C-differential uniformity for functions constructed via the Maiorana-McFarland bent function

Pantelimon Stănică

Applied Mathematics Department,
Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

Abstract. In this paper we use a method of Carlet [7], which constructs APN functions using the Maiorana-McFarland bent function, and investigate, in any prime characteristic p, some of these concatenations through the prism of the newly defined concept of c-differential uniformity. Among other results, we show that for example, $F(x,y)=(xy,L(xy))$ is APcN on $\mathbb{F}_{p^{2m}}$ for all $c=(1,c_2)\in\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}$, where L is a linearized polynomial on $\mathbb{F}_{p^m}$; also, for m,n integers with $n=2m\geq 2$, the c-differential uniformity of the function $F(x,y)=\left(xy, Ax^{p^k+1}+By^{p^k+1}\right)$ on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ is $p^{\gcd(k,m)}+1$, for all $c=(1,c_2), 1\neq c_2\in\mathbb{F}_{p^m}$, , $AB\neq 0$, $A,B\in\mathbb{F}_{2^m}$.

Keywords: Boolean and p-ary functions, c-differentials, differential uniformity, perfect and almost perfect c-nonlinearity
MSC 2020: 06E30, 11T06, 94A60, 94D10.

1 Introduction and basic definitions

In [12] we defined a new differential and Difference Distribution Table, in any finite field, and the corresponding perfect/almost perfect c-nonlinear functions and other notions (independently, in [3] the concept of quasi planarity was developed: a quasi planar function is a perfect c-nonlinear function for $c=-1$ – see below). This was prompted by a challenge from [5], who extended the differential attack on some ciphers by using a different type of differential. Right after the introduction of this concept, we extended the notion of Boomerang Connectivity Table in [18] and characterized some of the known perfect nonlinear functions and the inverse function through this new concept. In [1,2,12,17,20,21,13,25,24] various characterizations of the c-differential uniformity were found, and some of the known perfect and almost perfect nonlinear functions have been investigated. An approach on boomerang uniformity based upon Weil sums and characters was developed in [19].

Let p be a prime number and n be a positive integer n. We let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ be the multiplicative group; for $a \neq 0$, we often write $\frac{1}{a}$ to mean the inverse of a in the multiplicative group. We let $\mathbb{F}_p^n$ be the n-dimensional vector space over $\mathbb{F}_p$. We use $\#S, \bar{S}$ to denote the cardinality of a set S, respectively, the complement of S in a superset (usually, $\mathbb{F}_{p^n}$), which will be clear from the context.

We call a function from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ a *p-ary function* on n variables. For positive integers n and m, any map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \to \mathbb{F}_p^m$) is called a *vectorial p-ary function*, or *(n, m)-function*. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i,\ a_i \in \mathbb{F}_{p^n}$, whose *algebraic degree* is then the largest p-ary weight of the exponents i with $a_i \neq 0$. We let $\mathrm{Tr}_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the absolute trace function, given by $\mathrm{Tr}_n(x) = \displaystyle\sum_{i=0}^{n-1} x^{p^i}$. Also, $\mathrm{Tr}_d(x) = \sum_{i=0}^{\frac{n}{d}-1} x^{p^{di}}$ is the relative trace from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^d}$, where $d \,|\, n$.

For a Boolean or p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, we define the *Walsh-Hadamard transform* to be the complex-valued function ($\zeta_p = e^{\frac{2\pi i}{p}}$ is a complex p-root of 1; if $p = 2$, $\zeta_p = -1$)

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) + \mathrm{Tr}(ux)}.$$

For an (n, n)-function F and for $a, b \in \mathbb{F}_{2^n}$, we let the Walsh transform $\mathcal{W}_F(a, b)$ of F to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^n(bF(x))$ at a, that is,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(bF(x) + ax)}.$$

A *bent function* (p-ary or vectorial (n, k); it is known that $k \leq n/2$) is a function which has all of its absolute Walsh-Hadamard coefficients equal to $p^{n/2}$. As an example of bent function, we give the Maiorana-McFarland function $F(x, y) = xy$ on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$.

