Faculty and Researchers	Faculty and Researchers' Publications

2020-04-27

Investigations on c-Boomerang Uniformity and Perfect Nonlinearity

Stnic, Pantelimon

ArXiv

Investigations on c-Boomerang Uniformity and Perfect Nonlinearity

Pantelimon Stănică

Applied Mathematics Department,
Naval Postgraduate School, Monterey, USA.
E-mail: pstanica@nps.edu

April 27, 2020

Abstract

We defined in [21] a new multiplicative c-differential, and the corresponding c-differential uniformity and we characterized the known perfect nonlinear functions with respect to this new concept, as well as the inverse in any characteristic. The work was continued in [29], investigating the c-differential uniformity for some further APN functions. Here, we extend the concept to the boomerang uniformity, introduced at Eurocrypt '18 by Cid et al. [16], to evaluate S-boxes of block ciphers, and investigate it in the context of perfect nonlinearity and related functions.

Keywords: Boolean, p-ary functions, c-differentials, differential uniformity, boomerang uniformity, perfect and almost perfect c-nonlinearity
MSC 2000: 06E30, 11T06, 94A60, 94C10.

1 Introduction

In this paper we extend the notion of boomerang uniformity using a previously defined [21] multiplier differential (in any characteristic). We characterize some of the known perfect nonlinear functions and the inverse function through this new concept. We also characterize this concept via the Walsh transforms as Lie et al. [24] did for the classical boomerang uniformity.

The objects of this study are Boolean and p-ary functions (where p is an odd prime) and some of their differential properties. We will introduce here only some needed notation, and the reader can consult [9, 12, 13, 19, 27, 30] for more on Boolean and p-ary functions.

For a positive integer n and p a prime number, we let $\mathbb{F}_{p^n}$ be the finite field with p^n elements, and $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ be the multiplicative group (for $a \neq 0$, we often write $\frac{1}{a}$ to mean the inverse of a in the multiplicative group). We let $\mathbb{F}_p^n$ be the n-dimensional vector space over $\mathbb{F}_p$. We use $\#S$ to denote the cardinality of a set S and $\bar{z}$, for the complex conjugate. We call a function from $\mathbb{F}_{p^n}$ (or $\mathbb{F}_p^n$) to $\mathbb{F}_p$ a p-ary function on n variables. For positive integers n and m, any map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ (or, $\mathbb{F}_p^n \to \mathbb{F}_p^m$) is called a vectorial p-ary function, or (n,m)-function. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{p^n}$ (using some identification, via a basis, of the finite field with the vector space) of the form $F(x) = \sum_{i=0}^{p^n-1} a_i x^i$, $a_i \in \mathbb{F}_{p^n}$, whose algebraic degree is then the largest Hamming weight of the exponents i with $a_i \neq 0$. For $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ we define the Walsh-Hadamard transform to be the integer-valued function $\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{f(x) - \operatorname{Tr}_n(ux)}$, $u \in \mathbb{F}_{p^n}$, where $\zeta_p = e^{\frac{2\pi i}{p}}$ and $\operatorname{Tr}_n : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace function, given by $\operatorname{Tr}_n(x) = \sum_{i=0}^{n-1} x^{p^i}$ (we will denote it by Tr, if the dimension is clear from the context). The Walsh transform $\mathcal{W}_F(a, b)$ of an (n, m)-function F at $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$ is the Walsh-Hadamard transform of its component function $\operatorname{Tr}_m(bF(x))$ at a, that is,

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\operatorname{Tr}_m(bF(x)) - \operatorname{Tr}_n(ax)}.$$

(If one wishes to work with vector spaces, then one can replace the Tr by any scalar product on that environment.)

Given a p-ary function f, the derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the p-ary function $D_a f(x) = f(x + a) - f(x)$, for all $x \in \mathbb{F}_{p^n}$, which can be naturally extended to vectorial p-ary functions.

For an (n, n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - F(x) = b\}$. We call the quantity $\delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{p^n}, a \neq 0\}$ the differential uniformity of F. If $\delta_F = \delta$, then we say that F is differentially δ-uniform. If $\delta = 1$, then F is called a perfect nonlinear (PN) function, or planar function. If $\delta = 2$, then F is called an almost perfect nonlinear (APN) function. It is well known that PN functions do not exist if $p = 2$.

The paper is organized as follows. Section 2 contains some background on differential and boomerang uniformity and our extension to c-boomerang uniformity. Section 3 contains some characterizations of this concept and

connections with prior c-differential uniformity, and Section 4 gives its description via Walsh transforms. Section 5 puts together two lemmas needed in the remaining of the paper, and Section 6 deals with perfect nonlinearity and c-boomerang uniformity. Section 7 characterizes this uniformity for the inverse function in any characteristic and Section 8 concludes the paper. An appendix with some computational data follows the references.

2   Differential and boomerang uniformity

Wagner [32] introduced the boomerang attack against block ciphers using S-boxes. The concept was picked up and used in [3, 22] on some real ciphers (see also [2, 23]). Ten years later, however, a theoretical new cryptanalysis tool based upon this attack was introduced at EUROCRYPT 2018 by Cid et al. [16] namely, the Boomerang Connectivity Table (BCT) and Boomerang Uniformity. In [16], the authors analyzed some of the properties of BCT, like its relationship with the Differential Distribution Table (DDT). They proved that perfect nonlinear (APN) S-boxes (that is, with 2-uniform DDT) always have 2-uniform BCT and for any choice of the parameters, and also showed that the BCT uniformity is greater than or equal to the DDT uniformity (we will display below precisely the relationship between these).

The initial concept of boomerang uniformity was defined for permutations (of course, proper S-boxes) in the following way.

Definition 1. *Let F be a permutation on $\mathbb{F}_{2^n}$ and $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. We define the entries of the* Boomerang Connectivity Table (BCT) *by*

$$\mathcal{B}_F(a, b) = \#\{x \in \mathbb{F}_{2^n} | F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a\},$$

where F^{-1} is the compositional inverse of F. The boomerang uniformity *of F is defined as*
$$\beta_F = \max_{a, b \in \mathbb{F}_{p^n} *} \mathcal{B}_F(a, b).$$
We also say that F is a β_F-uniform BCT function.

Recently, BCT and the boomerang uniformity were further studied by Boura and Canteaut [6]. They showed that the boomerang uniformity is only an affine equivalence invariant but not necessarily, extended affine nor CCZ-equivalence invariant. Further, they also obtained the boomerang uniformity of the inverse function $F(x) = x^{2^n - 2}$ over $\mathbb{F}_{2^n}$, for n even, namely, $\beta_F = 4, 6$, when $n \equiv 2 \pmod 4$, respectively, $n \equiv 0 \pmod 4$. Also, for the

Gold function $G(x) = x^{2^t+1}$ over $\mathbb{F}_{2^n}$, where $n \equiv 2 \pmod 4$, t even with $\gcd(t, n) = 2$, then $\delta_G = \beta_G = 4$.

Mesnager et al. [28] continued the work and showed that the differential uniformity for quadratic functions on $\mathbb{F}_{q^n}$ (q is a 2-power) is always $\geq q$, and if it happens to be equal to q for a permutations F then its boomerang uniformity must be q, as well. In fact [24], in general, for quadratic permutations F, then we have,

$$\delta_F \leq \beta_F \leq \delta_F(\delta_F - 1).$$

It is also easy to show that for monomials $F(x) = x^d$, then $\beta_F = \max_{b \neq 0} \beta_F(1, b)$. For the Bracken-Tan-Tan function (which is an extension of Budaghyan-Carlet function [10]), $F(x) = \alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$ (under some conditions on the parameters), then $\beta_F = 4$ (see [28]). More work has been done recently on BCT, and we mention here [7, 11, 25, 31].

