Higher Order c-Differentials

Aaron Geary[1], Marco Calderini[2], Constanza Riera[3], Pantelimon Stănică[1]

[1] Applied Mathematics Department, Naval Postgraduate School, Monterey, USA; {aaron.geary, pstanica}@nps.edu

[2] Department of Informatics, University of Bergen Postboks 7803, N-5020, Bergen, Norway; Marco.Calderini@uib.no

[3]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway; csr@hvl.no

September 6, 2021

Abstract

In [9], the notion of c-differentials was introduced as a potential expansion of differential cryptanalysis against block ciphers utilizing substitution boxes. Drawing inspiration from the technique of higher order differential cryptanalysis, in this paper we propose the notion of higher order c-derivatives and differentials and investigate their properties. Additionally, we consider how several classes of functions, namely the multiplicative inverse function and the Gold function, perform under higher order c-differential uniformity.

Keywords: Boolean and p-ary function, higher order differential, differential uniformity, differential cryptanalysis

1 Introduction and background

The newly proposed c-differentials [9] modify the traditional differential cryptanalysis technique by applying a multiple "c" to one of the outputs of an S-box primitive F. If an input pair $(x, x+a)$ with difference "a" results in an output pair $(F(x), F(x+a))$ with difference $b = F(x+a) - F(x)$, then the couple (a, b) is the traditional *differential* traced throughout a cipher. A differential that appears with a high probability is used as the basis of a classical differential attack [3]. The new c-differential uses a modified output pair of $(cF(x), F(x+a))$, and the new output difference is then $b = F(x+a) - cF(x)$. Similar to other extensions and modifications of

differential cryptanalysis, c-differentials have been shown to result in higher probabilities than traditional differentials for some functions [9], [15], thus potentially resulting in attacks against ciphers that are resistant against other forms of differential cryptanalysis.

The introduction of c-differentials and the corresponding c-differential uniformity (cDU) has been met with substantial interest. Researchers have since submitted multiple papers (see [1, 15, 16, 19, 20], just to cite only a few of these works) further exploring the topic. These include investigations of the cDU of various classes of functions, finding functions with low cDU, construction and existence results on the so-called perfect c-nonlinear and almost perfect c-nonlinear functions, and generalizations of cryptographic properties to include the new c-differential.

In this paper, we continue this investigation by considering the extension of c-differentials into higher order. This is motivated by the extension of the original differential cryptanalysis technique into higher order differential cryptanalysis ([13], [12]). In contrast with the traditional higher order derivatives of Boolean or p-ary functions, the c-derivative and higher order c-derivative do not always reduce the degree of a function. However, in the same spirit as traditional higher order differentials, higher order c-differentials have the potential to allow for a better trace of multiple differences through an encryption scheme, and any resistance against such higher order differentials with large probabilities furthers the case of a cipher's security.

The rest of the paper is organized as follows. In Section 2 we provide the necessary notation and definitions to introduce the higher order c-derivative and investigate its properties in Section 3. In Sections 4 and 5 we consider specific higher order c-differential cases of the inverse function and Gold function over finite fields. Section 6 summarizes our findings.

2 Preliminaries

We introduce here some basic notations and definitions on Boolean and p-ary functions (where p is an odd prime); the reader can consult [5, 6, 8, 14, 18] for more on these objects. For a positive integer n and p a prime number, we denote by $\mathbb{F}_p^n$ the n-dimensional vector space over $\mathbb{F}_p$, and by $\mathbb{F}_{p^n}$ the finite field with p^n elements, while $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ will denote the 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 *(n, m, p)-function*. If $p = 2$ the function is called a vectorial Boolean function. In any characteristic, when $m = n$ the function F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ (using some identification, via a basis, of the finite field with the vector space) 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*, denoted by $\deg(F)$, is then the largest weight in the p-ary expansion of i (that is, the sum of the digits of the exponents i with $a_i \neq 0$). To (somewhat) distinguish between the vectorial and single-component output, we shall use upper/lower case to denote the functions.

Given a (n, m, p)-function F, the derivative of F with respect to $a \in \mathbb{F}_{p^n}$ is the (n, m, p)-function

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

The distribution of the derivatives of an (n, m, p)-function used in an S-box is important. If we let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - F(x) = b\}$, then we call the quantity $\delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{p^n}, a \neq 0\}$ the *differential uniformity* of F.

The i-th derivative of F at $(a_1, a_2, \ldots, a_i)$ is defined recursively as

$$D^{(i)}_{a_1,\ldots,a_i} F(x) = D_{a_i}(D^{(i-1)}_{a_1,\ldots,a_{i-1}} F(x)).$$

The new c-differential, which applies a multiplier to one of the outputs, immediately leads to a modified derivative. For an (n, m, p)-function F, and $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, 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

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

Equipped with this new c-derivative, a new c-autocorrelation function was defined in [16], and several cryptographic properties of (n, m, p)-functions were generalized. That work continues in this paper as we extend the c-derivative into higher order, investigate its properties, and then analyze the higher order c-differential uniformity of several functions.

