Cryptography and Communications
https://doi.org/10.1007/s12095-022-00573-8

# The binary Gold function and its *c*-boomerang connectivity table

**Sartaj Ul Hasan**[1] · **Mohit Pal**[1] · **Pantelimon Stănică**[2]

Received: 17 October 2021 / Accepted: 11 March 2022


**Abstract**
Here, we give a complete description of the entire *c*-Boomerang Connectivity Table for the Gold function over finite fields of even characteristic, by using double Weil sums. As a by-product, we generalize a result of Boura and Canteaut (IACR Trans. Symmetric Cryptol. 2018(3) : 290–310, 2018) for the classical boomerang uniformity (see also the extended abstract by Eddahmani and Mesnager at the Boolean Functions and their Applications (BFA 2021) conference).

**Keywords** Finite fields · Double Weil sums · Boomerang uniformity · *c*-boomerang uniformity

**Mathematics Subject Classification (2010):** 12E20 · 11T24 · 11T06 · 94A60

## 1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where $p$ is a prime and $n$ is a positive integer. The multiplicative cyclic group of nonzero elements of the finite field is denoted by $\mathbb{F}_q^* = \langle g \rangle$, where $g$ is a primitive element of $\mathbb{F}_q$. The *canonical additive character* is a homomorphism $\chi_1 : \mathbb{F}_q \to \mathbb{C}$ of the additive group of $\mathbb{F}_q$ defined as follows

$$\chi_1(x) = \exp\left(\frac{2\pi i \operatorname{Tr}(x)}{p}\right),$$

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

✉ Sartaj Ul Hasan
sartaj.hasan@iitjammu.ac.in

Mohit Pal
2018RMA0021@iitjammu.ac.in

Pantelimon Stănică
pstanica@nps.edu

[1] Department of Mathematics, Indian Institute of Technology Jammu, Jammu 181221, India

[2] Applied Mathematics Department, Naval Postgraduate School, 93943 Monterey, USA

sometimes write this as $\mathrm{Tr}_1^n$). We define the relative trace $\mathrm{Tr}_e : \mathbb{F}_{p^n} \to \mathbb{F}_{p^e}, e|n$, by $\mathrm{Tr}_e(x) = x + x^{p^e} + x^{p^{2e}} + \cdots + x^{p^{e(\frac{n}{e}-1)}}$. Note that all additive characters of $\mathbb{F}_q$ can be expressed in terms of $\chi_1$ [12, Theorem 5.7].

A Weil sum is an important character sum defined as follows

$$\sum_{x \in F_q} \chi(F(x)),$$

where $\chi$ is an additive character of $\mathbb{F}_q$ and $F$ is a polynomial in $\mathbb{F}_q[x]$. It is well-known that a polynomial $F(x)$ over finite field $\mathbb{F}_q$ is a permutation polynomial (PP) if and only if its Weil sum $\sum_{x \in \mathbb{F}_q} \chi(F(x)) = 0$ for all nontrivial additive characters $\chi$ of $\mathbb{F}_q$. Permutation polynomials are a very important class of polynomials as they have applications in coding theory and cryptography, especially in the substitution boxes (S-boxes) of the block ciphers. The security of the S-boxes relies on certain properties of the function $F(x)$, e.g., its differential uniformity, boomerang uniformity, nonlinearity etc.

Recently, Cid et al. [4] introduced a "new tool" for analyzing the boomerang style attack proposed by Wagner [21]. This new tool is usually referred to as Boomerang Connectivity Table (BCT). Boura and Canteaut [2] further studied BCT and coined the term boomerang uniformity, which is essentially the maximum value in the BCT. Li et al. [13] provided new insights in the study of BCT and presented an equivalent technique to compute BCT, which does not require the compositional inverse of the permutation polynomial $F(x)$ at all. In fact, Li et al. [13] also gave a characterization of BCT in terms of Walsh transform and gave a class of permutation polynomial with boomerang uniformity 4.

Recently, Stănică [16] extended the notion of BCT and boomerang uniformity. In fact, he defined what he termed as $c$-BCT and $c$-boomerang uniformity for an arbitrary polynomial function $F$ over $\mathbb{F}_q$ and for any $c \in \mathbb{F}_q^*$, in the following way. For $a, b \in \mathbb{F}_q$, the entry of the $c$-Boomerang Connectivity Table ($c$-BCT) at $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, denoted by ${}_c\mathcal{B}_F(a, b)$, is the number of solutions in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ of the following system

$$\begin{cases} F(x) - cF(y) = b \\ F(x + a) - c^{-1}F(y + a) = b. \end{cases} \tag{1.1}$$

The $c$-boomerang uniformity of $F$ is defined as

$$\beta_{F,c} = \max_{a,b \in \mathbb{F}_{p^n}^*} {}_c\mathcal{B}_F(a, b).$$

In yet other recent papers, Stănică [17, 18] further studied the $c$-BCT for the swapped inverse function and also gave an elegant description of the $c$-BCT entries of the power map in terms of double Weil sums. He further simplified his expressions for the Gold function $x^{p^k+1}$ over $\mathbb{F}_{p^n}$, for all $1 \le k < n$ and $p$ odd. In this paper, we shall complement the work of [18] to the finite fields of even characteristic ($p = 2$). As argued also in [18], while the Weil sums expressions may seem complicated from a theoretical perspective, they do have the advantage of being easily implementable. In fact, a simple Sage implementation achieved for all taken examples a speed up of more than 10 times for the current approach versus the Walsh transform or solutions counting approaches. Moreover, on the theoretical side, we generalize a result of Nyberg [15, Proposition 3], as well as a result of Boura and Canteaut [2, Proposition 8] on the classical boomerang uniformities of the Gold function (independently, Eddahmani and Mesnager [7] also explicitly determined the $c$-BCT entries of the permutation Gold functions using a different approach in the particular case of $c = 1$).

The paper is structured as follows. Section 2 contains some preliminary results that will be used throughout. Section 3 contains the characterization of $c$-BCT entries in terms of double Weil sums. For $c = 1$, we further simplify this expression in Section 4. In fact, Theorem 4.1 generalizes previously known results of Boura and Canteaut [2]. In Section 5, we consider the case when $c \in \mathbb{F}_{2^e} \backslash \{0, 1\}$, where $e = \gcd(k, n)$. In Section 6, we discuss the general case. Finally, in Section 7, we discuss the affine, extended affine and CCZ-equivalence as it relates to $c$-boomerang uniformity.

## 2 Preliminaries

We begin this section by first recalling the recent notion of $c$-differentials introduced in [8]. We shall assume that $q = 2^n$ for rest of the paper. For an $(n, n)$-function $F : \mathbb{F}_q \to \mathbb{F}_q$, and $c \in \mathbb{F}_q$, we define the (*multiplicative*) *c-derivative* of $F$ with respect to $a \in \mathbb{F}_q$ to be the function

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

Further, for $a, b \in \mathbb{F}_q$, we let the entries of the $c$-Difference Distribution Table ($c$-DDT) be defined by ${}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_q : F(x + a) - cF(x) = b\}$. We call the quantity

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

the *c-differential uniformity* of $F$. Note that the case $c = 1$ corresponds to the usual notion of differential uniformity. The interested reader may refer to [1, 9, 11, 14, 19, 20, 22] for some recent results concerning $c$-differential uniformity. It has been proved recently [10] that the differential uniformity is not necessarily smaller than the boomerang uniformity (for non-permutations), as it was previously shown for permutations.

The following theorem is a "binary" analogue of [18, Theorem 1], which gives a nice connection between $c$-BCT and $c$-DDT entries of the power map $x^d$ over $\mathbb{F}_{2^n}$.

**Theorem 2.1** *Let $F(x) = x^d$ be a power function on $\mathbb{F}_q$, $q = 2^n$ and $c \in \mathbb{F}_q^*$. Then, for fixed $b \in \mathbb{F}_q^*$, the c-Boomerang Connectivity Table entry ${}_c\mathcal{B}_F(1, b)$ at $(1, b)$ is given by*

$$ \frac{1}{q}\left( \sum_{w \in \mathbb{F}_q} ({}_c\Delta_F(w, b) + {}_{c^{-1}}\Delta_F(w, b)) \right) - 1 + \frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q, \alpha\beta \neq 0} \chi_1(b(\alpha + \beta))\, S_{\alpha,\beta}\, S_{\alpha c, \beta c^{-1}}, $$

*with*

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

*where $\chi_1$ is the canonical additive character of the additive group of $\mathbb{F}_q$, $\psi_k$ is the k-th multiplicative character of the multiplicative group of $\mathbb{F}_q$ and $G(\psi, \chi)$ is the Gauss sum.*

We shall now state some lemmas that will be used in the sequel. The following lemma is well-known and has been used in various contexts.

**Lemma 2.2** *Let* $e = \gcd(k, n)$. *Then*

$$= \gcd(2^k + 1, 2^n - 1) = \begin{cases} 1 & \text{if } n/e \text{ is odd,} \\ 2^e + 1 & \text{if } n/e \text{ is even.} \end{cases}$$

We shall also use the following lemma, which appeared in [5], describing the number of roots in $\mathbb{F}_{2^n}$ of a linearized polynomial $u^{2^k}x^{2^{2k}} + ux$, where $u \in \mathbb{F}_{2^n}^*$.