Surely, $\Delta_F(a, b) = 0, 2^n$ and $\mathcal{B}_F(a, b) = 2^n$ whenever $ab = 0$. It is well-known from prior work that $\delta_F = \delta_{F^{-1}}$ and $\beta_F = \beta_{F^{-1}}$. In general, for permutations, $\beta_F \geq \delta_F$ and they are equal for APN permutations. A natural question is what is the algebraic difference between these two concepts and Boura and Canteaut answered that question in [6], showing that

$$\mathcal{B}_F(a, b) = \Delta_F(a, b) + \sum_{\gamma \in \mathbb{F}_{p^n}^*, \gamma \neq b} \# \left(\mathcal{U}_{\gamma,a}^{F^{-1}} \cap \left(b + \mathcal{U}_{\gamma,a}^{F^{-1}} \right) \right),$$

where $\mathcal{U}_{\gamma,a}^{F^{-1}} = \{x \in \mathbb{F}_{p^n} | D_\gamma F^{-1}(x) = a\}$. This was reformulated by Mesnager et al. [28] in the following way:

$$\mathcal{B}_F(a, b) = \sum_{\gamma \in \mathbb{F}_{p^n}^*} \# \left(\mathcal{U}_{\gamma,a}^F \cap \left(b + \mathcal{U}_{\gamma,a}^F \right) \right),$$

where $\mathcal{U}_{\gamma,a}^F = \{x \in \mathbb{F}_{p^n} | D_\gamma F(x) = a\}$, and further, by Li et al. [24], as

$$\mathcal{B}_F(a, b) = \# \left\{ (x, y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \begin{matrix} F(x) + F(y) = b \\ F(x+a) + F(y+a) = b \end{matrix} \right\}$$

and easily observed in [28] that this transforms into (labeling $y = x + \gamma$),

$$\mathcal{B}_F(a, b) = \# \left\{ (x, \gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid \begin{matrix} F(x+\gamma) + F(x) = b \\ F(x+\gamma+a) + F(x+a) = b \end{matrix} \right\}$$

$$= \sum_{\gamma \in \mathbb{F}_{p^n}} \# \left\{ x \in \mathbb{F}_{p^n} \mid D_\gamma F(x) = b \text{ and } D_\gamma F(x+a) = b \right\}. \tag{1}$$

4

Avoiding the inverse of F, allows these last expressions to define the boomerang uniformity for functions that are not necessarily permutations.

Before, we continue with our approach, let us recall the concept we (along with others) introduced in [21] (we will define it in general on $\mathbb{F}_{p^n}$, p prime, not only for $p = 2$).

Inspired by a practical differential attack developed in [5] (though, via a different differential), we extended the definition of derivative and differential uniformity in [21], in the following way. For a p-ary (n, m)-function F : $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and $c \in \mathbb{F}_{p^m}$, the *(multiplicative) c-derivative* of F with respect to $a \in \mathbb{F}_{p^n}$ is the function

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

(Observe that, if $c = 1$, then we obtain the usual derivative, and, if $c = 0$ or $a = 0$, then we obtain a shift of the function, in the input/output.)

For an (n, n)-function F, and $a, b \in \mathbb{F}_{p^n}$, we let the entries of the c-Difference Distribution Table (c-DDT) be defined by $_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - cF(x) = b\}$. We call the quantity

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

the *c-differential uniformity* of F (observe that we slightly change here the way we denoted the c-differential uniformity in [21]). If $\delta_{F,c} = \delta$, then we say that F is differentially (c, δ)-uniform (or that F has c-uniformity δ, or for short, *F is δ-uniform c-DDT*). If $\delta = 1$, then F is called a *perfect c-nonlinear* (*PcN*) function (certainly, for $c = 1$, they only exist for odd characteristic p; however, as proven in [21], there exist PcN functions for $p = 2$, for all $c \neq 1$). If $\delta = 2$, then F is called an *almost perfect c-nonlinear* (*APcN*) function. When we need to specify the constant c for which the function is PcN or APcN, then we may use the notation c-PN, or c-APN. It is easy to see that if F is an (n, n)-function, that is, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, then F is PcN if and only if $_cD_aF$ is a permutation polynomial.

In light of the formulations (1) via differentials, by using our c-differential concept of [21], we extend the notion of boomerang uniformity to c-boomerang uniformity for all characteristics, in the following way (see Figure 1).

Definition 2. *For an (n, n)-function F, $c \neq 0$, and $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$, we define the c-Boomerang Connectivity Table (c-BCT) entry at (a, b) to be*

$$_c\mathcal{B}_F(a, b) = \#\left\{x \in \mathbb{F}_{p^n} \mid F^{-1}(c^{-1}F(x + a) + b) - F^{-1}(cF(x) + b) = a\right\}. \quad (2)$$

Further, the c-boomerang uniformity of F is defined by

$$\beta_{F,c} = \max_{a,b \in \mathbb{F}_{p^n}*} {_c\mathcal{B}_F(a, b)}.$$
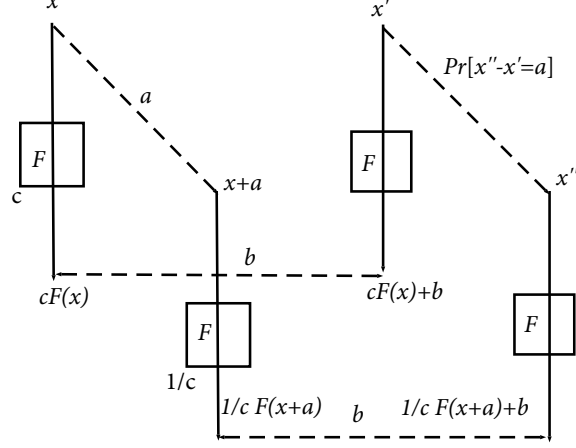
5

Figure 1: View on the c-boomerang uniformity

If $\beta_{F,c} = \beta$, we also say that F is a β-uniform c-BCT function.

3 Characterizations of c-boomerang uniformity

As in the classical case, we find an alternative formulation that avoids inverses, allowing the definition to be extended to all (n,n)-function, not only permutations. Though the proof is not complicated, we label as a theorem, since it is the way to extend the definition to non-permutations.

Theorem 3. *For an (n,n)-permutation function F, $c \neq 0$, the entries of the c-Boomerang Connectivity Table at $(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ are given by*

$$_c\mathcal{B}_F(a,b) = \# \left\{ (x,\gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \,\middle|\, \begin{matrix} F(x+\gamma)-cF(x)=b \\ F(x+\gamma+a)-c^{-1}F(x+a)=b \end{matrix} \right\}$$

$$= \sum_{\gamma \in \mathbb{F}_{p^n}} \# \left\{ x \in \mathbb{F}_{p^n} \,\middle|\, {}_cD_\gamma F(x) = b \text{ and } {}_{c^{-1}}D_\gamma F(x+a) = b \right\}.$$

(We shall call the system above, the c-boomerang system, for easy referral.)