As we did in [12], for a p-ary (n, m)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and $c \in \mathbb{F}_{p^m}$, the (*multiplicative*) *c-derivative* of F with respect to $a \in \mathbb{F}_{p^n}$ is the function

$${}_cD_a F(x) = F(x + a) - cF(x), \text{ for all } x \in \mathbb{F}_{p^n}.$$

For an (n, n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let the entries of the c-Difference Distribution Table (c-DDT) be defined by ${}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$. The *$c$-differential uniformity* of F is

$${}_c\Delta_F = \max\left\{{}_c\Delta_F(a, b) \,:\, a, b \in \mathbb{F}_{p^n}, \text{ and } a \neq 0 \text{ if } c = 1\right\}.$$

1. If ${}_c\Delta_F = \delta$, then we say that F is differentially (c, δ)-uniform (or that F has c-uniformity δ).
2. If $\delta = 1$, then F is called a *perfect c-nonlinear* (*PcN*) function (for $c = 1$, they only exist for odd characteristic p; however, there exist PcN functions for $p = 2$, for all $c \neq 1$, as shown in [12]).

3. If $\delta = 2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function.

It is easy to see that if F is an (n,n)-function, that is, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, then F is PcN if and only if ${}_cD_aF$ is a permutation polynomial. For $c = 1$, we obtain the classical derivative, PN, APN, etc., differential uniformity and DDT.

The reader can consult [6,9,11,15,23] for more on cryptographic Boolean functions and their properties.

2 Carlet, Zhou-Pott and Taniguchi classes of APN functions

In [7], Carlet showed that for $A, B, C, D \in \mathbb{F}_{p^m}$, $AB \neq 0$, and for any integers i, j with $\gcd(m, i - j) = 1$, the function $F_1 : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, built up via the Maiorana-McFarland bent function xy, namely,

$$\begin{aligned} &F_1(x,y) = (xy, G_1(x,y)), \text{ where} \\ &G_1(x,y) = Ax^{p^i+p^j} + Cx^{p^i}y^{p^j} + Dx^{p^j}y^{p^i} + By^{p^i+1} \end{aligned} \tag{1}$$

is APN if and only if $G_1(x,1) = Ax^{p^i+p^j} + Cx^{p^i} + Dx^{p^j} + B$ has no root in $\mathbb{F}_{p^m}$.

Zhou and Pott [26] found yet another class for m even,

$$\begin{aligned} &F_2(x,y) = (xy, G_2(x,y)), \text{ where} \\ &G_2(x,y) = x^{p^k+1} + \alpha y^{(p^k+1)p^j}, \end{aligned} \tag{2}$$

with $\gcd(m,k) = 1$, and j a positive integer. The APN-ess of F_2 is completely characterized via the condition $\alpha \notin \{a^{p^k+1}(t^{p^k} + t)^{1-p^j} \,:\, a, t \in \mathbb{F}_{p^m}\}$ (if j is even and α is not a cube is a sufficient condition for this to happen).

Carlet [8] extended these results and gave a general criterion for the APN-ess of functions of the form $F(x,y) = (xy, G(x,y))$, where $G(x,y) = P(x^{p^i+1}) + Q(x^{p^i}Y) + R(xy^{p^i}) + S(y^{p^i+1})$, for some linear functions P, Q, R, S, and $\gcd(m,i) = 1$. Precisely, he showed that F is APN if and only if for all $(a,b) \neq (0,0)$, letting $T_{a,b}(y) = P(a^{p^i+1}y) + Q(a^{p^i}by) + R(ab^{p^i}y) + S(b^{p^i+1}y)$, then:

- if m is odd, then $T_{a,b}$ is a permutation;
- if m is even, then the kernel $\ker(T_{a,b}) \cap \{u^{p^i+1}(t^{p^i} + t) \,:\, u, t \in \mathbb{F}_{p^m}\} = \{0\}$.

