The c-differential uniformity of some classes of permutation polynomials

Kirpa Garg[*], Sartaj Ul Hasan[*], and Pantelimon Stănică[**]

[*]Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India
[**]Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

Abstract

The notion of c-differential uniformity has recently received a lot of popularity because of its potential applications in cryptography (we point out that a connection with difference sets in some quasigroups is already realized for perfect c-nonlinear functions). The construction of functions, especially permutations, with low c-differential uniformity is an interesting problem in this area, and recent work has focused heavily in this direction. We provide a few classes of permutation polynomials with low c-differential uniformity. The technique we use involves handling Weil sums, as well as analyzing various equation in finite fields, and we believe these can be of independent interest.

1 Introduction

Let p be a prime number and n be a positive integer. We denote by $\mathbb{F}_q$ the finite field with q elements, by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$ and by $\mathbb{F}_q[X]$ the ring of polynomials in one variable X with coefficients in $\mathbb{F}_q$, where $q = p^n$. Let F be a function from $\mathbb{F}_q$ to itself. Lagrange's interpolation formula allows us to uniquely represent F as a polynomial in $\mathbb{F}_q[X]$ of degree at most $q-1$. A polynomial $F \in \mathbb{F}_q[X]$ is a permutation polynomial of $\mathbb{F}_q$ if the mapping $X \mapsto F(X)$ is a permutation of $\mathbb{F}_q$. It is worth emphasising that due to their numerous applications in coding theory [4, 5], combinatorial design theory [6], cryptography [14, 18], and other branches of mathematics and engineering, permutation polynomials over finite fields are highly significant objects. These functions, for instance, are frequently used in cryptography to construct substitution boxes (S-boxes), which are a key component of contemporary block ciphers.

There are many known attacks on block ciphers. One of the most powerful attacks on block ciphers is differential cryptanalysis, which was first developed by Biham and Shamir [2]. The concept of differential uniformity was first introduced by Nyberg [16] to measure a function's resistance to the differential attack, and it is defined as follows. For any function $F : \mathbb{F}_q \to \mathbb{F}_q$ and for any $a \in \mathbb{F}_q$, the derivative of F in the direction a is defined as $D_F(X, a) := F(X + a) - F(X)$ for all $X \in \mathbb{F}_q$. The Difference Distribution Table (DDT) entry of F at a point $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, denoted by $\Delta_F(a, b)$, is the number of solutions $X \in \mathbb{F}_q$ of the equation $D_F(X, a) = b$. The differential uniformity of F, denoted by Δ_F, is given by $\Delta_F := \max\{\Delta_F(a, b) : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$. When $\Delta_F = 1$, F is called perfect nonlinear (PN) function. When $\Delta_F = 2$, F is called almost perfect nonlinear (APN) function. It should be noted that there are no PN functions over finite fields with even characteristic.

The multiplicative differentials of the form $(F(cX), F(X))$ were introduced by Borisov et al. [3] who exploited this new class of differential to attack certain existing ciphers. Ellingsen et al. [7] extended on the idea of differential uniformity and developed a new (output) multiplicative differential as a result of the multiplicative differential. For any function $F : \mathbb{F}_q \to \mathbb{F}_q$ and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of F with respect to a is defined as

${}_c\Delta_F(X,a) := F(X+a) - cF(X)$ for all $X \in \mathbb{F}_q$. For any $a, b \in \mathbb{F}_q$, the c-Difference Distribution Table (c-DDT) entry ${}_c\Delta_f(a,b)$ at point (a,b) is the number of solutions $X \in \mathbb{F}_q$ of the equation ${}_cD_f(X,a) = b$. The c-differential uniformity of F, denoted by ${}_c\Delta_F$, is given by ${}_c\Delta_F := \max\{{}_c\Delta_F(a,b) : a, b \in \mathbb{F}_q \text{ and } a \neq 0 \text{ if } c = 1\}$. It is clear that when $c = 1$, differential uniformity and c-differential uniformity are same. We refer to F as a perfect c-nonlinear (PcN) function and an almost perfect c-nonlinear (APcN) function, respectively, for $c = 1$ and $c = 2$. Though an extension of the differential attack has not been realized, yet, we want to point out that in a recent manuscript [1], the graph of a PcN function was shown to correspond to a difference set in a quasigroup. Difference sets give rise to symmetric designs, which are known to construct optimal self complementary codes. Various types of designs can be also used in secret sharing and visual cryptography (see also [24, 25], where it is shown that difference sets can be used to construct a complex vector codebook that achieves the Welch bound on maximum crosscorrelation amplitude).