**Lemma 2.3** [5, *Theorem* 3.1] *Let* $g$ *be a primitive element of* $\mathbb{F}_{2^n}$ *and let* $e = \gcd(n, k)$. *For any* $u \in \mathbb{F}_{2^n}^*$ *consider the linearized polynomial* $L_u(x) = u^{2^k}x^{2^{2k}} + ux$ *over* $\mathbb{F}_{2^n}$. *Then for the equation* $L_u(x) = 0$, *the following are true*:

(1) *If* $n/e$ *is odd, then there are* $2^e$ *solutions to this equation for any choice of* $u \in \mathbb{F}_{2^n}^*$;
(2) *If* $n/e$ *is even and* $u = g^{t(2^e+1)}$ *for some* $t$, *then there are* $2^{2e}$ *solutions to the equation*;
(3) *If* $n/e$ *is even and* $u \neq g^{t(2^e+1)}$ *for any* $t$, *then* $x = 0$ *is the only solution*.

The explicit expression for the Weil sum of the form $\sum_{x\in\mathbb{F}_{2^n}} \chi_1(ux^{2^k+1} + vx)$, where $u, v \in \mathbb{F}_{2^n}$, is obtained in [5]. In what follows, we shall denote the Weil sum $\sum_{x\in\mathbb{F}_q} \chi(ux^{2^k+1} + vx)$ by $\mathfrak{S}(u, v)$. The following lemma gives the explicit expression for $\mathfrak{S}(u, 0)$.

**Lemma 2.4** [5] *Let* $\chi$ *be any nontrivial additive character of* $\mathbb{F}_q$ *and* $g$ *be the primitive element of the cyclic group* $\mathbb{F}_q^*$. *The following hold*:

(1) *If* $n/e$ *is odd, then*

$$\sum_{x\in\mathbb{F}_q} \chi(ux^{2^k+1}) = \begin{cases} q & \text{if } u = 0, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *Let* $n/e$ *be even so that* $n = 2m$ *for some integer* $m$. *Then*

$$\sum_{x\in\mathbb{F}_q} \chi(ux^{2^k+1}) = \begin{cases} (-1)^{m/e}2^m & \text{if } u \neq g^{t(2^e+1)} \text{ for any integer } t, \\ (-1)^{\frac{m}{e}+1}2^{m+e} & \text{if } u = g^{t(2^e+1)} \text{ for some integer } t. \end{cases}$$

From Lemma 2.2, it is easy to see that when $n/e$ is odd, the power map $x^{2^k+1}$ permutes $\mathbb{F}_{2^n}$. Therefore if $u \neq 0$, there exists a unique element $\gamma \in \mathbb{F}_q^*$ such that $\gamma^{2^k+1} = u$ and hence

$$\begin{aligned}\mathfrak{S}(u,v) &= \sum_{x\in\mathbb{F}_q} \chi(ux^{2^k+1} + vx)\\ &= \sum_{x\in\mathbb{F}_q} \chi(x^{2^k+1} + v\gamma^{-1}x)\\ &= \mathfrak{S}(1, v\gamma^{-1}).\end{aligned}$$

The following lemma gives the expression for the Weil sum $\mathfrak{S}(1,v)$ for $v\neq 0$ and $n/e$ odd.

**Lemma 2.5** [5, *Theorem* 4.2] *Let $v\neq 0$ and $n/e$ be odd. Then*

$$\mathfrak{S}(1,v) = \begin{cases} 0 & \text{if } \mathrm{Tr}_e(v)\neq 1,\\ \left(\frac{2}{n/e}\right)^e 2^{\frac{n+e}{2}} & \text{if } \mathrm{Tr}_e(v)=1,\end{cases}$$

*where $\left(\frac{2}{n/e}\right)$ is the Jacobi symbol.*

In the case when $u,v\neq 0$ and $n/e$ is even, the Weil sum $\mathfrak{S}(u,v)$ depends on whether or not the linearized polynomial $L_u(x) = u^{2^k}x^{2^{2k}} + ux$ is a permutation of $\mathbb{F}_{2^n}$. The following lemma gives the expression for Weil sum $\mathfrak{S}(u,v)$ for $u,v\neq 0$ and $n/e$ even.

**Lemma 2.6** [5, *Theorem* 5.3] *Let $u,v\in\mathbb{F}_q^*$ and $n/e$ be even so $n=2m$ for some integer $m$. Then*

(1) *If $u\neq g^{t(2^e+1)}$ for any integer $t$ then $L_u$ is a PP. Let $x_u\in\mathbb{F}_q$ be the unique solution of the equation $L_u(x)=v^{2^k}$. Then*

$$\mathfrak{S}(u,v) = (-1)^{m/e}2^m\chi_1(ux_u{}^{2^k+1}).$$

(2) *If $u=g^{t(2^e+1)}$ for some integer $t$, then $\mathfrak{S}(u,v)=0$ unless the equation $L_u(x)=v^{2^k}$ is solvable. If the equation $L_u(x)=v^{2^k}$ is solvable with some solution, say $x_u$, then*

$$\mathfrak{S}(u,v) = \begin{cases} (-1)^{m/e}2^m\chi_1(ux_u{}^{2^k+1}) & \text{if } \mathrm{Tr}_e(u)\neq 0,\\ (-1)^{\frac{m}{e}+1}2^{m+e}\chi_1(ux_u{}^{2^k+1}) & \text{if } \mathrm{Tr}_e(u)=0.\end{cases}$$

## 3 The binary Gold function

In this section, we shall give the explicit expression for the $c$-BCT entries of the 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 $\max_{b\in\mathbb{F}_{2^n}^*} {}_c\mathcal{B}_F(1,b)$, 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

$$\begin{cases} x^d + cy^d = b\\ (x+1)^d + c^{-1}(y+1)^d = b.\end{cases} \tag{1.2}$$

As done in [18], for $b\neq 0$ and fixed $c\neq 0$, the number of solutions $(x,y)\in\mathbb{F}_q^2$ of the system (1.2) is given by

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

where $S_{\alpha,\beta}=\sum_{x\in\mathbb{F}_q}\chi_1\big(\alpha x^d+\beta(x+1)^d\big)$. 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 $S_{c\alpha,c^{-1}\beta}$. Now, in the particular case when $d=2^k+1$, i.e., for the Gold case, we shall further simplify the expression for $S_{\alpha,\beta}$ as follows:

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

where $A=\alpha+\beta$ and $B=\beta^{2^{n-k}}+\beta$. Here one may note that $A=0$ if and only if $\alpha=\beta$. Also, $B=0$ if and only if $\beta\in\mathbb{F}_{2^e}$, since

$$
\begin{aligned}
B=0 &\Leftrightarrow \beta^{2^{n-k}}=\beta\\
&\Leftrightarrow \beta^{2^{n-k}-1}=1\\
&\Leftrightarrow \beta^{2^{\gcd(n-k,n)}-1}=1\\
&\Leftrightarrow \beta^{2^e-1}=1,\ (\text{ as }\ \gcd(n-k,n)=e)\\
&\Leftrightarrow \beta\in\mathbb{F}_{2^e}.
\end{aligned}
$$

Now we shall calculate $S_{\alpha,\beta}$ in two cases, namely, $n/e$ odd and $n/e$ even, respectively.

**Case 1**: $n/e$ is odd.

In this case, if $\alpha=\beta$ and $\beta\in\mathbb{F}_{2^e}$, then $S_{\alpha,\beta}=q\chi_1(\beta)$. If $\alpha=\beta$ and $\beta\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$ then $S_{\alpha,\beta}=0$. In the event of $\alpha\neq\beta$ and $\beta\in\mathbb{F}_{2^e}$, again we have $S_{\alpha,\beta}=0$. Finally, if $\alpha\neq\beta$ and $\beta\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$, by Lemma 2.5 we have,

$$S_{\alpha,\beta} = \begin{cases} 0 & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) \neq 1, \\ \left(\frac{2}{n/e}\right)^e 2^{\frac{n+e}{2}} \chi_1(\beta) & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) = 1, \end{cases}$$

where $\gamma \in \mathbb{F}_q$ is the unique element such that $\gamma^{2^k+1} = A$.

**Case 2**: $n/e$ is even.

Let $n = 2m$, for some positive integer $m$ and $g$ be a primitive element of the finite field $\mathbb{F}_q$. When $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^e}$ then $S_{\alpha,\beta} = q\chi_1(\beta)$. If $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ then again $S_{\alpha,\beta} = 0$. In the event of $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^e}$, by Lemma 2.4 we have

$$S_{\alpha,\beta} = \begin{cases} (-1)^{m/e} 2^m \chi_1(\beta) & \text{if } A \neq g^{t(2^e+1)} \text{ for any integer } t, \\ (-1)^{\frac{m}{e}+1} 2^{m+e} \chi_1(\beta) & \text{if } A = g^{t(2^e+1)} \text{ for some integer } t. \end{cases}$$

Finally, when $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$, we shall consider two cases depending on whether or not the linearized polynomial $L_A(x) = A^{2^k} x^{2^{2k}} + Ax$ is a permutation polynomial. From Lemma 2.3, $L_A$ is a permutation polynomial if and only if $n/e$ is even and $A \neq g^{t(2^e+1)}$ for any integer $t$. Therefore, when $n/e$ is even and $A \neq g^{t(2^e+1)}$ for any integer $t$, the equation $L_A(x) = B^{2^k}$ will have a unique solution, say $x_A$. Therefore, by Lemma 2.6, we have

$$S_{\alpha,\beta} = (-1)^{m/e} 2^m \chi_1(\beta) \chi_1(A x_A^{2^k+1}).$$

Now if the linearized polynomial $L_A$ is not permutation, i.e, $n/e$ is even and $A = g^{t(2^e+1)}$ for some integer $t$, we again have two cases depending on whether or not the equation $L_A(x) = B^{2^k}$ is solvable. In the case when equation $L_A(x) = B^{2^k}$ is solvable, let $x_A$ be one of its solution. Therefore, by Lemma 2.6 we have,

$$S_{\alpha,\beta} = \begin{cases} (-1)^{\frac{m}{e}+1} 2^{m+e} \chi_1(\beta) \chi_1\left(A x_A^{2^k+1}\right) & \text{if } \mathrm{Tr}_e(A) = 0, \\ (-1)^{\frac{m}{e}} 2^m \chi_1(\beta) \chi_1\left(A x_A^{2^k+1}\right) & \text{if } \mathrm{Tr}_e(A) \neq 0. \end{cases}$$

If $L_A(x) = B^{2^k}$ is not solvable, again, by Lemma 2.6, $S_{\alpha,\beta} = 0$.

