Low c-differential uniformity for functions modified on subfields

Daniele Bartoli[1], Marco Calderini[2,3], Constanza Riera[4] and Pantelimon Stănică[5*]

[1]Department of Mathematics and Informatics, University of Perugia, Via Vanvitelli, 1, Perugia, 06123, Italy.
[2]Department of Informatics, University of Bergen, Postboks 7803, Bergen, N-5020, Norway.
[3]Department of Mathematics, University of Trento, Via Sommarive, 14, Trento, 38122, Italy.
[4]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, 5020, Norway.
[5]Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA.

*Corresponding author(s). E-mail(s): pstanica@nps.edu;
Contributing authors: daniele.bartoli@unipg.it; marco.calderini@unitn.it; csr@hvl.no;

Abstract

In this paper, we construct some piecewise defined functions, and study their c-differential uniformity. As a by-product, we improve upon several prior results. Further, we look at concatenations of functions with low differential uniformity and show several results. For example, we prove that given β_i (a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$), some functions f_i of c-differential uniformities δ_i, and L_i (specific linearized polynomials defined in terms of β_i), $1 \leq i \leq n$, then $F(x) = \sum_{i=1}^{n} \beta_i f_i(L_i(x))$ has c-differential uniformity equal to $\prod_{i=1}^{n} \delta_i$.

Keywords: Boolean and p-ary functions, c-differentials, differential uniformity, perfect and almost perfect c-nonlinearity

MSC Classification: 06E30 , 11T06 , 94A60 , 94D10

1 Introduction and basic definitions

Let p be a prime number and n be a positive integer. We let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, and $\mathbb{F}_{p^n}^\star = \mathbb{F}_{p^n} \setminus \{0\}$ be its multiplicative group.

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 an (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 weight in the p-ary expansion of i (that is, the sum of the digits of the exponents i) with $a_i \neq 0$.

Motivated by [3], who extended the differential attack on some ciphers by using a new type of differential, in [9], the authors introduced a new differential and Difference Distribution Table, in any characteristic, along with the corresponding perfect/almost perfect c-nonlinear functions and other notions (this was also developed independently in [2] where the authors introduce the concept of quasi planarity). In [1, 9, 10, 13], various characterizations of the c-differential uniformity were found, and some of the known perfect and almost perfect nonlinear functions have been investigated.

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

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

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 ${}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$. We call the quantity

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

the *c-differential uniformity* of F. If $\delta_{F,c} = \delta$, then we say that F is differentially (c, δ)-uniform (or that F has c-uniformity δ). If $\delta = 1$, then F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as proven in [9], there exist PcN functions for $p = 2$, for all $c \neq 1$). 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 recover the classical derivative, PN, APN, differential uniformity and DDT.

In the last years, several constructions of low differentially uniform permutations have been introduced by modifying some functions on a subfield (see for instance [5, 12, 17, 18]).

There are many works constructing cryptographic Boolean functions (bent, plateaued, APN, etc.) starting with good such objects on smaller environments. In this work we will do the same, concentrating on subfields, and extend some of the results given in [5] to the case of the c-differential uniformity. From this

generalization, we are also able to improve the upper bound obtained in [16] for the case of a Gold APN function in even characteristics. Moreover, these results can be used also for providing an upper bound on the c-differential uniformity of several differentially 4-uniform functions constructed by modifying the inverse functions on a subfield, such as those in [12, 17, 18].

2 An upper bound on the differential uniformity of a piecewise defined function

Here, we shall give a general result concerning an upper bound for the c-differential uniformity of a piecewise defined function, thus generalizing a result of [5].

Before considering the case of the c-differential uniformity, we will give a property for some functions having $\delta_{F,1} = 4$ when $p = 2$. Indeed, recently in [7], Carlet noticed that for an APN function $F \in \mathbb{F}_{2^s}[x]$ defined on an extension $\mathbb{F}_{2^{ms}}$, with m odd, we have that the equation $F(x+a)+F(x) = b$ does not admit solutions $x \notin \mathbb{F}_{2^s}$, whenever $a \in \mathbb{F}_{2^s}^\star$ and $b \in \mathbb{F}_{2^s}$. This result can be extended to the case of differentially $2k$-uniform functions, under some conditions on the extension.

Proposition 2.1 *Let $n = sm$, where s and m are integers, and let $F \in \mathbb{F}_{2^s}[x]$ be a differentially $(1, 2k)$-uniform function over $\mathbb{F}_{2^n}$, with $k \geq 2$. If m is not divisible by any integer $2 \leq t \leq k$, then $F(x+a)+F(x) = b$ does not admit solutions $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$, whenever $a, b \in \mathbb{F}_{2^s}, a \neq 0$.*

Remark 2.2 *We restrict to $k \geq 2$ for ease of notation with the constrain $2 \leq t \leq k$, but the result is true for $k = 1$ if m is odd, as proven in [7]. For m odd, this gives an extension of the result of [7], not only for APN functions, but also for 4-differential uniform functions.*

Proof Let us consider $a, b \in \mathbb{F}_{2^s}, a \neq 0$. Without loss of generality, we can suppose that the equation $F(x) + F(x+a) = b$ admits $2k$ solutions, that can be denoted by $x_1, \ldots, x_k, x_1 + a, \ldots, x_k + a$. Suppose $x_1 \notin \mathbb{F}_{2^s}$ and consider the set $O_{x_1} = \{x_1^{2^{is}} : 0 \leq i \leq m-1\} = \{x_1^{2^{is}} : 0 \leq i \leq 2k-1\}$. This last equality holds since the polynomial $F(x)+F(x+a)+b$ has all coefficients in $\mathbb{F}_{2^s}$. If x is a solution, then also x^{2^s} is a solution.

Now, if $|O_{x_1}| \leq k$, then there exists $0 < i \leq k$ such that $x_1^{2^{is}} = x_1$, implying $x_1 \in \mathbb{F}_{2^s}$, which gives us a contradiction.