3 Higher order c-differentials

Inspired by the concept of higher order derivatives of functions between Abelian groups and their applications to cryptography in [13], we propose the following definition.

Definition 3.1. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be an (n, m, p)-function. The i-th c-derivative of F at $(a_1, a_2, \ldots, a_i)$ is*

$$_cD^{(i)}_{a_1,\ldots,a_i} F(x) = \ _cD_{a_i}(_cD^{(i-1)}_{a_1,\ldots,a_{i-1}} F(x)),$$

where $_cD^{(i-1)}_{a_1,\ldots,a_{i-1}} F(x)$ is the $(i-1)$-th derivative of F at $(a_1, a_2, \ldots, a_{i-1})$.

This implies the 0-th c-derivative is the function F itself and the 1st c-derivative is the c-derivative defined in Section 2. Notice that, when $c = 1$, we recover the traditional (n, m, p)-function higher order derivative.

Before we explore these new higher order derivatives we need to ensure several basic properties carry over from the traditional (i.e. $c = 1$) case. First, we see that the sum rule holds. That is, that the c-derivative of a sum is a sum of the c-derivatives.

$$\begin{aligned} {}_cD_a(F+G)(x) &= F(x+a) + G(x+a) - c(F(x) + G(x)) \\ &= F(x+a) - cF(x) + G(x+a) - cG(x) \\ &= {}_cD_aF(x) + {}_cD_aG(x). \end{aligned}$$

A product rule exists for the traditional derivative, $D_a(FG)(x) = F(x+a)D_aG(x) + D_aF(x)G(x)$. We find something similar with the c-derivative,

$$\begin{aligned} {}_cD_a(FG)(x) &= F(x+a)G(x+a) - cF(x)G(x) \\ &= F(x+a)\left(G(x+a) - cG(x)\right) + \left((F(x+a) - F(x)\right)cG(x) \\ &= F(x+a)\ {}_cD_aG(x) + \ {}_cD_aF(x)\ cG(x). \end{aligned}$$

Now we consider the higher order c-derivatives. When $i = 2$ we have

$$\begin{aligned} {}_cD^{(2)}_{a_1,a_2}F(x) =& {}_cD_{a_2}({}_cD_{a_1}F(x)) \\ =& {}_cD_{a_2}(F(x+a_1) - cF(x)) \\ =& F(x+a_1+a_2) - cF(x+a_2) - c(F(x+a_1) - cF(x)) \\ =& F(x+a_1+a_2) - cF(x+a_2) - cF(x+a_1) + c^2F(x). \end{aligned}$$

Taking another iteration, we have

$$\begin{aligned} {}_cD^{(3)}_{a_1,a_2,a_3}F(x) = & F(x+a_1+a_2+a_3) \\ & - c\left[F(x+a_1+a_2) + F(x+a_1+a_3) + F(x+a_2+a_3)\right] \\ & + c^2\left[F(x+a_1) + F(x+a_2) + F(x+a_3)\right] - c^3F(x). \end{aligned}$$

We see a similar pattern to Proposition 1 in [13], albeit with the additional complication of powers of c, and we find the following identity:

$$\begin{aligned} F(x+a_1+a_2+a_3) = & \ {}_cD^{(3)}_{a_1,a_2,a_3}F(x) \\ & + c\left[{}_cD^{(2)}_{a_1,a_2}F(x) + {}_cD^{(2)}_{a_1,a_3}F(x) + {}_cD^{(2)}_{a_2,a_3}F(x)\right] \\ & + c^2\left[{}_cD_{a_1}(F(x)) + {}_cD_{a_2}(F(x)) + {}_cD_{a_3}(F(x))\right] \\ & + c^3F(x). \end{aligned}$$

The pattern holds in general, as we now show.

Theorem 3.2. *Let F be an (n,m,p)-function with ${}_cD^{(i)}_{a_1,\ldots,a_i}F(x)$ the i-th c-derivative of F at $(a_1, a_2, \ldots, a_i)$. Then*

$$F\left(x + \sum_{i=1}^{n} a_i\right) = \sum_{i=0}^{n} \sum_{1 \le j_1 < \ldots < j_i \le n} c^{n-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x). \tag{1}$$

Proof. Equation (1) can also be written as

$$F\left(x+\sum_{i=1}^{n}a_i\right) = {}_cD^{(n)}_{a_1,\ldots,a_n}F(x)+\sum_{i=0}^{n-1}\sum_{1\le j_1<\ldots<j_i\le n-1} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x),$$

which implies

$${}_cD^{(n)}_{a_1,\ldots,a_n}F(x) = F\left(x+\sum_{i=1}^{n}a_i\right)-\sum_{i=0}^{n-1}\sum_{1\le j_1<\ldots<j_i\le n-1} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x).$$