Thus we have computed $S_{\alpha,\beta}$ in all possible cases. Similarly, we can find $S_{c\alpha,c^{-1}\beta}$ by putting $c\alpha$ and $c^{-1}\beta$ in place of $\alpha$ and $\beta$, respectively. We shall now explicitly compute the $c$-BCT entry ${}_cB_F(1,b)$ for $c = 1$, $c \in \mathbb{F}_{2^e} \backslash \{0,1\}$ and $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ in the forthcoming sections.

## 4 The case $c = 1$

When $c = 1$, $S_{\alpha,\beta}$ and $S_{c\alpha,c^{-1}\beta}$ coincide, therefore for any fixed $b \neq 0$, the $c$-BCT entry is given by,

$${}_1\mathcal{B}_F(1,b) = \frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q} \chi_1(b(\alpha+\beta)) S_{\alpha,\beta}^2.$$

Let us denote $T_b = S_{\alpha,\beta}^2$. Now we shall consider two cases, namely, $n/e$ odd and $n/e$ even, respectively.

**Case 1**: $n/e$ is odd. We consider the following subcases.

(1) If $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^e}$, then

$$T_b^{[1]} = q^2\, \chi_1(\beta)^2 = q^2.$$

(2) If $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$, then

$$T_b^{[2]} = 0.$$

(3) If $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^e}$, then

$$T_b^{[3]} = 0.$$

(4) If $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ then

$$T_b^{[4]} = \begin{cases} 0 & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) \neq 1, \\ 2^{n+e} & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) = 1. \end{cases}$$

Nyberg [15, 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 uniformity as well as the boomerang uniformity of the Gold function $x \mapsto x^{2^k+1}$ is 4. Our first theorem in this section generalizes the two previously mentioned results, and gives the boomerang uniformity of the Gold function for any parameters, when $\frac{n}{e}$ is odd. Note that we would require the notion of Walsh-Hadamard transform in the proof of this theorem, which is defined as follows.

For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer-valued function

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

The Walsh transform $\mathcal{W}_F(a, b)$ of an $(n, m)$-function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ at $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}$ is the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at $a$, that is,

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

**Theorem 4.1** *Let $F(x) = x^{2^k+1}$, $1 \leq k < n$, be a function on $\mathbb{F}_q$, $q = 2^n$, $n \geq 2$. 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*

$${}_1\mathcal{B}_F(1, b) = 0, \text{ or, } 2^e,$$

*if* $\mathrm{Tr}_e\left(b^{\frac{1}{2}}\right) = 0$, *respectively*, $\mathrm{Tr}_e\left(b^{\frac{1}{2}}\right) \neq 0$.

***Proof*** For every $\alpha, \beta$, let $A = \alpha + \beta, B = \beta^{2^{-k}} + \beta$, and $\gamma \in \mathbb{F}_q$ be the unique element such that $\gamma^{2^k+1} = A$. Further, let

$$\begin{aligned}
\mathcal{A} =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid \alpha=\beta\in\mathbb{F}_{2^e}\},\\
\mathcal{B} =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid \alpha=\beta\in\mathbb{F}_q\backslash\mathbb{F}_{2^e}\},\\
\mathcal{C} =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid \alpha\neq\beta \text{ and } \beta\in\mathbb{F}_{2^e}\},\\
\mathcal{D} =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid \alpha\neq\beta \text{ and } \beta\in\mathbb{F}_q\backslash\mathbb{F}_{2^e}\},\\
\mathcal{E} =&\{(\alpha,\beta)\in\mathcal{D} \mid \mathrm{Tr}_e(B\gamma^{-1})\neq 1\},\\
\mathcal{F} =&\{(\alpha,\beta)\in\mathcal{D} \mid \mathrm{Tr}_e(B\gamma^{-1})= 1\}.
\end{aligned}$$

Then,

$$\begin{aligned}
{}_1\mathcal{B}_F(1,b) =&\frac{1}{q^2}\Bigg(\sum_{(\alpha,\beta)\in\mathcal{A}}\chi_1(b(\alpha+\beta))T_b^{[1]}+\sum_{(\alpha,\beta)\in\mathcal{B}}\chi_1(b(\alpha+\beta))T_b^{[2]}+\sum_{(\alpha,\beta)\in\mathcal{C}}\chi_1(b(\alpha+\beta))T_b^{[3]}\\
&+\sum_{(\alpha,\beta)\in\mathcal{E}}\chi_1(b(\alpha+\beta))T_b^{[4]}+\sum_{\alpha,\beta\in\mathcal{F}}\chi_1(b(\alpha+\beta))T_b^{[4]}\Bigg)\\
=&\frac{1}{q^2}\Bigg(\sum_{(\alpha,\beta)\in\mathcal{A}}q^2+\sum_{(\alpha,\beta)\in\mathcal{F}}\chi_1(b(\alpha+\beta))2^{n+e}\Bigg)\\
=&2^e+\frac{2^e}{2^n}\sum_{(\alpha,\beta)\in\mathcal{F}}\chi_1(b(\alpha+\beta)).
\end{aligned}$$

As customary, $t^{-1}=t^{2^n-2}$, rendering $0^{-1}=0$. For each $\beta\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^e}$, we let (if $\beta\in\mathbb{F}_{2^e}$, $Y_\beta=\mathbb{F}_{2^n}$)

$$Y_\beta=\left\{\gamma^{-1}\in\mathbb{F}_{2^n}\ :\ \mathrm{Tr}_e\Big((\beta^{2^{-k}}+\beta)\gamma^{-1}\Big)=1\right\},$$

and

$$T_\beta=\left\{d\in\mathbb{F}_{2^n}\ :\ \mathrm{Tr}_e((\beta^{2^{-k}}+\beta)d)=0\right\}=\langle\beta^{2^{-k}}+\beta\rangle^{\perp_e}.$$

We shall use below that when $\frac{n}{e}$ is odd, then $\mathrm{Tr}_e(1)=1$. We label by $\langle S\rangle_e$ the $\mathbb{F}_{2^e}$-linear subspace in $\mathbb{F}_{2^n}$ generate by $S$ and we write $S^{\perp_e}$, for the trace orthogonal (via the relative trace $\mathrm{Tr}_e$) of the subspace $\langle S\rangle_e$ (if $e=1$, we drop the subscripts). Since $\mathrm{Tr}_e(1)=1$, then, $(\beta^{2^{-k}}+\beta)^{-1}\in Y_\beta$. If $\gamma_1^{-1},\gamma_2^{-1}\in Y_\beta$, then $\gamma_1^{-1}+\gamma_2^{-1}\in T_\beta$, of cardinality $|T_\beta|=2^{n-1}$. Reciprocally, if $\gamma^{-1}\in Y_\beta$ and $d\in T_\beta$, it is easy to see that $\gamma^{-1}+d\in Y_\beta$. Therefore, $Y_\beta$ is the affine subspace $Y_\beta=\gamma_\beta+T_\beta$, where $\gamma_\beta=(\beta^{2^{-k}}+\beta)^{-1}$.

Next, we observe that the kernel of $\phi:\beta\mapsto\beta^{2^{-k}}+\beta$, say $\ker(\phi)$, is an $\mathbb{F}_2$-linear space of dimension $e$ (in fact, it is exactly $\mathbb{F}_{2^e}$) and the image of $\phi$, say $\mathrm{Im}(\phi)$, is an $\mathbb{F}_2$-linear space of dimension $n-e$. Further, we show that $\mathrm{Im}(\phi)^{\perp_e}=\ker(\phi)$. We use below the fact that $\mathrm{Tr}_e(x^{2^e})=\mathrm{Tr}_e(x)$ and $e\mid k$. Let $u\in\mathrm{Im}(\phi)^{\perp_e}$, that is, for all $\beta\in\mathbb{F}_{2^n}$,

$$0=\mathrm{Tr}_e(u(\beta^{2^{-k}}+\beta))=\mathrm{Tr}_e(u\beta^{2^{-k}})+\mathrm{Tr}_e(u\beta)=\mathrm{Tr}_e(u^{2^k}\beta)+\mathrm{Tr}_e(u\beta)=\mathrm{Tr}_e((u+u^{2^k})\beta),$$

and so, $u^{2^k}+u=0$, which shows the claim. For easy referral, if we speak of the dimension of an $\mathbb{F}_{2^e}$-linear space $S$, we shall be using the notation $\dim_e S$ (no subscript if $e=1$).

