The (generalized) boomerang uniformity of some classes of functions over finite fields

Sartaj Ul Hasan*, Mohit Pal*, 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

We give a general result that associates the entries of the c-boomerang connectivity table of an arbitrary function to double Weil sums over finite fields. We then use our general result to compute simple expressions for the entries of the (classical) boomerang connectivity table of the binary Gold function. Moreover, we investigate the c-boomerang uniformity of perfect nonlinear Dembowski-Ostrom polynomials, perfect c-nonlinear functions and almost perfect c-nonlinear functions.

1 Introduction

In 1999, Wagner [14] proposed the boomerang attack on block ciphers. The theoretical tool (Boomerang Connectivity Table (BCT) of a permutation F) to analyze this attack was introduced at Eurocrypt 2018 by Cid et al. [4]. Recently, thereafter, Boura and Canteaut [2] further studied BCT and defined a new parameter called boomerang uniformity, the maximum value in the BCT. Based upon a recent c-differential concept, one of us [12] generalized the concept of BCT and boomerang uniformity using this new differential. Here, we analyze some further classes for their c-boomerang uniformity.

As usual, let p be a prime and n be a positive integer. We denote by $\mathbb{F}_q$ the finite field with $q = p^n$ elements and by $\mathbb{F}_q^*$, the multiplicative cyclic group of nonzero elements of $\mathbb{F}_q$. Since they are used in the design of substitution boxes (S-boxes) of block ciphers, permutation polynomials have been the object of intense investigation. The security of S-boxes depends on its resistance against the known attacks, such as the differential attack, boomerang attack, to name just a few. To measure the resistance against the differential attack, the concept of differential uniformity was introduced in the following way.

Let F be an (n, n)-function, $F : \mathbb{F}_q \to \mathbb{F}_q$. For any $a, b \in \mathbb{F}_q$, let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_q \mid F(x + a) - F(x) = b\}$. Then $\Delta_F(a, b)$ is called the (a, b)-th entry of the Difference Distribution Table (DDT) of $F(x)$ and the value $\delta_F = \max\{\Delta_F(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}$, is called the *differential uniformity* of F. When $\delta_F = 1$, we call F to be *perfect nonlinear* (PN) function and if $\delta_F = 2$, F is called *almost perfect nonlinear* (APN) function. The S-boxes with low differential uniformity provide the optimal resistance against the differential attack. In [5], the notion of c-differentials was introduced (see also [1] for a particular quasi-planar case $c = -1$): the (*multiplicative*) *c-derivative* of F with respect to $a \in \mathbb{F}_q$ is the function

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

The entries of the c-Difference Distribution Table (c-DDT) are

$$ {}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_q : F(x + a) - cF(x) = b\}, $$

and

$$ \delta_{F,c} = \max\left\{ {}_c\Delta_F(a, b) \,|\, a, b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1 \right\}, $$

is the *c-differential uniformity* (cDU) of F. It is interesting to note that the standard cipher [8], Kuznyechik, has the cDU of its inverse equal to 120. Perhaps an attack can be mounted using that observation.

We now go back to introducing the Boomerang Connectivity Table, as well as the boomerang uniformity. For a permutation $F : \mathbb{F}_q \to \mathbb{F}_q$ and $a, b \in \mathbb{F}_q$, we let $\mathcal{B}_F(a,b) = \#\{x \in \mathbb{F}_q \mid F^{-1}(F(x+a)+b) - F^{-1}(F(x)+b) = a\}$ be the (a,b)-th entry of the Boomerang Connectivity Table (BCT) and the value $\beta_F = \max\{\mathcal{B}_F(a,b) \mid a, b \in \mathbb{F}_q^*\}$ be the boomerang uniformity of F. Later, Li et. al [9] gave an equivalent definition to compute BCT, which does not involve the compositional inverse of the function F, allowing one to define/compute the BCT and the boomerang uniformity of non-permutation functions. Recently, the third-named author [12] generalized these two concepts. If one restricts to permutations, the notion simply looks at the probability of the propagations $cF(x)+b$ and $c^{-1}F(x+a)+b$, being the same constant a, as the propagation of the input, under the inverse S-box.