If $|O_{x_1}| > k$, consider $J = \{j : x_j, x_j + a \in O_{x_1}\}$. We have $J \neq \emptyset$, and there must exists $j \in J$ for which there exist $0 < i \leq k$ such that $x_j^{2^{is}} = x_j + a$. Indeed, consider the sequence

$$x_1, x_1^{2^s}, \ldots$$

and suppose that for all the pairs $x_j, x_j + a$ in this sequence we cannot have $x_j^{2^{is}} = x_j + a$, for $i \leq k$. Then, up to relabeling the solutions, we would have that the first

k elements of the sequence are

$$x_1, x_2(= x_1^{2^s}), \ldots, x_k.$$

Now, for the next element we need to have one among $x_1+a, \ldots, x_k+a$. So, we would obtain a pair x_j, x_j+a for which there exists $i \leq k$ such that $x_j^{2^{is}} = x_j+a$. Therefore, $x_j^{2^{2is}} = x_j$ for some $i \leq k$ and so $x_j \in \mathbb{F}_{2^s}$, implying $x_1 \in \mathbb{F}_{2^s}$, contradiction. □

From Proposition 2.1, we can simplify Theorem 4.1 from [5] for some dimensions.

Theorem 2.3 *Let $n = sm$, where s and m are integers. Let f and g be two polynomials with coefficients in $\mathbb{F}_{2^s}$, that is, $f, g \in \mathbb{F}_{2^s}[x]$, and g permuting $\mathbb{F}_{2^n}$. Suppose that f is a $\delta_{f,1}$-uniform function over $\mathbb{F}_{2^s}$ and g is a $\delta_{g,1}$-uniform function over $\mathbb{F}_{2^n}$, and m is not divisible by any integer $2 \leq t \leq k$, where $k = \frac{\delta_{g,1}}{2}$. Then, the function*

$$F(x) = f(x) + (f(x) + g(x))(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{2^s}, \\ g(x), & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is such that, for any $b \in \mathbb{F}_{2^n}$,

$${}_1\Delta_F(a,b) \leq \begin{cases} \max\{\delta_{f,1}, \delta_{g,1}\}, & \text{if } a \in \mathbb{F}_{2^s}, \\ \delta_{g,1} + 2, & \text{if } a \notin \mathbb{F}_{2^s}. \end{cases}$$

From Theorem 2.3, we have that all the results given in [5] for the differentially 4-uniform Gold and Bracken-Leander functions can be extended to other functions, such as the differentially 4-uniform Kasami function [4, 6, 8, 11]. Indeed, the assumption on the solutions of the derivatives of the modified function is needed for applying Theorem 4.1 in [5]. In particular, we have the following result.

Theorem 2.4 *Let $n = sm$, with s even such that $s/2$ and m are odd. Let k be such that $\gcd(k, n) = 2$ and $f(x) = A_1 \circ Inv \circ A_2(x)$, with $Inv(x) = x^{-1}$ (where $0 \mapsto 0$) and A_1, A_2 are affine permutations over $\mathbb{F}_{2^s}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}-2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{2^s}, \\ x^{2^{2k}-2^k+1}, & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially $(1, 6)$-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 2$, then the algebraic degree of F is $n-1$. The nonlinearity of F is at least $2^{n-1} - 2^{\frac{s}{2}+1} - 2^{\frac{n}{2}}$.

Proof The proof follows in a similar way as in [5, Theorem 4.2, Proposition 4.1]. □

Theorem 4.1 in [5] can be extended to the case of p-ary functions and $c \neq 1$. In the following result, we do not request any condition on the solutions of the derivatives of our functions. Furthermore, we shall consider piecing more than two functions, but we prefer to state the result for two functions separately since it is the usual subfield modification, and the general case will be more evident.

Theorem 2.5 *Let p is a prime, $n > 2$ be an integer, s be a divisor of n, $1 \neq c \in \mathbb{F}_{p^n}$ fixed, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n,n)-function defined by*

$$F(x) = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{p^s}, \\ g(x), & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s,s)-function of c'-differential uniformity $\delta_{f,c'}$ (for all c') and $g \in \mathbb{F}_{p^n}[x]$ is an (n,n)-function of c'-differential uniformity $\delta_{g,c'}$ (for all c'). Then, the c-differential uniformity of F is

$$\delta_{F,c} \leq \begin{cases} \delta_{f,0} + \delta_{g,0}, & \text{if } c = 0, \\ \max\left\{\delta_{f,c_1} + \delta_{g,c}, \delta_{g,c} + 2p^s\delta_{g,0}\right\}, & \text{if } c \neq 0, \end{cases}$$

where $c = \sum_{i=1}^{m} c_i g_i$, with $c_i \in \mathbb{F}_{p^s}$ and $\{g_1 = 1, g_2, \ldots, g_m\}$ is a basis of the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^s}$.

NB: Note that, if $c \in \mathbb{F}_{p^s}$, we have $c = c_1$, and $\delta_{f,c_1} = \delta_{f,c}$.

Proof We first observe that the polynomial representation of F is $F(x) = f(x) + (g(x) - f(x))(x^{p^s} - x)^{p^n-1}$ (here, we consider the embedding of f as an (n,n)-function, by taking $f(x) = 0$ for $x \notin \mathbb{F}_{p^s}$). We consider the c-differential equation, $F(x+a) - cF(x) = b$, of F at $(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$,

$$\begin{aligned} f(x+a) + (g(x+a) - f(x+a))\left(x^{p^s} - x + a^{p^s} - a\right)^{p^n-1} \\ - cf(x) - c(g(x) - f(x))(x^{p^s} - x)^{p^n-1} = b. \end{aligned} \tag{1}$$

If $c = 0$, the equation is either $f(x+a) = b$, or $g(x+a) = b$, depending upon $x + a$ being in $\mathbb{F}_{p^s}$ or not. The first claim follows.

If $c \neq 0$, we consider several cases.

Case 1. Let $a \in \mathbb{F}_{p^s}$. If $x \in \mathbb{F}_{p^s}$, Equation (1) becomes

$$f(x+a) - cf(x) = b.$$

Since $\mathbb{F}_{p^n}$ is an extension of degree m over $\mathbb{F}_{p^s}$, we can write $c = \sum_{i=1}^{m} c_i g_i$ and $b = \sum_{i=1}^{m} b_i g_i$, where $b_i, c_i \in \mathbb{F}_{p^s}$ and $\{g_1 = 1, g_2, \ldots, g_m\}$ is a basis of the extension. Then, the equation above becomes

$$f(x+a) - \left(\sum_{i=1}^{m} c_i g_i\right) f(x) = \sum_{i=1}^{m} b_i g_i,$$

which implies

$$f(x+a) - c_1 f(x) = b_1 \text{ and } -c_i f(x) = b_i, \ \forall i = 2, \ldots, m.$$

This gives a (probably loose, though the b_i, and therefore the $\frac{b_i}{c_i}$, go through all values) bound for the number of solutions given by δ_{f,c_1}.

NB: Note that, if $c \in \mathbb{F}_{p^s}$, we have $c = c_1$, and this bound becomes $\delta_{f,c}$.