Finding functions, particularly permutations, with low c-differential uniformity has received a lot of interest since the concept of c-differential uniformity was established. In [8, 15, 22, 23, 26], numerous functions with low c-differential uniformity were investigated. Only a few PcN and APcN functions are known over a finite field with even characteristic; see, for example, [9, 11, 17, 21]. Recently, Li et al. [12] extended Dillon's switching method to c-differentials and applied 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. Further, using this technique, the authors give some classes of PcN and APcN functions as well. In this paper, we study the c-differential uniformity of some classes of permutation polynomials introduced in [13]. The paper is organised as follows. In Section 2, we recall some relevant results that are required in the subsequent sections. The c-differential uniformity of two classes of permutation polynomials over finite fields of even characteristic has been considered in Section 3. However, the Section 4 deals with c-differential uniformity of a class of permutation polynomials over finite fields of characteristic 3. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section, we first review a definition and provide some lemmas to be used later. In what follows, we shall use Tr_m^n to denote the (relative) trace function from $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, i.e., $\mathrm{Tr}_m^n(X) = \sum_{i=0}^{n-m} X^{p^i}$, where m and n are positive integers and $m|n$. When $m = 1$, we use Tr to denote the absolute trace.

Definition 2.1 [10] *For a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_p$, the Walsh transform of F at $v \in \mathbb{F}_{p^n}$, is defined as*

$$\mathcal{W}_F(v) = \sum_{X \in \mathbb{F}_{p^n}} \omega^{F(X) - \mathrm{Tr}(vX)},$$

where $\omega = e^{\frac{2\pi i}{p}}$ is a complex primitive pth root of unity.

Lemma 2.2 [13, Proposition 4] *For a positive integer m and a fixed δ in $\mathbb{F}_{2^{3m}}$, the polynomial*

$$F(X) = (X^{2m} + X + \delta)^s + X$$

is a permutation of $\mathbb{F}_{2^{3m}}$ if one of the following conditions holds:

(1) $s = 2^{2m} + 1$;

(2) $s = 2^{im-1} + 2^{m-1}, \gcd((i-1)m - 1, 3m) = 1, i \in \{2, 3\}$.

Lemma 2.3 [13, Proposition 3] *For an even positive integer m and a fixed $\delta \in \mathbb{F}_{3^{2m}}$, the polynomial*

$$F(X) = (X^{3m} - X + \delta)^{3^{2m-1}+2(3^{m-1})} + X$$

is a permutation of $\mathbb{F}_{3^{2m}}$.

Lemma 2.4 [12, Theorem 12] *Let $q = 2$, $k \geq 1$, and L be a q-linearized permutation polynomial such that $L(-1) = -1$. Let $G_{k_1 \leq k_2 \leq \cdots \leq k_s}(X) = L(X) + \prod_{i=1}^{s} (\alpha_i \mathrm{Tr}_m^n(X^{2^{k_i}+1} + \delta_i))^{g_i}$, $g_i \in \mathbb{N}$, $\delta_i \in \mathbb{F}_{2^n}$, $\alpha_i \in \mathbb{F}_{2^m}^*$, $1 \leq k_i \leq n-1$ on $\mathbb{F}_{2^n}, n \geq 3$. Then $G_{k_1 \leq k_2 \leq \cdots \leq k_s}$ is either PcN or APcN with respect to all $c \neq 1$, and PcN for $c = 0$.*

The following lemma can be inferred from the proof of [10, Proposition 2].

Lemma 2.5 *Let $n = 2m$ and $a_i \in \mathbb{F}_{p^n} (i = 0, \cdots, m)$ for an odd prime p. Then the absolute square of Walsh transform coefficient of the function $f : X \mapsto \mathrm{Tr}\left(\sum_{i=0}^{m} a_i X^{p^i+1}\right)$ at $-v \in \mathbb{F}_{p^n}$ is given by*

$$|\mathcal{W}_f(-v)|^2 = \begin{cases} p^{n+\ell} & \text{if } f(X) + \mathrm{Tr}(vX) \equiv 0 \text{ on } Ker(L); \\ 0 & \text{otherwise,} \end{cases}$$

where ℓ is dimension of kernel $Ker(L)$ of the linearized polynomial $L(X) = \sum_{i=0}^{m} (a_i X^{p^i} + a_i X^{p^{n-i}})$.

We also recall that in [20], the authors computed the c-DDT entries by means of the Weil sums approach. We will quickly go over the general technique for expressing the number of solutions to a given equation over finite fields in terms of Weil sums for the reader's convenience. Let $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ be the canonical additive character of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(X) := \exp\left(\frac{2\pi i \mathrm{Tr}(X)}{p}\right).$$

It is easy to observe (see, for instance [19]) that the number of solutions $(X_1, X_2, \ldots, X_n) \in \mathbb{F}_q^n$ of the equation

$$F(X_1, X_2, \ldots, X_n) = b,$$

denoted by $N(b)$, is given by

$$N(b) = \frac{1}{q} \sum_{X_1, X_2, \ldots, X_n \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi_1(\beta(F(X_1, X_2, \ldots, X_n) - b)). \tag{2.1}$$

The expression from Equation (2.1), as well as very delicate investigation of the involved equations over finite fields, are some of the methods we used to prove some our results on the computation of the c-differential uniformity of a few permutations over finite fields.

