 0$, *or* $\mathrm{Tr}_1^m(c) = 0$, *the c-differential uniformity of* $F$ *is* 3.

**Lemma 2.7** ([12, 19])**.** *Let $q$ be odd and $c \in \mathbb{F}_q$. Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be the inverse function defined by $F(x) = x^{q-2}$. We have:*

(1) *If $c = 0$, then $F$ is $PcN$ (this is equivalent to $F$ being a permutation).*

(2) *If $c \neq 1$, and $\chi(c^2 - 4c) = 1$ or $\chi(1 - 4c) = 1$, the $c$-differential uniformity of $F$ is 3.*

(3) *If $c = 1$ and $\chi(-3) = 0$, the $c$-differential uniformity of $F$ is 3.*

(4) *If $c = 1$ and $\chi(-3) = 1$, the $c$-differential uniformity of $F$ is 4.*

(5) *In all other cases, the $c$-differential uniformity of $F$ is 2.*

# 3 The main results

In this section, we mainly focus on the bivariate functions of the form $F(x, y) = (G(x, y), H(x, y))$. We will investigate the $c$-differential uniformity properties of $F$ for certain functions $G, H$, and present several families of bivariate functions with low $c$-differential uniformity. It is worth noting that many P$c$N and AP$c$N functions can be produced from our constructions.

## 3.1 Functions with low $c$-differential uniformity for any $c \in \mathbb{F}_{q^2}$

Firstly, we consider the bivariate function $F(x, y)$ of the form $F(x, y) = (g(x), h(y) + g(x))$, for some univariate $g, h$. According to Definition 2.3, the $c$-differential uniformity of $F(x, y)$ is given by

$$\begin{cases} g(x + a_1) - (c_1 - tc_2)g(x) + tc_2h(y) &= b_1, \\ g(x + a_1) - c_1g(x) + h(y + a_2) - (c_1 - c_2)h(y) &= b_2. \end{cases} \tag{3.1}$$

We first give the upper bound about the $c$-differential uniformity of $F(x, y)$ as follows.

**Lemma 3.1.** *Let $F(x, y) = (g(x), h(y) + g(x))$ and $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$. If $g(x)$ is differentially $(c_1 - tc_2, \delta_1)$-uniform and $h(x)$ is differentially $(c_1 - (1 - t)c_2, \delta_2)$-uniform, then ${}_c\Delta_F \leq \delta_1\delta_2$. In particular, ${}_c\Delta_F = \delta_1\delta_2$ when $c_2 = 0$.*

In particular, if $g(x)$ is a linearized polynomial over $\mathbb{F}_q$ and $h(y)$ is a permutation polynomial over $\mathbb{F}_q$ in Lemma 3.1, then we have the following result.

**Theorem 3.2.** *Let $q = p^m$ and $F(x, y) = (L(x), h(y) + L(x))$, where $L(x)$ is a linearized permutation polynomial, $h(y)$ is a permutation polynomial over $\mathbb{F}_q$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$ and denote $A = (c_1 - c_2)(1 - c_1 + tc_2) + tc_2(1 - c_1)$ and $B = 1 - c_1 + tc_2$. If $AB = 0$, then $F(x, y)$ is a PcN function; If $AB \neq 0$ and ${}_{\frac{A}{B}}\Delta_h = \delta$, then $F(x, y)$ is differentially $(c, \delta)$-uniform.*

*Proof.* By Equation (3.1), we need to solve the following system of equations

$$\begin{cases} (1 - c_1 + tc_2)L(x) + tc_2 h(y) = b_1 - L(a_1), & (3.2) \\ (1 - c_1)L(x) + h(y + a_2) - (c_1 - c_2)h(y) = b_2 - L(a_1), & (3.3) \end{cases}$$

where $(a_1, a_2),\ (b_1, b_2) \in \mathbb{F}_q^2$. If $c = (c_1, c_2) = (0, 0)$, it can be easily checked that ${}_c\Delta_F = 1$. We assume now that $c = (c_1, c_2) \neq (0, 0)$ and $B = 1 - c_1 + tc_2$.

**Case I:** If $B = 0$, then $c_2 \neq 0$ due to $(c_1, c_2) \neq (1, 0)$. From Equation (3.2) and $h(y)$ permuting $\mathbb{F}_q$, we can see that $y$ is uniquely determined by $a_1$, $b_1$. Moreover, for a fixed $y$ satisfying (3.2), there is exactly one solution $x$ to Equation (3.3) due to $L(x)$ being a linearized permutation polynomial. Thus, we have ${}_c\Delta_F = 1$.

**Case II:** If $B \neq 0$, by Equation (3.2), then

$$L(x) = \frac{b_1 - L(a_1) - tc_2 h(y)}{B}. \tag{3.4}$$

Substituting Equation (3.4) into Equation (3.3), we get

$$h(y + a_2) - \Big(c_1 - c_2 + \frac{tc_2(1 - c_1)}{B}\Big)h(y) = b_2 - L(a_1) - (1 - c_1)\frac{b_1 - L(a_1)}{B}.$$

Since $b_1$ and $b_2$ run through $\mathbb{F}_q$, it is equivalent to considering

$$h(y + a_2) - \frac{A}{B}h(y) = b_3 \tag{3.5}$$

with $A = (c_1 - c_2)(1 - c_1 + tc_2) + tc_2(1 - c_1)$ and $b_3 \in \mathbb{F}_q$. Note that $L(x)$ is a permutation polynomial, which implies that $x$ can be uniquely determined by $y$ from (3.4). Therefore, in this case, the number of solutions of Equations (3.2)-(3.3) is equivalent to that of Equation (3.5). Now, we focus on solving Equations (3.5). Firstly, we claim that $\frac{A}{B} \neq 1$. Suppose $\frac{A}{B} = 1$, then $(1 - c_1)tc_2 = (1 - c_1 + c_2)(1 - c_1 + tc_2)$, which can be reduced to $tc_2^2 + (1 - c_1)c_2 + (1 - c_1)^2 = 0$. This is impossible due to $(c_1, c_2) \neq (1, 0)$ and Equation (2.1). Further, we can see that Equations (3.5) always has only one solution when $A = 0$. When $AB \neq 0$, then $F(x, y)$ is differentially $(c, \delta)$-uniform, since ${}_{\frac{A}{B}}\Delta_h = \delta$. □

**Remark 3.3.** *From the proof above we can see that when $L(x)$ is an $s$-to-1 linearized polynomial in Theorem* 3.2*, we can derive the following result:*

(1) *If $AB = 0$, then ${}_c\Delta_F = s$;*

(2) *If $AB \neq 0$ and ${}_{\frac{A}{B}}\Delta_h = \delta$, then ${}_c\Delta_F \leq \delta s$.*

According to the result in Theorem 3.2, we can construct many functions with low $c$-differential uniformity from the known functions. Moreover, P$c$N and AP$c$N functions can be derived in our constructions. By employing inverse functions and Gold functions, the following corollaries can be directly obtained by Lemmas 2.6 and 2.7.

**Corollary 3.4.** *Let $q = 2^m$ with $m \geq 3$ being a positive integer and $F(x, y) = (L(x), y^{-1} + L(x))$, where $L(x)$ is a linearized permutation polynomial over $\mathbb{F}_q$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$ and denote $A = (c_1 + c_2)(1 + c_1 + tc_2) + tc_2(1 + c_1)$ and $B = 1 + c_1 + tc_2$.*

(1) *If $AB = 0$, then $F(x, y)$ is a PcN function;*

(2) *If $AB \neq 0$, then $F(x, y)$ is differentially $(c, 3)$-uniform when $\mathrm{Tr}_1^m(\frac{A}{B}) \cdot \mathrm{Tr}_1^m(\frac{B}{A}) = 0$; otherwise, $F(x, y)$ is an APcN function.*

**Corollary 3.5.** *Let $q = p^m$ with $m$ being a positive integer and $p$ being an odd prime, $F(x, y) = (L(x), \frac{1}{y} + L(x))$, where $L(x)$ is a linearized permutation polynomial over $\mathbb{F}_q$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$. Denote $A = (c_2 - c_1)(1 - c_1 + tc_2) - tc_2(1 - c_1)$ and $B = 1 - c_1 + tc_2$. Then:*

(1) *If $AB = 0$, then $F(x, y)$ is a PcN function;*

(2) *If $AB \neq 0$, when $\frac{A}{B} = 4, 4^{-1}$ or $\frac{A}{B}\left(\frac{A}{B} - 4\right) \in NSQ$ and $\frac{A}{B}(\frac{B}{A} - 4) \in NSQ$, then $F(x, y)$ is an APcN function; when $\frac{A}{B} \neq 4, 4^{-1}$, $\frac{A}{B}\left(\frac{A}{B} - 4\right) \in SQ$, or $\frac{A}{B}(\frac{B}{A} - 4) \in SQ$, $F(x, y)$ is differentially $(c, 3)$-uniform.*