If $x \notin \mathbb{F}_{p^s}$, Equation (1) transforms into

$$g(x+a) - cg(x) = b,$$

which has at most $\delta_{g,c}$ solutions. Therefore, in this case we get at most $\delta_{f,c_1} + \delta_{g,c}$ solutions for (1).

Case 2. Let $a \notin \mathbb{F}_{p^s}$. If $x + a \in \mathbb{F}_{p^s}, x \notin \mathbb{F}_{p^s}$, then Equation (1) becomes

$$f(x+a) - cg(x) = b. \tag{2}$$

We raise Equation (2) to the power p^s and get $f(x+a) - c^{p^s} g(x)^{p^s} = b^{p^s}$ (using the fact that $(f(x+a))^{p^s} = f(x+a)$, since $x+a \in \mathbb{F}_{p^s}$ and f is an (s,s)-function), which combined with (2) renders

$$g(x) - c^{p^s-1} g(x)^{p^s} = \frac{b^{p^s} - b}{c}. \tag{3}$$

The polynomial $c^{p^s-1}X^{p^s} - X$ is a linearized polynomial whose kernel is of dimension s. Thus, there are at most $p^s \delta_{g,0}$ (since, for any root X_0 of $c^{p^s-1}X^{p^s} - X + \frac{b^{p^s}-b}{c}$, there are at most $\delta_{g,0}$ values of x such that $g(x) = X_0$) solutions to Equation (3).

Next, if $x + a \notin \mathbb{F}_{p^s}, x \in \mathbb{F}_{p^s}$, then (1) becomes $g(x+a) - cf(x) = b$, and an argument similar to the one above gives

$$g(x+a)^{p^s} - c^{p^s-1} g(x+a) = b^{p^s} - c^{p^s-1} b,$$

with at most $p^s \delta_{g,0}$ solutions.

It remains to consider $x, x+a \notin \mathbb{F}_{p^s}$. In this case, Equation (1) transforms into $g(x+a) - cg(x) = b$, which has at most $\delta_{g,c}$ solutions. Putting these counts together, we obtain the result claimed on the theorem.

□

Remark 2.6 *In the proof above, if $g \in \mathbb{F}_{p^s}[x]$, when $a \notin \mathbb{F}_{p^s}$ we can get: for the case $x + a \in \mathbb{F}_{p^s}$ at most $\delta_{g,1/c^{p^s-1}} = \delta_{g,c^{p^s-1}}$ solutions; and for the case $x \in \mathbb{F}_{p^s}$, we get at most $\delta_{g,c^{p^s-1}}$ solutions. Indeed, from Equation (2) we would have (recalling that $x + a \in \mathbb{F}_{p^s}$)*

$$g(x)^{p^s} - \frac{1}{c^{p^s-1}} g(x) = g(x + a - a^{p^s}) - \frac{1}{c^{p^s-1}} g(x) = \frac{b - b^{p^s}}{c^{p^s}}.$$

The number of solutions $x \notin \mathbb{F}_{p^s}$ such that $x + a \in \mathbb{F}_{p^s}$ is upper bounded by $\delta_{g,1/c^{p^s-1}} = \delta_{g,c^{p^s-1}}$. The same is true for the case $x \in \mathbb{F}_{p^s}$ and $x + a \notin \mathbb{F}_{p^s}$. Therefore, for $c \neq 0$, we get $\delta_{F,c} \leq \max\left\{\delta_{f,c_1} + \delta_{g,c}, \delta_{g,c} + 2\delta_{g,c^{p^s-1}}\right\}$.

We can generalize this result as follows:

Theorem 2.7 *Let $t \geq 2$, $k_i \,|\, k_{i+1}$, $1 \leq i \leq t-1$, $k_t = n$, be a sequence of integer divisors, and f_i, $1 \leq i \leq t$, be some (k_i, k_i)-functions of c'-differential uniformity $\delta_{f_i,c'}$ (for all c'). Further, let $c \in \mathbb{F}_{p^n}$ be fixed, and $F_t : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n,n)-function defined by*

$$F_t(x) = \begin{cases} f_1(x), & \text{if } x \in \mathbb{F}_{p^{k_1}}, \\ f_2(x), & \text{if } x \in \mathbb{F}_{p^{k_2}} \setminus \mathbb{F}_{p^{k_1}}, \\ \dots & \dots\dots\dots \\ f_t(x), & \text{if } x \in \mathbb{F}_{p^{k_t}} \setminus \mathbb{F}_{p^{k_{t-1}}}. \end{cases}$$

Then, the c-differential uniformity of f is

$$\delta_{F_t,c} \leq \delta_{f_t,c} + \sum_{i=1}^{t-1} \max\left\{\delta_{f_i,c^{(i)}}, 2p^{k_i} \sum_{j=1}^{t-i-1} \delta_{f_j,0}\right\},$$

where $c^{(i)}$ are the projections of c onto $\mathbb{F}_{p^{k_i}}$, via some bases of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^{k_i}}$.

Proof We use induction on t. The case of $t = 2$ was treated in the proof of Theorem 2.5, and the general case follows similarly.

If $c = 0$, the same argument as before will show that $\delta_{F_t,0} \leq \sum_{i=1}^{t} \delta_{f_i,0}$. Using the notation

$$F_{t-i+1}(x) = \begin{cases} f_i(x), & \text{if } x \in \mathbb{F}_{p^{k_i}}, \\ f_{i+1}(x), & \text{if } x \in \mathbb{F}_{p^{k_{i+1}}} \setminus \mathbb{F}_{p^{k_i}}, \\ \cdots & \cdots\cdots\cdots \\ f_t(x), & \text{if } x \in \mathbb{F}_{p^{k_t}} \setminus \mathbb{F}_{t-1}, \end{cases}$$

and applying the induction assumption, we find that

$$\delta_{F_t,c} \leq \delta_{F_{t-1},c} + \max\{\delta_{f_1,c^{(1)}}, 2p^{k_1}\delta_{F_{t-1},0}\},$$

if $c \neq 0$. By the proof of Theorem 2.5, $\delta_{F_{t-1},0} \leq \sum_{i=1}^{t-1} \delta_{f_i,0}$. Moreover, $\delta_{F_{t-1},c} \leq \delta_{F_{t-2},c} + \max\{\delta_{f_2,c^{(2)}}, 2p^{k_2}\sum_{i=1}^{t-2}\delta_{f_i,0}\}$, and by iteration we see that

$$\delta_{F_t,c} \leq \delta_{f_t,c} + \sum_{i=1}^{t-1} \max\left\{\delta_{f_i,c^{(i)}}, 2p^{k_i}\sum_{j=1}^{t-i-1}\delta_{f_j,0}\right\}.$$

The proof is done. □

Surely, there are other ways of piecing a function together, and we look at such a way below.