Proof. Let $y = F^{-1}(cF(x)+b)$ in (2). If that is the case, then $F(y)-cF(x) = b$. Further, from (2), we obtain,

$$F^{-1}(c^{-1}F(x+a)+b) = y+a,$$

6

and so,

$$c^{-1}F(x+a) + b = F(y+a) \iff F(y+a) - c^{-1}F(x+a) = b.$$

The reciprocal is immediate by backtracking the argument: the second equation in the system implies $F(y+a) = c^{-1}F(x+a) + b$ and applying F^{-1}, we get $F^{-1}(c^{-1}F(x+a) + b) = y + a = F^{-1}(F(y)) + a = F^{-1}(cF(x) + b) + a$, using the first equation. Finally, taking $y = x + \gamma$, the theorem follows. □

Remark 1. *We could have defined the BCT entries of F at (a, b) to be*

$$_c\mathcal{B}_F(a, b) = \#\left\{(x, \gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \,\middle|\, \begin{matrix} F(x+\gamma)-cF(x)=b \\ cF(x+\gamma+a)-F(x+a)=cb \end{matrix}\right\},$$

thus allowing $c = 0$. However, in the case of $c = 0$, we would obtain $_0\mathcal{B}_F(a, b) = \#\left\{(x, \gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \,\middle|\, F(x+\gamma) = b \text{ and } F(x+a) = 0\right\}$; when F is a permutation, we get $x = F^{-1}(0) - a$ and $\gamma = F^{-1}(b) - F^{-1}(0) + a$, rendering $\beta_{F,0} = 1$, regardless of the function. For this reason, we decided to remove $c = 0$ out of allowable multipliers.

Remark 2. *For whatever reason, one can define the c-DDT and c-BCT, and the respective uniformities, even for arbitrary (n, m)-functions. That is the reason why in some of our results, when it makes no difference for the proofs (except tracking carefully the parameters, of course), we take arbitrary (n, m)-functions.*

While we already knew that, in general, the c-differential uniformity of F, F^{-1} are not the same, we show below a connection (that we did not observe in [21]) between some of the entries in the c-Differential Distribution Table of a permutation monomial F and the one of the inverse of F.

Proposition 4. *Let $F(x) = x^d$ be a permutation (hence, $\gcd(d, p^n - 1) = 1$) monomial function on $\mathbb{F}_{p^n}$ and $c \neq 0$. Then,*

$$_c\Delta_{F^{-1}}(a, b) = {}_{c^{-d}}\Delta_F(bc^{-1}, -a\,c^{-d}).$$

Proof. Observe that, in general (assuming $c \neq 0$),

$$F^{-1}(x+a) - cF^{-1}(x) = b \iff$$
$$F(F^{-1}(x+a)) = F(cF^{-1}(x) + b) \iff$$
$$F(cF^{-1}(x) + b) - x = a \iff$$
$$F(F^{-1}(x)) - F(cF^{-1}(x) + b) = a.$$

If F is the monomial x^d, then the last equation above becomes

$$F(F^{-1}(x)) - c^d F(F^{-1}(x) + bc^{-1}) = a \iff$$
$$F(F^{-1}(x) + bc^{-1}) - c^{-d} F(F^{-1}(x)) = -ac^{-d},$$

and the proposition will follow easily. □

We next show a connection between c-differential and c-boomerang uniformities.

Theorem 5. *Let F be a permutation function on $\mathbb{F}_{p^n}$, $(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ and $c \neq 0, 1$. Then $_c\mathcal{B}_F(0,b) = {}_c\Delta_F(0,b)$. If $p = 2$, then*

$$_c\mathcal{B}_F(a,b) = {}_c\Delta_F(a,b) + \sum_{a \neq \gamma \in \mathbb{F}_{p^n}} \# \left\{ x \in \mathbb{F}_{p^n} \; \middle| \; \begin{matrix} cD_\gamma F(x)=b \\ c^{-1}D_\gamma F(x+a)=b \end{matrix} \right\},$$

if either $c = -1$ or $b = 0$. Consequently, $\beta_{F,-1} \geq \delta_{F,-1}$, for all permutations F (it is known [6] that $\beta_{F,1} \geq \delta_{F,1}$).

Proof. If $a = 0$ and $c \neq 0, \pm 1$, then

$$_c\mathcal{B}_F(0,b) = \# \left\{ (x,\gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \; \middle| \; \begin{matrix} F(x+\gamma)-cF(x)=b \\ F(x+\gamma)-c^{-1}F(x)=b \end{matrix} \right\},$$

and so, $F(x) = 0$ and $F(x + \gamma) = b$, which has only one solution $(x, \gamma) = (F^{-1}(0), F^{-1}(b) - F^{-1}(0))$. Further, $_c\Delta_F(0,b) = \#\{x \in \mathbb{F}_{p^n} \,|\, {}_cD_\gamma F(x) = F(x) - cF(x) = b\}$, which also has one solution, and so, $_c\mathcal{B}_F(0,b) = {}_c\Delta_F(0,b)$. When $a = 0$ and $c = -1$, the values of the two uniformities are the same, since

$$_{-1}\mathcal{B}_F(0,b) = \# \left\{ (x,\gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \; \middle| \; \begin{matrix} F(x+\gamma)+F(x)=b \\ F(x+\gamma)+F(x)=b \end{matrix} \right\}$$
$$= \# \left\{ (x,\gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \; \middle| \; F(x+\gamma) + F(x) = b \right\} = {}_{-1}\Delta_F(0,b),$$

and the first claim is shown.

Assume now that $a \neq 0$. If $\gamma = 0$, then (we use the logical conjunction "$\wedge$" to denote "and").

$$\left\{ x \in \mathbb{F}_{p^n} \; \middle| \; F(x) - cF(x) = b \wedge F(x+a) - c^{-1}F(x+a) = b \right\}$$
$$= \left\{ x \in \mathbb{F}_{p^n} \; \middle| \; F(x) = \frac{b}{1-c} \wedge F(x+a) = \frac{b}{1-c^{-1}} \right\}.$$

8

Thus, for c fixed, we get $x = F^{-1}\left(\frac{b}{1-c}\right)$ and so, $a = F^{-1}\left(\frac{b}{1-c^{-1}}\right) - F^{-1}\left(\frac{b}{1-c}\right)$, since F is a permutation. Thus, when $\gamma = 0$,

$$\#\left\{x \in \mathbb{F}_{p^n} \;\middle|\; \begin{matrix} F(x)-cF(x)=b \\ F(x+a)-c^{-1}F(x+a)=b \end{matrix}\right\} = \begin{cases} 1 & \text{if } a = F^{-1}\left(\frac{b}{1-c^{-1}}\right) - F^{-1}\left(\frac{b}{1-c}\right) \\ 0 & \text{otherwise.} \end{cases}$$

If $\gamma = a$ and $p = 2$, then

$$\left\{x \in \mathbb{F}_{p^n} \;\middle|\; \begin{matrix} F(x+a)-cF(x)=b \\ F(x)-c^{-1}F(x+a)=b \end{matrix}\right\} = \left\{x \in \mathbb{F}_{p^n} \;\middle|\; \begin{matrix} F(x+a)-cF(x)=b \\ F(x+a)-cF(x)=-bc \end{matrix}\right\},$$

which is $\emptyset$, unless $b = 0$, or $c = -1$, in which case we have

$$\#\left\{x \in \mathbb{F}_{p^n} \;\middle|\; F(x+a) - cF(x) = b\right\} = {}_c\Delta_F(a,b),$$

Thus,

$$_c\mathcal{B}_F(a,b) = {}_c\Delta_F(a,b) + \sum_{a \neq \gamma \in \mathbb{F}_{p^n}} \#\left\{x \in \mathbb{F}_{p^n} \;\middle|\; \begin{matrix} cD_\gamma F(x)=b \\ c^{-1}D_\gamma F(x+a)=b \end{matrix}\right\},$$

if either $c = -1$ or $b = 0$. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

4 Characterizing c-boomerang uniformity via the Walsh transform

Using a method of Carlet [14] and Chabaud and Vaudenay [15] connecting the differential uniformity of an (n,m)-function to its Walsh coefficients, we characterized the c-differential uniformity in [21] and Li et al. [24] characterized the boomerang uniformity. We can use a similar method to do the same for the c-boomerang uniformity, in any characteristic.