Recently, Taniguchi [22] proposed yet another class,

$$\begin{aligned} &F_3(x,y) = (xy, G_3(x,y)), \text{ where} \\ &G_3(x,y) = x^{p^{3i}+p^{2i}} + \alpha x^{p^{2i}}y^{p^i} + \beta y^{p^i+1}, \end{aligned} \tag{3}$$

where, $\gcd(m,i) = 1$, $\alpha \in \mathbb{F}_{p^m}, \beta \in \mathbb{F}_{p^m}^*$. In this case, F is APN if and only if $G_3(x,1) = x^{p^i+1} + \alpha x + \beta$ has no root in $\mathbb{F}_{p^m}$. If $\alpha = 0$, this function belongs to the Zhou-Pott [26] class. In general, Taniguchi functions are CCZ-inequivalent to F_1, F_2. Taking $P(x) = x^{p^i}, Q(x) = \alpha x^{p^i}, R(x) = 0, S(x) = \beta x$, we see that Taniguchi functions are part of Carlet's class [8].

It is the intent of this paper to investigate some of these classes and derive conditions on G such that $F(x, y) = (xy, G(x, y))$ has the newly defined concept of c-differential uniformity equal to δ (in particular, we will construct PcN/APcN functions via the Maiorana-McFarland bent function).

3 The results

Let p be a prime number. We first derive general conditions such that $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $F(x, y) = (xy, G(x, y))$ has its c-differential uniformity ${}_c\Delta_f \le \delta$. We adopt the usual convention that $0^{-1} = 0$.

Theorem 1 *Let δ be a positive integer, $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ be an (n, n)-function, $n = 2m$, defined by $F(x, y) = (xy, G(x, y))$, where $G : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ is an arbitrary (n, n)-function. Then, the $c = (1, c_2)$-differential uniformity of F satisfies ${}_c\Delta_F \le \delta$, if and only if:*

(1) *For all y fixed, $G_y(x) = G(x, y)$ has the c_2-differential uniformity ${}_{c_2}\Delta_{G_y} \le \delta$;*
(2) *For all x fixed, $G_x(y) = G(x, y)$ has the c_2-differential uniformity ${}_{c_2}\Delta_{G_x} \le \delta$;*
(3) *For all $(a, b), (e, d) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, with $ab \ne 0$, the equation $G_{a,b,d}(x + 1) - c_2 G_{a,b,d}(x) = e$ has at most δ solutions, that is, ${}_{c_2}\Delta_{G_{a,b,d}} \le \delta$, where $G_{a,b,d}(x) = G(ax, -bx + d)$.*

If $c_1 \ne 1$, then ${}_c\Delta_F \le \delta$, if and only if $\delta_1 + \delta_2 \le \delta$, where δ_1, δ_2 is the maximum number of solutions for (with $\alpha = \frac{1}{c_1 - 1}$)

$$G\left(a(1 + \alpha), y + b\right) - c_2 G\left(a\alpha, y\right) = e,$$

respectively,

$$G\left(x + a, b(1 + \alpha) + \frac{d\alpha^2 + ab(1 + \alpha)\alpha}{x - a\alpha}\right) - c_2 G\left(x, b\alpha + \frac{d\alpha^2 + ab(1 + \alpha)\alpha}{x - a\alpha}\right) = e,$$

where $a, b, d, e \in \mathbb{F}_{p^m}$.

Proof. Next, we consider the differential equation of F at $(a, b), (d, e) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, for $(1, 1) \ne c = (c_1, c_2), c_1, c_2 \in \mathbb{F}_{p^m}$:

$$F(x + a, y + b) - cF(x, y) = (d, e),$$

that is,

$$\begin{cases} (1 - c_1)xy + bx + ay = d - ab \\ G(x + a, y + b) - c_2 G(x, y) = e. \end{cases} \tag{4}$$

Case 1. Let $c_1 = 1$ (hence $c_2 \ne 1$). We note that the system has at most δ solutions if and only if:

(1) For all y fixed, $G_y(x) = G(x, y)$ has the c_2-differential uniformity ${}_{c_2}\Delta_{G_y} \le \delta$ (this corresponds to $b = 0$);

(2) For all x fixed, $G_x(y) = G(x, y)$ has the c_2-differential uniformity ${}_{c_2}\Delta_{G_x} \le \delta$ (this corresponds to $a = 0$);

$(\tilde{3})$ For all $(a, b), (e, d) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with $ab \neq 0$ (note that $y = \frac{d-ab}{a} - \frac{b}{a}x$), then $G(x+a, -\frac{b}{a}x + \frac{d-ab}{a} + b) + c_2 G(x, -\frac{b}{a}x + \frac{d-ab}{a}) = e$ has at most δ solutions.