Theorem 2.8 *Let p is a prime, $n > 2$ be an integer, $n = st$, and $\gcd(s,t) = 1$. Let $1 \neq c \in \mathbb{F}_{p^n}$ fixed, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n,n)-function defined by*

$$F(x) = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{p^t}, \\ g(x), & \text{if } x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p, \\ h(x), & \text{if } x \notin (\mathbb{F}_{p^s} \cup \mathbb{F}_{p^t}), \end{cases}$$

where f is a (t,t)-function of c'-differential uniformity $\delta_{f,c'}$ (for all c'), g is an (s,s)-function of c'-differential uniformity $\delta_{g,c'}$ (for all c'), and h is an (n,n)-function of c'-differential uniformity $\delta_{h,c'}$ (for all c'). Then, the c-differential uniformity of F is upper bounded by

$$\begin{cases} \delta_{f,0} + \delta_{g,0} + \delta_{g,0}, & \text{if } c = 0, \\ \delta_{h,c} + \max\Big\{\delta_{f,c_1} + \delta_{g,c_1'}, \delta_{f,c_1} + 2p^s\delta_{h,0}, 2p^t\delta_{h,0} + 2\min\{p^t\delta_{g,0}, p^s\delta_{f,0}\} \\ \quad + \delta_{g,c_1'}, 2\min\{p^t\delta_{g,0}, p^s\delta_{f,0}\} + (2p^t + 2p^s)\delta_{h,0}\Big\}, & \text{if } c \neq 0, \end{cases}$$

where $c = \sum_{i=1}^{s} c_i g_i = \sum_{i=1}^{t} c_i' g_i'$, with $c_i \in \mathbb{F}_{p^t}, c_i' \in \mathbb{F}_{p^s}$, and $\{g_1 = 1, g_2, \ldots, g_s\}$, $\{g_1' = 1, g_2', \ldots, g_t'\}$ are bases of the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^t}$, respectively, $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^s}$.

Proof We need to investigate the number of solutions of

$$F(x + a) - cF(x) = b.$$

If $c = 0$, for any a, b, the equation is either $f(x+a) = b$, $g(x+a) = b$ or $h(x+a) = b$. The first claim follows.

Let now $c \neq 0$ and $a \in \mathbb{F}_p$. We can distinguish three cases:
Case 1) $x \in \mathbb{F}_{p^t}$: In this case, the equation is

$$f(x+a) - cf(x) = b.$$

As in the proof of Theorem 2.5, this implies that the number of solutions is upper bounded by δ_{f,c_1}, where $c = \sum_{i=1}^{s} c_i g_i$, where $c_i \in \mathbb{F}_{p^t}$ and $\{g_1 = 1, g_2, \ldots, g_s\}$ is a basis of the extension of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^t}$.
Case 2) $x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$: In this case, the equation is

$$g(x+a) - cg(x) = b.$$

Similarly as in case 1), the number of solutions is upper bounded by $\delta_{g,c_1'}$, where $c = \sum_{i=1}^{t} c_i' g_i'$, where $c_i' \in \mathbb{F}_{p^s}$ and $\{g_1' = 1, g_2', \ldots, g_t'\}$ is a basis of the extension of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^s}$.
Case 3) $x \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$: In this case, the equation is

$$h(x+a) - ch(x) = b.$$

The upper bound is here $\delta_{h,c}$.

Let now $c \neq 0$ and $a \in \mathbb{F}_{p^t} \setminus \mathbb{F}_p$. We can distinguish four cases:
Case 1. $x \in \mathbb{F}_{p^t}$, $x + a \in \mathbb{F}_{p^t}$: In this case the equation is

$$f(x+a) - cf(x) = b.$$

As above, this implies that the number of solutions is upper bounded by δ_{f,c_1}.
Case 2. $x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$: In this case, the equation is

$$h(x+a) - cg(x) = b.$$

Raising to the power p^s and subtracting, we obtain the equation

$$(h(x+a))^{p^s} - c^{p^s-1} h(x+a) = b^{p^s} - c^{p^s-1} b,$$

which has as a solution set $b + \mathbb{F}_{p^s}$ (note that, if $c \in \mathbb{F}_{p^s}^*$, $c^{p^s-1} = 1$, and, if $b \in \mathbb{F}_{p^s}$, $b + \mathbb{F}_{p^s} = \mathbb{F}_{p^s}$, so this covers all cases (with nonzero c)). The number of solutions is thus upper-bounded by $p^s \delta_{h,0}$.
Case 3. $x \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$, $x + a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$: In this case, the equation is

$$g(x+a) - ch(x) = b.$$

By similar arguments as the previous case, we obtain the bound $p^s \delta_{h,0}$.
Case 4. $x, x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$: In this case, the equation is

$$h(x+a) - ch(x) = b,$$

so we have at most $\delta_{h,c}$ solutions.

Let now $c \neq 0, a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$. We have now six cases:
Case A. $x \in \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$. In this case, the equation is

$$g(x+a) - cf(x) = b.$$

If we raise to p^t, we see that the number of solutions is upper-bounded by $p^t \delta_{g,0}$. However, raising to p^s, we obtain an upper bound of $p^s \delta_{f,0}$. From this case, then, we get $\min\{p^t \delta_{g,0}, p^s \delta_{f,0}\}$.
Case B. $x \in \mathbb{F}_{p^t} \setminus \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$: In this case, the equation is

$$h(x+a) - cf(x) = b,$$

which has at most $p^t \delta_{h,0}$ solutions.

Case C. $x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^t}$: this case is only possible if $x + a \in \mathbb{F}_p$. Here the equation is

$$f(x + a) - cg(x) = b.$$

Similarly as in Case *A*, we get $\min\{p^t\delta_{g,0}, p^s\delta_{f,0}\}$.
Case D. $x, x + a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$: Here the equation is

$$g(x + a) - cg(x) = b,$$

which gives an upper bound of $\delta_{g,c_1'}$.
Case E. $x \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s}), x + a \in \mathbb{F}_{p^t}$: Here the equation is

$$f(x + a) - ch(x) = b,$$

which has at most $p^t\delta_{h,0}$ solutions.
Case F. $x, x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$. In this case, the equation is

$$h(x + a) - ch(x) = b,$$

which gives an upper bound of $\delta_{h,c}$.