**Example 3.6.** *Let $q = 2^4$ and $t = w^3$, where $w$ is a primitive element of $\mathbb{F}_q$. Then $f(x) = x^2 + x + t$ is an irreducible polynomial over $\mathbb{F}_q[x]$. Let $F(x, y) = (x, y^{-1} + x)$ and $c = (c_1, c_2) \in \mathbb{F}_{2^4}^2 \backslash \{(1, 0)\}$. Magma experiments show that when $(c_1 + c_2 + \frac{tc_2(1+c_1)}{1+c_1+tc_2})(1 + c_1 + tc_2) = 0$ or $(c_1, c_2) = (0, 0)$, $F(x, y)$ is PcN; when $\left(c_1 + c_2 + \frac{tc_2(1+c_1)}{1+c_1+tc_2}\right)(1 + c_1 + tc_2) \neq 0$ and $(c_1, c_2) \neq 0$, $F(x, y)$ is differentially $(c, 3)$-uniform if $\mathrm{Tr}_1^m\left(c_1 + c_2 + \frac{tc_2(1+c_1)}{1+c_1+tc_2}\right) = 0$ or $\mathrm{Tr}_1^m\left(\left(c_1 + c_2 + \frac{tc_2(1+c_1)}{1+c_1+tc_2}\right)^{-1}\right) = 0$; otherwise, $F(x, y)$ is APcN. It is consistent with the result in Corollary* 3.4*.*

**Example 3.7.** *Let $q = 2^3$. Then $f(x) = x^2+x+1$ is an irreducible polynomial over $\mathbb{F}_q[x]$. Let $F(x, y) = (x^2 + x, y^{-1} + x^2 + x)$ and $c = (c_1, c_2) \in \mathbb{F}_{2^3}^2 \backslash \{(1, 0)\}$. Magma experiments show that when $(c_1 + c_2 + \frac{c_2(1+c_1)}{1+c_1+c_2})(1 + c_1 + c_2) = 0$ or $(c_1, c_2) = 0$, $F(x, y)$ is differentially $(c, 2)$-uniform; otherwise, $F(x, y)$ is $(c, 6)$-uniform which is consistent with the result in Remark 3.3.*

**Theorem 3.8.** *Let $F(x, y) = (L(x), y^{p^k+1} + \alpha y + L(x))$, where $L(x)$ is a linearized permutation polynomial, $k < m$ is a positive integer and $\alpha \in \mathbb{F}_q$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$.*

(1) *When $m \neq 2k$, if $\alpha = 0$ and $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2} \in \mathbb{F}_{p^{\gcd(m,k)}}$, then ${}_c\Delta_F = \gcd(p^k + 1, p^m - 1)$. Otherwise, we have ${}_c\Delta_F = p^{\gcd(m,k)} + 1$.*

(2) *When $m = 2k$, if $\alpha \neq 0$ and $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2} \in \mathbb{F}_{p^k}$, then ${}_c\Delta_F = 2$. Otherwise, we have ${}_c\Delta_F = p^k + 1$.*

*Proof.* By Definition 2.3, it is sufficient to solve the system of equations

$$\begin{cases} (1 - c_1 + tc_2)L(x) + tc_2 y^{p^k+1} + tc_2\alpha y = b_1, & (3.6) \\ (1 - c_1 + c_2)y^{p^k+1} + a_2 y^{p^k} + (a_2^{p^k} + \alpha(1 - c_1 + c_2))y + (1 - c_1)L(x) = b_2, & (3.7) \end{cases}$$

where $a_2$, $b_1$, $b_2 \in \mathbb{F}_q$. Note that $1 - c_1 + tc_2$ and $1 - c_1$ cannot be zero simultaneously. Otherwise, we can infer that $(c_1, c_2) = (1, 0)$, which contradicts the assumption. Next, we discuss the above system of equations by splitting the analysis into two cases.

**Case I:** $1 - c_1 + tc_2 = 0$. Then there are at most $\gcd(p^k + 1, p^m - 1)$ solutions $y \in \mathbb{F}_q$ satisfying Equation (3.6) when $\alpha = 0$ and at most $p^{\gcd(m,k)} + 1$ solutions when $\alpha \neq 0$ by Lemma 2.4. Further, for each $y$, Equation (3.7) has exactly one solution $x \in \mathbb{F}_q$ due to $L(x)$ being a permutation polynomial. Since $b_1$ runs over $\mathbb{F}_q$, one has ${}_c\Delta_F = \gcd(p^k+1, p^m-1)$ for $\alpha = 0$. When $\alpha \neq 0$, we can see that if $m = 2k$, then ${}_c\Delta_F = 2$ again by Lemma 2.4 and otherwise, ${}_c\Delta_F = p^{\gcd(m,k)} + 1$.

**Case II:** $1 - c_1 + tc_2 \neq 0$. For this case, $L(x) = \frac{b_1 - tc_2 y^{p^k+1} - tc_2\alpha y}{1-c_1+tc_2}$ by Equation (3.6). Substituting $L(x)$ into Equation (3.7), one gets

$$A_1 y^{p^k+1} + A_2 y^{p^k} + A_3 y + A_4 = 0, \quad (3.8)$$

where $A_1 = tc_2^2 + (1 - c_1)c_2 + (1 - c_1)^2$, $A_2 = (1 - c_1 + tc_2)a_2$, $A_3 = (1 - c_1 + tc_2)a_2^{p^k} + \alpha A_1$ and $A_4 = b_1(1 - c_1) - b_2(1 - c_1 + tc_2)$. Note that $A_1 \neq 0$ from Equation (2.1).

When $\alpha = 0$, Equation (3.8) has at most $\gcd(p^k+1, p^m-1)$ solutions in $\mathbb{F}_q$ if $(\frac{A_2}{A_1})^{p^k} = \frac{A_3}{A_1}$. When $\alpha \neq 0$, Equation (3.8) has at most $p^{\gcd(m,k)} + 1$ solutions if $m \neq 2k$ by Lemma

2.4 and also at most $p^k+1$ solutions if $m=2k$ which is possible by choosing $a_2=0$ and $b_1$, $b_2$, properly.

Similarly, when $\alpha\neq 0$, observe that if $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2}\notin \mathbb{F}_{p^{\gcd(m,k)}}$, then there always exists $a_2\in\mathbb{F}_q$ such that $(\frac{A_2}{A_1})^{p^k}=\frac{A_3}{A_1}$. Therefore, by Lemma 2.4, one has that the above equation has at most $p^{\gcd(m,k)}+1$ solutions for the case $m\neq 2k$. If $m=2k$, it has at most $p^k+1$ solutions when $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2}\notin\mathbb{F}_{p^k}$, otherwise, it has at most two solutions.

The result follows by combining Cases I and II, which completes the proof. □

**Remark 3.9.** *It is well known* [11] *that* $\gcd(2^k+1,2^m-1)=\frac{2^{\gcd(2k,m)}-1}{2^{\gcd(k,m)}-1}$ *and when* $p>2$ *and* $\frac{m}{\gcd(m,k)}$ *is odd,* $\gcd\left(p^k+1,p^m-1\right)=2$. *Therefore, one can see from Theorem* 3.8 *that when* $m\neq 2k$, $\frac{m}{\gcd(m,k)}$ *is odd, if* $\alpha=0$ *and* $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2}\in\mathbb{F}_{p^{\gcd(m,k)}}$, *then* $F(x,y)$ *is PcN when* $p=2$ *and APcN when* $p>2$.

**Example 3.10.** *Let* $q=2^4$ *and* $t=w^3$, *where* $w$ *is a primitive element of* $\mathbb{F}_{2^4}$. *Then* $f(x)=x^2+x+t$ *is an irreducible polynomial over* $\mathbb{F}_{2^4}[x]$. *Let* $F(x,y)=(x,y^5+\alpha y+x)$ *and* $c=(c_1,c_2)\in\mathbb{F}_{2^4}^2\backslash\{(1,0)\}$. *Magma experiments show that when* $\alpha\neq 0$ *and* $\frac{1+c_1+tc_2}{tc_2^2+(1+c_1)c_2+(1+c_1)^2}\in\mathbb{F}_{2^2}$, $F(x,y)$ *is APcN; otherwise,* $F(x,y)$ *is differential* $(c,5)$*-uniform which is consistent with the result in Theorem* 3.8.

**Example 3.11.** *Let* $q=3^3$ *and* $t=w^2$, *where* $w$ *is a primitive element of* $\mathbb{F}_{3^3}$. *Then* $f(x)=x^2+x+t$ *is an irreducible polynomial over* $\mathbb{F}_{3^3}[x]$. *Let* $F(x,y)=(x,y^{10}+\alpha y+x)$ *and* $c=(c_1,c_2)\in\mathbb{F}_{3^3}^2\backslash\{(1,0)\}$. *Magma experiments show that when* $\alpha=0$ *and* $\frac{1-c_1+tc_2}{tc_2^2+(1-c_1)c_2+(1-c_1)^2}\in\mathbb{F}_3$, $F(x,y)$ *is APcN; otherwise,* $F(x,y)$ *is differential* $(c,4)$*-uniform which is also consistent with the result in Theorem* 3.8.

In the following, we present another class of bivariate functions $F(x,y)$ which is different from that of Lemma 3.1.