Theorem 6. *Let $c \in \mathbb{F}_{p^m}^*$ and n, m, δ be fixed positive integers. Let F be an (n,m)-function, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and $\phi_\beta(x) = \sum_{j \geq 0} A_j x^j$ be a polynomial over $\mathbb{R}$ such that $\phi_\beta(x) = 0$ for $x \in \mathbb{Z}, 1 \leq x \leq \beta$, and $\phi_\beta(x) > 0$, for*

9

$x \in \mathbb{Z}, x > \beta$. We then have

$$p^{m+n}A_0 + \sum_{j \geq 1} p^{-(2j-1)(m+n)} A_j \sum_{\substack{w_1,\ldots,w_j \in \mathbb{F}_{p^n} \\ z_1,\ldots,z_j \in \mathbb{F}_{p^n} \\ u_1,\ldots,u_j \in \mathbb{F}_{p^m} \\ v_1,\ldots,v_j \in \mathbb{F}_{p^m} \\ \sum_{i=1}^{j}(w_i+z_i)=0 \\ \sum_{i=1}^{j}(u_i+v_i)=0}}$$

$$\prod_{i=1}^{j} \left(\mathcal{W}_F(u_i, z_i)\overline{\mathcal{W}_F}(cu_i, -w_i)\mathcal{W}_F(v_i, -z_i)\overline{\mathcal{W}_F}(c^{-1}v_i, w_i) \right) \geq 0,$$

with equality if and only if F is β-uniform c-BCT.

Proof. We follow mostly [14, 21, 24], pointing out the differences, where applicable. Let $a \in \mathbb{F}_{p^n}, d \in \mathbb{F}_{p^m}$ be arbitrary elements. We let $n_F(a,b,c) = \#\{(x,\gamma) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid {}_cD_\gamma F(x) = {}_cD_\gamma F(b), {}_{c^{-1}}D_\gamma F(x+a) = {}_cD_\gamma F(b)\} = \#\{(x,y) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \mid F(y) - cF(x) = b, F(y+a) - c^{-1}F(x+a) = b\} \geq 0$. From the definition of ϕ_β, for c fixed, and for all $a, b \in \mathbb{F}_{p^n}$, then,

$$\sum_{j \geq 0} A_j \left(n_F(a,b,c) \right)^j \geq 0,$$

with equality if and only if ${}_c\mathcal{B}_F(a,b) = \beta$. Consequently, running with all $a, b \in \mathbb{F}_{p^n}$, any (n,m)-function F satisfies

$$\sum_{j \geq 0} A_j \sum_{a,b \in \mathbb{F}_{p^n}} \left(n_F(a,b,c) \right)^j \geq 0,$$

with equality if and only of $\beta_{F,c} = \beta$.

Using the well-known,

$$\sum_{v \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_m(v\alpha)} = \begin{cases} 0 & \text{if } \alpha \neq 0 \\ p^m & \text{if } \alpha = 0, \end{cases} \tag{3}$$

we see that

$$n_F(a,b,c) = p^{-2m} \sum_{x,y \in F_{p^n}, u,v \in F_{p^m}} \zeta_p^{\mathrm{Tr}_m(u(F(y)-cF(x)-b))+\mathrm{Tr}_m(v(F(y+a)-c^{-1}F(x+a)-b))},$$

which, when run for all j tuples of parameters ($j \geq 1$ is fixed) renders

$$\sum_{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}} (n_F(a,b,c))^j$$

$$= p^{-2jm} \sum_{\substack{a \in \mathbb{F}_{p^n} \ x_1,\ldots,x_j \in \mathbb{F}_{p^n} \\ b \in \mathbb{F}_{p^m} \ y_1,\ldots,y_j \in \mathbb{F}_{p^n} \\ u_1,\ldots,u_j \in \mathbb{F}_{p^m} \\ v_1,\ldots,v_j \in \mathbb{F}_{p^m}}} \zeta_p^{\sum_{i=1}^{j} \left[\mathrm{Tr}_m(u_i(F(y_i)-cF(x_i)-b)) + \mathrm{Tr}_m(v_i(F(y_i+a)-c^{-1}F(x_i+a)-b)) \right]}.$$

By (3), $\sum_{w_i \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(w_i(x_i'-x_i-a))} = p^n$, if $x_i' = x_i + a$ and 0, otherwise; similarly,

$\sum_{z_i \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_n(z_i(y_i'-y_i-a))} = p^n$, if $y_i' = y_i + a$ and 0, otherwise. Therefore,

$$\sum_{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}} (n_F(a,b,c))^j = p^{-2mj} \, p^{-2nj} \sum_{\substack{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m} \ x_1,\ldots,x_j,x_1',\ldots,x_j' \in \mathbb{F}_{p^n} \\ y_1,\ldots,y_j,y_1',\ldots,y_j' \in \mathbb{F}_{p^n} \\ w_1,\ldots,w_j,z_1,\ldots,z_j \in \mathbb{F}_{p^n} \\ u_1,\ldots,u_j,v_1,\ldots,v_j \in \mathbb{F}_{p^m}}}$$

$$\zeta_p^{\sum_{i=1}^{j} \left[\mathrm{Tr}_m(u_i(F(y_i)-cF(x_i)-b)) + \mathrm{Tr}_m(v_i(F(y_i')-c^{-1}F(x_i')-b)) + \mathrm{Tr}_n(w_i(x_i'-x_i-a)) + \mathrm{Tr}_n(z_i(y_i'-y_i-a)) \right]}$$

$$= p^{-2(m+n)j} \sum_{\substack{w_1,\ldots,w_j,z_1,\ldots,z_j \in \mathbb{F}_{p^n} \\ u_1,\ldots,u_j,v_1,\ldots,v_j \in \mathbb{F}_{p^m}}} \prod_{i=1}^{j} \left(\mathcal{W}_F(u_i,z_i)\overline{\mathcal{W}_F}(cu_i,-w_i)\mathcal{W}_F(v_i,-z_i)\overline{\mathcal{W}_F}(c^{-1}v_i,w_i) \right)$$

$$\sum_{a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_m\left(-a\sum_{i=1}^{j}(w_i+z_i)-b\sum_{i=1}^{j}(u_i+v_i)\right)}$$

$$= p^{-(2j-1)(m+n)} \sum_{\substack{w_1,\ldots,w_j \in \mathbb{F}_{p^n} \\ z_1,\ldots,z_j \in \mathbb{F}_{p^n} \\ u_1,\ldots,u_j \in \mathbb{F}_{p^m} \\ v_1,\ldots,v_j \in \mathbb{F}_{p^m} \\ \sum_{i=1}^{j}(w_i+z_i)=0 \\ \sum_{i=1}^{j}(u_i+v_i)=0}} \prod_{i=1}^{j} \left(\mathcal{W}_F(u_i,z_i)\overline{\mathcal{W}_F}(cu_i,-w_i)\mathcal{W}_F(v_i,-z_i)\overline{\mathcal{W}_F}(c^{-1}v_i,w_i) \right).$$