Now, let us consider the case $c \neq 0, a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$. We consider here seven cases:
Case a. $x \in \mathbb{F}_{p^t}$, $x + a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$. Here the equation is

$$g(x + a) - cf(x) = b,$$

which gives an upper bound of $\min\{p^t\delta_{g,0}, p^s\delta_{f,0}\}$.
Case b. $x \in \mathbb{F}_{p^t}$, $x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$. Here the equation is

$$h(x + a) - cf(x) = b,$$

which gives an upper bound of $p^t\delta_{h,0}$.
Case c. $x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^t}$. Here the equation is

$$f(x + a) - cg(x) = b,$$

which gives an upper bound of $\min\{p^t\delta_{g,0}, p^s\delta_{f,0}\}$.
Case d. $x \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$, $x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$. Here the equation is

$$h(x + a) - cg(x) = b,$$

which gives an upper bound of $p^s\delta_{h,0}$.
Case e. $x \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$, $x + a \in \mathbb{F}_{p^t}$. Here the equation is

$$f(x + a) - ch(x) = b,$$

which gives an upper bound of $p^t\delta_{h,0}$.
Case f. $x \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$, $x + a \in \mathbb{F}_{p^s} \setminus \mathbb{F}_p$. Here the equation is

$$g(x + a) - ch(x) = b,$$

which gives an upper bound of $p^s\delta_{h,0}$.
Case g. $x, x + a \in \mathbb{F}_{p^n} \setminus (\mathbb{F}_{p^t} \cup \mathbb{F}_{p^s})$. Here the equation is

$$h(x + a) - ch(x) = b,$$

which gives an upper bound of $\delta_{h,c}$. □

Remark 2.9 *Note that, if* $c \in \mathbb{F}_{p^s}^*$ *and* $h \in \mathbb{F}_{p^s}[x]$ *or* $c \in \mathbb{F}_{p^t}^*$ *and* $h \in \mathbb{F}_{p^t}[x]$ *we can reduce the bound, in a similar way as in Remark* 2.6.

If we introduce some extra conditions on the solutions of the derivatives of the function g, we can obtain another upper bound on the c-differential uniformity of the modified function.

Theorem 2.10 *Let p be a prime, $n > 2$ be an integer, s be a divisor of n, $1 \neq c \in \mathbb{F}_{p^s}$ fixed, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n, n)-function defined by*

$$F(x) = \begin{cases} f(x), & \text{if } x \in \mathbb{F}_{p^s}, \\ g(x), & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s, s)-function of c-differential uniformity $\delta_{f,c}$ and $g \in \mathbb{F}_{p^s}[x]$ is an (n, n)-function of c-differential uniformity, $\delta_{g,c}$. Suppose that:

- $(H1)$ *for any $a \in \mathbb{F}_{p^s}^\star$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x+a) - g(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.*
- $(H2)$ *for any $a \in \mathbb{F}_{p^s}$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x+a) - cg(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.*

Then, the c-differential uniformity of F is

$${}_c\Delta_F(a, b) \leq \begin{cases} \max\{\delta_{f,c}, \delta_{g,c}\}, & \text{if } a \in \mathbb{F}_{p^s}, \\ \delta_{g,c} + 2 \cdot \delta_{g,0}, & \text{if } a \notin \mathbb{F}_{p^s}. \end{cases}$$

Proof In order to get the c-differential uniformity of F, we need to check the number of solutions of the equation

$$F(x + a) - cF(x) = b. \tag{4}$$

Let us consider $a \in \mathbb{F}_{p^s}$. Then, for a solution x, we can have that both x and $x + a$ are in $\mathbb{F}_{p^s}$ or none is in $\mathbb{F}_{p^s}$. In the first case, (4) becomes

$$f(x + a) - cf(x) = b,$$

which has at most $\delta_{f,c}$ solutions if $b \in \mathbb{F}_{p^s}$ and none when $b \notin \mathbb{F}_{p^s}$.

In the second case, we obtain

$$g(x + a) - cg(x) = b.$$

From (H2) we have no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$ if $b \in \mathbb{F}_{p^s}$. If $b \notin \mathbb{F}_{p^s}$, the number of solutions is at most $\delta_{g,c}$. Then, for $a \in \mathbb{F}_{p^s}$ we can have at most $\delta = \max\{\delta_{f,c}, \delta_{g,c}\}$.

Let $a \notin \mathbb{F}_{p^s}$. Given a solution x of (4), we can have the following cases:

1. $x \notin \mathbb{F}_{p^s}$ and $x + a \in \mathbb{F}_{p^s}$;
2. $x \in \mathbb{F}_{p^s}$ and $x + a \notin \mathbb{F}_{p^s}$;
3. both x and $x + a$ are not in $\mathbb{F}_{p^s}$.

Let us consider Case 1. Then, (4) becomes

$$f(x + a) - cg(x) = b. \tag{5}$$

Let us note that $b \notin \mathbb{F}_{p^s}$, otherwise we cannot have a solution of this type since $g(x) \notin \mathbb{F}_{p^s}$, which is derived from (H2) with $a = 0$.

From this, raising (5) by p^s and substracting (5), we obtain

$$g(x)^{p^s} - g(x) = -\left(\frac{b}{c}\right)^{p^s} + \frac{b}{c}.$$

Denoting by $y = g(x)$ and by $b' = -\frac{b}{c}$, we obtain

$$y^{p^s} - y = b'^{p^s} - b'.$$

The solutions of this last equation are the elements of the coset $b' + \mathbb{F}_{p^s}$. Now, $x \in a + \mathbb{F}_{p^s}$. Therefore, we need to check how many elements we have in $g(a + \mathbb{F}_{p^s}) \cap \left(b' + \mathbb{F}_{p^s}\right)$, where $g(a + \mathbb{F}_{p^s}) := \{g(x) : x \in a + \mathbb{F}_{p^s}\}$. Suppose that $\left|g(a + \mathbb{F}_{p^s}) \cap \left(b' + \mathbb{F}_{p^s}\right)\right| \geq 2$. Then, there exist $x_1, x_2, y_1, y_2 \in \mathbb{F}_{p^s}$ such that $b' + y_1 = g(a + x_1)$, $b' + y_2 = g(a + x_2)$ and $x_1 \neq x_2$, $y_1 \neq y_2$. Thus,

$$g(a + x_1) - g(a + x_2) = y_1 - y_2.$$

Denoting by $x' = a + x_2 \notin \mathbb{F}_{p^s}$ and $a' = x_1 - x_2 \in \mathbb{F}_{p^s}$, we obtain that

$$g(x' + a') - g(x') = y_1 - y_2.$$

This is not possible by (H1). Therefore, $\left|g(a + \mathbb{F}_{p^s}) \cap \left(b' + \mathbb{F}_{p^s}\right)\right| \leq 1$, implying that we have at most $\delta_{g,0}$ solutions in Case (1), since for any element y in $g(a + \mathbb{F}_{p^s})$ we have $|g^{-1}(y)| \leq \delta_{g,0}$.