**Theorem 3.12.** *Let* $\alpha\in\mathbb{F}_q^*$, $F(x,y)=(x+y,x^{p^i}y+\alpha xy^{p^j})$ *and* $c=(c_1,c_2)\in\mathbb{F}_q^2\backslash\{(1,0)\}$. *Denote* $A=\big\{(c_1,c_2)\in\mathbb{F}_q^2\backslash\{(1,0)\}:c_2\neq 0$ *and* $\mathrm{Tr}_1^m\Big(\frac{1-c_1}{tc_2}\Big)=\mathrm{Tr}_1^m\Big(\frac{(1-c_1+c_2)(c_1-1)}{tc_2}-c_2\Big)=0\big\}$. *Then*:

(1) *If* $\alpha=-1$ *and* $(i,j)=(0,1)$, *then* ${}_c\Delta_F\leq p+1$ *for* $c\in\{(c_1,0):c_1\in\mathbb{F}_q\backslash\{1\}\}$; ${}_c\Delta_F\leq q+p-1$ *for* $c\in A$ *and* ${}_c\Delta_F\leq 2p$, *otherwise;*

(2) *If* $\alpha=-1$ *and* $(i,j)=(0,m-1)$, *then* ${}_c\Delta_F=q+p-1$ *for* $c\in A$, *and* ${}_c\Delta_F\leq 2p$, *otherwise;*

(3) *If* $\alpha \neq -1$ *and* $(i,j) = (1,1)$ *or* $(i,j) = (m-1, m-1)$, *then* ${}_c\Delta_F \leq p+1$ *for* $c \in \{(c_1, 0) : c_1 \in \mathbb{F}_q \backslash \{1\}\}$, *and* ${}_c\Delta_F \leq p^2 + p$, *otherwise.*

*Proof.* We only give the proof for the case $(i,j) = (1,1)$, since the other cases can be similarly proved. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1,0)\}$. It is sufficient to solve the following system of equations

$$\begin{cases} tc_2(x^p y + \alpha x y^p) + (1-c_1)x + (1-c_1)y = b_1, & (3.9) \\ (1+c_2-c_1)(x^p y + \alpha x y^p) + a_2 x^p + \alpha a_1 y^p + (\alpha a_2^p - c_2)x + (a_1^p - c_2)y = b_2, & (3.10) \end{cases}$$

where $(a_1, a_2)$, $(b_1, b_2) \in \mathbb{F}_q^2$. When $c_2 = 0$, then we have $c_1 \neq 1$ due to $(c_1, c_2) \neq (1,0)$ and $x = \frac{b_1}{1-c_1} - y$ from Equation (3.9). Replacing it into Equation (3.10), we obtain an equation whose degree is actually $p+1$ due to $\alpha \neq -1$. Thus, we have ${}_c\Delta_F \leq p+1$. Next, we assume that $c_2 \neq 0$. Multiplying Equation (3.9) by $-\frac{1+c_2-c_1}{tc_2}$ and then adding it to Equation (3.10) gives us

$$a_2 x^p + B_1 x + \alpha a_1 y^p + B_2 y = b_3, \tag{3.11}$$

where $B_1 = \alpha a_2^p - c_2 - \frac{(1+c_2-c_1)(1-c_1)}{tc_2}$, $B_2 = a_1^p - c_2 - \frac{(1+c_2-c_1)(1-c_1)}{tc_2}$ and $b_3 = b_2 - \frac{b_1(1+c_2-c_1)}{tc_2}$. By Equation (2.1), we can see that $a_2$ and $B_1$ cannot be zero at the same time.

**Case I:** $a_2 = 0$. In this case, we have $B_1 \neq 0$ and $x = \frac{b_3 - B_2 y - \alpha a_1 y^p}{B_1}$ from Equation (3.11). Substituting it into Equation (3.9), we get an equation in $y$ only, whose highest degree is $p^2+1$ when $a_1 \neq 0$. When $a_1 = 0$, then we have $B_1 = B_2$ and $x = \frac{b_3}{B_1} - y$ from Equation (3.11). Combining this expression with Equation (3.9) gives an equation about $y$ whose highest degree is $p+1$ due to $\alpha \neq -1$. Thus, there is at most $p^2+1$ solutions for Equations (3.9)-(3.10).

**Case II:** $a_2 \neq 0$. If $B_1 = 0$, then $x^p = \frac{b_3 - B_2 y - \alpha a_1 y^p}{a_2}$. Similarly as in Case I, by taking $p$-th powers on both sides of Equation (3.9) and then eliminating $x^p$, we can derive an equation in $y$ only, whose highest degree can reach $p^2+p$. Thus, Equations (3.9)-(3.10) has at most $p^2+p$ solutions. If $B_1 \neq 0$, then multiplying Equation (3.11) by $-\frac{tc_2}{a_2}y$ and adding it to Equation (3.9) gives

$$(tc_2\alpha y^p - \frac{B_1 tc_2}{a_2}y + 1 - c_1)x - \frac{\alpha tc_2 a_1}{a_2}y^{p+1} - \frac{B_2 tc_2}{a_2}y^2 + (1 - c_1 + \frac{b_3 tc_2}{a_2})y = b_1. \tag{3.12}$$

**Subcase (II-1):** If there exists $y_1$ such that $tc_2\alpha y_1^p - \frac{B_1 tc_2}{a_2}y_1 + 1 - c_1 = 0$, then Equation (3.12) has solutions if and only if $b_1 = -\frac{\alpha tc_2 a_1}{a_2}y_1^{p+1} - \frac{B_2 tc_2}{a_2}y_1^2 + (1 - c_1 + \frac{b_3 tc_2}{a_2})y_1$ and for such $y_1$, Equation (3.9) has at most $p$ solutions on $x$.

**Subcase (II-2):** If $y$ satisfies $tc_2\alpha y^p - \frac{B_1tc_2}{a_2}y + 1 - c_1 \neq 0$, then $x$ can be uniquely expressed by $y$ from Equation (3.12). Replacing $x$ by $y$ in Equation (3.11), we can obtain an equation with the highest degree being $p^2 + p$. Thus, Equations (3.9)-(3.10) has at most $p^2 + p$ solutions in this case.

When Subcases (II-1) and (II-2) happen simultaneously, then we have

$$\begin{aligned} x &= \frac{\frac{\alpha tc_2a_1}{a_2}y^{p+1} + \frac{B_2tc_2}{a_2}y^2 - (1 - c_1 + \frac{b_3tc_2}{a_2})y + b_1}{tc_2\alpha y^p - \frac{B_1tc_2}{a_2}y + 1 - c_1} \\ &= \frac{\frac{\alpha tc_2a_1}{a_2}(y^{p+1} - y_1^{p+1}) + \frac{B_2tc_2}{a_2}(y^2 - y_1^2) - (1 - c_1 + \frac{b_3tc_2}{a_2})(y - y_1)}{tc_2\alpha(y^p - y_1^p) - \frac{B_1tc_2}{a_2}(y - y_1)}. \end{aligned}$$

from Subcase (II-2). Dividing by $y - y_1$ on both sides of the above equation and then substituting it into Equation (3.11) derives an equation with the highest degree being $p^2$. Therefore, one can see that Equations (3.9)-(3.10) has also at most $p^2 + p$ solutions when Subcases (II-1) and (II-2) happen at the same time. Based on the above analysis, one can conclude that ${}_c\Delta_F \leq p^2 + p$. This completes the proof. □

**Example 3.13.** *Let* $F(x, y) = (x + y, x^{p^i}y + \alpha xy^{p^j})$ *and* $c = (c_1, c_2) \in \mathbb{F}_{2^4}^2\backslash\{(1, 0)\}$. *Magma experiments show that*

(1) *If* $\alpha = 1$ *and* $(i, j) = (0, 1)$, *then* ${}_c\Delta_F = 3$ *for* $c \in \mathbb{F}_{2^4}$; ${}_c\Delta_F = 17$ *for those* $c = (c_1, c_2)$ *which satisfy* $c_2 \neq 0$ *and* $\mathrm{Tr}_1^4\big(\frac{1+c_1}{tc_2}\big) = \mathrm{Tr}_1^4\big(\frac{(1+c_1+c_2)(c_1+1)}{tc_2} + c_2\big) = 0$. *Otherwise,* ${}_c\Delta_F = 4$.

(2) *If* $\alpha = 1$ *and* $(i, j) = (0, 3)$, *then* ${}_c\Delta_F = 17$ *if* $c = (c_1, c_2)$ *satisfies* $c_2 \neq 0$ *and* $\mathrm{Tr}_1^4\big(\frac{1+c_1}{tc_2}\big) = \mathrm{Tr}_1^4\big(\frac{(1+c_1+c_2)(c_1+1)}{tc_2} + c_2\big) = 0$ *and otherwise,* ${}_c\Delta_F = 4$.

(3) *If* $\alpha = w$ *and* $(i, j) = (1, 1)$ *or* $(i, j) = (3, 3)$, *where* $w$ *is a primitive element in* $\mathbb{F}_{2^4}$, *then* ${}_c\Delta_F = 3$ *for* $c \in \mathbb{F}_{2^4}$ *and otherwise,* ${}_c\Delta_F = 6$.

**Example 3.14.** *Let* $F(x, y) = (x + y, x^{p^i}y + \alpha xy^{p^j})$ *and* $c = (c_1, c_2) \in \mathbb{F}_{3^3}^2\backslash\{(1, 0)\}$. *Magma experiments show that*

(1) *If* $\alpha = -1$ *and* $(i, j) = (0, 1)$ *or* $(i, j) = (0, 2)$, *then* ${}_c\Delta_F = 4$ *for* $c \in \mathbb{F}_{3^3}$; ${}_c\Delta_F = 29$ *for those* $c = (c_1, c_2)$ *which satisfy* $c_2 \neq 0$ *and* $\mathrm{Tr}_1^3\big(\frac{1-c_1}{tc_2}\big) = \mathrm{Tr}_1^3\big(\frac{(1-c_1+c_2)(c_1-1)}{tc_2} - c_2\big) = 0$. *Otherwise,* ${}_c\Delta_F = 6$.