We will be using below the Poisson summation formula (see [3, Corollary 8.9] and [6, Theorem 2.15]), which states that if $f:\mathbb{F}_{2^n}\to\mathbb{R}$ and $S$ is a subspace of $\mathbb{F}_{2^n}$ of dimension $\dim S$, then

$$\sum_{u\in\alpha+S}\mathcal{W}_f(u)(-1)^{\mathrm{Tr}(\beta u)}=2^{\dim S}(-1)^{\mathrm{Tr}(\alpha\beta)}\sum_{u\in\beta+S^\perp}f(u)(-1)^{\mathrm{Tr}(\alpha u)},$$

and in particular,

$$\sum_{u\in S}\mathcal{W}_f(u)=2^{\dim S}\sum_{u\in S^\perp}f(u).$$

Now, we are able to compute our sum (labelling $\alpha=\beta+\gamma^{2^k+1}$, and writing $\phi^{-1}(t)=\{\beta\ :\ \phi(\beta)=t\}$; we also note that when $\frac{n}{e}$ is odd, $\gcd(2^k+1,2^n-1)=1$, and so $\gamma\mapsto\gamma^{2^k+1}$ is a permutation)

$$\begin{aligned}
{}_1\mathcal{B}_F(1,b)&=2^e+\frac{2^e}{2^n}\sum_{\substack{\beta\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^e},\gamma\in\mathbb{F}_{2^n}\\ \mathrm{Tr}_e\left((\beta^{2^{-k}}+\beta)\gamma^{-1}\right)=1}}\chi_1\left(b\gamma^{2^k+1}\right)\\
&=2^e+\frac{2^e}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^e}}\sum_{\gamma^{-1}\in Y_\beta}\chi_1\left(b\gamma^{2^k+1}\right)\\
&=2^e+\frac{2^e}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{x\in(\beta^{2^{-k}}+\beta)^{-1}+\langle\beta^{2^{-k}}+\beta\rangle^\perp_e}\chi_1\left(bx^{-2^k-1}\right)\\
&\qquad\text{(we used here that } Y_\beta=(\beta^{2^{-k}}+\beta)^{-1}+T_\beta\text{; we also added}\\
&\qquad\beta\in\mathbb{F}_{2^e},\ \text{as it contributes 0 to the inner sum)}\\
&=2^e+\frac{2^e}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}2^{-\dim S}\sum_{u\in\left(\langle\beta^{2^{-k}}+\beta\rangle^\perp_e\right)^\perp}\mathcal{W}_{g_\beta}(u)(-1)^{\mathrm{Tr}\left(u(\beta^{2^{-k}}+\beta)^{-1}\right)}\\
&\qquad\text{(by Poisson summation with } S^\perp=\langle\beta^{2^{-k}}+\beta\rangle^\perp_e,\ \text{and } g_\beta(x)=\chi_1\left(bx^{-2^k-1}\right)).
\end{aligned}$$

We now analyze the $\mathbb{F}_2$-linear space

$$\left(\langle\beta^{2^{-k}}+\beta\rangle^\perp_e\right)^\perp=\{x\in\mathbb{F}_{2^n}\ :\ \mathrm{Tr}(dx)=0,\forall d\text{ with }\mathrm{Tr}_e(d(\beta^{2^{-k}}+\beta))=0\}.$$

Further, $\mathbb{F}_{2^n}$ has dimension $n/e$ as an $\mathbb{F}_{2^e}$-linear space and so, $\dim_e\langle\beta^{2^{-k}}+\beta\rangle^\perp_e=\frac{n}{e}-1$ as an $\mathbb{F}_{2^e}$-linear space, and since $\mathbb{F}_{2^e}$ has dimension $e$ as an $\mathbb{F}_2$-linear space, then $\dim\langle\beta^{2^{-k}}+\beta\rangle^\perp_e=n-e$ as an $\mathbb{F}_2$-linear space. Thus, $\dim\left(\langle\beta^{2^{-k}}+\beta\rangle^\perp_e\right)^\perp=e$. Moreover, $\mathrm{Tr}_e(\beta^{2^{-k}}+\beta)=0$ and if $u\in\mathbb{F}_{2^e}$ then $\mathrm{Tr}_e(u(\beta^{2^{-k}}+\beta))=u\mathrm{Tr}_e(\beta^{2^{-k}}+\beta)=0$, and consequently (since the dimensions match and $(\beta^{2^{-k}}+\beta)\mathbb{F}_{2^e}\subseteq S$)

$$S=\left(\langle\beta^{2^{-k}}+\beta\rangle^\perp_e\right)^\perp=(\beta^{2^{-k}}+\beta)\mathbb{F}_{2^e}.$$

We are now ready to continue the computation, thus,

$$
\begin{aligned}
{}_1\mathcal{B}_F(1,b) &= 2^e + \frac{2^e}{2^n}2^{-e}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{u\in(\beta^{2^{-k}}+\beta)\mathbb{F}_{2^e}} \mathcal{W}_{g_\beta}(u)(-1)^{\mathrm{Tr}\left(u(\beta^{2^{-k}}+\beta)^{-1}\right)}\\
&=2^e + \frac{2^e}{2^n}2^{-e}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{d'\in\mathbb{F}_{2^e}} \mathcal{W}_{g_\beta}(d'(\beta^{2^{-k}}+\beta))(-1)^{\mathrm{Tr}(d')}\\
&=2^e + \frac{2^e}{2^n}2^{-e}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{d'\in\mathbb{F}_{2^e}}\sum_{x\in\mathbb{F}_{2^n}} \chi_1\left(bx^{-2^k-1}+d'x(\beta^{2^{-k}}+\beta)+d'\right)\\
&=2^e + \frac{2^e}{2^n}2^{-e}\sum_{d'\in\mathbb{F}_{2^e}}\sum_{x\in\mathbb{F}_{2^n}} \chi_1\left(bx^{-2^k-1}+d'\right)\sum_{\beta\in\mathbb{F}_{2^n}} \chi_1\left(d'x(\beta^{2^{-k}}+\beta)\right)\\
&=2^e + \frac{2^e}{2^n}2^{-e}\sum_{d'\in\mathbb{F}_{2^e}}\sum_{x\in\mathbb{F}_{2^n}} \chi_1\left(bx^{-2^k-1}+d'\right)\sum_{\beta\in\mathbb{F}_{2^n}} \chi_1\left(\left((d'x)^{2^k}+d'x\right)\beta\right)\\
&\qquad\left(\text{ since } \mathrm{Tr}\left(d'x(\beta^{2^{-k}}+\beta)\right) = \mathrm{Tr}\left(((d'x)^{2^k}+d'x)\beta\right) = \mathrm{Tr}(d'(x^{2^k}+x)\beta)\right)\\
&=2^e + \frac{2^e}{2^n}2^{n-e}\sum_{\substack{d'\in\mathbb{F}_{2^e},x\in\mathbb{F}_{2^n}\\ d'(x^{2^k}+x)=0}} \chi_1\left(bx^{-2^k-1}+d'\right)\\
&=2^e + \frac{2^e}{2^n}2^{n-e}\sum_{d'\in\mathbb{F}^*_{2^e},x\in\mathbb{F}_{2^e}} \chi_1(bx^{-2}+d') + \sum_{x\in\mathbb{F}_{2^n}}\chi_1(bx^{-2^k-1})\\
&=2^e + \frac{2^e}{2^n}2^{n-e}\sum_{d'\in\mathbb{F}^*_{2^e},x\in\mathbb{F}_{2^e}} \chi_1(bx^{-2}+d')\\
&=2^e - 2^e\delta_0\left(\mathrm{Tr}_e\left(b^{\frac{1}{2}}\right)\right),
\end{aligned}
$$

where $\delta_0$ is the Dirac symbol, defined by $\delta_0(c) = 1$, if $c = 0$, and 0, otherwise. Thus, ${}_1\mathcal{B}_F(1,b) \in \{0, 2^e\}$, and the claim of our theorem is shown.

***Remark 4.2*** Note that independently, Eddahmani and Mesnager [7] have explicitly determined the $c$-BCT entries of the permutation Gold functions via a different approach in the particular case of $c = 1$. However, we determine the expressions for $c$-BCT entries for an arbitrary value of $c$.

**Case 2**: $n/e$ is even.

(1) If $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^e}$, then

$$T_b^{[1]} = q^2\,\chi_1(\beta)^2 = q^2.$$

(2) If $\alpha = \beta$ and $\beta \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$, then

$$T_b^{[2]} = 0.$$

(3) If $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^e}$, then

$$T_b^{[3]} = \begin{cases} 2^n & \text{if } A \neq g^{t(2^e+1)} \text{ for any integer } t, \\ 2^{n+2e} & \text{if } A = g^{t(2^e+1)} \text{ for some integer } t. \end{cases}$$

(4) If $\alpha \neq \beta$ and $\beta \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$, then

(a) If $A \neq g^{t(2^e+1)}$ for any integer $t$, then

$$T_b^{[4(a)]} = 2^n.$$

(b) If $A = g^{t(2^e+1)}$ for some integer $t$, then

(i) If the equation $L_A(x) = B^{2^k}$ is not solvable, where $L_A(x) = A^{2^k}x^{2^{2k}} + Ax$, then

$$T_b^{[4(b)(i)]} = 0.$$

(ii) If the equation $L_A(x) = B^{2^k}$ is solvable, then

$$T_b^{[4(b)(ii)]} = \begin{cases} 2^n & \text{if } \mathrm{Tr}_e(A) \neq 0, \\ 2^{n+2e} & \text{if } \mathrm{Tr}_e(A) = 0. \end{cases}$$

Now we shall summarize the above discussion in the following theorem.

