C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity

Pål Ellingsen[*], Patrick Felke[**], Constanza Riera[*], Pantelimon Stănică[***], and Anton Tkachenko[*]

[*]Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, 5020 Bergen, Norway
[**]University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden, Germany
[***]Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216

Abstract

We defined recently [3] a new (output) multiplicative differential, and the corresponding c-differential uniformity, which is first characterized via a convolution of Walsh transforms. With this new differential concept, even for characteristic 2, there are perfect c-nonlinear (PcN) functions. We looked at some of the known classes of perfect nonlinear (PN) functions and show that only one remains a PcN function, under a different condition on the parameters. Surprisingly, the p-ary Gold PN function increases its c-differential uniformity significantly, under some conditions on the parameters. We then characterize the c-differential uniformity of the inverse function (in any dimension and characteristic).

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables and denote the set of all such functions by $\mathcal{B}_n$. For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)},$$

where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

An (n, m)-*function* (often called a *vectorial Boolean function* if there is no need to explicitly specify the dimensions n and m) is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. When $m = n$, it can be represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$) of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i,\ a_i \in \mathbb{F}_{2^n}$. The algebraic degree of the function is then the largest Hamming weight of an exponent i, with $a_i \neq 0$. For an (n, m)-function F, we define the Walsh transform $W_F(a, b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}.$$

For an (n, n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a, b) = |\{x \in \mathbb{F}_{2^n} : F(x+a)+F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F = \delta$, then we say that F is differentially δ-uniform. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function.

At the Fast Software Encryption (FSE 2002) conference, N. Borisov, M. Chew, R. Johnson, D. Wagner used a new type of differential that is quite useful for the cryptanalysis of ciphers that utilize modular multiplication as a primitive operation. It is an extension of a type of differential cryptanalysis and it was used to cryptanalyse some existing ciphers (like a variant of the well-known IDEA cipher).

Inspired by the previously mentioned successful attempt, we started a theoretical analysis of an (output) multiplicative differential. Given 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

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

(Note that, if $c = 1$, then we obtain the usual derivative, and, if $c = 0$ or $a = 0$, then we obtain a shift of the function.) For an (n,n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let ${}_c\Delta_F(a,b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - cF(x) = b\}$. We call the quantity

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

(surely, including $a = 0$ for the case $c \neq 1$, the equation $F(x) - cF(x) = b$ is of course, $F(x) = b(1-c)^{-1}$, so we are looking here at how close F is to a permutation polynomial, and similarly in the case $c = 0$ for any a) the *c-differential uniformity* of F. If ${}_c\Delta_F = \delta$, then we say that F is differentially (c,δ)-uniform. 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, one wonders whether they can exist for $p = 2$ for $c \neq 1$, and we shall argue later that that is actually true). 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.

In the work [3] we first characterized the c-differential uniformity of a function via a generalized convolution of Walsh transforms. As particular examples, we show that if m, n are fixed positive integers and $c \in \mathbb{F}_{p^m}$, $c \neq 1$, F is an (n,m)-function, then

$$\sum_{\substack{u \in \mathbb{F}_{p^n} \\ v \in \mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2 \geq p^{3n+m},$$

with equality if and only if F is a perfect c-nonlinear (PcN) function; Furthermore, we have

$$\begin{aligned} &\sum_{\substack{u_1,u_2 \in \mathbb{F}_{p^n} \\ v_1,v_2 \in \mathbb{F}_{p^m}}} \overline{\mathcal{W}_F}(u_1+u_2, v_1+v_2)\mathcal{W}_F(u_1+u_2, c(v_1+v_2)) \\ &\qquad \cdot \overline{\mathcal{W}_F}(u_1,v_1)\overline{\mathcal{W}_F}(u_2,v_2)\mathcal{W}_F(u_1,cv_1)\mathcal{W}_F(u_2,cv_2) \\ &\geq 3 \cdot p^{m+n} \sum_{\substack{u \in \mathbb{F}_{p^n} \\ v \in \mathbb{F}_{p^m}}} |\mathcal{W}_F(u,v)|^2 |\mathcal{W}_F(u,cv)|^2 - 2 \cdot p^{2(2n+m)}, \end{aligned}$$

with equality if and only if F is an almost perfect c-nonlinear (APcN).