For Case 2, we obtain, in a similar way, that $|g(a + \mathbb{F}_{p^s}) \cap (b + \mathbb{F}_{p^s})| \leq 1$, which implies that we have at most $\delta_{g,0}$ solutions.

In the last case, we obtain the equation

$$g(x + a) - cg(x) = b,$$

which admits at most $\delta_{g,c}$ solutions for any b. Then, for $a \notin \mathbb{F}_{p^s}$, Equation (4) admits at most $\delta_{g,c} + 2 \cdot \delta_{g,0}$ solutions. □

Remark 2.11 *We can note that if we remove condition (H2) in Theorem 2.10, we would obtain that*

$${}_c\Delta_F(a, b) \leq \begin{cases} \delta_{f,c} + \delta_{g,c} & \text{if } a \in \mathbb{F}_{p^s} \\ \delta_{g,c} + 2 \cdot \delta_{g,0} & \text{if } a \notin \mathbb{F}_{p^s}. \end{cases}$$

Moreover, if g permutes $\mathbb{F}_{p^n}$ then we have also that $\delta_{g,0} = 1$.

For PcN and APcN functions we have a similar result as in Proposition 2.1.

Proposition 2.12 *Let $n = sm$, with s and m positive integers. Let $c \in \mathbb{F}_{p^s}$ and $F \in \mathbb{F}_{p^s}[x]$. Then,*

i) if F is PcN, $F(x + a) - cF(x) = b$ does not admit solution $x \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$, whenever $a, b \in \mathbb{F}_{p^s}$ ($a \neq 0$, if $c = 1$).

ii) if F is APcN and m is odd, $F(x + a) - cF(x) = b$ does not admit solution $x \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$, whenever $a, b \in \mathbb{F}_{p^s}$ ($a \neq 0$, if $c = 1$).

Proof Suppose that F is APcN and m is odd. We have then that the polynomial $F(x + a) - cF(x) - b$ admits at most 2 roots for any a and b. Then, if $a, b \in \mathbb{F}_{p^s}$, we have that if x_1 is a solution so is $x_1^{p^s}$, since $F(x + a) - cF(x) - b$ is a polynomial with coefficients over $\mathbb{F}_{p^s}$ ($a \neq 0$, if $c = 1$).

Suppose next that $x_1 \notin \mathbb{F}_{p^s}$. Then, $x_1^{p^s} = x_2$, where x_2 is the second root. So, $x_2^{p^s}$ must be equal to x_1, implying $x_1^{p^{2s}} = x_1$. Therefore $x_1 \in \mathbb{F}_{p^{2s}} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^s}$, which gives us a contradiction.

For the PcN case, we have no restriction on m since we have only one root x_1 of $F(x+a) - cF(x) - b$, and thus $x_1^{p^s}$ must be equal to x_1. □

As for the case of the differential uniformity we can extend the previous result as follows.

Proposition 2.13 *Let $n = sm$, $c \in \mathbb{F}_{p^s}$, and F is a $\delta_{F,c}$ c-differentially uniform function over $\mathbb{F}_{p^n}$, with coefficients on the subfield $\mathbb{F}_{p^s}$. Then, if for any prime $q \leq \delta_{F,c}$, $q \nmid m$, the equation $F(x+a) - cF(x) = b$ does not admit solution $x \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$, whenever $a, b \in \mathbb{F}_{p^s}$.*

Proof Let x be a solution of $F(x+a) - cF(x) = b$. Then, all the elements in $O_x = \{x^{p^{is}} : 0 \leq i \leq m-1\}$ are solutions of this equation. Moreover, since $|O_x| \leq \delta_{F,c}$, for some integer $j \leq \delta_{F,c}$ we have $x^{p^{js}} = x$, implying that $x \in \mathbb{F}_{p^{\gcd(js,n)}} = \mathbb{F}_{p^s}$. □

We can use Theorem 2.10 to provide an upper bound on the c-differential uniformity of several functions that have been introduced in the recent years, such as the 4-uniform functions given in [12, 17, 18]. In particular, we have the following result, which includes the functions defined in [12, 17, 18].

Theorem 2.14 *Let $n = sm$ with m odd. Let β and γ in $\mathbb{F}_{2^s}$, with $\beta \neq 0$. Let $A : \mathbb{F}_{2^s} \to \mathbb{F}_{2^s}$ be an affine permutation, and consider the function*

$$F(x) = \begin{cases} \beta(A(x))^{2^n-2} + \gamma, & \text{if } x \in \mathbb{F}_{2^s} \\ x^{-1}, & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

Then, we have:

- *$\delta_{F,c} \leq 4$, for $c \in \mathbb{F}_{2^s} \setminus \mathbb{F}_2$ such that $\mathrm{Tr}(c) = \mathrm{Tr}(1/c) = 1$;*
- *if $3 \nmid m$, $\delta_{F,c} \leq 4$ for $c \in \mathbb{F}_{2^s} \setminus \mathbb{F}_2$ such that $\mathrm{Tr}(c) = 0$ or $\mathrm{Tr}(1/c) = 0$.*

Proof Let us note that for any function $f(x)$, the c-differential uniformity of the function $f'(x) = \beta f(A(x)) + \gamma$ is equal to the c-differential uniformity of f. Indeed, the number of solutions of

$$f'(x+a) - cf'(x) = b$$

is the same as for the equation

$$f(x + A(a) + A(0)) - cf(x) = \frac{b + (c-1)\gamma}{\beta}.$$

Now, for the inverse function x^{-1}, from Theorem 12 in [9], we have that the c-differential uniformity is 2 if $\mathrm{Tr}(c) = \mathrm{Tr}(1/c) = 1$, and 3 if $\mathrm{Tr}(c) = 0$ or $\mathrm{Tr}(1/c) = 0$. Therefore, from Proposition 2.13 and Theorem 2.10 we have our claim. Indeed, for the case $\mathrm{Tr}(c) = \mathrm{Tr}(1/c) = 1$, we have immediately the upper bound since $\delta_{x^{-1},c} = 2$.