**Theorem 4.3** *Let $F(x) = x^{2^k+1}$, $1 \leq k < n$ be a function on $\mathbb{F}_{2^n}$, $n \geq 2$. Let $c = 1$ and $n/e$ be even, where $e = \gcd(k, n)$. Then the c-BCT entry ${}_1\mathcal{B}_F(1, b)$ of $F$ at $(1, b)$ is given by*

$$2^e + \frac{1}{2^n} \sum_{(\alpha,\beta)\in G\cup I\cup K} \chi_1(b(\alpha+\beta)) + \frac{2^{2e}}{2^n} \sum_{(\alpha,\beta)\in H\cup L} \chi_1(b(\alpha+\beta)),$$

*with $A = \alpha + \beta$, $B = \beta^{2^{n-k}} + \beta$, $L_A(x) = A^{2^k}x^{2^{2k}} + Ax$, and*

$$\begin{aligned}
\mathcal{G} &= \{(\alpha,\beta) \in \mathcal{C} \mid A \neq g^{t(2^e+1)} \text{ for any integer } t\}, \\
\mathcal{H} &= \{(\alpha,\beta) \in \mathcal{C} \mid A = g^{t(2^e+1)} \text{ for some integer } t\}, \\
\mathcal{I} &= \{(\alpha,\beta) \in \mathcal{D} \mid A \neq g^{t(2^e+1)} \text{ for any integer } t\}, \\
\mathcal{K} &= \{(\alpha,\beta) \in \mathcal{D} \mid A = g^{t(2^e+1)} \text{ for some integer } t,\ \mathrm{Tr}_e(A) \neq 0, L_A(x) = B^{2^k} \text{ is solvable}\}, \\
\mathcal{L} &= \{(\alpha,\beta) \in \mathcal{D} \mid A = g^{t(2^e+1)} \text{ for some integer } t,\ \mathrm{Tr}_e(A) = 0, L_A(x) = B^{2^k} \text{ is solvable}\}.
\end{aligned}$$

***Proof*** For the proof, we need to define

$$\mathcal{J} = \{(\alpha,\beta) \in \mathcal{D} \mid A = g^{t(2^e+1)} \text{ for an integer } t, L_A(x) = B^{2^k} \text{ is not solvable}\}.$$

Then

$$
\begin{aligned}
{}_1\mathcal{B}_F(1,b) =& \frac{1}{q^2}\Bigg( \sum_{(\alpha,\beta)\in\mathcal{A}} \chi_1(b(\alpha+\beta))T_b^{[1]} + \sum_{(\alpha,\beta)\in\mathcal{B}} \chi_1(b(\alpha+\beta))T_b^{[2]} \\
&+ \sum_{(\alpha,\beta)\in\mathcal{G}} \chi_1(b(\alpha+\beta))T_b^{[3]} + \sum_{(\alpha,\beta)\in\mathcal{H}} \chi_1(b(\alpha+\beta))T_b^{[3]} \\
&+ \sum_{(\alpha,\beta)\in\mathcal{I}} \chi_1(b(\alpha+\beta))T_b^{[4(a)]} + \sum_{(\alpha,\beta)\in\mathcal{J}} \chi_1(b(\alpha+\beta))T_b^{[4(b)(i)]} \\
&+ \sum_{(\alpha,\beta)\in\mathcal{K}} \chi_1(b(\alpha+\beta))T_b^{[4(b)(ii)]} + \sum_{(\alpha,\beta)\in\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(b)(ii)]} \Bigg) \\
=& \frac{1}{q^2}\Bigg( \sum_{(\alpha,\beta)\in\mathcal{A}} q^2 + 2^n \sum_{(\alpha,\beta)\in\mathcal{G}\cup\mathcal{I}\cup\mathcal{K}} \chi_1(b(\alpha+\beta)) + 2^{n+2e} \sum_{(\alpha,\beta)\in\mathcal{H}\cup\mathcal{L}} \chi_1(b(\alpha+\beta)) \Bigg) \\
=& 2^e + \frac{1}{2^n} \sum_{(\alpha,\beta)\in\mathcal{G}\cup\mathcal{I}\cup\mathcal{K}} \chi_1(b(\alpha+\beta)) + \frac{2^{2e}}{2^n} \sum_{(\alpha,\beta)\in\mathcal{H}\cup\mathcal{L}} \chi_1(b(\alpha+\beta)).
\end{aligned}
$$

This completes the proof.

**Corollary 4.4** *Let $F(x) = x^{2^k+1}$, $1 \le k < n$, be a function on $\mathbb{F}_q$, $n \ge 2$. Let $c = 1$ and $n/e$ be even, where $e = \gcd(k,n)$. With the notations of the previous theorem, the c-boomerang uniformity of F satisfies*

$$\beta_{F,c} \le 2^e + 2^{-n}|\mathcal{G}\cup\mathcal{I}\cup\mathcal{K}| + 2^{2e-n}|\mathcal{H}\cup\mathcal{L}|.$$

## 5 The case $c \in \mathbb{F}_{2^e}\setminus\{0,1\}$

Since the case $c = 1$ has already been considered in the previous section, throughout this section we assume that $c \ne 1$. Notice that when $c \in \mathbb{F}_{2^e}^*$, $\beta \in \mathbb{F}_{2^e} \Leftrightarrow \beta c^{-1} \in \mathbb{F}_{2^e}$. Recall that for any fixed $b \ne 0$, the $c$-BCT entry is given by,

$$ {}_c\mathcal{B}_F(1,b) = \frac{1}{q^2} \sum_{\alpha,\beta\in\mathbb{F}_q} \chi_1(b(\alpha+\beta))S_{\alpha,\beta}S_{c\alpha,c^{-1}\beta}.$$

Let us denote $T_b = S_{\alpha,\beta}S_{c\alpha,c^{-1}\beta}$ (we will use superscripts to point out the case we are in, for its value). Recall that $A = \alpha+\beta$ and $B = \beta^{2^{n-k}} + \beta$. Let us denote $\gamma = A^{\frac{1}{2^k+1}}$, $A' = c\alpha + c^{-1}\beta$ and $B' = (c^{-1}\beta)^{2^{n-k}} + c^{-1}\beta$. It is easy to observe that the conditions $B = 0$ and $B' = 0$ are equivalent. Now we shall consider two cases namely, $\frac{n}{e}$ odd and $\frac{n}{e}$ even, respectively.

**Case 1**: $\frac{n}{e}$ is odd.

(1) Let $A = 0, B = 0$.

(a) If $A' = 0, B' = 0$, then

$$T_b^{[1(a)]} = q^2\chi_1((1+c^{-1})\beta).$$

(b) If $A' \ne 0, B' = 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[1(b)]} = 0.$$

(2) Let $A = 0, B \neq 0$. In this case $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[2]} = 0.$$

(3) Let $A \neq 0, B = 0$. Again $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[3]} = 0$$

(4) Let $A \neq 0, B \neq 0$.

(a) Assume $A' = 0, B' \neq 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[4(a)]} = 0.$$

(b) Assume $A' \neq 0, B' \neq 0$. In this case, recall that $\gamma^{2^k+1} = A$ and let $\gamma' \in \mathbb{F}_q$ such that $(\gamma')^{2^k+1} = A'$.

(i) If $\mathrm{Tr}_e(B\gamma^{-1}) \neq 1$, then $S_{\alpha,\beta} = 0$ and hence

$T_b^{[4(b)(i)]} = 0.$

(ii) If $\mathrm{Tr}_e(B\gamma^{-1}) = 1$ and $\mathrm{Tr}_e(B'(\gamma')^{-1}) \neq 1$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$T_b^{[4(b)(ii)]} = 0.$

(iii) If $\mathrm{Tr}_e(B\gamma^{-1}) = 1$ and $\mathrm{Tr}_e(B'(\gamma')^{-1}) = 1$, then

$T_b^{[4(b)(iii)]} = 2^{n+e}\chi_1((1 + c^{-1})\beta).$

We now use the above discussion in the following theorem.

**Theorem 5.1** *Let $F(x) = x^{2^k+1}, 1 \leq k < n$ be a function on $\mathbb{F}_{2^n}$, $n \geq 2$. Let $c \in \mathbb{F}_{2^e}\backslash\{0, 1\}$ and $n/e$ be odd, where $e = \gcd(k, n)$. Then the c-BCT entry ${}_c\mathcal{B}_F(1, b)$ of $F$ at $(1, b)$ is given by*

$$1 + \frac{2^e}{2^n} \sum_{(\alpha,\beta)\in\mathcal{F}\cap\mathcal{F}_{\simeq}} \chi_1(b\alpha + (1 + c^{-1} + b)\beta)),$$

*where*

$$F = \{(\alpha, \beta) \in \mathbb{F}_q^2 \mid A, B \neq 0 \text{ and } \mathrm{Tr}_e(B\gamma^{-1}) = 1\},$$
$$F' = \{(\alpha, \beta) \in \mathbb{F}_q^2 \mid A', B' \neq 0 \text{ and } \mathrm{Tr}_e(B'(\gamma')^{-1}) = 1\},$$

*and* $A = \alpha + \beta$, $B = \beta^{2^{n-k}} + \beta$, $A' = c\alpha + c^{-1}\beta$ *and* $B' = (c^{-1}\beta)^{2^{n-k}} + c^{-1}\beta$, $\gamma = A^{\frac{1}{2^k+1}}$, $\gamma' = A'^{\frac{1}{2^k+1}}$.