(2) *If* $\alpha = w$ *and* $(i, j) = (1, 1)$ *or* $(i, j) = (2, 2)$, *where* $w$ *is a primitive element in* $\mathbb{F}_{3^3}$, *then* ${}_c\Delta_F = 4$ *for* $c \in \mathbb{F}_{3^3}\backslash\{1\}$ *and otherwise,* ${}_c\Delta_F = 12$.

If $F$ is a function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q \times \mathbb{F}_q$, by a similar process as before, we can also derive the expression of the $c$-differential equation of $F$. Let $n = 2m$. In the following, we present another class of functions that have low $c$-differential uniformity by using the inverse function.

**Theorem 3.15.** *Let $H(x) = \mathrm{Tr}_m^n\left(\frac{\gamma}{x}\right)$, where $\gamma \notin \mathbb{F}_q$. Let $F(x) = (\mathrm{Tr}_m^n(x), H(x))$ and $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1,0)\}$. Then ${}_c\Delta_F \leq 6$. More precisely, if $c = 0$, then $F$ is APcN; if $c \in \{(c_1, c_2) : c_1 = 1 \text{ or } c_2 = 0 \text{ or } (1-c_1)(c_1-c_2) = tc_2^2\}$, then ${}_c\Delta_F \leq 4$ and otherwise, ${}_c\Delta_F \leq 6$.*

*Proof.* By Definition 2.3, in order to determine the $c$-differential uniformity for $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1,0)\}$, it is sufficient to calculate the maximum number of solutions in $\mathbb{F}_{q^2}$ of the following system of equations

$$\begin{cases} (1-c_1)\mathrm{Tr}_m^n(x) + tc_2 H(x) = b_1, & (3.13) \\ H(x+a) - (c_1 - c_2)H(x) - c_2\mathrm{Tr}_m^n(x) = b_2 & (3.14) \end{cases}$$

when $a$ and $b = (b_1, b_2)$ run over $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$, respectively.

**Case I:** $c_2 = 0$. In this case, $c_1 \neq 1$ due to $c \neq (1,0)$. Since $H(x) = \mathrm{Tr}_m^n\left(\frac{\gamma}{x}\right)$, then Equation (3.14) can be reduced to

$$\frac{\gamma^q}{x^q + a^q} + \frac{\gamma}{x+a} - \frac{c_1\gamma^q}{x^q} - \frac{c_1\gamma}{x} = b_2. \tag{3.15}$$

On the other hand, from Equation (3.13), one has that all the solutions of Equation (3.13) can be expressed as $y + x_0$, where $y^q + y = 0$ and $x_0$ is a solution of Equation (3.13). If System (3.13)-(3.14) has one solution, either $x = 0$ or $x = -a$, without loss of generality, we may assume that $x = 0$ is a solution of (3.13)-(3.14). Then (3.15) becomes

$$\frac{\gamma^q}{-y + a^q} + \frac{\gamma}{y+a} + \frac{c_1(\gamma^q - \gamma)}{y} = b_2$$

which has at most three solutions in the set $\{y \in \mathbb{F}_{q^2}^* : y^q + y = 0\}$. The case that $x = -a$ is a solution of (3.13)-(3.14) can be similarly approached. If $x = 0$ and $x = -a$ are the solutions of System (3.13)-(3.14), simultaneously, then $a^q + a = 0$ and so, Equation (3.15) becomes

$$\frac{\gamma - \gamma^q}{y+a} + \frac{c_1(\gamma^q - \gamma)}{y} = b_2$$

which has at most two solutions in the set $\{y \in \mathbb{F}_{q^2}^* \backslash \{-a\} : y^q + y = 0\}$. If both $x = 0$ and $x = -a$ are not the solutions of (3.13)-(3.14), then by replacing $x$ with $y + x_0$, (3.15) has

at most four solutions since $y^q + y = 0$. Therefore, one can conclude that System (3.13)-(3.14) has at most four solutions in this case. In particular, when $c = 0$, i.e., $c_1 = 0$, it can be proved that $F(x) = b$ for any $b \in \mathbb{F}_q^2$ has at most two solutions, by the above analysis.

**Case II:** $c_2 \neq 0$. Since $H(x) = \mathrm{Tr}_m^n\left(\frac{\gamma}{x}\right)$ and $a$, $b = (b_1, b_2)$ run over $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$, respectively, it is equivalent to solve the following system of equations

$$\begin{cases} A_1\mathrm{Tr}_m^n(x) + \mathrm{Tr}_m^n(\frac{\gamma}{x}) = b_1, & (3.16) \\ A_2\mathrm{Tr}_m^n(x) + \mathrm{Tr}_m^n(\frac{\gamma}{x+a}) = b_2, & (3.17) \end{cases}$$

where $A_1 = \frac{1-c_1}{tc_2}$ and $A_2 = \frac{(1-c_1)(c_1-c_2)}{tc_2} - c_2$. One should note that $A_1 \neq A_2$, which is obvious by Equation (2.1). On the other hand, if $x = 0$ (or $x = -a$, respectively) is a solution of System (3.16)-(3.17), then $b_1 = 0$ and $b_2 = \mathrm{Tr}_m^n(\frac{\gamma}{a})$ (or $b_1 = -A_1\mathrm{Tr}_m^n(a) - \mathrm{Tr}_m^n(\frac{\gamma}{a})$ and $b_2 = -A_2\mathrm{Tr}_m^n(a)$, respectively). Firstly, we claim that $x = 0$ and $x = -a$ ($a \neq 0$) cannot be the solutions, simultaneously. If System (3.16)-(3.17) has the solutions $x = 0$, $x = -a$ ($a \neq 0$) at the same time, then $b_1 = -A_1\mathrm{Tr}_m^n(a) - \mathrm{Tr}_m^n(\frac{\gamma}{a}) = 0$ and $b_2 = \mathrm{Tr}_m^n(\frac{\gamma}{a}) = -A_2\mathrm{Tr}_m^n(a)$. It implies $(A_1 - A_2)\mathrm{Tr}_m^n(a) = 0$. Thus, we have $\mathrm{Tr}_m^n(a) = 0$ due to $A_1 \neq A_2$. Further, we can obtain that $b_1 = -\mathrm{Tr}_m^n(\frac{\gamma}{a}) = 0$. Observe that $\mathrm{Tr}_m^n(\frac{\gamma}{a}) = \frac{\gamma}{a} + \frac{\overline{\gamma}}{\overline{a}} = \frac{\gamma-\overline{\gamma}}{a}$ since $\mathrm{Tr}_m^n(a) = 0$. Thus, one has that $\mathrm{Tr}_m^n(\frac{\gamma}{a}) = \frac{\gamma-\overline{\gamma}}{a} = 0$, which is impossible when $a \neq 0$ due to $\gamma \notin \mathbb{F}_q$. Now, we assume that $x \neq 0$ and $x \neq -a$. Then System (3.16)-(3.17) can be reduced to

$$\begin{cases} A_1\mathrm{Tr}_m^n(x\overline{x}^2) + b_1x\overline{x} + \mathrm{Tr}_m^n(\overline{\gamma}x) = 0, & (3.18) \\ A_2\mathrm{Tr}_m^n(x\overline{x}^2 + a\overline{x}^2) + B_1x\overline{x} + \overline{B}_2\overline{x} + B_2x + B_3 = 0, & (3.19) \end{cases}$$

where

$$\begin{aligned} B_1 &= \mathrm{Tr}_m^n(\overline{a}A_2) - b_2, \\ B_2 &= a\overline{a}A_2 + \overline{\gamma} - \overline{a}b_2, \\ B_3 &= \mathrm{Tr}_m^n(\overline{a}\gamma) - a\overline{a}b_2. \end{aligned}$$

Next, we consider the above system of equations case by case.

**Subcase I:** $A_1 = 0$. In this subcase, we have $A_2 \neq 0$. When $b_1 = 0$, then $\overline{x} = -\gamma^{q-1}x$ from Equation (3.18) and then Equation (3.19) becomes

$$A_2\gamma^{q-1}(\gamma^{q-1} - 1)x^3 + ((a\gamma^{q-1}A_2 - B_1)\gamma^{q-1} + \overline{a}A_2)x^2 + (B_2 - \overline{B}_2\gamma^{q-1})x + B_3 = 0.$$

The above equation has at most 3 solutions in $\mathbb{F}_{q^2}\backslash\{0, -a\}$ due to $A_2\gamma^{q-1}(\gamma^{q-1} - 1) \neq 0$.