We proceed by induction. For $n = 1$ we see (1) follows directly from the definition and $n = 2, 3$ can be seen in the discussion before the theorem. Assuming Equation (1) holds for $n-1$, we have

$$\begin{aligned}
&{}_cD^{(n)}_{a_1,\ldots,a_n}F(x) = {}_cD_{a_n}\left({}_cD^{(n-1)}_{a_1,\ldots,a_{n-1}}F(x)\right)\\
&= {}_cD_{a_n}\left(F\left(x+\sum_{i=1}^{n-1}a_i\right)-\sum_{i=0}^{n-2}\sum_{1\le j_1<\ldots<j_i\le n-2} c^{n-2-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right)\\
&= F\left(x+\sum_{i=1}^{n}a_i\right)-cF\left(x+\sum_{i=1}^{n-1}a_i\right)\\
&- {}_cD_{a_n}\left(\sum_{i=0}^{n-2}\sum_{1\le j_1<\ldots<j_i\le n-2} c^{n-2-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right).
\end{aligned}$$

We apply the induction hypothesis to $cF(x+a_1+\cdots+a_{n-1})$, and noticing the last double sum is composed of all the c-derivatives that include a_n, we have

$$\begin{aligned}
&F\left(x+\sum_{i=1}^{n}a_i\right)-cF\left(x+\sum_{i=1}^{n-1}a_i\right)\\
&- {}_cD_{a_n}\left(\sum_{i=0}^{n-2}\sum_{1\le j_1<\ldots<j_i\le n-2} c^{n-2-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right)\\
&= F\left(x+\sum_{i=1}^{n}a_i\right)-c\left(\sum_{i=0}^{n-2}\sum_{1\le j_1<\ldots<j_i\le n-2} c^{n-2-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right)\\
&- \left(\sum_{i=0}^{n-1}\sum_{1\le j_1<\ldots<j_i\le n-1} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i},a_n}F(x)\right)\\
&= F\left(x+\sum_{i=1}^{n}a_i\right)-\left(\sum_{i=0}^{n-2}\sum_{1\le j_1<\ldots<j_i\le n-2} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right)
\end{aligned}$$

$$+\left(\sum_{i=0}^{n-1}\sum_{1\le j_1<\ldots<j_i\le n-1} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i},a_n}F(x)\right)$$
$$=F\left(x+\sum_{i=1}^{n}a_i\right)-\left(\sum_{i=0}^{n-1}\sum_{1\le j_1<\ldots<j_i\le n-1} c^{n-1-i}\ {}_cD^{(i)}_{a_{j_1},\ldots,a_{j_i}}F(x)\right).$$

The claim is shown. □

While we have shown several properties of the c-derivative closely align with the traditional derivative, one key property does not follow. A fundamental property of traditional derivatives is that the degree of a polynomial function is reduced by at least one for every derivative taken. That is, $\deg(D_aF)\le\deg(F)-1$. This is not always true in the case of c-derivatives when $c\neq 1$. For example, consider the linearized monomial $F(x)=x^{p^k}$ over $\mathbb{F}_{p^n}$ with k an integer between 0 and n. This function has degree 1 (recall that the p-ary weight of p^k is 1) and the c-derivative of F at a is $(x+a)^{p^k}-cx^{p^k}=(1-c)x^{p^k}+a^{p^k}$, which is also of degree 1 for all $c\neq 1$. Thus, the reduction of degree is not a general property of the c-derivative.

We will now show that higher order c-derivatives are invariant under permutation of the a_i's.

Proposition 3.3. *Let $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, denote $[t]:=\{1,\ldots,t\}$, and let $|I|$ be the cardinality of the subsets $I\subseteq[t]$. Then,*

$${}_cD^{(t)}_{a_1,\ldots,a_t}F(x)=\sum_{I\subseteq[t]}(-c)^{t-|I|}F\left(x+\sum_{i\in I}a_i\right).$$

In particular, for any permutation π of $\{1,\ldots,t\}$ we have ${}_cD^{(t)}_{a_1,\ldots,a_t}F(x)={}_cD^{(t)}_{a_{\pi(1)},\ldots,a_{\pi(t)}}F(x)$.

Proof. It is easy to see that ${}_cD^{(2)}_{a_1,a_2}F(x)=\sum_{I\subseteq[2]}(-c)^{2-|I|}F(x+\sum_{i\in I}a_i)$, and by induction we get

$${}_cD^{(t)}_{a_1,\ldots,a_t}F(x)={}_cD^{(t-1)}_{a_1,\ldots,a_{t-1}}F(x+a_t)-c\,{}_cD^{(t-1)}_{a_1,\ldots,a_{t-1}}F(x)$$
$$=\sum_{I\subseteq[t-1]}(-c)^{(t-1)-|I|}F\left(x+a_t+\sum_{i\in I}a_i\right)-c\sum_{I\subseteq[t-1]}(-c)^{(t-1)-|I|}F\left(x+\sum_{i\in I}a_i\right)$$
$$=\sum_{\substack{I'\subseteq[t]\\ a_t\in I'}}(-c)^{(t-1)-(|I'|-1)}F\left(x+\sum_{i\in I'}a_i\right)+\sum_{\substack{I'\subseteq[t]\\ a_n\notin I'}}(-c)^{t-|I'|}F\left(x+\sum_{i\in I'}a_i\right)$$
$$=\sum_{I\subseteq[t]}(-c)^{t-|I|}F\left(x+\sum_{i\in I}a_i\right).$$