When $\mathrm{Tr}(c) = 0$ or $\mathrm{Tr}(1/c) = 0$, we have that $\delta_{x^{-1},c} = 3$, so we would have the upper bound $\delta_{x^{-1},c}+2 = 5$ from Theorem 2.10. However, from the proof of Theorem 2.10, in the last case, we should count the solutions for which both x and $x+a$ (with $a \notin \mathbb{F}_{2^s}$) are not in $\mathbb{F}_{2^s}$. From the proof of Theorem 12 in [9], when the equation

$$(x+a)^{-1} - cx^{-1} = b$$

admits three solutions, then one of these is 0 or a. In our case, these solutions do not have to be counted. So, we have at most two solutions with x and $x+a$ not in $\mathbb{F}_{2^s}$, and thus $\delta_{F,c} \leq 4$. □

2.1 Shifting Gold-like functions on a subfield

In [16], the author studied the c-differential uniformity of the modified Gold function. In particular he obtained the following result.

Theorem 2.15 *Let $n = sm$. Let*

$$G(x) = x^{2^k+1} + \alpha(x^{2^s} + x)^{2^n-1} + \alpha = \begin{cases} x^{2^k+1} + \alpha, & \text{if } x \in \mathbb{F}_{2^s}, \\ x^{2^k+1}, & \text{if } x \notin \mathbb{F}_{2^s}, \end{cases}$$

where $1 \leq k < n$, $\gcd(k,n) = 1$, $\alpha \in \mathbb{F}_{2^s}^\star$. Then, for $c \neq 1$, the $c-$differential uniformity of G is $\delta_{G,c} \leq 9$.

Remark 2.16 *The c-differential uniformity of a Gold function $g(x) = x^{2^k+1}$ has been characterized in* [13, Theorem 4]. *In particular, for $c \neq 1$ we have $\delta_{g,c} \leq 2^{\gcd(k,n)}+1$. Applying Theorem 2.5 and Remark 2.6 we obtain that the c-differential uniformity of $G(x) = x^{2^k+1} + \alpha(x^{2^s} + x)^{2^n-1} + \alpha$ satisfies*

$$\delta_{G,c} \leq \begin{cases} 2 \cdot (2^{\gcd(k,n)} + 1) & \text{if } c = 0 \\ 3 \cdot (2^{\gcd(k,n)} + 1) & \text{if } c \neq 0. \end{cases}$$

Therefore, the upper bound in Theorem 2.15 can be obtained applying Theorem 2.5 and Remark 2.6. Indeed, for $\gcd(k,n) = 1$ we have

$$\delta_{G,c} \leq \begin{cases} 6 & \text{if } c = 0 \\ 9 & \text{if } c \neq 0. \end{cases}$$

For a Gold-like function defined over $\mathbb{F}_{2^n}$, we can observe the following.

Proposition 2.17 *Let $n = sm$, with m odd. For a Gold function $g(x) = x^{2^k+1}$ with $\gcd(n,k) = t$ such that $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$, we have that*

$$g(x+a) + g(x) = b$$

does not admit solutions in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$, whenever $a \in \mathbb{F}_{2^s}^\star$ and $b \in \mathbb{F}_{2^s}$.

Proof The proof follows in a similar way as Lemma 4.1 in [5]. Indeed, we can consider just the equation

$$x^{2^k} + x = b.$$

If $b \in \mathbb{F}_{2^s}$ we obtain that $(x^{2^k} + x)^{2^s} = x^{2^k} + x$, which implies $x^{2^s} + x \in \mathbb{F}_{2^k}$. Therefore, $x^{2^s} + x \in \mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$. Then, $(x^{2^s} + x)^{2^s} + x^{2^s} + x = 0$ implies $x^{2^{2s}} = x$, and thus $x \in \mathbb{F}_{2^{2s}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^s}$. □

Remark 2.18 *Note that the above proposition cannot be derived directly from Proposition 2.1, for $t \geq 2$. Indeed, the Gold-like function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = t$ has differential uniformity equal to 2^t. So, for applying Proposition 2.1 we need $i \nmid m$ for any $2 \leq i \leq 2^{t-1}$, while in Proposition 2.17 we just require $2 \nmid m$. For $t = 1$, the result follows from [7].*

Theorem 2.19 *Let $n = sm$, with m odd. For a Gold function $g(x) = x^{2^k+1}$, with $\gcd(n, k) = t$ such that $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$, and n/t odd, $n/t \geq 3$ ($n \geq 3$). Then, for any fixed $\alpha \in \mathbb{F}_{2^s}^\star$, $G(x) = x^{2^k+1} + \alpha(x^{2^s} + x)^{2^n-1} + \alpha$ is such that $\delta_{G,c} \leq 3$, for any $c \in \mathbb{F}_{2^t} \setminus \{1\}$.*

Proof From Proposition 2.17, we have that $g(x) = x^{2^k+1}$ satisfies (H1) in Theorem 2.10.

Since n/t is odd we have that g is a permutation of $\mathbb{F}_{2^n}$, so $\delta_{g,0} = 1$. Moreover, from Theorem 4 in [13] we have that g is PcN for $c \in \mathbb{F}_{2^t} \setminus \{1\}$.

From Proposition 2.12 we have that (H2) holds. Therefore, $\delta_{G,c} \leq 3$ by Theorem 2.10. □

Theorem 2.20 *Let $n = sm$, with n odd. Given the Gold function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = 1$, then, for any fixed $\alpha \in \mathbb{F}_{2^s}^\star$, $G(x) = x^{2^k+1} + \alpha + \alpha(x^{2^s} + x)^{2^n-1}$ is such that $\delta_{G,c} \leq 6$, for any $c \in \mathbb{F}_{2^s} \setminus \{1\}$. Moreover, if $3 \nmid m$, then $\delta_{G,c} \leq 5$.*

Proof If $3 \nmid m$, then since the map is 3 c-differentially uniform from Proposition 2.13 we have that (H2) in Theorem 2.10 is satisfied. The same for (H1) by Proposition 2.1. Therefore, from Theorem 2.10 we have that $\delta_{G,c} \leq 5$ ($\delta_{g,0} = 1$).