When $b_1 \neq 0$, then $\overline{x}(b_1x+\gamma) = -\overline{\gamma}x$ by Equation (3.18). Note that $b_1x+\gamma \neq 0$. Otherwise, if $b_1x+\gamma = 0$, one then has $x = 0$ which contradicts the assumption. Therefore, one can obtain that $\overline{x} = -\frac{\overline{\gamma}x}{b_1x+\gamma}$. Substituting this expression into Equation (3.19) renders

$$(\overline{a}b_1 - \overline{\gamma})b_1A_2x^4 + C_1x^3 + C_2x^2 + C_3x + B_3\gamma^2 = 0,$$

where

$$\begin{aligned}
C_1 &= (\overline{\gamma}-\gamma)\overline{\gamma}A_2 + 2\overline{a}b_1\gamma A_2 - b_1\overline{\gamma}B_1 + b_1^2B_2,\\
C_2 &= \mathrm{Tr}_m^n(a\overline{\gamma})A_2 - \gamma\overline{\gamma}B_1 - b_1\overline{\gamma}\overline{B}_2 + 2b_1\gamma B_2 + b_1^2B_3,\\
C_3 &= -\gamma\overline{\gamma}\overline{B}_2 + \gamma^2B_2 + 2b_1\gamma B_3,
\end{aligned}$$

which has at most 4 solutions when $a$, $b = (b_1, b_2)$ go through $\mathbb{F}_{q^2}$ and $\mathbb{F}_q^2$, respectively.

**Subcase II:** $A_2 = 0$. By letting $x = y - a$, System (3.16)-(3.17) becomes

$$\begin{cases}
A_1\mathrm{Tr}_m^n(y) + \mathrm{Tr}_m^n(\dfrac{\gamma}{y-a}) = b_1 + A_1\mathrm{Tr}_m^n(a),\\
\mathrm{Tr}_m^n(\dfrac{\gamma}{y}) = b_2.
\end{cases}$$

Since $x \neq 0, -a$, then $y \neq 0, a$. And therefore, the equation has at most 4 solutions, as proved in Subcase I.

**Subcase III:** $A_1A_2 \neq 0$. System (3.19) $\times A_1$ − (3.18) $\times A_2$ implies

$$A_1A_2\mathrm{Tr}_m^n(a\overline{x}^2) + (A_1B_1 - b_1A_2)x\overline{x} + \mathrm{Tr}_m^n((A_1B_2 - \overline{\gamma}A_2)x) + A_1B_3 = 0. \tag{3.20}$$

When $a = 0$, we have $B_1 = -b_2$, $B_2 = \overline{\gamma}$ and $B_3 = 0$. Further, Equation (3.20) is reduced to

$$(1 - (A_1b_2 + A_2b_1)x)\overline{x} + (A_1 - A_2)\overline{\gamma}x = 0.$$

Observe that $1 - (A_1b_2 + A_2b_1)x \neq 0$. Otherwise, one has $x = 0$ due to $(A_1 - A_2)\overline{\gamma} \neq 0$, which contradicts the assumption $x \neq 0, -a$. Hence, we have

$$\overline{x} = \frac{(A_1 - A_2)\overline{\gamma}x}{1 - (A_1b_2 + A_2b_1)x}.$$

Substituting the above equation into Equation (3.18) renders a quartic equation. It implies that System (3.18)-(3.19) has at most 4 solutions in $\mathbb{F}_{q^2}\backslash\{0, -a\}$, in this case.

When $a \neq 0$, (3.20) $\times x$ − (3.18) $\times aA_2$ gives that

$$(D_1x^2 + D_2x - D_3)\overline{x} = -E_1x^3 + E_2x^2 + E_3x, \tag{3.21}$$

where

$$D_1 = A_1B_1 - b_1A_2 - aA_1A_2,\ D_2 = A_1\overline{B}_2 - (\gamma + ab_1)A_2,\ D_3 = a\gamma A_2$$

and

$$E_1 = \overline{a}A_1A_2,\ E_2 = \overline{\gamma}A_2 - A_1B_2,\ E_3 = a\overline{\gamma}A_2 - A_1B_3.$$

If there exists $x_0 \neq 0, -a$ such that $D_1x_0^2 + D_2x_0 - D_3 = 0$, then Equation (3.21) has $x_0$ as one of its solutions only if $-E_1x_0^3 + E_2x_0^2 + E_3x_0 = 0$, which is equivalent to $-E_1x_0^2 + E_2x_0 + E_3 = 0$ due to $x_0 \neq 0$. One should note that there are at most two $x_0$'s that satisfy $D_1x_0^2 + D_2x_0 - D_3 = 0$ and $-E_1x_0^2 + E_2x_0 + E_3 = 0$. Let $x_1 \in \mathbb{F}_{q^2}\backslash\{0, -a\}$ be a solution of System (3.18)-(3.19) with $D_1x_1^2 + D_2x_1 - D_3 \neq 0$. When there are exactly two $x_0$'s which satisfy this condition, then $D_1x^2 + D_2x - D_3 = \mu(-E_1x^2 + E_2x + E_3)$ for some $\mu \in \mathbb{F}_{q^2}^*$. Then we have $\overline{x}_1 = \frac{x_1}{\mu}$ and further, Equation (3.18) has at most two solutions in $\mathbb{F}_{q^2}^*$. When there is only one $x_0$ which satisfies the above condition, we then have

$$\begin{aligned}
\overline{x}_1 &= \frac{-E_1x_1^3 + E_2x_1^2 + E_3x_1}{D_1x_1^2 + D_2x_1 - D_3} \\
&= \frac{E_2(x_1^2 - x_0^2) + E_3(x_1 - x_0)}{D_1(x_1^2 - x_0^2) + D_2(x_1 - x_0)} \\
&= \frac{E_2(x_1 + x_0) + E_3}{D_1(x_1 + x_0) + D_2}.
\end{aligned}$$

Substituting the above expression into Equation (3.18) renders a quartic equation, which has at most 4 solutions when $a$ runs over $\mathbb{F}_{q^2}^*$ and $b$ ranges over $\mathbb{F}_q^2$. Therefore, we conclude that System (3.18)-(3.19) has at most 5 solutions in $\mathbb{F}_{q^2}\backslash\{0, -a\}$, when this case happens.

If there is no $x \in \mathbb{F}_{q^2}\backslash\{0, -a\}$ such that $D_1x^2 + D_2x - D_3 = -E_1x^2 + E_2x + E_3 = 0$, we then have

$$\overline{x} = \frac{-E_1x^3 + E_2x^2 + E_3x}{D_1x^2 + D_2x - D_3}.$$

Similarly, by replacing it into Equation (3.18), we obtain an equation with the highest degree 7, namely,

$$A_1E_1(E_1 - D_1)x^7 + L_1x^6 + L_2x^5 + L_3x^4 + L_4x^3 + L_5x^2 + D_3(\overline{\gamma}D_3 - \gamma E_3)x = 0, \quad (3.22)$$

where

$$\begin{aligned}
L_1 &= A_1(D_1E_2 - D_2E_1 - 2E_1E_2) - b_1D_1E_1,\\
L_2 &= A_1(E_2(E_2 + D_2) + E_3(D_1 - E_1) + E_1(D_3 - E_3))\\
&\quad +b_1(D_1E_2 - D_2E_1) + D_1(\overline{\gamma}D_1 - \gamma E_1),\\
L_3 &= A_1(E_3(D_2 + E_2) + E_2(E_3 - D_3)) + b_1(D_1E_3 + D_2E_2 + D_3E_1)\\
&\quad +\gamma(D_1E_2 - D_2E_1) + 2\overline{\gamma}D_1D_2,\\
L_4 &= A_1E_3(E_3 - D_3) + b_1(D_2E_3 - D_3E_2) + \overline{\gamma}(D_2^2 - 2D_1D_3)\\
&\quad +\gamma(D_1E_3 + D_2E_2 + D_3E_1),\\
L_5 &= \gamma(D_2E_3 - D_3E_2) - 2\overline{\gamma}D_2D_3.
\end{aligned}$$

Obviously, Equation (3.22) has at most 6 solutions in $\mathbb{F}_{q^2}^*$. Therefore, System (3.18)-(3.19) has at most 6 solutions in $\mathbb{F}_{q^2}\backslash\{0, -a\}$, when this case happens.

From Subcases I-III, we can see that System (3.16)-(3.17) has at most 4 solutions in when $\mathbb{F}_{q^2}\backslash\{0, -a\}$, when $A_1A_2 = 0$, and at most 6 solutions in when $\mathbb{F}_{q^2}\backslash\{0, -a\}$, when $A_1A_2 \neq 0$.

Recall that $x = 0$ and $x = -a$ $(a \neq 0)$ cannot be the solutions of System (3.16)-(3.17), simultaneously. Assume that $x = 0$ is a solution of (3.16)-(3.17), then $b_1 = 0$ and $b_2 = \mathrm{Tr}_m^n(\frac{\gamma}{a})$. By Subcase I, one can easily check that the System (3.16)-(3.17) has at most 3 solutions in $\mathbb{F}_{q^2}^*$ due to $b_1 = 0$. Similarly, the System (3.16)-(3.17) has also at most 3 solutions in Subcase II. As for Subcase III, since $B_3 = \mathrm{Tr}_m^n(\overline{a}\gamma) - a\overline{a}b_2 = \mathrm{Tr}_m^n(\overline{a}\gamma) - a\overline{a}\mathrm{Tr}_m^n(\frac{\gamma}{a}) = 0$ and further, $\overline{\gamma}D_3 - \gamma E_3 = a\gamma\overline{\gamma}A_2 - \gamma(a\overline{\gamma}A_2 - A_1B_3) = 0$. Hence, one can see that Equation (3.22) has at most 5 solutions in $\mathbb{F}_{q^2}^*$. It implies that the System (3.16)-(3.17) has at most 6 solutions in $\mathbb{F}_{q^2}$ when $x = 0$ is a solution of System (3.16)-(3.17).