As Carlet did in [7] for $c = 1$, replacing x by ax, $\frac{d-ab}{a}$ by d, and labeling $G_{a,b,d}(x) = G(ax, -bx + d)$, Condition $(\tilde{3})$ is thus equivalent to:

(3) For all $(a, b), (e, d) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, with $ab \neq 0$, the equation $G_{a,b,d}(x+1) - c_2 G_{a,b,d}(x) = e$ has at most δ solutions, that is, ${}_{c_2}\Delta_{G_{a,b,d}} \le \delta$.

Further, if G is quadratic, then one can merge the expressions in d into the constant e and consequently, one can assume that $d = 0$, in that case.

Case 2. Let $c_1 \neq 1$. If $x = \frac{a}{c_1 - 1}$ in (4), then the first equation is independent of y, $d = \frac{abc_1}{c_1-1}$, and so, the solutions $(x, y) = \left(\frac{a}{c_1-1}, y\right)$ of (4) satisfy

$$G\left(\frac{ac_1}{c_1 - 1}, y + b\right) - c_2 G\left(\frac{a}{c_1 - 1}, y\right) = e.$$

Let δ_1 be the number of solutions for the above equation.

We now assume that $x \neq \frac{a}{c_1-1}$, and so, the first equation of (4) renders $y = \frac{b}{c_1-1} + \frac{d+abc_1}{(1-c_1)((1-c_1)x+a)}$ (observe that x and y are in one-to-one correspondence). Thus, the solutions x for the second equation of (4) satisfy

$$G\left(x + a, \frac{bc_1}{c_1 - 1} + \frac{d + abc_1}{(1 - c_1)((1 - c_1)x + a)}\right) \\ - c_2 G\left(x, \frac{b}{c_1 - 1} + \frac{d + abc_1}{(1 - c_1)((1 - c_1)x + a)}\right) = e.$$

Let δ_2 be the number of solutions x for the above equation.

Consequently, we must have $\delta_1 + \delta_2 \le \delta$, and the theorem is shown.

We now proceed to give some concrete examples based upon our previous result.

Theorem 2 *Let $m \ge 2$, $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ be the quadratic function defined by $F(x, y) = (xy, L(xy))$, where $L \in \mathbb{F}_{p^m}[x]$ is a linearized permutation polynomial on $\mathbb{F}_{p^m}$. Then ${}_c\Delta_F = 2$ (F is APcN), for all $c = (1, c_2)$, $c_2 \in \mathbb{F}_{p^m}$.*

Proof. We first let $c = (1, c_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $c_2 \neq 1$. By Theorem 1, we need to show that both $y \to L(xy)$ and $x \to L(xy)$ are PcN. Since the arguments are similar, we will show the first claim, only. For arbitrary a, e, c_2 and fixed y in $\mathbb{F}_{p^m}$, the corresponding c-differential equation for $y \to L(xy)$ is then

$$L((x + a)y) - c_2 L(xy) = e,$$

which is equivalent to $L(xy) = \frac{e-L(ay)}{1-c_2}$, which has only one solution x since L is a permutation polynomial.

We now look at the third condition of Theorem 1 for $ab \neq 0$. We need to show that for fixed $1 \neq c_2$, and arbitrary $ab \neq 0$, e, d, all in $\mathbb{F}_{p^m}$, we have only one solution x for the equation