Definition 1.1 *Let F be a function from $\mathbb{F}_q$ to itself and $c \in \mathbb{F}_q^*$. Then the entries of the c-BCT at $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$, denoted by ${}_c\mathcal{B}_F(a,b)$ is the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the (c-boomerang) system*

$$\begin{cases} F(x) - cF(y) = b \\ F(x+a) - c^{-1}F(y+a) = b. \end{cases} \tag{1}$$

The c-boomerang uniformity of F is defined as $\beta_{F,c} = max\ \{{}_c\mathcal{B}_F(a,b) \mid a, b \in \mathbb{F}_q^*\}$.

We note that for power map $F(x) = x^d$, it is sufficient to consider $a = 1$ in (1), and c-boomerang uniformity of F is $\beta_{F,c} = \max\{{}_c\mathcal{B}_F(1,b) \mid b \in \mathbb{F}_q^*\}$.

Boura and Canteaut [2] showed that the BCT table is preserved under the affine equivalence but not under the extended affine equivalence (and consequently under the CCZ-equivalence). It is quite natural to ask a similar question in the context of c-BCT. It is straightforward to see that in the case of even characteristic, c-BCT and c^{-1}-BCT entries of an (n,n)-function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are the same under the transformations $x \mapsto x+a$ and $y \mapsto y+a$, since the c-boomerang system

$$\begin{cases} F(x) + cF(y) = b \\ F(x+a) + c^{-1}F(y+a) = b \end{cases} \implies \begin{cases} F(x) + c^{-1}F(y) = b \\ F(x+a) + cF(y+a) = b. \end{cases}$$

Further, we argue in the full paper that the c-BCT is not preserved under the (output applied) affine equivalence, however, if the affine transformation is applied to the input, that is, $G(x) = (F \circ L)(x)$, then the c-BCT spectrum is preserved, as was the case for the c-differential uniformity.

After the definitions and preliminary results from Section 2, we state in Section 3 a general result that associates the entries of the c-boomerang connectivity table of an arbitrary function to double Weil sums over finite fields. We use it to obtain explicit expressions for the classical BCT entries of the binary Gold function in Section 3. Section 4 deals with the PN Dembowski-Ostrom polynomials, as well as some PcN/APcN functions over $\mathbb{F}_q$, for $c = \pm 1$.

2 Preliminaries

In this section, we shall first recall some results concerning Weil sums. The *canonical additive character* is a (additive group) homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$, $\chi_1(x) = \exp\left(\frac{2\pi i \operatorname{Tr}(x)}{p}\right)$, where $\mathbb{C}$ is the field of complex numbers and $\operatorname{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace defined by $\operatorname{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}$ (to emphasize the dimension, we sometimes write this as Tr_1^n). We define the relative trace $\operatorname{Tr}_e : \mathbb{F}_{p^n} \to \mathbb{F}_{p^e}, e|n$, by $\operatorname{Tr}_e(x) = x + x^{p^e} + x^{p^{2e}} + \cdots + x^{p^{e(\frac{n}{e}-1)}}$. Note that all additive characters of $\mathbb{F}_q$ can be expressed in terms of χ_1 [10, Theorem 5.7]. For each $0 \le k \le q-2$, the k-th multiplicative character is a (multiplicative group) homomorphism $\psi_k : \mathbb{F}_q \to \mathbb{C}$, $\psi_k\left(g^\ell\right) = \exp\left(\frac{2\pi i k\ell}{q-1}\right)$ for $\ell = 0, \ldots, q-2$. It is well-known that the group of

multiplicative characters of $\mathbb{F}_q$ is a cyclic group of order $q-1$ with identity element ψ_0 [10, Corollary 5.9].

In the theory of finite fields, exponential sums are important tools in the study of number of solutions of equations over finite fields. As a special case, the Gauss' sums are defined as follows $G(\psi,\chi) = \sum_{x\in\mathbb{F}_q^*} \psi(x)\chi(x)$, where χ and ψ are additive and multiplicative characters of $\mathbb{F}_q$, respectively. A Weil sum is yet another important character sum defined as follows $\sum_{x\in\mathbb{F}_q} \chi(F(x))$, where χ is an additive character of $\mathbb{F}_q$ and $F(x)$ is a polynomial in $\mathbb{F}_q[x]$. To explicitly evaluate Weil sums is often quite difficult and some results are known only for a few families of polynomials. Recall the following lemmas.