***Proof*** Let

$$\begin{aligned}
A' =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid c\alpha = c^{-1}\beta \text{ and } c^{-1}\beta\in\mathbb{F}_{2^e}\},\\
B' =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid c\alpha = c^{-1}\beta \text{ and } c^{-1}\beta\in\mathbb{F}_q\backslash\mathbb{F}_{2^e}\},\\
C' =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid c\alpha \neq c^{-1}\beta \text{ and } c^{-1}\beta\in\mathbb{F}_{2^e}\},\\
D' =&\{(\alpha,\beta)\in\mathbb{F}_q^2 \mid c\alpha \neq c^{-1}\beta \text{ and } c^{-1}\beta\in\mathbb{F}_q\backslash\mathbb{F}_{2^e}\},\\
E' =&\{(\alpha,\beta)\in D' \mid \mathrm{Tr}_e(B'(\gamma')^{-1}) \neq 1\}.
\end{aligned}$$

Then,

$$\begin{aligned}
{}_cB_F(1,b) =&\frac{1}{q^2}\Bigg(\sum_{(\alpha,\beta)\in A\cap A'}\chi_1(b(\alpha+\beta))T_b^{[1(a)]} + \sum_{(\alpha,\beta)\in A\cap C'}\chi_1(b(\alpha+\beta))T_b^{[1(b)]}\\
&+\sum_{(\alpha,\beta)\in B}\chi_1(b(\alpha+\beta))T_b^{[2]} + \sum_{(\alpha,\beta)\in C}\chi_1(b(\alpha+\beta))T_b^{[3]}\\
&+\sum_{(\alpha,\beta)\in D\cap B'}\chi_1(b(\alpha+\beta))T_b^{[4(a)]} + \sum_{(\alpha,\beta)\in E}\chi_1(b(\alpha+\beta))T_b^{[4(b)(i)]}\\
&+\sum_{(\alpha,\beta)\in F\cap E'}\chi_1(b(\alpha+\beta))T_b^{[4(b)(ii)]} + \sum_{(\alpha,\beta)\in F\cap F'}\chi_1(b(\alpha+\beta))T_b^{[4(b)(iii)]}\Bigg)\\
=&\sum_{(\alpha,\beta)\in A\cap A'}\chi_1(b\alpha+(1+c^{-1}+b)\beta))\\
&+\frac{2^e}{2^n}\sum_{(\alpha,\beta)\in F\cap F'}\chi_1(b\alpha+(1+c^{-1}+b)\beta))\\
=&1+\frac{2^e}{2^n}\sum_{(\alpha,\beta)\in F\cap F'}\chi_1(b\alpha+(1+c^{-1}+b)\beta)).
\end{aligned}$$

This completes the proof.

**Corollary 5.2** *Let $F(x)=x^{2^k+1}$, $1\le k<n$, be a function on $\mathbb{F}_q$, $n\ge 2$. Let $c\in\mathbb{F}_{2^e}\setminus\{0,1\}$ and $n/e$ be odd, where $e=\gcd(k,n)$. With the notations of the previous theorem, the c-boomerang uniformity of F satisfies*

$$\beta_{F,c}\le 1+2^{e-n}|F\cap F'|.$$

**Case 2**: *n/e* is even.

(1) Let $A=0, B=0$.

(a) If $A'=0, B'=0$, then

$$T_b^{[1(a)]}=\chi_1((1+c^{-1})\beta)\,q^2.$$

(b) If $A'\neq 0, B'=0$, let

$G'=\{(\alpha,\beta)\in C' \mid A'\neq g^{t(2^e+1)} \text{ for any integer } t\}$,

$$H' = \{(\alpha, \beta) \in C' \mid A' = g^{t(2^e+1)} \text{ for some integer } t\}.$$

Then,

$$T_b^{[1(b)]} = \begin{cases} (-1)^{\frac{m}{e}} 2^{m+n} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in A \cap G', \\ (-1)^{\frac{m}{e}+1} 2^{m+n+e} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in A \cap H'. \end{cases}$$

(2) Let $A = 0, B \neq 0$. In this case $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[2]} = 0.$$

(3) Let $A \neq 0, B = 0$.

(a) If $A' = 0, B' = 0$, then $T_b^{[3(a)]}$ is given by

$$\begin{cases} (-1)^{\frac{m}{e}} 2^{m+n} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in A' \cap G, \\ (-1)^{\frac{m}{e}+1} 2^{m+n+e} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in A' \cap H. \end{cases}$$

(b) If $A' \neq 0, B' = 0$, then

$$T_b^{[3(b)]} = \begin{cases} 2^n \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in G \cap G', \\ -2^{n+e} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in G \cap H', \\ -2^{n+e} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in H \cap G', \\ 2^{n+2e} \chi_1((1+c^{-1})\beta) & \text{if } (\alpha, \beta) \in H \cap H'. \end{cases}$$

(4) Let $A \neq 0, B \neq 0$.

(a) If $A' = 0, B' \neq 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[4(a)]} = 0.$$

(b) If $A' \neq 0, B' \neq 0$, let

$$\begin{aligned} I' =& \{(\alpha, \beta) \in D' \mid A' \neq g^{t(2^e+1)} \text{ for any integer } t\}, \\ J' =& \{(\alpha, \beta) \in D' \mid A' = g^{t(2^e+1)} \text{ for some integer } t, \\ & L'_A(x) = (B')^{2^k} \text{ is not solvable }\}, \\ K' =& \{(\alpha, \beta) \in D' \mid A' = g^{t(2^e+1)} \text{ for some integer } t, \\ & \mathrm{Tr}_e(A') \neq 0, L_{A'}(x) = (B')^{2^k} \text{ is solvable}\}, \\ L' =& \{(\alpha, \beta) \in D' \mid A' = g^{t(2^e+1)} \text{ for some integer } t, \\ & \mathrm{Tr}_e(A') = 0, L_{A'}(x) = (B')^{2^k} \text{ is solvable}\}. \end{aligned}$$

Then,

$$T_b^{[4(b)]} = \begin{cases} 2^n \cdot M & \text{if } (\alpha,\beta) \in (I \cup K) \cap (I' \cup K'), \\ 0 & \text{if } (\alpha,\beta) \in (I \cup K \cup L) \cap J', \\ -2^{n+e} \cdot M & \text{if } (\alpha,\beta) \in (I \cup K) \cap L', \\ 0 & \text{if } (\alpha,\beta) \in J \cap (I' \cup J' \cup K' \cup L'), \\ -2^{n+e} \cdot M & \text{if } (\alpha,\beta) \in L \cap (I' \cup K'), \\ 2^{n+2e} \cdot M & \text{if } (\alpha,\beta) \in L \cap L', \end{cases}$$

where $M = \chi_1((1+c^{-1})\beta)\chi_1\left(AA' x_A^{2^k+1} x_{A'}^{2^k+1}\right)$ and $x_A, x_{A'}$ are the solutions of the equations $L_A(x) = B^{2^k}$ and $L_{A'}(x) = (B')^{2^k}$, respectively.

We now summarize the above discussion in the following theorem.

**Theorem 5.3** *Let $F(x) = x^{2^k+1}, 1 \le k < n$ be a function on $\mathbb{F}_{2^n}$, $n \ge 2$. Let $c \in \mathbb{F}_{2^e} \setminus \{0,1\}$ and $n/e$ be even, where $e = \gcd(k,n)$. With the previous notations, the c-BCT entry ${}_c\mathcal{B}_F(1,b)$ of $F$ at $(1,b)$ is given by*

$$\begin{aligned} \frac{1}{q^2}\Bigg( & \sum_{(\alpha,\beta)\in A\cap A'} \chi_1(b(\alpha+\beta))T_b^{[1(a)]} + \sum_{(\alpha,\beta)\in A\cap G'} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} \\ & + \sum_{(\alpha,\beta)\in A\cap H'} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} + \sum_{(\alpha,\beta)\in A'\cap G} \chi_1(b(\alpha+\beta))T_b^{[3(a)]} \\ & + \sum_{(\alpha,\beta)\in A'\cap H} \chi_1(b(\alpha+\beta))T_b^{[3(a)]} + \sum_{(\alpha,\beta)\in G\cap G'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\ & + \sum_{(\alpha,\beta)\in G\cap H'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + \sum_{(\alpha,\beta)\in H\cap G'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\ & + \sum_{(\alpha,\beta)\in H\cap H'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + + \sum_{(\alpha,\beta)\in (I\cup K)\cap (I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[4(b)]} \\ & + \sum_{(\alpha,\beta)\in (I\cup K)\cap L'} \chi_1(b(\alpha+\beta))T_b^{[4(b)]} + \sum_{(\alpha,\beta)\in L\cap (I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[4(b)]} \\ & + \sum_{(\alpha,\beta)\in L\cap L'} \chi_1(b(\alpha+\beta))T_b^{[4(b)]} \Bigg). \end{aligned}$$

## 6 The general case

Since the case $c \in \mathbb{F}_{2^e}$ has already been considered in previous sections, throughout this section we assume that $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^e}$. Recall that for any fixed $b \neq 0$, the $c$-BCT entry is given by,

$${}_cB_F(1,b) = \frac{1}{q^2} \sum_{\alpha,\beta\in\mathbb{F}_q} \chi_1(b(\alpha+\beta))S_{\alpha,\beta}S_{c\alpha,c^{-1}\beta}.$$

Let us denote $T_b = S_{\alpha,\beta}S_{c\alpha,c^{-1}\beta}$. Recall that $A = \alpha + \beta$, $B = \beta^{2^{n-k}} + \beta$, $A' = c\alpha + c^{-1}\beta$ and $B' = (c^{-1}\beta)^{2^{n-k}} + c^{-1}\beta$. Notice that, when $c \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$ then $\beta \in \mathbb{F}_{2^e}^*$, and so, $\beta c^{-1} \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$, otherwise $c \in \mathbb{F}_{2^e}$. Thus $B = 0 = B'$ if and only if $\beta = 0$. Also, observe that the conditions $A = 0 = A'$ if and only if $\alpha = 0 = \beta$. Now we shall consider two cases namely, $\frac{n}{e}$ is odd and $\frac{n}{e}$ is even, respectively.

**Case 1**: $\frac{n}{e}$ is odd.

(1) Let $A = 0, B = 0$. Notice that the cases $A' = 0, B' \neq 0$, and $A' \neq 0, B' = 0$ would not arise, therefore, we shall calculate $T_b$ in remaining two cases only.