Surely, if $j = 0$, $\sum_{\substack{a \in \mathbb{F}_{p^n} \\ b \in \mathbb{F}_{p^m}}} (n_F(a,b,c))^j = p^{m+n}$ and the theorem follows. $\square$

As a particular case, we want to characterize the 1-uniform c-BCT functions. We can take the polynomial $\phi_1(x) = x - 1$, which certainly satisfies

11

the conditions of Theorem 6. Thus $A_0 = -1, A_1 = 1$ and the relation of Theorem 6 simplifies to

$$- p^{n+m} + p^{-(n+m)} \sum_{\substack{w,z \in \mathbb{F}_{p^n} \\ u,v \in \mathbb{F}_{p^m} \\ w=-z, u=-v}} \mathcal{W}_F(u, z) \overline{\mathcal{W}_F}(cu, -w) \mathcal{W}_F(v, -z) \overline{\mathcal{W}_F}(c^{-1}v, w)$$

$$= \sum_{\substack{z \in \mathbb{F}_{p^n} \\ v \in \mathbb{F}_{p^m}}} \mathcal{W}_F(-v, z) \overline{\mathcal{W}_F}(-cv, z) \mathcal{W}_F(v, -z) \overline{\mathcal{W}_F}(c^{-1}v, -z) \geq 0.$$

Thus, we obtain the next result.

Proposition 7. *Let m, n be fixed positive integers and $c \in \mathbb{F}_{p^m}$, $c \neq 0, 1$. Let F be an (n, m)-function. Then*

$$\sum_{\substack{z \in \mathbb{F}_{p^n} \\ v \in \mathbb{F}_{p^m}}} \mathcal{W}_F(-v, z) \overline{\mathcal{W}_F}(-cv, z) \mathcal{W}_F(v, -z) \overline{\mathcal{W}_F}(c^{-1}v, -z) \geq p^{2(n+m)},$$

with equality if and only if F is a 1-uniform c-BCT function.

5   Some needed lemmas

In the next few sections, we will investigate some known perfect nonlinear, as well as the inverse function (in all characteristics) with respect to the c-boomerang uniformity. We will need the following two lemmas. The proof of Lemma 8(i) can be found in [1] and Lemma 8(ii) is easy and argued in [21]. The proof of Lemma 9 is contained in [21].

Lemma 8. *Let n be a positive integer. We have:*

(i) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, has two solutions in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{b}{a^2}\right) = 0$, and zero solutions otherwise.*

(ii) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_{p^n}$, p odd, has (two, respectively, one) solutions in $\mathbb{F}_{p^n}$ if and only if the discriminant $a^2 - 4b$ is a (nonzero, respectively, zero) square in $\mathbb{F}_{p^n}$.*

Lemma 9. *Let p, k, n be integers greater than or equal to 1 (we take $k \leq n$, though the result can be shown in general). Then*

$$\gcd(2^k + 1, 2^n - 1) = \frac{2^{\gcd(2k,n)} - 1}{2^{\gcd(k,n)} - 1}, \ \ \textit{and if } p > 2, \textit{ then,}$$

$$\gcd(p^k + 1, p^n - 1) = 2, \ \ \textit{if } \frac{n}{\gcd(n,k)} \textit{ is odd,}$$

$$\gcd(p^k + 1, p^n - 1) = p^{\gcd(k,n)} + 1, \ \ \textit{if } \frac{n}{\gcd(n,k)} \textit{ is even.}$$

Consequently, if either n is odd, or $n \equiv 2 \pmod 4$ and k is even, then $\gcd(2^k + 1, 2^n - 1) = 1$ and $\gcd(p^k + 1, p^n - 1) = 2$, if $p > 2$.

We will be using throughout Hilbert's Theorem 90 (see [8]), which states that if $\mathbb{F} \hookrightarrow \mathbb{K}$ is a cyclic Galois extension and σ is a generator of the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$, then for $x \in \mathbb{K}$, the relative trace $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(x) = 0$ if and only if $x = \sigma(y) - y$, for some $y \in \mathbb{K}$.

6 Perfect nonlinearity and c-boomerang uniformity

The following are some of the known (see, for instance, [18, 20]) classes of PN functions (p must be odd).

Theorem 10. *The following functions $: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are perfect nonlinear:*

(1) $F(x) = x^2$ on $\mathbb{F}_{p^n}$.

(2) $F(x) = x^{p^k + 1}$ on $\mathbb{F}_{p^n}$ is PN if and only if $\frac{n}{\gcd(k,n)}$ is odd.

(3) $F(x) = x^{(3^k + 1)/2}$ is PN over $\mathbb{F}_{3^n}$ if and only if $\gcd(k, n) = 1$ and n is odd.

(4) $F(x) = x^{10} \pm x^6 - x^2$ is PN over $\mathbb{F}_{3^n}$ if and only if $n = 2$ or n is odd. In general, for $u \in \mathbb{F}_{3^n}$, $F(x) = x^{10} - ux^6 - u^2 x^2$ is PN over $\mathbb{F}_{3^n}$ if n is odd.

It is known that the boomerang uniformity equals the differential uniformity for perfect nonlinear functions. It is, of course, a natural question to ask what is the connection between these in the "c-context". The reader is pointed to [21] where we discussed the c-differential uniformity of the functions in Theorem 10. We will now concentrate on the c-boomerang uniformity of all of these classes (for the last function we will just provide some

computational data in the appendix). For $c \in \mathbb{F}_{3^n}$, and b fixed, we let μ_c denote the cardinality

$$\#\left\{(x,\gamma) \;\middle|\; \begin{array}{l} 2T_{\frac{3^k+1}{2}}(x+\gamma-1)-(c-c^{-1})T_{\frac{3^k+1}{2}}(x-1)+(c+c^{-1})T_{\frac{3^k-1}{2}}(x-1)=2b \\ 2T_{\frac{3^k-1}{2}}(x+\gamma-1)+(c+c^{-1})T_{\frac{3^k+1}{2}}(x-1)+(c^{-1}-c)T_{\frac{3^k-1}{2}}(x-1)=0 \end{array}\right\}, \quad (4)$$

where $T_\ell(w) = u^\ell + u^{-\ell}$, under $w = u + u^{-1}$, is the Chebyshev polynomial of the first kind. We will be using below the trivial identity, $T_{2\ell}(w)+2 = T_\ell^2(w)$.

Theorem 11. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ (p is an odd prime number) be the monomial $F(x) = x^d$, and $c \neq 0, 1$ be fixed. The following statements hold:*

(i) *If $d = 2$, then $\beta_{F,c} \leq 4$.*

(ii) *If $d = p^k + 1$, $\delta_d := \#\{\gamma \in \mathbb{F}_{p^n} \mid z^{p^k} + z + d = 0\}$, then*

$$\beta_{F,c} \geq \delta_{1-c^{-1}} \cdot (\delta_{1+c} + 1).$$

Moreover, when $n/\gcd(n,k)$ is odd, then $\beta_{F,c} \geq 2$, and when $n/\gcd(n,k)$ is even and $c^{-1} = z^{p^k} + z$, for some $z \neq 0$, then the c-boomerang uniformity of f is $\beta_{F,c} \geq p^g$, where $g = \gcd(n,k)$.