Lemma 2.1 [10, Theorem 6.37] *Let $\mathbb{F}_q$ be a finite field. For $b \in \mathbb{F}_q^*$, the number N of the solutions of the diagonal equation $a_1{x_1}^{d_1} + a_2{x_2}^{d_2} + \cdots + a_k{x_k}^{d_k} = b$ in $\mathbb{F}_q^k$ satisfies*

$$|N - q^{k-1}| \le [(e_1-1)\cdots(e_k-1) - (1-q^{-1/2})M(e_1,e_2,\ldots,e_k)]q^{(k-1)/2}, \tag{2}$$

where $e_i = \gcd(d_i, q-1)$ and $M(e_1,e_2,\ldots,e_k)$ is the number of k-tuples $(j_1,j_2,\ldots,j_k) \in \mathbb{Z}^k$ such that $1 \le j_i \le e_i - 1$ and $\frac{j_1}{e_1} + \frac{j_1}{e_1} + \cdots + \frac{j_k}{e_k} \in \mathbb{Z}$ for $1 \le i \le k$.

An upper bound for the c-boomerang uniformity of the power map x^d can be easily obtained from [13, Theorem 1] and is given by $\beta_{F,c} \le \frac{\delta_{F,c}+\delta_{F,c^{-1}}}{p^n} + p^{2n} - 2$. Notice that, a bound on the c-boomerang uniformity of the power maps can also be obtained from Lemma 2.1, which is $q+(e-1)(e-2)\sqrt{q}+e-1$, where $e=\gcd(d,q-1)$. This bound is better than the one obtained from Lemma 2.1 if $\gcd(d,n)$ is small, but it is weaker if $\gcd(d,n)$ is rather large.

3 The c-BCT entries and double Weil sums

One of us showed in [13] a general theorem expressing the entries in the c-BCT ($c \neq 0$) of power function x^d in terms of double Weil sums. Here, we shall slightly extend that result.

Theorem 3.1 *Let $F(x)$ be an arbitrary function on $\mathbb{F}_q$ and $c \in \mathbb{F}_q^*$. Then, for fixed $a,b \in \mathbb{F}_q^*$, the c-BCT entry ${}_c\mathcal{B}_F(a,b)$ at (a,b) is given by*

$$\frac{1}{q}\left(\sum_{w\in\mathbb{F}_q} ({}_c\Delta_F(w,b) +_{c^{-1}} \Delta_F(w,b))\right) - 1 + \frac{1}{q^2}\sum_{\alpha,\beta\in\mathbb{F}_q^*} \chi_1(-b(\alpha+\beta))\, S_{\alpha,\beta}\, S_{-\alpha c,-\beta c^{-1}},$$

with

$$\begin{aligned} S_{\alpha,\beta} &= \sum_{x\in\mathbb{F}_q} \chi_1\left(\alpha F(x) + \beta F(x+a)\right) \\ &= \frac{1}{(q-1)^2}\sum_{j,k=0}^{q-2} G(\bar{\psi}_j,\chi_1)G(\bar{\psi}_k,\chi_1) \sum_{x\in\mathbb{F}_q} \psi_1\left((\alpha F(x))^j(\beta F(x+a))^k\right). \end{aligned}$$

Using the general result above, we shall now give explicit expressions for the c-BCT entries of the binary Gold function x^{2^k+1} over $\mathbb{F}_{2^n}$, for all $c \neq 0$. Recall that the c-boomerang uniformity of a power function $F(x)=x^d$ over $\mathbb{F}_{2^n}$ is given by $\max\{{}_c\mathcal{B}_F(1,b) \mid b \in \mathbb{F}_{2^n}^*\}$, where ${}_c\mathcal{B}_F(1,b)$ is the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$, $q=2^n$, of the following system

$$\begin{cases} x^d + cy^d = b \\ (x+1)^d + c^{-1}(y+1)^d = b. \end{cases} \tag{3}$$

As in [13], for $b \neq 0$ and fixed $c \neq 0$, the number of solutions $(x,y) \in \mathbb{F}_q^2$ of (3) is

$${}_c\mathcal{B}_F(1,b) = \frac{1}{q^2}\sum_{x,y\in\mathbb{F}_q}\sum_{\alpha\in\mathbb{F}_q} \chi_1\left(\alpha\left(x^d + cy^d + b\right)\right)\sum_{\beta\in\mathbb{F}_q} \chi_1\left(\beta\left((x+1)^d + c^{-1}(y+1)^d + b\right)\right)$$

$$= \frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q} \chi_1 \left(b\left(\alpha+\beta\right)\right) S_{\alpha,\beta} S_{c\alpha,c^{-1}\beta}, \text{ where } S_{\alpha,\beta} = \sum_{x \in \mathbb{F}_q} \chi_1 \left(\alpha x^d + \beta(x+1)^d\right).$$