From this we can see that permuting the elements a_i does not change the value of the higher order c-derivative. □

Another easy fact to check is that for power functions the t-order c-differential uniformity can be computed by considering $a_1 = 1$.

Proposition 3.4. *Let $F(x) = x^d$ on $\mathbb{F}_{p^n}$ and denote by ${}_c\Delta(a_1, \ldots, a_t; b) = \#\{x : {}_cD^{(t)}_{a_1,\ldots,a_t}F(x) = b\}$. Then, assuming that not all a_i's are zero (and without loss of generality we can assume that $a_1 \neq 0$), ${}_c\Delta(a_1, \ldots, a_t; b) = {}_c\Delta\left(1, a_2/a_1 \ldots, a_t/a_1; b/(a_1)^d\right)$.*

One of the key findings of higher order derivatives of binary functions is that if the i inputs are not linearly independent, then the ith derivative is exactly 0. That is, if $a_1, a_2, \ldots, a_i$ are linearly dependent, then $D^{(i)}_{a_1,\ldots,a_i}F(x) = 0$. This limits the number of pairs that can be attempted in a higher order differential attack to the dimension of the vector space and reduces the combinations of differences that can be traced simultaneously. However, this property, and therefore the limits, do not apply for higher order c-derivatives when $c \neq 1$, which can be seen by considering the definition of the c-derivative. If we let $a = 0$, then

$$ {}_cD_0F(x) = F(x + 0) - cF(x) = (1 - c)F(x). $$

Thus, even in the extreme case of zero difference between the input pairs, the c-derivative results in a nonzero function. In higher order c-derivatives this property remains true. For example the 2nd c-derivative has the form

$$ {}_cD^{(2)}_{a_1,a_2}F(x) = F(x + a_1 + a_2) - cF(x + a_2) - cF(x + a_1) + c^2F(x). $$

Even if $a_1 = a_2$ (and thus linearly dependent), the 2nd c-derivative is not identically zero due to the introduction of the c multiplier. This fact increases the input (or output) differences that can be traced through an encryption scheme and potentially increases the vulnerability of a cipher if a c-differential attack is realized in the future.

As for the 1st order derivative, for an (n, m, p)-function we can introduce the *t-order c-differential uniformity* of F at c to be

$$ {}_c\delta^{(t)}_F = \max_{a_1,\ldots,a_t \in \mathbb{F}_{p^n}} {}_cD^{(t)}_{a_1,\ldots,a_t}F(x) = b $$

(if $c = 1$, not all a_i's are allowed to be zero). If $t = 1$, we recover the c-differential uniformity ${}_c\delta^{(1)}_F = {}_c\delta_F$, as defined in [9].

Proposition 3.5. *For any (n, m)-function F, any order $t \in \mathbb{Z}_+$ (positive integers), and any $c \neq 1$, the t-order c-differential uniformity of F is greater than or equal to its $(t-1)$-order c-differential uniformity, $\delta^{(t)}_{F,c} \geq \delta^{(t-1)}_{F,c}$.*

Proof. For any (n, m)-function F and any $c \neq 1$, and taking $a_t = 0$, we obtain that ${}_cD^{(t)}_{a_1,a_2,\ldots,a_{t-1},0}F(x) = (1 - c)\,{}_cD^{(t-1)}_{a_1,a_2,\ldots,a_{t-1}}F(x)$, which implies our claim. □

4 The inverse function

Next we consider an example of a higher order c-derivative and compare it to the traditional higher order derivative (i.e. when $c = 1$). The function we investigate is the multiplicative inverse function over finite fields of characteristic 2, a popular function used in S-boxes that can be represented by a monomial $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^{2^n-2}$. In [9] the authors investigate the first c-derivative of this function, focusing on the newly defined c-differential uniformity property. Specifically, they count the maximum number of solutions of ${}_cD_aF(x) = b$ for some $a, b, c \in \mathbb{F}_{2^n}$. In this section we count solutions to the second order c-differential equation ${}_cD^{(2)}_{a_1,a_2}F(x) = b$ with $c, a_1, a_2, b \in \mathbb{F}_{2^n}$.

The traditional ($c = 1$) second order differential spectrum of the inverse function over $\mathbb{F}_{2^n}$ was recently investigated in [17]. It was shown that for $n \geq 3$ the number of solutions to $D_{a_1,a_2}x^{2^n-2} = b$ is in the set $\{0, 4, 8\}$ and that there are multiple a_1, a_2, b that provide 8 solutions for $n \geq 6$.