$$L\left((ax+a)(-bx-b+d) - c_2 L(ax(-bx+d)\right) = e.$$

This is equivalent to

$$(1-c_2)L(ax(-bx+d)) + L(-2abx) = e - L(a(b-d)),$$

and further,

$$L(ab(c_2-1)x^2 + a((1-c_2)d-2b)x) = e - L(a(b-d)).$$

Since L is a permutation polynomial, writing $\ell_0 = L^{-1}\left(e - L(a(b-d))\right)$, the above equation is then $ab(c_2-1)x^2 + a((1-c_2)d-2b)x - \ell_0 = 0$, which has at most two solutions. The bound is easily attained, which can be seen by taking $e = 0, b = d$ and so, $\ell_0 = 0$, with our equation becoming $x((c_2-1)x-(c_2+1)) = 0$ of solutions $x = 0, \frac{c_2+1}{c_2-1}$. The solutions are distinct unless $p > 2$ and $c_2 = -1$. In that case, is is easy to choose ℓ_0 such that the discriminant of the quadratic equation is a square, and consequently the equation has two roots. The proof is done.

Surely, there are other forms for G one can consider, obtaining low c-differential uniformity via this method, and we challenge the readers to do so. In that spirit, we would like to investigate the c-differential uniformity of this construction if G is defined via the usual PN/APN candidates (Gold, inverse, etc.).

Theorem 3 *Let p be a prime number, m, n integers with $n = 2m \geq 2$, and $F(x,y) = \left(xy, Ax^{p^k+1} + By^{p^k+1}\right)$ on $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $AB \neq 0$, $A, B \in \mathbb{F}_{p^m}$. Then, if $c = (1, c_2), 1 \neq c_2 \in \mathbb{F}_{p^m}$, the c-differential uniformity of F is $p^{\gcd(k,m)} + 1$.*

Proof. From Theorem 1, we need to show that both $y \to G(x,y) = x^{p^k+1} + y^{p^k+1}$, as well as $x \to G(x,y)$ have their c-differential uniformities upper bounded by $p^{\gcd(k,m)} + 1$. We will only argue the first claim, as the second is similar. Thus, for $a, e \in \mathbb{F}_{2^m}$, we need to consider the equation

$$A(x+a)^{p^k+1} + By^{p^k+1} - c_2 Ax^{p^k+1} - c_2 By^{p^k+1} = e,$$

that is,

$$A(x+a)^{p^k+1} - c_2 Ax^{p^k+1} = e - (1-c_2)By^{p^k+1},$$

which is a $\frac{c_2}{A}$-differential uniformity equation for the Gold function $x \to x^{p^k+1}$. From [17], if $p = 2$, the Gold function has differential uniformity $\frac{2^{\gcd(2k,m)}-1}{2^{\gcd(k,m)}-1}$, for $\frac{c_2}{A} \in \mathbb{F}_{2^{\gcd(k,m)}}$ and $2^{\gcd(k,m)} + 1$, if $\frac{c_2}{A} \notin \mathbb{F}_{2^{\gcd(k,m)}}$. If $p > 2$, and $\frac{c_2}{A} \in \mathbb{F}_{p^{\gcd(k,m)}}$, the c_2-differential uniformity is $\gcd(p^k+1, p^m-1)$. If $p > 2$, and $\frac{c_2}{A} \notin \mathbb{F}_{p^{\gcd(k,m)}}$, the c_2-differential uniformity of F is $p^{\gcd(k,m)} + 1$ (see [12,17,24]).

Now, we need to investigate the equation

$$G(ax+a,-bx-b+d)-c_2G(ax,-bx+d)=e,$$

which is equivalent to

$$A(ax+a)^{p^k+1}+B(-bx-b+d)^{p^k+1}-c_2Aa^{p^k+1}x^{p^k+1}-c_2B(-bx+d)^{p^k+1}=e.$$

By expanding and combining terms, we can write

$$\begin{aligned}(1-c_2)(Aa^{p^k+1}+Bb^{p^k+1})x^{p^k+1}+(Aa^{p^k+1}+Bb^{p^k+1}+(c_2-1)Bb^{p^k}d)x^{p^k}\\+(Aa^{p^k+1}+Bb^{p^k+1}+(c_2-1)Bb\,d^{p^k})x-e_0=0,\end{aligned}$$

