Dillon's switching method generalized to c-differentials

Chunlei Li[1], Constanza Riera[2], Pantelimon Stănică[3]

[1] Department of Informatics, University of Bergen,
5020, Bergen, Norway; chunlei.li@uib.no
[2]Department of Computer Science, Electrical Engineering
and Mathematical Sciences,
Western Norway University of Applied Sciences,
5020 Bergen, Norway; csr@hvl.no
[3] Department of Applied Mathematics, Naval Postgraduate School
Monterey, CA 93943-5212, U.S.A.; pstanica@nps.edu

Abstract

In this paper we generalize Dillon's switching method to characterize the exact c-differential uniformity of functions constructed via this method. More precisely, we modify some PcN/APcN and other functions with good c-differential uniformity in a controllable number of coordinates to render more such functions. We present several applications of the method in constructing PcN and APcN functions with respect to all $c \neq 1$. As a byproduct, we generalize a result of [10]. Computational results rendering functions with low differential uniformity, as well as, other good cryptographic properties are sprinkled throughout the paper.

Keywords. Boolean functions, differential uniformity, c-differential uniformity, (almost) perfect nonlinearity

1 Background

As customary, for a positive integer n and prime p, we let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ (for $a \neq 0$, by $\frac{1}{a}$ we mean the inverse of a). Further, let $\mathbb{F}_p^m$ denote the m-dimensional vector space over $\mathbb{F}_p$. The cardinality of a set S is denoted by $\#S$. We call a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ a *Boolean* (for $p = 2$) or *p-ary* (for $p > 2$) *function* on n variables. For $m \,|\, n$, we let the *relative trace* be defined by $\mathrm{Tr}_{p^n/p^m}(x) = \mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{mi}}$. When $m = 1$, we will denote this *absolute trace* by Tr_n (abusing notation, for $q = p^t$, where $t > 0, n \geq 2$ are integers, we will denote by Tr_n the absolute trace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, when the base field $\mathbb{F}_q$ is

clear from the context). 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 $\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - \mathrm{Tr}_n(ux)}$, where $\zeta_p = e^{\frac{2\pi i}{p}}$ is a primitive p-th root of unity. For an (n, n)-function F (that is, a function from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$) and for $a, b \in \mathbb{F}_{p^n}$, we let the Walsh transform $\mathcal{W}_F(a, b)$ of F be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^n(bF(x))$ at a, that is, $\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(bF(x) - ax)}$. 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 $p^{n/2}$. A p-ary (or vectorial function) f is called *plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, p^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{F}_{p^n}$ for a fixed integer s depending on f (we also call f then *s-plateaued*).

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* [4] of F with respect to $a \in \mathbb{F}_{p^n}$ is the function ${}_cD_aF(x) = F(x + a) - cF(x)$, for all $x \in \mathbb{F}_{p^n}$. Note that, if $c = 1$, then we obtain the usual derivative, which we denote by D_a, 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 ${}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$ and

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

be the *c-differential uniformity* (cDU) of F. If ${}_c\Delta_F = \delta$, then we say that F is differentially (c, δ)-uniform. If $\delta = 1$, then F is a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as proven in [4], there exist PcN functions for $p = 2$, for all $c \neq 1$). If $\delta = 2$, then F is an *almost perfect c-nonlinear* (*APcN*) function. When we specify the constant c for which the function is PcN or APcN, then we may use the notation c-PN, or c-APN. We note 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. There has been a flurry of papers on this topic in the last few years and we just mention [4, 5, 6, 8, 9, 10, 11, 12], for the interested reader.

In this paper we extend Dillon's switching method (see [2, 3]) to c-differentials, and apply it to find necessary and sufficient conditions for such a constructed function to be PcN or APcN, as well as to generalize it to any c-differential uniformity. A side note, but very important, is that, since the c-differential uniformity is not invariant under the CCZ-equivalence, an approach to improve the c-differential uniformity of a classical PN/APN function whose c-differential uniformity is not very good (like the Gold function) is to "switch" it via a Boolean/p-ary linearized function, and *decrease*, if possible, its c-differential uniformity while preserving its classical differential uniformity. This theme occurs in some of our results, though we push the method a lot further by also constructing other low c-differential functions from known ones.

Proofs of the results are not included here due to lack of space, but they will be included in the full paper, among other results.

2 The c-switching method

We first recall the *switching method* introduced by Dillon [2] and pushed further by Edel and Pott [3] (there are several proofs of this result besides the original one; we point to [1] for a very detailed argument).