With this understanding of the behavior of the second traditional derivative of the inverse function, we now consider the second c-derivative of the inverse function and compare the two. Starting with ${}_cD^{(2)}_{a_1,a_2}F(x) = b$, we have

$$(x + a_1 + a_2)^{2^n-2} + c(x + a_2)^{2^n-2} + c(x + a_1)^{2^n-2} + c^2x^{2^n-2} = b. \qquad (2)$$

It was shown in [9] that the inverse function has a bijective first c-derivative when $c = 0$. Later in [16] we showed that any permutation will have a bijective (i.e. balanced) first c-derivative when $c = 0$. For the second c-derivative of the inverse function, when $c = 0$, we get $(x+a_1+a_2)^{2^n-2} = b$. If $b = 0$, $x = a_1 + a_2$ is the only solution. If $b \neq 0$, then $x \neq a_1 + a_2$ and $\frac{1}{x+a_1+a_2} = b$. Thus, $x = \frac{1}{b} + a_1 + a_2$ is the only solution and we see when $c = 0$ the second c-derivative of the inverse function is a bijection, as is in the case of the first c-derivative when $c = 0$.

In fact, from Theorem 3.2, we see that the nth 0-derivative of a function F is $F(x + a_1 + a_2 + \cdots + a_n)$, which is bijective if and only if F is bijective. Thus permutations have bijective n-th c-derivatives for all n when $c = 0$.

For $c \neq 0$, we consider multiple cases.
Case (i). Let $a_1 = a_2$. Recall this leads to a trivial result in traditional derivatives. Equation (2) becomes $x^{2^n-2} + c^2x^{2^n-2} = b$, that is, $(1 + c^2)x^{2^n-2} = b$. When $b = 0$, $x = 0$ is the only solution. If $b \neq 0$, then $x \neq 0$ and $\frac{1+c^2}{x} = b$ gives us one solution $x = \frac{1+c^2}{b}$.
Case (ii). $a_1 \neq a_2$, and $x = a_1, a_2, a_1 + a_2$, or 0. Equation (2) becomes, respectively,

$$a_2^{2^n-2} + c(a_1 + a_2)^{2^n-2} + c^2a_1^{2^n-2} = b, \text{ or,}$$
$$a_1^{2^n-2} + c(a_1 + a_2)^{2^n-2} + c^2a_2^{2^n-2} = b, \text{ or,}$$

$$ca_2^{2^n-2} + ca_1^{2^n-2} + c^2(a_1+a_2)^{2^n-2} = b, \text{ or,}$$
$$(a_1+a_2)^{2^n-2} + ca_2^{2^n-2} + ca_1^{2^n-2} = b.$$

When $c = 1$ all four of these solutions are the same and can be true simultaneously. However, when $c \neq 1$ we cannot combine all four of these solutions. In fact, the most that can be combined are two. Consider the solutions for a_1 and a_2 (the first two above). If we could combine these, then we would have,

$$a_2^{2^n-2} + c(a_1+a_2)^{2^n-2} + c^2a_1^{2^n-2} = a_1^{2^n-2} + c(a_1+a_2)^{2^n-2} + c^2a_2^{2^n-2},$$

which simplifies to

$$a_2^{2^n-2} + c^2a_1^{2^n-2} = a_1^{2^n-2} + c^2a_2^{2^n-2}, \text{ or,} (1+c^2)a_1^{2^n-2} = (1+c^2)a_2^{2^n-2}.$$

For $c \neq 1$ (which is an assumption throughout), a_1 must equal a_2 which is not true in this case. Therefore, the solutions cannot be combined and we have that no more than three solutions can be true simultaneously.

Now we consider the possibility of combining $x = 0$ with $x = a_1 + a_2$. This gives us

$$ca_2^{2^n-2} + ca_1^{2^n-2} + c^2(a_1+a_2)^{2^n-2} = (a_1+a_2)^{2^n-2} + ca_2^{2^n-2} + ca_1^{2^n-2},$$

which simplifies to $c^2(a_1+a_2)^{2^n-2} = (a_1+a_2)^{2^n-2}$. This is only true when $c = 1$ or $a_1 = a_2$, neither of which are allowed in this case. From this we immediately see that we can combine at most two of the solutions in Case (ii). There are only at most four values of c which allow the combination of two of these solutions. As we have seen, there are only four possible combinations (which in some cases might be equal): $x = 0$ and $x = a_1$, $x = 0$ and $x = a_2$, $x = a_1 + a_2$ and $x = a_1$, and $x = a_1 + a_2$ and $x = a_2$.