(iii) *Let $p = 3$. If $d = \dfrac{3^k+1}{2}$ and $ab \neq 0$, then $_c\mathcal{B}_F(a,b) \geq \mu_c$, where μ_c is defined in (4). In particular, when $c = -1$, then*

$$_c\mathcal{B}_F(a,b) \geq \#\left\{(x,\gamma) \;\middle|\; \begin{array}{l} T_{\frac{3^k+1}{2}}(x+\gamma-1)+T_{\frac{3^k-1}{2}}(x-1)=2b \\ T_{\frac{3^k-1}{2}}(x+\gamma-1)-T_{\frac{3^k+1}{2}}(x-1)=0 \end{array}\right\}.$$

Proof. Let $d = 2$ and consider the system $_cD_\gamma F(x) = b$, $_{c^{-1}}D_\gamma F(x + a) = b$. We do not care for the cases when $ab = 0$. If $ab \neq 0$, dividing by a^2 and relabeling, we may assume that $a = 1$. Next, subtracting the first from the second equation, we obtain

$$(x + \gamma) = \frac{c^{-1}(x+1)^2 - cx^2 - 1}{2},$$

which, when replaced back into the first equation, and expanded, renders

$$(1 - 2c^2 + c^4)x^4 + (4 - 4c^2)x^3 + (6 - 2c - 2c^2 - 2c^3)x^2$$
$$+ (4 - 4c)x + (1 - 2c + c^2 - 4bc^2) = 0.$$

which has at most four roots, so $_c\mathcal{B}_F(a,b) \leq 4$. We will see in the appendix that all values occur for the first few cases we considered.

We now consider the Gold case, $d = p^k + 1$. The c-boomerang system $_cD_\gamma F(x) = b$, $_{c^{-1}}D_\gamma F(x+a) = b$ (dividing by $a^{p^k+1} \neq 0$ and relabeling, we can assume that $a = 1$) becomes

$$(x+\gamma)^{p^k+1} - cx^{p^k+1} = b$$
$$(x+\gamma)^{p^k+1} - c^{-1}(x+1)^{p^k+1} + (x+\gamma)^{p^k} + (x+\gamma) + 1 = b,$$

eliminating $(x+\gamma)^{p^k+1}$ and expanding the remaining powers, renders

$$cx^{p^k+1} - c^{-1}(x^{p^k+1} + x^{p^k} + x + 1) + x^{p^k} + \gamma^{p^k} + x + \gamma + 1 = 0, \text{ or,}$$
$$(c - c^{-1})x^{p^k+1} + (1 - c^{-1})x^{p^k} + (1 - c^{-1})x + \left(\gamma^{p^k} + \gamma + (1 - c^{-1})\right) = 0. \tag{5}$$

The idea is to vanish the parenthesis containing γ, that is, $\gamma^{p^k} + \gamma + (1 - c^{-1}) = 0$ and the polynomial in x, namely, $(c - c^{-1})x^{p^k+1} + (1 - c^{-1})x^{p^k} + (1 - c^{-1})x = 0$, which is equivalent to $x\left((c+1)x^{p^k} + x^{p^k-1} + 1\right) = 0$. By relabeling $x \mapsto 1/x$, the second factor can be put into the form

$$x^{p^k} + x + (c+1) = 0,$$

For more accurate count, we let $\delta_d = \#\{\gamma \,|\, z^{p^k} + z + d = 0\}$. We easily infer now that, if $ab \neq 0$, $_c\mathcal{B}_F(a,b) \geq \delta_{1-c^{-1}} \cdot (\delta_{1+c} + 1)$.

Now, to show the second claim of (ii), we want to argue that for some $c \neq 0, 1$, we can always find some root γ for $\gamma^{p^k} + \gamma + (1 - c^{-1}) = 0$ in $\mathbb{F}_{p^n}$, p an odd prime. Let $g = \gcd(n, k)$.

We recall here the result from [17, 26] (we simplify some parameters, though). Let $f(z) = z^{p^k} - Az - B$ in $\mathbb{F}_{p^n}$, $g = \gcd(n, k)$, $m = n/\gcd(n, k)$ and $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^g}}$ be the relative trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^g}$. For $0 \leq i \leq m - 1$, we define $t_i = \frac{p^{nm} - p^{n(i+1)}}{p^n - 1}$, $\alpha_0 = A, \beta_0 = B$. If $m > 1$ (note that, if $m = 1$, gives $F(x) = x^2$, which was treated earlier), then, for $1 \leq r \leq m - 1$, we let $\alpha_r = A^{\frac{p^{k(r+1)}-1}{p^k-1}}$ and $\beta_r = \sum_{i=0}^r A^{s_i}B^{p^{ki}}$, where $s_i = \frac{p^{k(r+1)} - p^{k(i+1)}}{p^k-1}$, for $0 \leq i \leq r - 1$ and $s_r = 0$. The trinomial f has no roots in $\mathbb{F}_{p^n}$ if and only if $\alpha_{m-1} = 1$ and $\beta_{m-1} \neq 0$. If $\alpha_{m-1} \neq 1$, then it has a unique root, namely $x = \beta_{m-1}/(1 - \alpha_{m-1})$, and, if $\alpha_{m-1} = 1, \beta_{m-1} = 0$, it has p^g roots in $\mathbb{F}_{p^n}$ given by $x + \delta\tau$, where $\delta \in \mathbb{F}_{p^g}$, τ is fixed in $\mathbb{F}_{p^n}$ with $\tau^{p^k-1} = a$

(that is, a $(p^k - 1)$-root of a), and, for any $e \in \mathbb{F}_{p^n}^*$ with $\mathrm{Tr}_g(e) \neq 0$, then

$$x = \frac{1}{\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_{p^g}}(e)} \sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} e^{p^{kj}} \right) A^{t_i} B^{p^{ki}}.$$

Since in our case $A = -1$, $B = c+1$, and, as we did in [21], if n/g is odd, then $\gamma^{p^k} + \gamma + (1 - c^{-1}) = 0$ has a unique root in $\mathbb{F}_{p^n}$, since $\alpha_{\frac{n}{g}-1} = -1$, independent of c. Now, looking at $x^{p^k} + x + (c+1) = 0$, and by the same argument, it has a unique root, under n/g odd, and so, $_c\mathcal{B}_F(a,b) \geq 2$ in this case (we use the prior root $x = 0$, too).

Let $m := n/g$ be even. We switch the technique now. The equation in x already has a root, namely $x = 0$, so we want to show that there are values of c, for which $\gamma^{p^k} + \gamma + (1 - c^{-1}) = 0$ has p^g roots. We will, in fact, find many such classes of parameters c, below.

We denote by $\sigma_t \equiv t \pmod 2 \in \{0,1\}$ the parity of t. Observe that $\alpha_0 = \beta_0 = -1$. Since $\alpha_{m-1} = 1$ for equation $\gamma^{p^k} + \gamma + (1 - c^{-1}) = 0$, we need to show that $\beta_{m-1} = 0$, to be able to use [17]. We compute (using the fact that the parities of s_i, $0 \leq i \leq m-2$, are $\sigma_{s_i} = (m - 2 - i + 1) \pmod 2 = \sigma_{i-1}$, since m is even),

$$\begin{aligned} \beta_{m-1} &= \sum_{i=0}^{m-1} (-1)^{s_i} (1 - c^{-1})^{p^{ki}} = \sum_{i=0}^{m-1} (-1)^{i-1} \left(1 - (-c^{-1})^{p^{ki}} \right) \\ &= \sum_{i=0}^{m-1} (-1)^{i-1} - \sum_{i=0}^{m-1} (-1)^{i-1+p^{ki}} (c^{-1})^{p^{ki}}, \quad \text{since } m \text{ is even} \\ &= \sum_{i=0}^{m-1} (-1)^{i-1} (c^{-1})^{p^{ki}}. \end{aligned}$$