3 Permutations over $\mathbb{F}_{2^n}$ with low c-differential uniformity

In this section, we first deal with the computation of the c-differential uniformity of $F(X) = (X^{2m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$. From Lemma 2.2, we know that F is a permutation polynomial over $\mathbb{F}_{2^n}$. Here we find conditions on c and δ for which F turns out to be either a PcN or an APcN function. Notice that in our case, $F(X) = L(X) + \mathrm{Tr}_m^{3m}(X^{2^m+1} + 1)$, where $L(X) = X^2 + \mathrm{Tr}_m^{3m}(X)$. As L is a non-permutation over $\mathbb{F}_{2^n}$ with $L(1) = 0$, our case is different from the function discussed in Lemma 2.4. Moreover, the method developed in [12] cannot be used to treat our class of functions.

Theorem 3.1 *Let $F(X) = (X^{2^m} + X + \delta)^{2^{2m}+1} + X$ over $\mathbb{F}_{2^n}$, where $n = 3m$ and $\delta \in \mathbb{F}_{2^n}$. Let $\Gamma_1 := \{\delta \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^{3m}(\delta) = 1\}$. Then:*

(1) *F is PcN for all $c \in \mathbb{F}_{2^m} \setminus \{1\}$ and for all $\delta \in \mathbb{F}_{2^n}$;*

(2) *F is APcN for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \Gamma_1$;*

(3) *F is of c-differential uniformity 4 for all $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and for all $\delta \in \mathbb{F}_{2^n} \setminus \Gamma_1$.*

In the following theorem, we discuss the c-differential uniformity of another class of permutation polynomial given in Lemma 2.2 depending on where the values of c and δ lie. As one observes, the considered permutations display very good c-differential properties, here and in the next section.

Theorem 3.2 . *Let* $F(X) = (X^{2^m} + X + \delta)^{2^{im-1}+2^{m-1}} + X$ *over* $\mathbb{F}_{2^n}$, *where* $n = 3m, \delta \in \mathbb{F}_{2^n}$ *and* $\gcd((i-1)m - 1, 3m) = 1, i \in \{2, 3\}$. *Let* $\Gamma_0 := \{\delta \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^{3m}(\delta) = 0\}$. *Then*:

(1) F *is PcN for all* $c \in \mathbb{F}_{2^m} \setminus \{1\}$ *and for all* $\delta \in \mathbb{F}_{2^n}$;

(2) F *is APcN for all* $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ *and for all* $\delta \in \Gamma_0$;

(3) F *is of c-differential uniformity* 4 *for all* $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ *and for all* $\delta \in \mathbb{F}_{2^n} \setminus \Gamma_0$.

4 Permutations over $\mathbb{F}_{3^n}$ with low c-differential uniformity

In the preceding section, we studied the c-differential uniformity of some classes of permutation polynomials over fields of even characteristic. However, in this section, we discuss the c-differential uniformity of permutations over fields of odd characteristic. It is clear from Lemma 2.3 that the polynomial $F(X) = (X^{3^m} - X + \delta)^{3^{2^m-1}+2\cdot 3^{m-1}} + X$ is a permutation over $\mathbb{F}_{3^n}$, where $\delta \in \mathbb{F}_{3^n}$ and $n = 2m$, and we compute the c-differential uniformity of this permutation in the following theorem.

Theorem 4.1 *Let* $F(X) = (X^{3^m} - X + \delta)^{3^{2^m-1}+2\cdot 3^{m-1}} + X$ *over* $\mathbb{F}_{3^n}$, *where* $n = 2m$ *and* $\delta \in \mathbb{F}_{3^n}$. *Let* $\Gamma_0 := \{\delta \in \mathbb{F}_{2^n} : \mathrm{Tr}_m^{2m}(\delta) = 0\}$. *Then*:

(1) F *is PcN for all* $c \in \mathbb{F}_{3^m} \setminus \{1\}$ *and for all* $\delta \in \mathbb{F}_{3^n}$;

(2) F *is PcN for all* $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ *and for all* $\delta \in \Gamma_0$. *Moreover, it is of c-differential uniformity* 3 *for all* $c \in \mathbb{F}_{3^n} \setminus \mathbb{F}_{3^m}$ *and for all* $\delta \in \mathbb{F}_{3^n} \setminus \Gamma_0$.