(a) If $A' = 0, B' = 0$, then

$$T_b^{[1(a)]} = \chi_1((1 + c^{-1})\beta)\, q^2.$$

(b) If $A' \neq 0, B' \neq 0$, then

$$T_b^{[1(b)]} = \begin{cases} 0 & \text{if } \mathrm{Tr}_e(B'(\gamma')^{-1}) \neq 1, \\ \left(\frac{2}{n/e}\right)^e 2^{\frac{3n+e}{2}} \chi_1((1 + c^{-1})\beta) & \text{if } \mathrm{Tr}_e(B'(\gamma')^{-1}) = 1. \end{cases}$$

(2) Let $A = 0, B \neq 0$. In this case $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[2]} = 0.$$

(3) Let $A \neq 0, B = 0$. Again, $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[3]} = 0.$$

(4) Let $A \neq 0, B \neq 0$.

(a) If $A' = 0, B' = 0$, then

$$T_b^{[4(a)]} = \begin{cases} 0 & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) \neq 1, \\ \left(\frac{2}{n/e}\right)^e 2^{\frac{3n+e}{2}} \chi_1((1 + c^{-1})\beta) & \text{if } \mathrm{Tr}_e(B\gamma^{-1}) = 1. \end{cases}$$

(b) If $A' = 0, B' \neq 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[4(b)]} = 0.$$

(c) If $A' \neq 0, B' = 0$, then again $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[4(c)]} = 0.$$

(d) If $A' \neq 0, B' \neq 0$, then the only relevant case is and

$$T_b^{[4(d)]} = \begin{cases} 2^{n+e}\chi_1((1 + c^{-1})\beta) & \text{if } (\alpha, \beta) \in F \cap F', \\ 0 & \text{otherwise.} \end{cases}$$

We now summarize the above discussion in the following theorem.

**Theorem 6.1** *Let $F(x) = x^{2^k+1}, 1 \le k < n$ be a function on $\mathbb{F}_{2^n}$, $n \ge 2$. Let $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ and $n/e$ be odd, where $e = \gcd(k, n)$. Then the c-BCT entry ${}_cB_F(1, b)$ of $F$ at $(1, b)$ is given by*

$$1 + \frac{2^{\frac{e}{2}}}{2^n} \sum_{(\alpha,\beta)\in(A\cap F')\cup(A'\cap F)} \chi_1(b\alpha + (1 + c^{-1} + b)\beta)) + \frac{2^e}{2^n} \sum_{(\alpha,\beta)\in F\cap F'} \chi_1(b\alpha + (1 + c^{-1} + b)\beta)).$$

***Proof***

$$\begin{aligned} {}_cB_F(1, b) =& \frac{1}{q^2}\left( \sum_{(\alpha,\beta)\in A\cap A'} \chi_1(b(\alpha + \beta))T_b^{[1(a)]} + \sum_{(\alpha,\beta)\in A\cap F'} \chi_1(b(\alpha + \beta))T_b^{[1(b)]} \right. \\ &\left. + \sum_{(\alpha,\beta)\in F\cap A'} \chi_1(b(\alpha + \beta))T_b^{[4(a)]} + \sum_{(\alpha,\beta)\in F\cap F'} \chi_1(b(\alpha + \beta))T_b^{[4(d)]} \right) \\ =& 1 + \left(\frac{2}{n/e}\right)^e \cdot 2^{\frac{e-n}{2}} \sum_{(\alpha,\beta)\in(A\cap F')\cup(A'\cap F)} \chi_1(b\alpha + (1 + c^{-1} + b)\beta)) \\ &+ 2^{e-n} \sum_{(\alpha,\beta)\in F\cap F'} \chi_1(b\alpha + (1 + c^{-1} + b)\beta)). \end{aligned}$$

**Corollary 6.2** *Let $F(x) = x^{2^k+1}$, $1 \le k < n$, be a function on $\mathbb{F}_q$, $n \ge 2$. Let $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ and $n/e$ be odd, where $e = \gcd(k, n)$. With the notations of the previous theorem, the c-boomerang uniformity of $F$ satisfies*

$$\beta_{F,c} \le 1 + \left(\frac{2}{n/e}\right)^e \cdot 2^{\frac{e-n}{2}} |(A \cap F') \cup (A' \cap F)| + 2^{e-n}|F \cap F'|.$$

**Case 2**: *n/e* is even.

(1) Let $A = 0, B = 0$. Notice that the cases $A' = 0, B' \ne 0$, and $A' \ne 0, B' = 0$ would not arise, therefore, we shall calculate $T_b$ in remaining two cases only.

(a) If $A' = 0, B' = 0$, then

$$T_b^{[1(a)]} = \chi_1((1 + c^{-1})\beta)\, q^2.$$

(b) If $A' \ne 0, B' \ne 0$, then

$$T_b^{[1(b)]} = \begin{cases} (-1)^{\frac{m}{e}} 2^{m+n} M' & \text{if } (\alpha, \beta) \in A \cap (I' \cup K'), \\ 0 & \text{if } (\alpha, \beta) \in A \cap J', \\ (-1)^{\frac{m}{e}+1} 2^{m+n+e} M' & \text{if } (\alpha, \beta) \in A \cap L', \end{cases}$$

where $M' = \chi_1((1 + c^{-1})\beta)\chi_1(A' x_{A'}^{2^k+1})$.

(2) Let $A = 0, B \ne 0$. In this case $S_{\alpha,\beta} = 0$ and hence

$$T_b^{[2]} = 0$$

(3) Let $A \ne 0, B = 0$. Notice that the case $A' = 0, B' = 0$ would not arise. Now we shall calculate $T_b$ in the remaining cases.

(a) If $A' = 0, B' \neq 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[3(a)]} = 0.$$

(b) If $A' \neq 0, B' = 0$, then

$$T_b^{[3(b)]} = \begin{cases} 2^n \chi_1((1+c^{-1})\beta) & if\ (\alpha,\beta) \in G \cap G', \\ -2^{n+e}\chi_1((1+c^{-1})\beta) & if\ (\alpha,\beta) \in G \cap H', \\ -2^{n+e}\chi_1((1+c^{-1})\beta) & if\ (\alpha,\beta) \in H \cap G', \\ 2^{n+2e}\chi_1((1+c^{-1})\beta) & if\ (\alpha,\beta) \in H \cap H'. \end{cases}$$

(c) If $A' \neq 0, B' \neq 0$, then

$$T_b^{[3(c)]} = \begin{cases} 2^n M' & if\ (\alpha,\beta) \in G \cap (I' \cup K'), \\ 0 & if\ (\alpha,\beta) \in (G \cup H) \cap J', \\ -2^{n+e}M' & if\ (\alpha,\beta) \in G \cap L', \\ -2^{n+e}M' & if\ (\alpha,\beta) \in H \cap (I' \cup K'), \\ 2^{n+2e}M' & if\ (\alpha,\beta) \in H \cap L'). \end{cases}$$

(4) Let $A \neq 0, B \neq 0$.

(a) If $A' = 0, B' = 0$, then

$$T_b^{[4(a)]} = \begin{cases} (-1)^{\frac{m}{e}} 2^{m+n} M'' & if\ (\alpha,\beta) \in A' \cap (I \cup K), \\ 0 & if\ (\alpha,\beta) \in A' \cap J, \\ (-1)^{\frac{m}{e}+1} 2^{m+n+e} M'' & if\ (\alpha,\beta) \in A' \cap L, \end{cases}$$

where $M'' = \chi_1((1+c^{-1})\beta)\chi_1(Ax_A^{2^k+1})$.

(b) If $A' = 0, B' \neq 0$, then $S_{c\alpha,c^{-1}\beta} = 0$ and hence

$$T_b^{[4(b)]} = 0.$$

(c) If $A' \neq 0, B' = 0$, then

$$T_b^{[4(c)]} = \begin{cases} 2^n M'' & if\ (\alpha,\beta) \in G' \cap (I \cup K), \\ 0 & if\ (\alpha,\beta) \in (G' \cup H') \cap J, \\ -2^{n+e}M'' & if\ (\alpha,\beta) \in G' \cap L, \\ -2^{n+e}M'' & if\ (\alpha,\beta) \in H' \cap (I \cup K), \\ 2^{n+2e}M'' & if\ (\alpha,\beta) \in H' \cap L. \end{cases}$$

(d) If $A' \neq 0, B' \neq 0$, then

$$T_b^{[4(d)]} = \begin{cases} 2^n M''' & if\ (\alpha,\beta) \in (I \cup K) \cap (I' \cup K'), \\ 0 & if\ (\alpha,\beta) \in (I \cup K \cup L) \cap J', \\ -2^{n+e}M''' & if\ (\alpha,\beta) \in (I \cup K) \cap L', \\ 0 & if\ (\alpha,\beta) \in J \cap (I' \cup J' \cup K' \cup L'), \\ -2^{n+e}M''' & if\ (\alpha,\beta) \in L \cap (I' \cup K'), \\ 2^{n+2e}M''' & if\ (\alpha,\beta) \in \mathcal{L} \cap \mathcal{L}', \end{cases}$$

where $M''' = \chi_1((1+c^{-1})\beta)\chi_1(Ax_A^{2^k+1} + A'x_{A'}^{2^k+1})$.

We now summarize the above discussion in the form of following theorem.