Now, let $z \neq 1$ be such that $z^{p^{km}-1} - 1 = 0$ (this always exists since km is a multiple of n). Observe (we will be using that later) that $z^{p^{km}} - z = 0$ and $z \neq 0, 1$. We now set $c^{-1} = z^{p^k} + z$ and so, the previous displayed equation becomes

$$\begin{aligned} \beta_{m-1} &= \sum_{i=0}^{m-1} (-1)^{i-1} (z^{p^k} + z)^{p^{ki}} \\ &= \sum_{i=0}^{m-1} (-1)^{i-1} z^{p^{k(i+1)}} + \sum_{i=0}^{m-1} (-1)^{i-1} z^{p^{ki}} \\ &= \sum_{i=1}^{m-1} \left((-1)^{i-1} + (-1)^i \right) z^{p^{ki}} + z - z^{p^{km}} \end{aligned}$$

16

$$= z - z^{p^{km}} = 0, \text{ from our choice of } z.$$

Therefore, by the result of [17, 26], we infer that the equation $z^{p^k} + z + (1 - c^{-1}) = 0$ has p^g solutions in $\mathbb{F}_{p^n}$. Thus, the initial Equation (5) has at least p^g solutions, and so, the c-boomerang uniformity in this case (under $\frac{n}{\gcd(n,k)}$ even) is at least p^g, where $g = \gcd(n, k)$.

Let us treat now the case of $d = (3^k + 1)/2$ in $\mathbb{F}_{3^n}$, where the system is now (recall that, since $p = 3$, $1 = -2$)

$$(x + \gamma)^{\frac{3^k+1}{2}} - cx^{\frac{3^k+1}{2}} = b$$

$$(x + \gamma + 1)^{\frac{3^k+1}{2}} - c^{-1}(x + 1)^{\frac{3^k+1}{2}} = b.$$

We will not use the same method as in [17], or [21] as permutation polynomials are not visibly involved here, rather we will modify the "seed" of the technique. Since $2|3^n - 1$, for all n, then we can always write $x - 1 = y + y^{-1}$ and $x + \gamma - 1 = z + z^{-1}$, for some $y, z \in \mathbb{F}_{3^n}$. The system becomes

$$(z + z^{-1} - 2)^{\frac{3^k+1}{2}} - c(y + y^{-1} - 2)^{\frac{3^k+1}{2}} = b$$

$$(z + z^{-1} + 2)^{\frac{3^k+1}{2}} - c^{-1}(y + y^{-1} + 2)^{\frac{3^k+1}{2}} = b,$$

that is,

$$\frac{(z - 1)^{3^k+1}}{z^{\frac{3^k+1}{2}}} - c\frac{(y - 1)^{3^k+1}}{y^{\frac{3^k+1}{2}}} = b$$

$$\frac{(z + 1)^{3^k+1}}{z^{\frac{3^k+1}{2}}} - c^{-1}\frac{(y + 1)^{3^k+1}}{y^{\frac{3^k+1}{2}}} = b,$$

which, by expansion, renders

$$\frac{z^{3^k+1} - z^{3^k} - z + 1}{z^{\frac{3^k+1}{2}}} - c\frac{y^{3^k+1} - y^{3^k} - y + 1}{y^{\frac{3^k+1}{2}}} = b$$

$$\frac{z^{3^k+1} + z^{3^k} + z + 1}{z^{\frac{3^k+1}{2}}} - c^{-1}\frac{y^{3^k+1} + y^{3^k} + y + 1}{y^{\frac{3^k+1}{2}}} = b, \text{ or,}$$

$$T_{\frac{3^k+1}{2}}(x + \gamma - 1) - T_{\frac{3^k-1}{2}}(x + \gamma - 1) - cT_{\frac{3^k+1}{2}}(x - 1) + cT_{\frac{3^k-1}{2}}(x - 1) = b$$

$$T_{\frac{3^k+1}{2}}(x + \gamma - 1) + T_{\frac{3^k-1}{2}}(x + \gamma - 1) + c^{-1}T_{\frac{3^k+1}{2}}(x - 1) + c^{-1}T_{\frac{3^k-1}{2}}(x - 1) = b,$$

17

where $T_\ell(u + u^{-1}) = u^\ell + u^{-\ell}$ is the Chebyshev polynomial of the first kind. Adding and subtracting these two equations will give

$$2T_{\frac{3^k+1}{2}}(x + \gamma - 1) - (c - c^{-1})T_{\frac{3^k+1}{2}}(x - 1) + (c + c^{-1})T_{\frac{3^k-1}{2}}(x - 1) = 2b$$
$$2T_{\frac{3^k-1}{2}}(x + \gamma - 1) + (c + c^{-1})T_{\frac{3^k+1}{2}}(x - 1) + (c^{-1} - c)T_{\frac{3^k-1}{2}}(x - 1) = 0. \tag{6}$$

Thus, $_c\mathcal{B}_F(a, b) \geq \#\{(x, \gamma) \mid (x, \gamma) \text{ satisfies (6)}\} = \mu_c.$ $\qquad\square$

7 The c-boomerang uniformity for the inverse function

We now deal with the binary inverse function.

Theorem 12. *Let $n \geq 3$ be a positive integer, $0, 1 \neq c \in \mathbb{F}_{2^n}$ and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the inverse function defined by $F(x) = x^{2^n - 2}$. If $n = 2$, $_c\mathcal{B}_F(a, b) \leq 1$ and if $n = 3$, $_c\mathcal{B}_F(a, b) \leq 2$. If $n \geq 4$, $_c\mathcal{B}_F(a, b) \leq 3$. Furthermore, $_c\mathcal{B}_F(a, ab) = 3$ (so, the c-boomerang uniformity of F is $\beta_{F,c} = 3$) if and only if any of the conditions happen:*

(i) $\mathrm{Tr}(c) = 0$ *and there exists b such that $(b^2 c + bc^2 + b + c^2 + 1)^2 \neq 0$ and* $\mathrm{Tr}\left(\frac{b^2 c^2 (bc + c + 1)}{(b^2 c + bc^2 + b + c^2 + 1)^2}\right) = 0.$

(ii) $\mathrm{Tr}(1/c) = 0$ *and there exists b such that $(b^2 c + bc^2 + b + c^2 + 1)^2 \neq 0$ and $\mathrm{Tr}\left(\frac{b^2 c^2 (bc + c + 1)}{(b^2 c + bc^2 + b + c^2 + 1)^2}\right) = 0.$*

(iii) $\mathrm{Tr}\left(\frac{c^3}{(c^2 + c + 1)^2}\right) = 0$ *and there exists b such that $(b^2 c + bc^2 + b + c^2 + 1)^2 \neq 0$ and $\mathrm{Tr}\left(\frac{b^2 c^2 (bc + c + 1)}{(b^2 c + bc^2 + b + c^2 + 1)^2}\right) = 0.$*

(iv) $c^2 + c + 1 = 0$ *(so, $n \equiv 0 \pmod 2$) and there exists b such that $b^2 + b + 1 \neq 0$ and $\mathrm{Tr}\left(\frac{b^2 c(b+c)}{(b^2 + b + 1)^2}\right) = 0.$*

Proof. The claim about $n = 2, 3$ follows from the computation displayed in the appendix, so we now assume $n \geq 4$.