Assume that $x = -a$ $(a \neq 0)$ is a solution of (3.16)-(3.17), then $b_1 = -A_1\mathrm{Tr}_m^n(a) - \mathrm{Tr}_m^n(\frac{\gamma}{a})$ and $b_2 = -A_2\mathrm{Tr}_m^n(a)$. When $A_1 = 0$, we have $\frac{\gamma}{x} = \mu - \frac{\gamma}{a}$ and $\mu + \overline{\mu} = 0$ from Equation (3.16). Therefore, Equation (3.17) becomes

$$A_2\mathrm{Tr}_m^n(\frac{a\gamma}{a\mu - \gamma}) + \mathrm{Tr}_m^n(\frac{a\gamma\mu - \gamma^2}{a^2\mu}) = -A_2\mathrm{Tr}_m^n(a).$$

The above equation can be further reduced to

$$A_2(\frac{a\gamma}{a\mu - \gamma} - \frac{\overline{a\gamma}}{\overline{a}\mu + \overline{\gamma}}) + \frac{a\gamma\mu - \gamma^2}{a^2\mu} + \frac{\overline{a\gamma}\mu + \overline{\gamma}^2}{\overline{a}^2\mu} = 0,$$

which has at most 3 solution in $\{\mu \in \mathbb{F}_{q^2} | \mu + \overline{u} = 0 \text{ and } \mu \neq \frac{\gamma}{a}\}$. The case $A_2 = 0$ can be similarly proved. Therefore, when $A_1 A_2 = 0$, System (3.16)-(3.17) has at most 4 solutions in this case. When $A_1 A_2 \neq 0$, let $x = y - a$, then System (3.16)-(3.17) becomes

$$\begin{cases} A_1 \mathrm{Tr}_m^n(y) + \mathrm{Tr}_m^n(\frac{\gamma}{y-a}) = -\mathrm{Tr}_m^n(\frac{\gamma}{a}), \\ A_2 \mathrm{Tr}_m^n(y) + \mathrm{Tr}_m^n(\frac{\gamma}{y}) = 0. \end{cases}$$

According to the analysis for the case that $x = 0$ is a solutions of (3.16)-(3.17), we can derive that the above system of equations has at most 5 solutions in $\mathbb{F}_{q^2}^*$, that is, System (3.16)-(3.17) has at most 5 solutions in $\mathbb{F}_{q^2} \backslash \{-a\}$ when $x = -a$ is a solution of System (3.16)-(3.17). This completes the proof. □

## 3.2 Functions with low $c$-differential uniformity for $c \in \mathbb{F}_q$

On one hand, it is difficult to find new bivariate functions whose $c$-differential uniformity is always low for any $c \in \mathbb{F}_q^2$. On the other hand, due to the complexity of the $c$-differential equation of bivariate functions $F(x, y)$, generally speaking, it is not easy to determine the $c$-differential uniformity for $F(x, y)$. However, if we select $c = (c_1, 0)$, then System (2.4) is reduced to

$$\begin{cases} G(x + a_1, y + a_2) - c_1 G(x, y) &= b_1, \\ H(x + a_1, y + a_2) - c_1 H(x, y) &= b_2, \end{cases} \tag{3.23}$$

which seems more hopeful to deal with. Thus, in what follows, we aim to construct more low $c$-differential uniformity functions $F(x, y)$, including P$c$N and AP$c$N functions with respect to $c \in \mathbb{F}_q \backslash \{1\}$.

**Proposition 3.16.** *Let $F(x, y) = (g(x), H(x, y))$ with $H(x, y) = h_1(x)L_1(y) + \gamma_1 h_2(x) + \gamma_2 L_2(y)$, where $\gamma_1$, $\gamma_2 \in \mathbb{F}_q$, $g(x)$, $h_i(x)$ are functions from $\mathbb{F}_q$ to $\mathbb{F}_q$ and $L_i$ is a linearized polynomial over $\mathbb{F}_q$ for $1 \leq i \leq 2$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1, 0)\}$ and $\gamma_2 \neq 0$. If $g(x)$ is a PcN function with respect to some $c \in \{(c_1, 0) : c_1 \in \mathbb{F}_q \backslash \{1\}\}$ and $L_2(y) + \gamma L_1(y)$ is either 2-to-1 or permutation for any $\gamma \in \mathbb{F}_q$, then ${}_c\Delta_F \leq 2$.*

*Proof.* Note that $c \in \mathbb{F}_q \backslash \{1\}$. Thus, one has $c = (c_1, 0)$ for some $c_1 \neq 1$. For any $a = (a_1, a_2)$, $b = (b_1, b_2)$, the $c$-differential equation of $F(x, y)$ can be expressed as

$$\begin{cases} g(x + a_1) - c_1 g(x) &= b_1, \\ \left(h_1(x + a_1) - c_1 h_1(x)\right) L_1(y) + \gamma_2(1 - c_1) L_2(y) &= b' \end{cases}$$

by Equation (3.23), where

$$b' = b_2 - \gamma_1 \left(h_2(x + a_1) - c_1 h_2(x)\right) - \gamma_2 L_2(a_2) - h_1(x + a_1) L_1(a_2),$$

which is linear on $b_2$. Since $g(x)$ is P$c$N and $L_2(y) + \gamma L_1(y)$ is 2-to-1 or permutation for any $\gamma \in \mathbb{F}_q$, then $g(x + a_1) - c_1 g(x) = b_1$ has exactly one solution for any $a_1,\ b_1 \in \mathbb{F}_q$ and there are at most two solutions for the second equation. Then the result follows. □

**Remark 3.17.** *Note that if $h_1$ is a non-zero constant polynomial in Proposition* 3.16*, namely, $F$ has the form $F(x, y) = (g(x), h(y) + f(x))$, where $f(x)$ is any polynomial over $\mathbb{F}_q[x]$ and $h$ is not necessarily a linearized polynomial. In this case, we can check that if $g$ is $(c, \delta_1)$-uniform and $h$ is $(c, \delta_2)$-uniform for the same $c \in \mathbb{F}_q \backslash \{1\}$, then $F$ is $(c, \delta_1\delta_2)$-uniform. Therefore, if we choose $g$ and $h$ such that both of them are either PcN or APcN, then the c-differential uniformity of $F$ is at most* 4*. Based on the known PcN and APcN functions, an abundance of new classes of PcN and APcN functions can be produced by this way. For instance, let $g(x) = x^{\frac{p^{k_1}+1}{2}}$ and $h(y) = y^{p^{k_2}+1}$ with $p > 2$, $\frac{2m}{\gcd(2m,k_1)}$ and $\frac{m}{\gcd(m,k_2)}$ are odd, then $g$ is PcN and $h$ is APcN for $c = -1$ by* [17, Theorem 3 and Theorem 6]*. By selecting $f$ at random, Magma experiments always show that $F(x, y) = (g(x), h(y) + f(x))$ is APcN with respect to $c = -1$.*

Next, we give certain examples to prove the existence of functions in Proposition 3.16.

**Example 3.18.** *Let $q = 2^m$ and $g(x)$ be any linearized permutation polynomial over $\mathbb{F}_q$. Let $L_2(x) = x$ and $h_2(x) = x^{2^k}$ with $\gcd(k, m) = 1$. Obviously, one can easily check that $L_2(x) + \gamma h_2(x)$ is a permutation when $\gamma = 0$ or 2-to-1 when $\gamma \neq 0$. Selecting $\gamma_1 L_1(x) = x^2 + x$ or $\gamma_1 = 0$, $h_1(x) = x^{-1}$ or $h_1(x) = x^{2^k+1}$, Magma always shows that $F(x, y)$ is APcN for $c \in \mathbb{F}_q \backslash \{1\}$.*

**Example 3.19.** *Let $q = 3^m$ with $m$ odd and $F(x, y) = (x^{\frac{3^k+1}{2}}, y^3 + \gamma y)$, where $k$ is even and $\gamma$ is a square element in $\mathbb{F}_q^*$. Then one has $g(x) = x^{\frac{3^k+1}{2}}$ is PcN with respect to $c = -1$ from* [17, Theorem 6] *and $y^3 + \gamma y$ permutes $\mathbb{F}_q$. Magma experiments show that $F(x, y)$ is PcN for $c = (-1, 0)$. This is consistent with the result in Proposition* 3.16*.*

By employing quadratic functions and linearized polynomials, we present two classes of functions as below.