Dillon's Switching Method. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function, $u \in \mathbb{F}_{2^n}^*$, $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function, and $H(x) = F(x) + u\, f(x)$. Then H is an APN function if and only if $D_a f(x) + D_a f(y) = 0$, whenever $D_a F(x) + D_a F(y) = u$, for all $a \neq 0, x, y \in \mathbb{F}_{2^n}$.*

Below, we generalize the switching method to characterize the PcN functions constructed by changing only some components. We will use the univariate representation, as it is more convenient in this context. We will write the theorem for any characteristic p. Throughout this paper, $q = p^t$, where p is a prime and $t > 0, n \geq 2$ are integers.

Theorem 1. *Let $u_i \in \mathbb{F}_{q^n}^*$, $1 \leq i \leq k$, be a PcN function $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $f_i : \mathbb{F}_{q^n} \to \mathbb{F}_q$, and $H^{(k)}(x) = F(x) + \sum_{i=1}^k u_i f_i(x)$. Then $H^{(k)}$ is not PcN if and only if, for some $a \in \mathbb{F}_{q^n}$, there exist $x \neq y$ such that ${}_cD_a f_i(x) - {}_cD_a f_i(y) = \epsilon_i$, $1 \leq i \leq k$, whenever ${}_cD_a F(x) - {}_cD_a F(y) = -\sum_{i=1}^k u_i \epsilon_i$, $\epsilon_i \in \{\alpha - c\beta \,|\, \alpha, \beta \in \mathbb{F}_q\}$ (not all ϵ_i are zero), $1 \leq i \leq k$.*

As an example, for $n = 5$, $H(x) = x^3 + \mathrm{Tr}_3(gx^3)$, where g is a primitive element of $\mathbb{F}_{2^5}$, is an APN permutation (optimal) on $\mathbb{F}_{2^5}$, which is plateaued with nonlinearity 12 (optimal); and the cDU is either 5 or 6 for all values of c. Further, $H(x) = x^5 + \mathrm{Tr}_6(x^9)$ on $\mathbb{F}_{2^6}$ is a 4-differentially uniform permutation for $c = 1$, PcN for two other values of c, and has cDU=5 for all other values of c, in addition to being plateaued and having nonlinearity 24 (optimal, bent concatenation bound).

Remark 2. *We can rewrite the previous theorem in a "positive" manner, by describing the PcN property in lieu of the negation. For example, $H^{(1)}$ is PcN if and only if ${}_cD_a f(x) - {}_cD_a f(y) \neq \epsilon$, whenever ${}_cD_a F(x) - {}_cD_a F(y) = -\epsilon\, u$, where $\epsilon \in \{\alpha - c\beta \,:\, \alpha, \beta \in \mathbb{F}_q, \alpha - c\beta \neq 0\}$.*

Remark 3. *Note that the proof of the theorem also implies that, if F is PcN, $H^{(1)}$ has c-differential uniformity at most q^2 for $c \notin \mathbb{F}_q$ and at most q for $c \in \mathbb{F}_q$.*

It is rather interesting that we can easily construct new PcN functions from old ones, via our Theorem 1, and we record that construction below. In addition, we generalize [10, Theorem 5].

Theorem 4. *Let $q = p^t$ be a power of a prime p, $n > 2$, and $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a PcN function for some $c \in \mathbb{F}_q$, and let $u, v \in \mathbb{F}_{q^n}$ with $\mathrm{Tr}_{q^n/q}(-uv) \neq 1$. Then $H(x) = F(x) + u\mathrm{Tr}_{q^n/q}(vF(x))$ is PcN with respect to c.*

For example, we obtain that $x^{\frac{3^k+1}{2}} + u\mathrm{Tr}_n\left(vx^{\frac{3^k+1}{2}}\right)$ is PcN on $\mathbb{F}_{3^n}$ for $c = -1$, when $\mathrm{Tr}_{q^n/q}(-uv) \neq 1$, $\gcd(k, n) = 1$ and n is odd. Another example is $x^5 + g^2\mathrm{Tr}_3(gx^5)$ on $\mathbb{F}_{3^3}$, where g is a primitive element of $\mathbb{F}_{3^3}$, which is a 4-differentially uniform (with respect to $c = 1$) permutation and PcN (with respect to $c = -1$), and $cDU = 5$ for all $c \neq \pm 1$.

We can generalize Theorem 1 to any c-differential uniformity.