5 Conclusion

We have studied the c-differential uniformity of three classes of permutation polynomials over fields, and it turns out that they are of low c-differential uniformity. Moreover, we prove that under what conditions these permutation polynomials are indeed PcN or APcN.

References

[1] N. Anbar, T. Kalayci, W. Meidl, C. Riera, P. Stănică, *On the combinatorial structure of c-differentials*, manuscript; Preliminary version presented at the Ernst Selmer International Workshop, August 2022.

[2] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptol. 4:1 (1991), 3–72.

[3] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In International Workshop on Fast Software Encryption (pp. 17-33). Springer, Berlin, Heidelberg (2002).

[4] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory,* Finite Fields Appl. 13 (2007), 58–70.

[5] C. Ding, T. Helleseth, *Optimal ternary cyclic codes from monomials,* IEEE Trans. Inf. Theory 59 (2013), 5898–5904.

[6] C. Ding, J. Yuan, *A family of skew Hadamard difference sets,* J. Comb. Theory, Ser. A 113 (2006) 1526–1535.

[7] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *c-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity,* IEEE Trans. Inf. Theory 66:6 (2020), 5781–5789.

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

[9] S. U. Hasan, M. Pal, P. Stănică, *On the c-differential uniformity and boomerang uniformity of two classes of permutation polynomials*, IEEE Trans. Inf. Theory 68 (2022), 679–691.

[10] T. Helleseth, A. Kholosha, *Monomial and quadratic bent functions over the finite fields of odd characteristic.* IEEE Trans. Inf. Theory 52, no. 5 (2006), 2018–2032.

[11] J. Jeong, N. Koo, S. Kwon, *On non-monomial APcN permutations over finite fields of even characteristic*, arXiv (2022). `https://arxiv.org/abs/2205.11418`.

[12] C. Li, C. Riera, P. Stănică, *Low c-differentially uniform functions via an extension of Dillon's switching method*, arXiv (2022). `https://arxiv.org/abs/2204.08760`.

[13] L. Li, S. Wang, C. Li, X. Zeng, *Permutation polynomials* $(x^{p^m}-x+\delta)^{s_1}+(x^{p^m}-x+\delta)^{s_2}+x$ *over* $\mathbb{F}_{p^n}$*,* Finite Fields Appl. 51 (2018), 31–61.

[14] R. Lidl, W.B. Mullen, *Permutation polynomials in RSA-cryptosystems,* in: Advances in Cryptology, Plenum, New York, 1984, pp. 293–301.

[15] S. Mesnager, C. Riera, P. Stănică, H. Yan, and Z. Zhou, *Investigations on c-(Almost) Perfect Nonlinear Functions*, IEEE Trans. Inf. Theory 67:10 (2021), 6916–6925.

[16] K. Nyberg, *Differentially uniform mappings for cryptography,* In T. Helleseth (ed), Advances in Cryptology-EUROCRYPT'93, 765 55–64, Springer, Heidelberg (1994).

[17] M. Pal *Some new classes of (almost) perfect c-nonlinear permutations*, arXiv (2022). `https://arxiv.org/pdf/2208.01004`

[18] J. Schwenk, K. Huber, *Public key encryption and digital signatures based on permutation polynomials,* Electron. Lett. 34 (1998), 759–760.

[19] P. Stănică, *Using double Weil sums in finding the c-boomerang connectivity table for monomial functions on finite fields,* Appl. Algebra Eng. Commun. Comput. (2021), `https://doi.org/10.1007/s00200-021-00520-9`.

[20] P. Stănică, C. Riera, A. Tkachenko, *Characters, Weil sums and c-differential uniformity with an application to the perturbed Gold function*, Cryptogr. Commun. (2021), `https://doi.org/10.1007/s12095-021-00485-z`.

[21] Z. Tu, X. Zeng, Y. Jiang, X. Tang, *A class of APcN power functions over finite fields of even characteristic*, `https://arxiv.org/abs/2107.06464v1`

[22] X. Wang, D. Zheng, L. Hu, *Several classes of PcN power functions over finite fields*, Discrete Applied Mathematics 322 (2022), 1710–182.

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

[24] P. Xia, S. Zhou, G. B. Giannakis, *Achieving the Welch Bound with Difference Sets*, IEEE Trans. Inf. Theory 51:5 (2005), 1900–1907.

[25] P. Xia, S. Zhou, G. B. Giannakis, *Correction to "Achieving the Welch bound with difference sets"*, IEEE Trans. Inf. Theory 52:7 (2006), 3359.

[26] Z. Zha, L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Des. Codes Cryptogr., vol. 89, pp.1193-1210, (2021).