Therefore, the problem of computing the c-BCT entry ${}_c\mathcal{B}_F(1,b)$ is reduced to the computation of the product of the Weil sums $S_{\alpha,\beta}$ and $S_{c\alpha,c^{-1}\beta}$. When $d = 2^k+1$, the Gold case, we further simplify the expression for $S_{\alpha,\beta}$ as follows:

$$\begin{aligned} S_{\alpha,\beta} &= \sum_{x \in \mathbb{F}_q} \chi_1 \left(\alpha x^{2^k+1} + \beta(x+1)^{2^k+1}\right) = \chi_1(\beta) \sum_{x \in \mathbb{F}_q} \chi_1((\alpha+\beta)x^{2^k+1}) \ \chi_1((\beta^{2^{n-k}}x)^{2^k} + \beta x) \\ &= \chi_1(\beta) \sum_{x \in \mathbb{F}_q} \chi_1((\alpha+\beta)x^{2^k+1} + (\beta^{2^{n-k}}+\beta)x) = \chi_1(\beta) \sum_{x \in \mathbb{F}_q} \chi_1(Ax^{2^k+1} + Bx), \end{aligned}$$

where $A = \alpha+\beta$ and $B = \beta^{2^{n-k}} + \beta$. When $c = 1$, we further simplify ${}_c\mathcal{B}_F(1,b)$ and establish a relation between differential uniformity and boomerang uniformity of the Gold function. Nyberg [11, Proposition 3] showed that the differential uniformity of the Gold function $x \mapsto x^{2^k+1}$ over $\mathbb{F}_{2^n}$ is 2^e, where $e = \gcd(k,n)$. Also, from [4], we know that the boomerang uniformity of the APN function equals 2. Boura and Canteaut [2, Proposition 8] proved that when n/e is odd and $n \equiv 2 \pmod 4$, then the differential as well as the boomerang uniformity of the Gold function $x \mapsto x^{2^k+1}$ is 4. The following theorem we showed in [6] generalizes the two previously mentioned results, and gives the boomerang uniformity of the Gold function for any parameters, when $\frac{n}{e}$ is odd.

Theorem 3.2 *Let $F(x) = x^{2^k+1}$, $1 \le k < n$, be a function on $\mathbb{F}_q$, $q = 2^n$, $n \ge 2$. Let $c = 1$ and n/e be odd, where $e = \gcd(k,n)$. Then the c-BCT entry ${}_1\mathcal{B}_F(1,b)$ of F at $(1,b)$ is ${}_1\mathcal{B}_F(1,b) = 0, 2^e$, if $\mathrm{Tr}_e\left(b^{\frac{1}{2}}\right) = 0$, respectively, $\mathrm{Tr}_e\left(b^{\frac{1}{2}}\right) \neq 0$.*

We can also find a bound for the c-BU for p and n/d odd, for some c.

Theorem 3.3 *Let $c \in \mathbb{F}_{p^d} \backslash \{0,1,-1\}$ and n/d be odd. Then the c-BU of the Gold function $x^{p^\ell+1}$ over $\mathbb{F}_q$ is $\beta_{F,c} \le q$.*

We can use Theorem 3.1 to compute the c-BCT entries of a general linearized polynomial $L(x)$. For any fixed $c \neq 0$, we let

$$\mathcal{U}_c = \{\alpha, \beta \in \mathbb{F}_q^* \mid \tilde{L}(\alpha+\beta) = 0 = \tilde{L}(-c\alpha - c^{-1}\beta)\},$$

where $\tilde{L}(x) = \sum_{i=0}^{n-1} (a_i x)^{p^{n-i}}$ be the companion polynomial of $L(x)$.