**Proposition 3.20.** *Let $q = p^m$ and $F(x, y) = (x^{p^k+1} + \gamma y^{p^k+1}, L(x + y))$, where $L$ is a linearized permutation polynomial over $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q \backslash \{-1\}$. Let $c \in \{(c_1, 0) : c_1 \in$*

$\mathbb{F}_q\backslash\{1\}\}$ *and* $d = \gcd(p^k+1, p^m-1)$. *If* $c, \gamma \in \mathbb{F}_{p^{\gcd(m,k)}}$, *then* $F$ *is* $(c,d)$*-uniform. Otherwise,* $F$ *is* $(c, p^{\gcd(m,k)}+1)$*-uniform.*

*Proof.* According to Equation (3.23), it suffices to determine the maximum number of solutions of

$$\begin{cases} (x+a_1)^{p^k+1} + \gamma(y+a_2)^{p^k+1} - c_1 x^{p^k+1} - c_1\gamma y^{p^k+1} = b_1, & (3.24) \\ (1-c_1)L(x+y) + L(a_1+a_2) = b_2, & (3.25) \end{cases}$$

when $a = (a_1, a_2)$, $b = (b_1, b_2)$ run over $\mathbb{F}_q^2$. From Equation (3.25), we have $y = L^{-1}\left(\frac{b_2 - L(a_1+a_2)}{1-c_1}\right) - x$. Replacing it into Equation (3.24) gives that

$$A_1 x^{p^k+1} + A_2 x^{p^k} + A_3 x + A_4 = 0, \tag{3.26}$$

where

$$\begin{aligned} A_1 &= (1+\gamma)(1-c_1), & A_2 &= a_1 - (b_2' + a_2 - c_1 b_2')\gamma, \\ A_3 &= a_1^{p^k} - ((b_2'+a_2)^{p^k} - c_1 b_2'^{p^k})\gamma, & A_4 &= a_1^{p^k+1} + ((b_2'+a_2)^{p^k+1} - c_1 b_2'^{p^k+1})\gamma - b_1 \end{aligned}$$

with $b_2' = L^{-1}\left(\frac{b_2 - L(a_1+a_2)}{1-c_1}\right)$. Note that $A \neq 0$ due to $c_1 \neq 1$ and $\gamma \neq -1$. If $c, \gamma \in \mathbb{F}_{p^{\gcd(m,k)}}$, then $\left(\frac{A_2}{A_1}\right)^{p^k} = \frac{A_3}{A_1}$ and further, one has

$$\left(x + \frac{A_2}{A_1}\right)^{p^k+1} - \left(\frac{A_2}{A_1}\right)^{p^k+1} + \frac{A_4}{A_1} = 0,$$

which is a shift of $x^{p^k+1}$. Thus, $F(x,y)$ is $(c,d)$-uniform in this case.

If $c, \gamma \notin \mathbb{F}_{p^{\gcd(m,k)}}$, there always exist $A_1$, $A_2$, $A_3$ such that $\left(\frac{A_2}{A_1}\right)^{p^k} \neq \frac{A_3}{A_1}$, since $a$ and $b$ are arbitrary. Let $x = B_1 z + B_2$ with $B_1 = \left(\frac{A_3}{A_1} - \left(\frac{A_2}{A_1}\right)^{p^k}\right)^{p^{m-k}}$ and $B_2 = -\frac{A_2}{A_1}$, then we have

$$z^{p^k+1} + z + \frac{A_1 B_2^{p^k+1} + A_2 B_2^{p^k} + A_3 B_2 + A_4}{A_1 B_1^{p^k+1}} = 0$$

which has 0, 1, 2 or $p^{\gcd(k,m)}+1$ solutions by Lemma 2.4. When $m \neq 2k$, since the constant term of the above equation is linear on $b_1$, the value $p^{\gcd(k,m)}+1$ is achievable by Lemma 2.4. When $m = 2k$, again by Lemma 2.4, we can see that the above equation has at most two solutions. However, returning to Equation (3.26), we always have $(a_1, a_2)$,

$(b_1, b_2) \in \mathbb{F}_q^2$ such that $A_2 = A_3 = 0$, when $a_1 = a_2 = b_2 = 0$. Thus, Equation (3.26) has at most $p^k + 1$ solutions when $m = 2k$ in this case.

Note that $p^{\gcd(k,m)} + 1 \geq \gcd(p^k + 1, p^m - 1)$. Then the result follows by the above analysis, which completes the proof. □

**Remark 3.21.** *Recall that* $\gcd(2^k + 1, 2^m - 1) = \frac{2^{\gcd(2k,m)}-1}{2^{\gcd(k,m)}-1}$ *and* $\gcd\left(p^k + 1, p^m - 1\right) = 2$ *if* $p > 2$ *and* $\frac{m}{\gcd(m,k)}$ *is odd. Therefore, one can obtain that if* $c, \gamma \in \mathbb{F}_{p^{\gcd(m,k)}}$ *with* $c \neq 1$, $\gamma \neq -1$ *and* $\frac{m}{\gcd(m,k)}$ *is odd, then* $F$ *is PcN when* $p = 2$ *and APcN when* $p > 2$.

**Example 3.22.** *Choosing* $q = p^m = 2^6$, $k = 2$ *and* $L(x) = x$, *then* $d = \gcd(p^k + 1, p^m - 1) = 1$. *When* $\gamma \in \mathbb{F}_{p^2}\backslash\{1\}$, *Magma shows that* $F$ *in Proposition* 3.20 *is PcN for any* $c \in \mathbb{F}_{p^2}\backslash\{1\}$ *and* $F$ *is* $(c, 5)$*-uniform when* $c \in \mathbb{F}_q\backslash\mathbb{F}_{p^2}$.

**Example 3.23.** *Choosing* $q = p^m = 3^3$, $k = 2$ *and* $L(x) = x^3 + x$. *For any* $\gamma \in \mathbb{F}_q\backslash\{2\}$, *Magma shows* $F$ *is* $(c, 4)$*-uniform when* $c \in \mathbb{F}_q\backslash\{1\}$.

**Proposition 3.24.** *Let* $q = p^m$ *and* $F(x, y) = \left(xy, \sum_{i=1}^m \gamma_i (xy)^{p^i} + L(x + y)\right)$, *where* $L$ *is a linearized permutation polynomial over* $\mathbb{F}_q$ *and* $\gamma_i \in \mathbb{F}_q$ *for* $1 \leq i \leq m$. *If* $\gamma_l \neq 0$ *only for* $l \in \{i_1, i_2, \ldots, i_t\}$, *where* $1 \leq t \leq m$ *and let* $d = \gcd(i_1, i_2, \ldots, i_t, m)$, *then* $F$ *is APcN for* $c \in \mathbb{F}_{p^d}\backslash\{1\}$. *In particular, if* $\gamma_i = 0$ *for all* $1 \leq i \leq m$, *then* $F$ *is APcN for* $c \in \{(c_1, 0) : c_1 \in \mathbb{F}_q\backslash\{1\}\}$ *and* $F$ *is always APcN for* $c = (0, 0)$ *regardless of the values of* $\gamma_i's$.

*Proof.* Let $c \in \{(c_1, 0) : c_1 \in \mathbb{F}_q\backslash\{1\}\}$. By Equation (3.23), the $c$-differential equation of $F(x, y)$ can be written as

$$\begin{cases} (1 - c_1)xy + a_2x + a_1y + a_1a_2 = b_1, & (3.27) \\ \sum_{i=1}^m \gamma_i \left(((x + a_1)(y + a_2))^{p^i} - c_1(xy)^{p^i}\right) + (1 - c_1)L(x + y) = b_2 - L(a_1 + a_2). & (3.28) \end{cases}$$

By taking $p^i$-th power on both sides of (3.27) for $1 \leq i \leq m$ in turn, (3.28) can be reduced to

$$\sum_{i=1}^m \gamma_i \left(c^{p^i} - c\right)(xy)^{p^i} + (1 - c)L(x + y) = b_2 - L(a_1 + a_2) - \sum_{i=1}^m b_1^{p^i}\gamma_i.$$

Let $\gamma_{i_j} \neq 0$ for $1 \leq j \leq t$ and $\gamma_l = 0$ for $l \notin \{i_1, i_2, \ldots, i_t\}$. Since $d = \gcd(i_1, i_2, \ldots, i_t, m)$ and $c \in \mathbb{F}_{p^d}\backslash\{1\}$, the above equation can be reduced to

$$(1 - c)L(x + y) = b_2 - L(a_1 + a_2) - \sum_{i=i_1}^{i_t} b_1^{p^i}\gamma_i.$$

Thus, $y$ can be uniquely determined by $x$, that is,

$$y = L^{-1}\left(\frac{b_2 - L(a_1+a_2) - \sum_{i=i_1}^{i_t} b_1^{p^i}\gamma_i}{1-c}\right) - x.$$

Substituting it into Equation (3.27), then we can obtain a quadratic equation which has at most two solutions in $\mathbb{F}_q$ and it can attain two solutions when choosing $a$, $b$, properly. For example, if $a_1 = a_2 = b_1 = 0$ and $b_2 \neq 0$, then Equation (3.27) has the form $x^2+tx = 0$ with $t \neq 0$, which has exactly two solutions for any $c \in \mathbb{F}_q$.

In particular, if $\gamma_i = 0$ for all $1 \leq i \leq m$ or $c = 0$, it is immediate that $F$ is AP$c$N by the above analysis. This completes the proof. □

**Example 3.25.** *Let $q = 2^m$ and $F(x,y) = \Big(xy, (xy)^{2^4} + (xy)^{2^2} + x + y\Big)$. Magma experiments show that $F$ is an APcN function for $c \in \mathbb{F}_{2^2}$ and $c \neq 1$.*

As constructed in Theorem 3.15, if $F$ is a function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q \times \mathbb{F}_q$, we can give the following results (the first one can be similarly proved as in Theorem 3.15).