Theorem 5. *Let $u_i \in \mathbb{F}_{q^n}^*$, $1 \leq i \leq k$, $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be a (at most) (c, δ)-uniform function, $f_t : \mathbb{F}_{q^n} \to \mathbb{F}_q$, and $H^{(k)}(x) = F(x) + \sum_{t=1}^k u_t f_t(x)$. Then $H^{(k)}$ has c-differential uniformity ${}_c\Delta_{H^{(k)}} > \delta$ if and only if, for some $a \in \mathbb{F}_{q^n}$, there exist at least elements $x_1, x_2, \ldots, x_{\delta+1}$ (not all belonging to the same set $A_{a,\epsilon}$) such that, for all $i \neq j$, $a \in \mathbb{F}_{q^n}$, if ${}_cD_aF(x_i) - {}_cD_aF(x_j) = -\sum_{t=1}^k u_t\epsilon_t$ then ${}_cD_af_t(x_i) - {}_cD_af_t(x_j) = \epsilon_t$, where $\epsilon_t \in \{\alpha - c\beta : \alpha, \beta \in \mathbb{F}_q, \alpha - c\beta \neq 0\}$.*

For example, some functions with good c-differential uniformity and good cryptographic properties for odd characteristics p can be found using our theorems above are, for $p = 3$, $x^{\frac{p^2+3}{2}} + g\mathrm{Tr}(g^ix)$ $(i = 0, 1)$ (which is PN $(c = 1)$ and cDU=4 for all other c's, and has 6 values Walsh spectrum, $n = 4, 5, 6$), and, for $p = 5$, $x^{\frac{p+1}{2}} + g\mathrm{Tr}(x)$ (which is APN, cDU=5, 8 values Walsh spectrum, for $n = 2$; for $n = 3$, APN, 9 values Walsh spectrum, cDU$\in \{5, 7\}$; for $n = 4$, APN, cDU$\in \{8, 9\}$, 9 values Walsh spectrum).

In [7], polynomials of the form $x + \left(\mathrm{Tr}_{q^n/q^m}(x)^k + \gamma\right)^s$ and $x + \left(\mathrm{Tr}_{q^n/q^m}(x)^{k_1} + \gamma\right)^{s_1} + \left(\mathrm{Tr}_{q^n/q^m}(x)^{k_2} + \gamma\right)^{s_2}$, where $m|n$, are shown to be permutation polynomials (mostly, for $n = 2m$). We show the following result, which in some instances will reprove some results of [7] (recall that PcN with respect to $c = 0$ is simply the permutation property).

Theorem 6. *Let p be a prime number, m, n positive integers such that $m \,|\, n$ and $p \,|\, \frac{n}{m}$, $1 \leq t \in \mathbb{Z}_{>0}$, $u \in \mathbb{F}_{p^m}^*$, $\delta_i \in \mathbb{F}_{p^m}$, $1 \leq k_i, s_i \leq p^n - 1$, $1 \leq i \leq t$, and L a linearized permutation polynomial on $\mathbb{F}_{q^n}$. Then, the functions $H(x) = L(x) + u\sum_{i=1}^t \left(\mathrm{Tr}_{q^n/q^m}(x)^{k_i} + \delta_i\right)^{s_i}$ are PcN, with respect to all $c \in \mathbb{F}_{p^m} \setminus \{1\}$.*

References

[1] R. C. R. Carranza, *Construction of New Differentially δ–Uniform Families*, Ph.D. Dissertation, University of Puerto Rico, Rio Piedras, 2020.

[2] J. F. Dillon, *APN polynomials: an update*, In International Conference on Finite Fields and Applications – Fq9, 2009.

[3] Y. Edel, A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. 3:1 (2009), 59–81.

[4] 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.

[5] S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields*, Designs Codes Crypt. 89 (2021), 221–239.

[6] A. C. Geary, *C-differentials and generalized cryptographic properties of vectorial Boolean and p-ary functions*, Ph.D. Dissertation, Naval Postgraduate School, 2022.

[7] Z. Li, M. Wang, J. Wu, X. Zhu, *Some new forms of permutation polynomials based on the AGW criterion*, Finite Fields Applic. 61 (2020), 101584.

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

[9] X. Wang, D. Zheng, *Several classes of PcN power functions over finite fields*, 2021, `https://arxiv.org/pdf/2104.12942.pdf`.

[10] Y. Wu, N. Li, X. Zeng, *New PcN and APcN functions over finite fields*, Designs Codes Crypt. 89 (2021), 2637–2651.

[11] H. Yan, *On* (-1)*-differential uniformity of ternary APN power functions*, Cryptogr. Commun. 2 (2022), 357–369.

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