Let $x = 0$ and $x = a_1$ be both solutions of the equation above. Then,

$$(a_1+a_2)^{2^n-2} + ca_2^{2^n-2} + ca_1^{2^n-2} = a_2^{2^n-2} + c(a_1+a_2)^{2^n-2} + c^2a_1^{2^n-2}.$$

Rearranging terms, we arrive at

$$(1+c)(a_1+a_2)^{2^n-2} + (1+c)a_2^{2^n-2} + c(1+c)a_1^{2^n-2} = 0,$$

which, since $c \neq 1$, simplifies to $(a_1+a_2)^{2^n-2} + a_2^{2^n-2} + ca_1^{2^n-2} = 0$.

If $a_1 = 0$, then $x = 0$ and $x = a_1$ are the same solution, so we can assume that $a_1 \neq 0$. If $a_2 = 0$, we arrive at the equation $(1+c)a_1^{2^n-2} = 0$, which only has the forbidden solutions $c = 1$ or $a_1 = 0$. We can then assume that $a_1a_2 \neq 0$. The equation becomes then $c(a_1+a_2)a_2 + a_1^2 = 0$, which has a single solution $c_0 = \frac{a_1^2}{(a_1+a_2)a_2}$. It is easy to see that $c_0 = 0$ if and only if $a_1 = 0$. However, it is possible to obtain that $c_0 = 1$ if $a_1^2 + a_2^2 + a_1a_2 = 0$, which is achievable only if n is even and $a_1 = a_2\omega$ or $a_1 = a_2\omega^2$, where

$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. As long as $n \geq 5$, we can always chose valid a_1, a_2 to ensure that $c_0 \neq 1$. By symmetry, $x = 0$ and $x = a_2$ give $c_1 = \frac{a_2^2}{(a_1+a_2)a_1}$, with the same conditions as $x = 0$ and $x = a_1$.

Now, if $x = a_1 + a_2$ and $x = a_1$, then

$$ca_2^{2^n-2} + ca_1^{2^n-2} + c^2(a_1 + a_2)^{2^n-2} = a_2^{2^n-2} + c(a_1 + a_2)^{2^n-2} + c^2a_1^{2^n-2},$$

which, by rearranging, becomes $(1 + c)a_2^{2^n-2} + c(1 + c)a_1^{2^n-2} + c(1 + c)(a_1 + a_2)^{2^n-2} = 0$, and, since $c \neq 1$, this can be simplified to $a_2^{2^n-2} + ca_1^{2^n-2} + c(a_1 + a_2)^{2^n-2} = 0$. If $a_1 = 0$, then we have the case $x = 0, x = a_2$. If $a_2 = 0$, we do not have two different solutions. We can then assume $a_1a_2 \neq 0$. Then, the equation is equivalent to $(a_1 + a_2)a_1 + ca_2^2 = 0$, which has the solution $c_2 = \frac{a_1(a_1+a_2)}{a_2^2}$. It is easy to see that $c_2 \neq 0$, and that $c \neq 1$ under the same conditions as for $x = 0$ and $x = a_1$. By symmetry, $x = a_1 + a_2$ and $x = a_1$ gives $c_3 = \frac{a_2(a_1+a_2)}{a_1^2}$.

Case (iii). $a_1 \neq a_2$, $x \neq a_1, a_2, a_1 + a_2$, or 0. Equation (2) becomes

$$\frac{1}{x + a_1 + a_2} + \frac{c}{x + a_1} + \frac{c}{x + a_2} + \frac{c^2}{x} = b.$$

Multiplying through by $(x + a_1 + a_2)(x + a_1)(x + a_2)x$, collecting and rearranging terms, we arrive at

$$\begin{aligned} bx^4 + \left(1 + c^2\right)x^3 + \left(a_2 + ca_2 + ba_2^2 + a_1 + ca_1 + ba_1^2 + ba_1a_2\right)x^2 \\ + \left(a_1a_2 + ca_2^2 + c^2a_2^2 + ca_1^2 + c^2a_1^2 + c^2a_1a_2 + ba_1a_2^2 + ba_1^2a_2\right)x \\ + c^2a_1a_2(a_1 + a_2) = 0. \end{aligned} \tag{3}$$

This quartic polynomial has at most four solutions when $b \neq 0$ and at most three when $b = 0$. Without the four guaranteed solutions from Case (ii), we cannot reach the 8 solutions possible when $c = 1$. This means that, as in the case of the first c-derivative of the inverse function, when $c \neq 1$ the differential counts *decreases* from the traditional case. In fact, when combining Cases (ii) and (iii), a maximum of 6 solutions is possible, if $c \neq 1$.

Theorem 4.1. *Let $n \geq 4$, and $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$. Then, for any $c \in \mathbb{F}_{2^n} \setminus \{1\}$, ${}_c\delta_F^{(2)} \leq 6$.*

Some computations to demonstrate our findings are captured in Table 1. From here, we see that the maximum is attainable for $n = 8, 9$. We conjecture that it is attainable for all $n \geq 8$.