**Proposition 3.26.** *Let $H$ be a function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and $F(x) = (\mathrm{Tr}_m^n(x), H(x))$. Let $c = (c_1, c_2) \in \mathbb{F}_q^2 \backslash \{(1,0)\}$.*

(1) *When $H(x) = \mathrm{Tr}_m^n\left(\gamma x^{p^k+1}\right)$ with $\gamma^q + \gamma \neq 0$, if $\gcd(k,m) = 1$, then ${}_c\Delta_F(x) \leq 6$; if $c \in \{(c_1,0) : c_1 \in \mathbb{F}_q \backslash \{1\}\}$, then $F(x)$ is $(c, p^{\gcd(k,m)}+1)$-uniform;*

(2) *When $H(x) = x^{q+1}$, then $F(x)$ is APcN for $c \in \{(c_1,0) : c_1 \in \mathbb{F}_q \backslash \{1\}\}$.*

**Remark 3.27.** *In Proposition* 3.20, *$F(x,y)$ has the univariate form $F_1(z) = \frac{1}{\left(\beta-\overline{\beta}\right)^{p^k+1}}((\beta^{p^k+1}+\gamma)\overline{z}^{p^k+1} + (\overline{\beta}^{p^k+1}+\gamma)z^{p^k+1} - (\overline{\beta}^{p^k}\beta+\gamma)\overline{z}z^{p^k} - (\overline{\beta}\beta^{p^k}+\gamma)\overline{z}^{p^k}z) + \beta L(\frac{(\overline{\beta}-1)z-(\beta-1)\overline{z}}{\overline{\beta}-\beta})$, while $F$ from Proposition* 3.26(1) *has the univariate form $F_2(z) = \beta\gamma z^{p^k+1} + \beta\overline{\gamma z}^{p^k+1} + z + \overline{z}$ by Equation* (2.5). *We can see that $F_1(z)$ is not equal to $F_2(z)$. Recall that the c-differential uniformity of a given function $F(x)$ is preserved through $F \circ L$ (note that it is not preserved through $L_1 \circ F \circ L_2$ for affine permutations $L_1$ and $L_2$) and is not invariant under EA-equivalence and CCZ-equivalence mentioned in* [12]. *Therefore, we claim that $F$ of Proposition* 3.26(1) *is not equivalent to the function $F$ of Proposition* 3.20. *So do the functions $F$ of Proposition* 3.26(2) *and of Proposition* 3.24.

**Proposition 3.28.** *Let $H$ be a function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and $F(x) = (x^{q+1}, H(x))$. Let $c = (c_1, 0) \in \mathbb{F}_q \backslash \{1\}$ and $U = \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}$. Then $F$ is $(c,\delta)$-uniform if $H(x+a) - c_1 H(x) = b_2$ has at most $\delta$ solutions on $\beta U + \frac{a}{c_1-1}$ for any $\beta \in \mathbb{F}_{q^2}$ and $b_2 \in \mathbb{F}_q$.*

*Proof.* To complete the proof, we need to prove $F(x+a)-cF(x)=b$ has at most $\delta$ solutions for any $a \in \mathbb{F}_{q^2}$ and $b=(b_1,b_2) \in \mathbb{F}_q^2$. By Equation (3.23), one has $(x+a)^{q+1}-c_1x^{q+1}=b_1$. Let $x=y+\frac{a}{c_1-1}$, then $y^{q+1}=\frac{b_1(c_1-1)-ca^{q+1}}{(c_1-1)^2}$, which always has solutions with the form $y=\beta U$, $\beta \in \mathbb{F}_{q^2}$ and $\beta^{q+1}=\frac{b_1(c_1-1)-ca^{q+1}}{(c_1-1)^2}$. This completes the proof. □

**Example 3.29.** *Let $q=2^4$ and $H(x)=\mathrm{Tr}_m^n(x^5)$ and $c=(c_1,0)$. Magma experiments show that $F$ in Proposition 3.28 is APcN if $c_1 \in \mathbb{F}_{2^2}\backslash\{1\}$ and otherwise, $F$ is $(c,6)$-uniform.*

# 4 Conclusions

In this paper, we mainly focused on the construction of bivariate functions in $\mathbb{F}_q[x,y]$ with low $c$-differential uniformities. By analyzing the relationship between bivariate functions and univariate functions, we proposed a new concept of the $c$-differential equation for bivariate functions. By virtue of some known functions, such as the Gold function, the inverse function, the trace function and linearized polynomials, we presented four classes of bivariate functions with low $c$-differential uniformity for any $c \in \mathbb{F}_q^2\backslash\{(1,0)\}$ while several classes of bivariate functions with low $c$-differential uniformity for $c \in \mathbb{F}_q\backslash\{1\}\times\{0\}$. In particular, P$c$N and AP$c$N functions could be found from our constructions. Besides, this adds to the very few known classes of P$c$N functions in even characteristic (there are only two non-trivial classes of such, besides sporadic examples).

# Acknowledgment

The authors would like to thank the editor for efficiently handling our paper and the reviewers for their careful reading, beneficial comments and constructive suggestions. This work was supported by the National Natural Science Foundation of China (No. 62072162), the Natural Science Foundation of Hubei Province of China (No. 2021CFA079), the Innovation Group Project of the Natural Science Foundation of Hubei Province of China (No. 2023AFA021), the Knowledge Innovation Program of Wuhan-Basic Research (No. 2022010801010319), the China Scholarship Council (No. 202108420195) and the Postdoctoral Fellowship Program of CPSF(No. GZB20230815). The work is also supported by the Research Council of Norway under grant number 311646.

# References


[1] N. Anbar, T. Kalayci, W. Meidl, C. Riera, P. Stănică, *$P_{\wp}N$ functions, complete mappings and quasigroup difference sets*, J. Combin. Designs **31** (2023), 667–690; Preliminary version presented at the Ernst Selmer International Workshop, August 2022.

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

[3] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020), 187–213.

[4] E. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10:6 (1967), 553–564.

[5] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology 4:1 (1991), 3–72.

[6] A. W. Bluher, *On $x^{q+1} + ax + b$,* Finite Fields Appl. 10:3 (2004), 285–305.

[7] N. Borisov, M. Chew, R. Johnson, B. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.) Fast Software Encryption, LNCS 2365, pp. 17–33. Springer, Berlin, Heidelberg, 2002.

[8] M. Calderini, L. Budaghyan, C. Carlet, *On known constructions of APN and AB functions and their relation to each other*, Matematičke Znanosti 25 (2021), 79–105.

[9] C. Carlet, *Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions*, Des. Codes Cryptogr. 59 (2011), 89–109.

[10] C. Carlet, *More constructions of APN and differentially 4-uniform functions by concatenation*, Sci. China Math. 56 (2013), 1373–1384.

[11] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.

[12] S. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89:2 (2021), 221–239.

[13] K. H. Kim, J. Choe, S. Mesnager, *Solving* $X^{q+1} + X + a = 0$ *over finite fields*, Finite Fields Appl. 70 (2021), 101797.

[14] P. A. Leonard, K. S. Williams, *Quartics over* GF($2^n$). Proc. Amer. Math. Soc. 36:2 (1972), 347–350.

[15] C. Li, C. Riera, P. Stănică, *Dillon's switching method generalized to c-differentials*, Boolean Functions & Applic. (BFA), 2022, Paper #1.

[16] K. Li, Y. Zhou, C. Li and L. Qu, *Two new families of quadratic APN functions*, IEEE Trans. Inf. Theory 68:7 (2022), 4761–4769.

[17] S. Mesnager, C. Riera, Stănică, H. Yan, Z. Zhou, *Investigations on c-(almost) perfect nonlinear functions*, IEEE Trans. Inf. Theory 67:10 (2021), 6916–6925.

[18] K. Nyberg, *Differentially uniform mappings for cryptography*, In: Helleseth T. (ed.) EUROCRYPT 1993, LNCS 765, pp. 55–64. Springer, Heidelberg, 1994.

[19] M. Pal, P. Stănică, *A connection between the boomerang uniformity and the extended differential in odd characteristic and applications*, arxiv:2312.01434, 2023.

[20] P. Stănică, *C-differential uniformity for functions constructed via the Maiorana-McFarland bent function*, Workshop on Coding & Cryptography, WCC 2022, Paper #37.

[21] P. Stănică, *Low c-differential and c-boomerang uniformity of the swapped inverse function*, Discrete Math. 344:10 (2021), 112543.

[22] P. Stănică, A. Geary, *The c-differential behavior of the inverse function under the EA-equivalence*, Cryptogr. Commun. 13:2 (2021), 295–306.

[23] P. Stănică, C. Riera, A. Tkachenko, Characters, *Weil sums and c-differential uniformity with an application to the perturbed Gold function*, Cryptogr. Commun. 13 (2021), 891–907.

[24] H. Taniguchi, *On some quadratic APN functions*, Des. Codes Cryptogr. 87 (2019), 1973–1983.

[25] Z. Tu, X. Zeng, Y. Jiang, X. Tang, *A class of APcN power functions over finite fields of even characteristic*, arXiv:2107.06464v1.

[26] X. Wang, D. Zheng, L. Hu, *Several classes of PcN power functions over finite fields*, Discrete Appl. Math. 322 (2022), 171–182.

[27] Z. Zha, L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Des. Codes Cryptogr. 89 (2021), 1193–1210.

[28] Y. Zhou, A. Pott, *A new family of semifields with* 2 *parameters*, Adv. Math. 234 (2013), 43–60.