where $e_0=e-Aa^{p^k+1}-Bb^{p^k+1}+Bdb^{p^k}+Bbd^{p^k}+B(c_2-1)d^{p^k+1}$. By a result of Bluher [4] (see, also [16]), the above equation has $0,1,2$, or $p^{\gcd(k,m)}+1$ roots (for us, the upper bound is attainable for some a,b,e, since our free term is linear in e). By [12, Lemma 9], $\gcd(p^k+1,p^m-1)=\frac{2^{\gcd(2k,m)}-1}{2^{\gcd(k,m)}-1}$, if $p=2$, if $p>2$, $\gcd(p^k+1,p^m-1)=2$, when $\frac{m}{\gcd(m,k)}$ is odd, respectively, $p^{\gcd(k,m)}+1$, when $\frac{m}{\gcd(m,k)}$ is even. Thus, $p^{\gcd(k,m)}+1$ is an upper bound, and the claim is shown.

If we use $G(x,y)=x^{p^n-2}+y^{p^n-2}$ in the construction of $F(x,y)=(xy,G(x,y))$, then Conditions (1) and (2) of Theorem 1 will work out nicely for G_y,G_x, since ${}_{c_2}\Delta_{G_x}={}_{c_2}\Delta_{G_y}={}_{c_2}\Delta_{inverse}\in\{2,3\}$ (see [12]). However, Condition (3), for $ab\neq 0$, $a=b$, $d=0$, will happen for all x, and consequently, the $c=(1,c_2)$-differential uniformity for F becomes 2^m, which is the worst, for this construction.

We now let $G(x,y)=Ax^{p^k}y+Bxy^{p^k}+Cx+Dy$ and show the following result.

Theorem 4 *Let $F(x,y)=(xy,Ax^{p^k}y+Bxy^{p^k}+Cx+Dy)$, $A,B,C,D\in\mathbb{F}_{p^m}$, with $ABCD\neq 0$ and $\frac{-B}{A}\notin\{u^{p^{\gcd(k,m)}-1}:u\in\mathbb{F}_{p^m}\}$. Then the c-differential uniformity of F is $p^{\gcd(k,m)}+1$. In particular, if $p=2$ and $\gcd(k,m)=1$, we get the low c-differential uniformity of 3.*

Proof. We first check Condition (1) (similarly, for Condition (2)) of Theorem 1, and look at the equation in x (y is fixed), $G_y(x+a)-c_2G_y(x)=e$, namely,

$$\begin{aligned}Ax^{p^k}y+Aa^{p^k}y+Bxy^{p^k}+Bay^{p^k}+Cx+Ca+Dy\\-c_2Ayx^{p^k}-c_2By^{p^k}x-c_2Cx-c_2Dy=e,\end{aligned}$$

that is,

$$A(1-c_2)yx^{p^k}+(1-c_2)(C+by^{p^k})x-e_0=0,$$

where $e_0=e+aC+yD+aBy^{p^k}+Aa^{p^k}-Dc_2y$. A linearized trinomial $x^{p^k}+\alpha x+\beta$ has either $0,1,2$, or $p^{\gcd(k,m)}$ roots (see [10]), and so, the above displayed equation has at most $p^{\gcd(k,m)}$ roots.

We next look at Condition (3) of Theorem 1, namely, the equation

$$\begin{aligned}&A(a^{p^k}x^{p^k}+a^{p^k})(-bx-b+d)+B(ax+a)(-b^{p^k}x^{p^k}+(-b+d)^{p^k})\\&+(aC-bD)x+aC-bD+dD-c_2Aa^{p^k}x^{p^k}(-bx+d)\\&-c_2B(ax)(-b^{p^k}x^{p^k}+d^{p^k})-c_2Cax-c_2D(-bx+d)=e,\end{aligned}$$

which is equivalent to

$$\begin{aligned}&(c_2-1)(Aba^{p^k}+Bab^{p^k})x^{p^k+1}-(Aba^{p^k}+Bab^{p^k}-(1-c_2)Ada^{p^k})x^{p^k}\\&-(Aba^{p^k}+Bab^{p^k}+(1-c_2)Bad^{p^k}-(1-c_2)aC+(1-c_2)bD)x-e_0=0,\end{aligned}$$

with $e_0=e-Aa^{p^k}(-b+d)-Ba(-b+d)^{p^k}-Ca+Db-dD+dc_2D$. The coefficient $Aba^{p^k}+Bab^{p^k}$ of x^{p^k+1} is never zero, since if it were then $\left(\frac{a}{b}\right)^{p^k-1}=\frac{-B}{A}$, and so, $\frac{-B}{A}$ would be a $p^{\gcd(k,m)}-1$ power, but our imposed condition prohibits that. Consequently, via [4,16], the upper bound $p^{\gcd(k,m)}+1$ for the number of roots of the above equation holds. The result is shown.