If $3 \mid m$, then we cannot guarantee that (H2) in Theorem 2.10 is satisfied, but applying Remark 2.11 we have $\delta_{G,c} \leq 6$. □

Remark 2.21 *Theorem 2.20 improves the upper bound obtained by Stănică in [16], albeit when c is restricted to the subfield $\mathbb{F}_{2^s}$.*

3 Concatenating functions with low *c*-differential uniformity

In this section we will show how it is possible to obtain a function over $\mathbb{F}_{q^n}$, with low c-differential uniformity, concatenating n functions defined over $\mathbb{F}_q$.

Let $\{\beta_1, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{q^n}$ as vector space over $\mathbb{F}_q$. Let

$$A = \begin{pmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \vdots & & & \vdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{pmatrix}.$$

The matrix A is non-singular, so we let $A^{-1} = (a_{i,j})_{i,j}$.

Let us denote by e_k the column vector composed by all zeros but one in position k, for $1 \leq k \leq n$. We define the linear polynomial

$$L_k(x) = \sum_{i=1}^{n} a_{i,k} x^{q^{i-1}} = (x, x^q, \ldots, x^{q^{n-1}}) \cdot A^{-1} \cdot e_k.$$

Any element $x \in \mathbb{F}_{q^n}$ can be written as $x = \beta_1 x_1 + \cdots + \beta_n x_n$, with $x_i \in \mathbb{F}_q$. So, we have

$$L_k(x) = \left(\sum_{i=1}^{n} \beta_i x_i, \ldots, \sum_{i=1}^{n} \beta_i^{q^{n-1}} x_i \right) \cdot A^{-1} \cdot e_k = (x_1, \ldots, x_n) \cdot A \cdot A^{-1} \cdot e_k = x_k.$$

That is, L_k is the projection of the k-th component of x.

So we obtain the following result.

Theorem 3.1 *Let $c \in \mathbb{F}_q \setminus \{1\}$ and let $f_1, \ldots, f_n$ be n functions over $\mathbb{F}_q$ with c-differential uniformity $\delta_1, \ldots, \delta_n$, respectively. Let $\beta_1, \ldots, \beta_n$, L_k be defined as before. Then $F(x) = \sum_{k=1}^{n} \beta_k f_k(L_k(x))$ has c-differential uniformity equal to $\prod_{i=1}^{n} \delta_i$.*

Proof For any $a \in \mathbb{F}_{q^n}$, with $a = \beta_1 a_1 + \cdots + \beta_n a_n$, we have

$$\begin{aligned} F(x+a) - cF(x) &= \sum_{k=1}^{n} \beta_k f_k(x_k + a_k) - c \sum_{k=1}^{n} \beta_k f_k(x_k) \\ &= \sum_{k=1}^{n} \beta_k (f_k(x_k + a_k) - c f_k(x_k)). \end{aligned}$$

So if we consider $b = \beta_1 b_1 + \cdots + \beta_n b_n$ we have

$$F(x+a) - cF(x) = b, \text{ that is, } f_k(x_k + a_k) - c f_k(x_k) = b_k, \text{ for all } k.$$

The equation $f_k(x_k + a_k) - c f_k(x_k) = b_k$ admits at most δ_k solutions for any a_k and b_k in $\mathbb{F}_q$, and there exist some a_k and b_k for which we have δ_k solutions. So, we

obtain that $F(x+a)-cF(x)=b$ admits at most $\prod_{i=1}^{n}\delta_i$ solutions and we can find a, and b for which we obtain exactly $\prod_{i=1}^{n}\delta_i$ solutions. □

Using the previous result, we can construct a PcN function over $\mathbb{F}_{q^n}$ from n PcN functions over $\mathbb{F}_q$.

Corollary 3.2 *Let $c \in \mathbb{F}_q \setminus \{1\}$ and let $f_1, \ldots, f_n$ be n functions over $\mathbb{F}_q$ that are PcN. Then $F(x)=\sum_{k=1}^{n}\beta_k f_k(L_k(x))$ is PcN.*

4 Concluding remarks

In this work we extended some of the results given in [5] to the case of the c-differential uniformity. We piece together (in several ways) subfunctions and provide upper bounds for the c-differential uniformity of the obtained function. As a byproduct, we improve some prior results of [16]. Further, we look at concatenations of functions with low differential uniformity and check how their c-differential uniformity changes. In particular, we prove that given β_i (a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$), some functions f_i of c-differential uniformities δ_i, and some specific linearized polynomials L_i defined in terms of β_i, $1 \leq i \leq n$, then $F(x)=\sum_{i=1}^{n}\beta_i f_i(L_i(x))$ has c-differential uniformity equal to $\prod_{i=1}^{n}\delta_i$. We believe, it would also be of interest to investigate these constructions for the case of the newly defined generalized boomerang uniformity, as in [14] (see also [15], for other characterizations).

Acknowledgements. The authors would like to thank the editor for efficiently handling our paper and to the reviewers for their careful reading, beneficial comments and constructive suggestions.

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. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020), 187–213.

[3] 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.

[4] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer-Verlag, 2014.

[5] M. Calderini, *Differentially low uniform permutations from known* 4*-uniform functions*, Des. Codes Cryptogr. 89 (2021), 33–52.

[6] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge: Cambridge University Press, Cambridge, 2021.

[7] C. Carlet, *Revisiting some results on APN and algebraic immune functions*, Adv. Math. Communications, doi: 10.3934/amc.2021035, 2021.

[8] H. Dobbertin, *Another proof of Kasami's theorem*, Designs, Codes and Cryptography 17 (1999), 177–180.

[9] 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.

[10] S. Ul 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.

[11] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Information and Control 18 (1971), 369–394.

[12] J. Peng, C. H. Tan, *New differentially* 4*-uniform permutations by modifying the inverse function on subfields*, Cryptogr. Commun. (2017) 9:363–378

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

[14] P. Stănică, *Investigations on c-boomerang uniformity and perfect nonlinearity*, Discrete Appl. Mathematics 304 (2021), 297–314.

[15] P. Stănică, *Using double Weil sums in finding the Boomerang and the c-Boomerang Connectivity Table for monomial functions on finite fields*, Appl. Alg. Eng. Communic. Comput., https://doi.org/10.1007/s00200-021-00520-9, 2021.

[16] 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.

[17] G. Xu, and L. Qu, *Two classes of differentially* 4*-uniform permutations over* $\mathbb{F}_{2^n}$ *with n even*, Adv. Math. Communic. 14:1 (2019), 97–110.

[18] Z. Zha, L. Hu, S. Sun, *Constructing new differentially* 4*-uniform permutations from the inverse function*, Finite Fields Appl. 25 (2014), 64–78.