**Theorem 6.3** *Let $F(x) = x^{2^k+1}$, $1 \le k < n$ be a function on $\mathbb{F}_{2^n}$, $n \ge 2$. Let $c \in \mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$ and $n/e$ be even, where $e = \gcd(k, n)$. With the prior notations, the $c$-BCT entry ${}_c\mathcal{B}_F(1, b)$ of $F$ at $(1, b)$ is given by*

$$\begin{aligned}
\frac{1}{q^2}\Bigg( & \sum_{(\alpha,\beta)\in A\cap A'} \chi_1(b(\alpha+\beta))T_b^{[1(a)]} + \sum_{(\alpha,\beta)\in A\cap(I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} \\
& + \sum_{(\alpha,\beta)\in A\cap L'} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} + \sum_{(\alpha,\beta)\in G\cap G'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\
& + \sum_{(\alpha,\beta)\in G\cap H'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + \sum_{(\alpha,\beta)\in H\cap G'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\
& + \sum_{(\alpha,\beta)\in H\cap H'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + \sum_{(\alpha,\beta)\in G\cap(I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} \\
& + \sum_{(\alpha,\beta)\in G\cap L'} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} + \sum_{(\alpha,\beta)\in H\cap(I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} \\
& + \sum_{(\alpha,\beta)\in H\cap L'} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} + \sum_{(\alpha,\beta)\in A'\cap(I\cup K)} \chi_1(b(\alpha+\beta))T_b^{[4(a)]} \\
& + \sum_{(\alpha,\beta)\in A'\cap L} \chi_1(b(\alpha+\beta))T_b^{[4(a)]} + \sum_{(\alpha,\beta)\in G'\cap(I\cup K)} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} \\
& + \sum_{(\alpha,\beta)\in G'\cap L} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} + \sum_{(\alpha,\beta)\in H'\cap(I\cup K)} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} \\
& + \sum_{(\alpha,\beta)\in H'\cap L} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} + \sum_{(\alpha,\beta)\in(I\cup K)\cap(I'\cup K')} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \\
& + \sum_{(\alpha,\beta)\in(I\cup K)\cap L'} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} + \sum_{(\alpha,\beta)\in(I'\cup K')\cap L} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \\
& + \sum_{(\alpha,\beta)\in L'\cap L} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \Bigg).
\end{aligned}$$

***Remark 4.3*** It is natural to wonder if expressing the $c$-BCT entries via Weil sums will have an effect on computation. We implemented such a computation for small dimensions and achieved a speed up of at least tenfold over the brute force or even the Walsh-Hadamard characterization of the $c$-BCT [16].

## 7 Discussion on equivalence

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

**Table 1** $c$-BCT entries of $x^{17}$ and $x^5 + gx^{17}$

| $c$ | Set of $c$-BCT entries of $x^{17}$ | Set of $c$-BCT entries of $G(x)$ |
|---|---|---|
| $g$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^2$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^3$ | {0,1,2,3,5} | {0,1,2,3,4,5} |
| $g^4$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^5$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^6$ | {0,1,2,3,5} | {0,1,2,3,4,5,6} |
| $g^7$ | {0,1,2,3,4,5} | {0,1,2,3,4,5,6} |
| $g^8$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^9$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^{10}$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^{11}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{12}$ | {0,1,2,3,5} | {0,1,2,3,4,5} |
| $g^{13}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{14}$ | {0,1,2,3,4,5} | {0,1,2,3,4,5,6} |
| $g^{15}$ | {0,1,2,3,5} | {0,1,2,3,4,5} |
| $g^{16}$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^{17}$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^{18}$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^{19}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{20}$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^{21}$ | {0,1,4} | {0,1,4} |
| $g^{22}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{23}$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^{24}$ | {0,1,2,3,5} | {0,1,2,3,4,5,6} |
| $g^{25}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{26}$ | {0,1,2,3} | {0,1,2,3,4,5} |
| $g^{27}$ | {0,1,2,3,4} | {0,1,2,3,4,5,6} |
| $g^{28}$ | {0,1,2,3,4,5} | {0,1,2,3,4,5,6} |
| $g^{29}$ | {0,1,2,3,4} | {0,1,2,3,4,5} |
| $g^{30}$ | {0,1,2,3,5} | {0,1,2,3,4,5,6} |
| $g^{31}$ | {0,1,2,3,4} | {0,1,2,3,4,5} |

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

becomes

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

We consider the binomial $G(x) = x^{2^k+1} + ux^{2^{n-k}+1} \in \mathbb{F}_{2^n}[x]$, which is a PP if and only if $\frac{n}{e}$ is odd and $u \neq g^{t(2^e-1)}$, where $e = \gcd(n,k) = \gcd(n-k,k)$ and $g$ is the primitive element of $\mathbb{F}_{2^n}$. Notice that $G(x) = (L \circ F)(x)$ where $L(x) = x^{2^k} + ux$ and $F(x) = x^{2^{n-k}+1}$. When

$n = 6, k = 2$ and $u = g$, where $g$ is a root of the primitive polynomial $y^6 + y^4 + y^3 + y + 1$ over $\mathbb{F}_2$, then $L(x)$ and $G(x)$ are PP. It is easy to see from the Table 1 in the Appendix 1 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.

## Appendix

Let $G(x) = x^5 + gx^{17} = (x^4 + gx) \circ x^{17} \in \mathbb{F}_{2^6}[x]$, where $g$ is a root of the primitive polynomial $y^6 + y^4 + y^3 + y + 1$ over $\mathbb{F}_2$. The following Table 1 gives the set of the $c$-BCT entries for $x^{17}$ as well as $G(x) = x^5 + gx^{17}$ for all $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$. In view of the discussion in Section 7, it is sufficient to compute the set of $c$-BCT entries for either of $c$ or $c^{-1}$ as they are going to be exactly the same.

**Acknowledgements** The authors would like to thank the editor for efficiently handling our paper and to the reviewers for their careful reading, beneficial comments and constructive suggestions. Sartaj Ul Hasan is partially supported by MATRICS grant MTR/2019/000744 from the Science and Engineering Research Board, Government of India.

## References

1. Bartoli, D., Calderini, M.: On construction and (non)existence of $c$-(almost) perfect nonlinear functions. Finite Fields Appl. **72**, 101835 (2021)
2. Boura, C., Canteaut, A.: On the boomerang uniformity of cryptographic Sboxes. IACR Trans. Symmetric Cryptol. **2018**(3), 290–310 (2018)
3. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge, Cambridge (2021)
4. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: a new cryptanalysis tool. In: Nielsen, J., Rijmen, V. (eds.) Advances in Cryptology-EUROCRYPT 2018, LNCS 10821, pp. 683–714. Springer, Cham (2018)
5. Coulter, R.S.: On the evaluation of a class of Weil sums in characteristic 2. New Zealand J. Math. **28**, 171–184 (1999)
6. Cusick, T.W., Stănică, P.: Cryptographic boolean functions and applications (Ed. 2), Academic Press, San Diego, CA, (2017)
7. S. Eddahmani, S.: Mesnager, explicit values of the tables DDT, BCT, FBCT, and FBDT of the inverse, the Gold, and the Bracken-Leander functions, Boolean Functions and their Applications (BFA 2021) (2021)
8. Ellingsen, P., Felke, P., Riera, C., Stănică, P., Tkachenko, A.: C-differentials, multiplicative uniformity and (almost) perfect $c$-nonlinearity. IEEE Trans. Inform. Theory **66**(9), 5781–5789 (2020)
9. Hasan, S.U., Pal, M., Riera, C., Stănică, P.: On the $c$-differential uniformity of certain maps over finite fields. Des. Codes Cryptogr **89**(2), 221–239 (2021)
10. Hasan, S.U., Pal, M., Stănică, P.: Boomerang uniformity of a class of power maps. Des. Codes Cryptogr. **89**, 2627–2636 (2021)
11. Hasan, S.U., Pal, M., Stănică, P.: The $c$-differential uniformity and boomerang uniformity of two classes of permutation polynomials. IEEE Trans. Inform. Theory **68**(1), 679–691 (2022)
12. Lidl, R., Niederreiter, H.: FiniteFields (Ed. 2), Encycl. Math. Appl., vol.20, Cambridge Univ. Press, Cambridge (1997)
13. Li, K., Qu, L., Sun, B., Li, C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inform. Theory **65**(11), 7542–7553 (2019)
14. Mesnager, S., Riera, C., Stănică, P., Yan, H., Zhou, Z.: Investigations on $c$-(almost) perfect nonlinear functions. IEEE Trans. Inform. Theory **67**(10), 6916–6925 (2021)
15. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) Advances in Cryptology-EUROCRYPT 1993, LNCS 765, pp. 55–64. Springer, Berlin, Heidelberg (1994)

16. Stănică, P.: Investigations on $c$-boomerang uniformity and perfect nonlinearity. Discrete Appl. Math. **304**, 297–314 (2021)
17. Stănică, P.: Low $c$-boomerang uniformity of the swapped inverse function. Discrete Math. **344**(10), 112543 (2021)
18. Stănică, P.: 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
19. Stănică, P., Geary, A.: The $c$-differential behaviour of the inverse function under the $c$-equivalence. Cryptogr. Commun. **13**, 295–306 (2021)
20. Stănică, P., Riera, C., Tkachenko, A.: Characters, Weil sums and $c$-differential uniformity with an application to the perturbed Gold function, Cryptogr. Commun. **6**, 891–907 (2021)
21. Wagner, D.: The boomerang attack, In: Knudsen, L.R. (ed.) Fast Software Encryption-FSE 1999. LNCS 1636, Springer, Berlin, Heidelberg, pp. 156–170 (1999)
22. Zha, Z., Hu, L.: Some classes of power functions with low $c$-differential uniformity over finite fields. Des. Codes Cryptogr. **89**, 1193–1210 (2021)