4 Concluding remarks

In this paper, we investigate the c-differential uniformity of some functions constructed concatenating the outputs of some (n,m)-bent functions $(n=2m)$. As a by-product, we obtain an infinite class of PcN/APcN quadratic functions. On the other hand, we argue that using this construction, based upon the Maiorana-McFarland bent function, as well as a direct sum of Gold functions or inverse functions, the c-differential uniformity (for $c\neq 1$), in general increases, though there are some cases when its value is low.

References

1. D. Bartoli, M. Calderini, *On construction and (non)existence of c-(almost) perfect nonlinear functions*, Finite Fields Appl. 72 (2021), https://doi.org/10.1016/j.ffa.2021.101835.
2. D. Bartoli, M. Calderini, C. Riera, P. Stănică, *Low c-differential uniformity for functions modified on subfields*, Boolean Functions and Applications, BFA'21, Norway, 2021, Paper #23, https://boolean.w.uib.no/files/2021/09/BFA2021_BCRS-final.pdf.
3. D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020), 187–213.
4. A. W. Bluher, *On* $x^{q+1}+ax+b$, Finite Fields Appl. 10 (3) (2004), 285–305.
5. N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.), Fast Software Encryption, FSE 2002, LNCS 2365, pp. 17–33, Springer, Berlin, Heidelberg, 2002.
6. L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

7. C. Carlet, *Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions*, Des. Codes Cryptogr. 59 (2011), 89–109.
8. C. Carlet, *More constructions of APN and differentially* 4*-uniform functions by concatenation*, Sci. China Math. 56 (2013), 1373–1384.
9. C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge: Cambridge University Press, Cambridge, 2021.
10. R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.
11. T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.
12. 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.
13. S.U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Des. Codes Cryptogr. 89 (2021), 221–239.
14. R. Lidl, H. Niederreiter, FiniteFields (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge, 1997.
15. S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.
16. K. H. Kim, J. Choe, S. Mesnager, *Solving* $x^{q+1}+x+a=0$ *over finite fields*, Finite Fields Appl. 70:6 (2021), 101797.
17. S. Mesnager, C. Riera, P. Stanica, H. Yan, Z. Zhou, *Investigations on c-(almost) perfect nonlinear functions*, IEEE Trans. Inform. Theory 67:10 (2021), 6916–6925.
18. P. Stănică, *Investigations on c-boomerang uniformity and perfect nonlinearity*, Discrete Applied Mathematics 304 (2021), 297–314.
19. P. Stănică, *Using double Weil sums in finding the Boomerang and the c-Boomerang Connectivity Table for monomial functions on finite fields*, Applicable Algebra in Engineering, Communication and Computing, 2021.
20. P. Stănică, *Low c-differential uniformity for the Gold function modified on a subfield*, Proc. International Conf. on Security and Privacy, Springer (ICSP 2020), LNEE 744, Springer 2021, pp. 131–137.
21. P. Stănică, A. Geary, *The c-differential behavior of the inverse function under the EA-equivalence*, Cryptogr. Commun. 13 (2021), 295–306.
22. H. Taniguchi, On some quadratic APN functions, Des. Codes Cryptogr. 87 (2019), 1973–1983.
23. N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.
24. X. Wang, D. Zheng, *Several classes of PcN power functions over finite fields*, `https://arxiv.org/pdf/2104.12942.pdf`.
25. Y. Wu, N. Li, X. Zeng, *New PcN and APcN functions over finite fields*, `https://arxiv.org/pdf/2010.05396.pdf`.
26. Y. Zhou, A. Pott, *A new family of semifields with* 2 *parameters*, Adv. Math. 234 (2013), 43–60.