We then proceeded to investigate some of the known perfect nonlinear functions. We therefore show the following major theorem [3].

Theorem 1 *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the monomial $F(x) = x^d$, and $c \neq 1$ be fixed. The following statements hold:*

(i) If $d = 2$, then F is APcN, for all $c \neq 1$.

(ii) If $d = p^k + 1$, $p > 2$, then F is not PcN, for all $c \neq 1$. Moreover, when $(1-c)^{p^k-1} = 1$ and $n/\gcd(n,k)$ is even, the c-differential uniformity ${}_c\Delta_F \geq p^g + 1$, where $g = \gcd(n,k)$.

(iii) Let $p = 3$. If $d = \dfrac{3^k+1}{2}$, then F is PcN, for $c = -1$ if and only if $\dfrac{n}{\gcd(n,k)}$ is odd.

(iv) If $p = 3$ and $F(x) = x^{10} - ux^6 - u^2x^2$, the c-differential uniformity of F is ${}_c\Delta_F \geq 2$.

We then looked at the inverse function, which is APN for n odd and has differential uniformity 4 for n even and show the next two theorems [3].

Theorem 2 *Let n be a positive integer, $1 \neq c \in \mathbb{F}_{2^n}$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(x) = x^{2^n-2}$. We have:*

(i) If $c = 0$, then F is PcN (that is, F is a permutation polynomial).

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

(iii) If $c \neq 0$ and $\mathrm{Tr}_n(1/c) = 0$, or $\mathrm{Tr}_n(c) = 0$, the c-differential uniformity of F is 3.

Theorem 3 *Let p be an odd prime, $n \geq 1$ be a positive integer, $1 \neq c \in \mathbb{F}_{p^n}$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the inverse p-ary function defined by $F(x) = x^{p^n-2}$. We have:*

(i) If $c = 0$, then F is PcN (that is, F is a permutation polynomial).

(ii) If $c \neq 0, 4, 4^{-1}$, $(c^2 - 4c) \in (\mathbb{F}_{p^n})^2$, or $(1 - 4c) \in (\mathbb{F}_{p^n})^2$, the c-differential uniformity of F is 3.

(iii) If $c = 4, 4^{-1}$, the c-differential uniformity of F is 2 (and hence F is APcN).

(iv) If $c \neq 0$, $(c^2 - 4c) \notin (\mathbb{F}_{p^n})^2$ and $(1 - 4c) \notin (\mathbb{F}_{p^n})^2$, the c-differential uniformity of F is 2 (and hence F is APcN).

The computational data on c-differential uniformity presented in [3] on the Gold and Kasami cases prompted more investigation and a first step was taken in [5] with a complete description of the Gold case, as well as an investigation of some of the APN entries from the Helleseth-Rong-Sandberg table [4].

It would be quite interesting to continue with some of the other entries in the table [4], Dobbertin et al. [2] further examples, or even newer PN or APN classes of functions, through the prism of the newly defined c-differentials concept we introduced in [3].

References

[1] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds) Fast Software Encryption. FSE 2002. Lecture Notes in Computer Science, vol 2365. Springer, Berlin, Heidelberg, 2002.

[2] H. Dobbertin, D. Mills, E. N. Muller, A. Pott, and W. Willems, *APN functions in odd characteristic*, Discr. Math. 267 (1-3) (2003), 95–112.

[3] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory, 2020.

[4] T. Helleseth, C. Rong, D. Sandberg, *New families of almost perfect nonlinear power mappings*, IEEE Trans. Inf. Theory 45 (1999), 475–485.

[5] C. Riera, P. Stănică, *Investigations on c-(almost) perfect nonlinear functions*, manuscript, 2020.