5 The Gold function

The c-differential uniformity for quadratic functions was characterized in [1], where the authors focus on the PcN and APcN case though their proof

n	$c=1$	$c\neq 1$	$c=0$
4	4	5	1
5	4	4	1
6	8	5	1
7	8	5	1
8	8	6	1
9	8	6	1

Table 1: Maximum number of solutions to ${}_cD^{(2)}_{a_1,a_2}x^{2^n-2}=b$

applies for the general case. In particular from Theorem 3.1 in [1] we can obtain the following result.

Theorem 5.1. *Let $q=p^h$, $F:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be a quadratic function given by*

$$\sum_{i,j} c_{i,j}x^{q^i+q^j}+\sum_l c_l x^{p^l}.$$

Let $\delta=\max_{b\in\mathbb{F}_{p^n}}|F^{-1}(b)|$. Then, for $c\in\mathbb{F}_{p^{\gcd(n,h)}}\setminus\{1\}$, ${}_c\delta_F^{(t)}=\delta$.

Proof. From the proof of Theorem 3.1 in [1], we have that for $c\in\mathbb{F}_{p^{\gcd(n,h)}}\setminus\{1\}$ the c-derivative ${}_cD_aF(x)$ equals

$$(1-c)F\left(x+\frac{a}{1-c}\right)+F(a)-(1-c)F\left(\frac{a}{1-c}\right)=(1-c)F\left(x+\frac{a}{1-c}\right)+\beta,$$

with $\beta=F(a)-(1-c)F\left(\frac{a}{1-c}\right)$. From this we can easily see that for any $a_1,\ldots,a_t$ the higher-order c-derivative of F is

$${}_cD_{a_1,\ldots,a_t}F(x)=(1-c)^tF\left(x+\frac{a_1+\cdots+a_t}{1-c}\right)+\beta',$$

for some constant β' depending on the a_i's, and the claim follows. □

Theorem 5.2. *Let $F(x)=x^{p^k+1}$ on $\mathbb{F}_{p^n}$, and $1\neq c\in\mathbb{F}_{p^n}$. Then, the maximum number of solutions of ${}_cD^{(2)}_{a_1,a_2}F(x)=b$ is $p^{\gcd(k,n)}+1$, and there exist some b,a_1,a_2 such that this bound is obtained.*

Proof. The equation ${}_cD^{(2)}_{a_1,a_2}F(x)=b$ is

$$(x+a_1+a_2)^{p^k+1}-c(x+a_1)^{p^k+1}-c(x+a_2)^{p^k+1}+c^2x^{p^k+1}=b,$$

which renders $(1-2c+c^2)x^{p^k+1}+(a_1+a_2)(1-c)x^{p^k}+(a_1+a_2)^{p^k}(1-c)x+(a_1+a_2)^{p^k+1}-c(a_1^{p^k+1}+a_2^{p^k+1})=b$. Since $c\neq 1$, this yields

$$x^{p^k+1}+\frac{a_1+a_2}{1-c}x^{p^k}+\frac{(a_1+a_2)^{p^k}}{1-c}x+\frac{(a_1+a_2)^{p^k+1}-c(a_1^{p^k+1}+a_2^{p^k+1})}{(1-c)^2}=\frac{b}{(1-c)^2}.$$

Taking $a_2 = -a_1$, this equation becomes $x^{p^k+1} = \frac{b}{(1-c)^2}$, which has at most $\gcd(p^k+1, p^n-1)$ solutions, and exactly $\gcd(p^k+1, p^n-1)$ solutions for some b. This implies that the maximum number of solutions to ${}_cD^{(2)}_{a_1,a_2}F(x) = b$ is lower bounded by $\gcd(p^k+1, p^n-1)$ (also derived from Proposition 3.5).

Taking $a_1 \neq a_2$, and $x = y - \frac{a_1+a_2}{1-c}$, we can write this equation as

$$y^{p^k+1} + (a_1+a_2)^{p^k}\frac{(1-c)^{p^k-1}-1}{(1-c)^{p^k}}y + \frac{a_1^{p^k}a_2 + a_1a_2^{p^k} - b}{(1-c)^2} = 0.$$

If $(1-c)^{p^k-1} = 1$, then we obtain the equation $y^{p^k+1} + \frac{a_1^{p^k}a_2+a_1a_2^{p^k}-b}{(1-c)^2} = 0$, which has at most $\gcd(p^k+1, p^n-1)$ solutions, and exactly $\gcd(p^k+1, p^n-1)$ solutions for some b.

If $(1-c)^{p^k-1} \neq 1$, and $b = a_1^{p^k}a_2 + a_1a_2^{p^k}$, this equation can be written as $y\left(y^{p^k} + (a_1+a_2)^{p^k}\frac{(1-c)^{p^k-1}-1}{(1-c)^{p^k}}\right) = 0$, which has at most $\gcd(p^k, p^n-1)+1 = 2$ solutions, and exactly 2 solutions for some a_1, a_2.