Theorem 3.4 *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$ be a linearized polynomial over the finite field $\mathbb{F}_q$ and $c \in \mathbb{F}_q^*$. For $a, b \in \mathbb{F}_q^*$, the c-BCT entry ${}_c\mathcal{B}_L(a,b)$ is given by*

$$\frac{1}{q} \sum_{w \in F_q} \left({}_c\Delta_L(w,b) + {}_{c^{-1}}\Delta_L(w,b)\right) - 1 + \sum_{\alpha,\beta \in \mathcal{U}_c} \chi_1(-b(\alpha+\beta)) \chi_1\left(L(a)\beta(1-c^{-1})\right).$$

Consequently, the c-BU of L is ${}_c\mathcal{B}_L(a,b) \le {}_c\Delta_L + {}_{c^{-1}}\Delta_L + |\mathcal{U}_c| - 1$. Moreover, this value occurs at every (a,b), $b \neq L(a)(1-c^{-1})$ such that $\mathcal{U}_c$ is embedded in the line of slope $\frac{b}{L(a)(1-c^{-1})-b}$, passing through the origin (in the (α,β)-plane).

4 Further results and comments

In the full paper, we show that the c-boomerang uniformity of Dembowski-Ostrom (DO) polynomials over the finite field $\mathbb{F}_q$, namely $F(x) = \sum_{i,j} \alpha_{ij} x^{p^i+p^j}$, is zero, if they happen to be

perfect nonlinear, thus showing that the result of [4, Lemma 1], that is, for $p = 2$ and all (a, b), $\Delta_F(a, b) \leq \mathcal{B}_F(a, b)$, a result that will not hold in odd characteristic.

Though not phrased this way in the paper, the authors of [7, Proposition 3.4] showed that the (-1)-differential uniformity of a PN DO polynomial is 2. Here, we further show that the (-1)-boomerang uniformity of a PN DO polynomial is 2. It is known that the boomerang uniformity (for $c = 1$) of APN functions matches their differential uniformity. Here, we show that if $c = -1$, then the cBU of a PcN is zero and the one of an even APcN is 2.

Certainly, the c-boomerang uniformity is yet another differential characteristic, in addition to being an interesting mathematical concept, and, we believe, it deserves attention.

References

[1] D. Bartoli, M. Timpanella, *On a generalization of planar functions*, J. Algebr. Comb. 52 (2020), 187–213.

[2] C. Boura, A. Canteaut, *On the boomerang uniformity of cryptographic Sboxes,* IACR Trans. Symmetric Cryptol. 3 (2018), 290–310.

[3] J.S. Chahal, S.R. Ghorpade, *Carlitz-Wan conjecture for permutation polynomials and Weil bound for curves over finite fields*, Finite Fields Appl. 54 (2018), 366–375.

[4] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, *Boomerang connectivity table: a new cryptanalysis tool*. Advances in Cryptology- EUROCRYPT 2018, Lecture Notes in Computer Science, vol.10821. New York: Springer-Verlag, 2018, pp. 683–714.

[5] 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.

[6] S. Ul Hasan, M. Pal, P. Stănică, *The binary Gold function and its c-boomerang connectivity table*, manuscript.

[7] W. Jia, X.Y. Zeng, C. Li, T. Helleseth, L. Hu, *Permutation polynomials with low differential uniformity over finite fields of odd characteristic.* Sci China Math, 56 (2013), 1429–1440.

[8] Kuznyechik cipher, `https://datatracker.ietf.org/doc/rfc7801/`.

[9] K. Li, L. Qu, B. Sun, C. Li, *New results about the boomerang uniformity of permutation polynomials*, IEEE Trans. Inf. Theory 65(11) (2019), 7542–7553.

[10] R. Lidl, H. Niederreiter, FiniteFields (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge, 1997.

[11] K. Nyberg, *Differentially uniform mappings for cryptography.* In: Helleseth T. (eds.) Advances in Cryptology-EUROCRYPT 1993. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol 765 (1994), 55–64.

[12] P. Stănică, *Investigations on c-boomerang uniformity and perfect nonlinearity*, `https://arxiv.org/abs/2004.11859`, 2020.

[13] P. Stănică, *Using double Weil sums in finding the Boomerang and the c-Boomerang Connectivity Table for monomial functions on finite fields*, `https://arxiv.org/abs/2007.09553`, 2020.

[14] D. Wagner, *The boomerang attack*. Proc. Int. Workshop Fast Soft. Encryption, Mar. 1999, pp. 156–170.

[15] G. Weng, X. Zeng, *Further results on planar DO functions and commutative semifields*, Des. Codes Cryptogr. 63 (2012), 413–423.