Otherwise, taking $z = \alpha y$, where $\alpha^{p^k} = (a_1+a_2)^{p^k}\frac{(1-c)^{p^k-1}-1}{(1-c)^{p^k}}$ (note that the p^k-root exists since, for any p, $\gcd(p^k, p^n-1) = 1$ and x^{p^k} is therefore a permutation on $\mathbb{F}_{p^n}$), we get the equation $z^{p^k+1} + z + \beta = 0$, where $\beta = \alpha^{-(p^k+1)}\ \frac{a_1^{p^k}a_2+a_1a_2^{p^k}-b}{(1-c)^2}$.

It is easy to see that the equation fulfills the conditions imposed in [4], where it is shown that there are either 0,1,2 or p^d+1 solutions to this equation, where $d = \gcd(k,n)$. Taking $p > 2$, and if $m = \frac{n}{d}$ is even, we have (using [9]) that $\gcd(p^k+1, p^n-1) = p^d+1$. From the results above, this bound is obtained, and we have exactly p^d+1 solutions for the general equation for some a_1, a_2.

If m is odd, for $p \geq 2$, then $m > 2$ since otherwise $n = k$. Then, by [4], the amount of values of β such that there are p^d+1 solutions to the equation is nonzero. Since β is linear on b, the maximum number of solutions taken over all b is p^d+1.

One still has to study the case where $p = 2$ and $m = 2$. In this case, by [9], we have that $\gcd(2^k+1, 2^n-1) = \frac{2^{\gcd(2k,n)}-1}{2^{\gcd(k,n)}-1} = \frac{2^{2d}-1}{2^d-1} = 2^d+1$. So, in that case as well, by the previous results we obtain the bound p^d+1. □

The following corollary implies that, for any odd characteristic, we can always obtain functions whose higher differential uniformity is 2, regardless of the order of differentiation.

Corollary 5.3. *Let $F(x) = x^{p^k+1}$, and let $1 \neq c \in \mathbb{F}_{p^{\gcd(k,n)}}$. Then, the maximum number of solutions to ${}_cD^{(t)}_{a_1,a_2,\ldots,a_t}F(x) = b$ is* $\gcd(p^k+1, p^n-1)$.

Remark 5.4. *It is not difficult to modify the argument to obtain the same outcome as above for the t-order derivative taken with respect to different c's.*

6 Summary and further comments

In this paper we investigate higher order c-differentials, noting that traditional derivatives are a special case of our extension (i.e. when $c = 1$). We also look at the specific case of the inverse function over fields of even characteristic and the Gold function over any characteristic. While many properties of higher order c-differentials are preserved from the traditional higher order derivative, a key difference arises in that the higher order c-derivatives do not require linearly independent input differences. Thus, the higher order c-derivatives we have introduced could potentially allow the use of more input pairs (for encryption or decryption), which in turn could lead to differentials with higher probabilities than traditional higher order differential attacks or the new c-differential attack using one derivative.

References

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

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

[3] E. Biham, A Shamir. *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology 4.1 (1991), 3–72.

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

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

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

[7] R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.

[8] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications* (Ed. 2), Academic Press, San Diego, CA, 2017.

[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] T. Helleseth, A. Kholosha, *On the equation* $x^{2^\ell+1} + x + a = 0$ *over* $GF(2^k)$, Finite Fields Appl. 14 (2008), 159–176.

[11] K. H. Kim, J. Choe, S. Mesnager, *Solving* $x^{q+1} + x + a = 0$ *over Finite Fields*, Finite Fields Appl. 70:6 (2021), 101797.

[12] L. Knudsen *Truncated and higher order differentials*, In Internat. Workshop on Fast Software Encryption (FSE 1994), pp. 196–211. Springer, Berlin, Heidelberg, 1994.

[13] X. Lai *Higher order derivatives and differential cryptanalysis*, In Communications and Cryptography, pp. 227–233, Springer, Boston, MA, 1994.

[14] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.

[15] S. Mesnager, C. Riera, P. Stănică, H. Yan, Z. Zhou *Investigations on c-(almost) perfect nonlinear functions*, IEEE Trans. Inf. Theory, 2021, doi:10.1109/TIT.2021.3081348.

[16] P. Stănică, S. Gangopadhyay, A. Geary, C. Riera, A. Tkachenko *C-Differential Bent Functions and Perfect Nonlinearity*, https://arxiv.org/abs/2006.12535.

[17] D. Tang, B. Mandal, S. Maitra *Further Cryptographic Properties of the Multiplicative Inverse Function*, https://eprint.iacr.org/2020/920.

[18] N. Tokareva, *Bent Functions, Results and Applications to Cryptography*, Academic Press, San Diego, CA, 2015.

[19] Y. Wu, N. Li, X. Zeng *New* P*c*N and AP*c*N *functions over finite fields*, https://arxiv.org/abs/2010.05396.

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