By Theorem 3, we need to investigate the system

$$\begin{array}{rcl} (x + \gamma)^{2^n - 2} + cx^{2^n - 2} & = & b \\ (x + \gamma + a)^{2^n - 2} + c^{-1}(x + a)^{2^n - 2} & = & b. \end{array} \tag{7}$$

Observe that if $a = 0$, then the system becomes $(x + \gamma)^{2^n - 2} + cx^{2^n - 2} = b = (x + \gamma)^{2^n - 2} + c^{-1}x^{2^n - 2}$, rendering $(c + c^{-1})x^{2^n - 2} = 0$, and since $c \neq 0, 1$,

18

then $x = 0$. Thus, $\gamma^{2^n-2} = b$, which also has one solution γ, independent of b, so $_c\mathcal{B}_F(0, b) = 1$.

We next assume that $0 \neq c \neq 1, a \neq 0$. Dividing (7) by a and relabeling $x/a \mapsto x$, $\gamma/a \mapsto \gamma$ and $ab \mapsto b$ (all are linear equations), we are led to investigate the system

$$\begin{array}{rcl} (x + \gamma)^{2^n-2} + cx^{2^n-2} & = & b \\ (x + \gamma + 1)^{2^n-2} + c^{-1}(x + 1)^{2^n-2} & = & b. \end{array} \tag{8}$$

If $b = 0$, the system (8) transforms into $(x + \gamma)^{2^n-2} = cx^{2^n-2}, (x + \gamma + 1)^{2^n-2} = c^{-1}(x + 1)^{2^n-2}$. If $x = 0$, then $\gamma = 0$, which renders the non-permissible $c = 1$. Similarly, $x = 1$, $x = \gamma$, $x = \gamma + 1$ can only happen if $c = 1$ (assuming $b = 0$) and that is not allowed. If none of these values of x happen then the system becomes

$$x + \gamma = c^{-1}x, \ x + \gamma + 1 = cx + c,$$

with solutions $\gamma = 1, x = \frac{c}{c+1} \neq 0, 1$, so $x \notin \{0, 1, \gamma, \gamma+1\}$, hence $_c\mathcal{B}_F(a, 0) = 1$ (which holds for all a, using the previous discussion). We next assume that $b \neq 0$.

Case 1: $b \neq 0, x = 0$. The system (8) reduces to $\gamma^{2^n-2} = b$ and $(\gamma+1)^{2^n-2} - c^{-1} = b$. Since $b \neq 0$, then $\gamma = 1/b$, which can only happen if $\frac{b}{b+1} = b + c^{-1}$, that is, $b^2 + c^{-1}b + c^{-1} = 0$. This equation in b has two solutions, say, $b_1, b_1' = 1/(cb_1)$, if and only if, by Lemma 8, $\text{Tr}(c^{-1}/c^{-2}) = \text{Tr}(c) = 0$. Thus, in this case, we have a contribution of 1 (the solutions are $(x, \gamma) = (0, 1/b_1), (0, 1/b_1')$) to $_c\mathcal{B}_F(a, ab_1)$, respectively, $\mathcal{B}_F(a, ab_1')$, otherwise there is no contribution.

Case 2: $b \neq 0, x = 1$. The system (8) reduces to $(\gamma+1)^{2^n-2} = b+c, \gamma^{2^n-2} = b$. If $b = 1$, then $\gamma = 1$ and c must be 1, an impossibility. If $b = c \neq 1$, then $\gamma = 1/b$ and $(\gamma+1)^{2^n-2} = 0$, so, $\gamma = 1$, implying $b = 1$, and so, $c = 1$, which is not allowed. Thus, $1 \neq b \neq c$, and so, $\gamma = 1/b$ renders $b^2 + cb + c = 0$, which has two roots, say $b_2, b_2' = c/b_2$, if and only if, by Lemma 8, $\text{Tr}(1/c) = 0$. Therefore, if $\text{Tr}(1/c) = 0$, then we have a contribution of 1 to $_c\mathcal{B}_F(a, ab_2)$, respectively, $_c\mathcal{B}_F(a, ab_2')$ (the solutions are $(x, \gamma) = (1, 1/b_2), (1, 1/b_2')$).

Can b_1, b_1' equal b_2, b_2'? If that is so, then $c^{-1}b_1 + c^{-1} = cb_1 + c$, obtaining $b_1 = 1$, but that is impossible since it will not satisfy $b^2 + bc + c = 0$ (similarly for $b_1' = b_2$, etc.). Thus, the two contributions from Case 1 and 2 will not overlap.

Case 3: $b \neq 0, x = \gamma$. The system (8) reduces to $cx^{2^n-2} = b, 1 + c^{-1}(x + 1)^{2^n-2} = b$, so $x = c/b$. If $b = c$, then $x = 1$, and $b = 1$ (from the second

19

equation), an impossibility. If $b \neq c$, then we must have $b^2 + \frac{c^2+c+1}{c}b + c = 0$, and two roots b exist $(b_3, c/b_3)$, under $c^2 + c + 1 \neq 0$, by Lemma 8, if and only if $\text{Tr}\left(\frac{c^3}{(c^2+c+1)^2}\right) = 0$ (one such b_3' does exist even when $c^2 + c + 1 = 0$ (so, n is even), as then, $b_3' = c^{1/2}$, which always exists). Under these circumstances, we have a contribution of 1 to $_c\mathcal{B}_F(a, ab_3)$, $_c\mathcal{B}_F(a, ac/b_3)$, respectively, $_c\mathcal{B}_F(a, ab_3')$.

Can any of b_3, or b_3' be equal to b_1, or b_2?

- If $b_3 = b_1$, then as above we get that $b_1 = b_3 = \frac{c^2+c+1}{(c+1)^2}$, assuming $\text{Tr}(c) = \text{Tr}\left(\frac{c}{c^2+c+1}\right) = 0$. If that is so, plugging this value in any of the component equations, renders $\frac{c^4}{(c+1)^4} = 0$, an impossibility.

- If $b_3 = b_2$, similarly, we get that $b = \frac{c}{c+1}$, assuming $\text{Tr}\left(\frac{1}{c}\right) = 0$ and $\text{Tr}\left(\frac{c}{c^2+c+1}\right) = 0$. Putting the value of b in any of the component equations, gives $\frac{c}{(c+1)^2} = 0$, which is impossible.

- $b_3' = c^{1/2} = b_1$ (under $c^2 + c + 1 = 0$) when plugged into the equation of b_1, gives $c = 1$, a contradiction.

- $b_3' = c^{1/2} = b_2$, similarly renders (under $c^2 + c + 1 = 0$) when put into the equation of b_2, the value $c = 0$, a contradiction.

Case 4: $b \neq 0$, $x = \gamma + 1$. The system (8) reduces to $1 + cx^{2^n-2} = b$, $c^{-1}(x + 1) = b$. If $b = 1$, then $x = 0$, and so, $c^{-1} = b = 1$, a contradiction. Thus, $b \neq 1$ and $x = c/(b+1)$, which, when used in the first equation, gives

$$b^2 + \frac{c^2 + c + 1}{c}b + \frac{1}{c} = 0,$$

which renders two solutions, say $b_4, b_4' = 1/(cb_4)$, if and only if $\text{Tr}\left(\frac{c}{(c^2+c+1)^2}\right) = 0$. For such a c, we get a contribution of 1 to $_c\mathcal{B}_F(a, ab_4)$, respectively, $_c\mathcal{B}_F(a, ab_4')$, assuming $\text{Tr}\left(\frac{c}{(c^2+c+1)^2}\right) = 0$.

Can b_4 (or b_4') be equal to $b_1, b_1', b_2, b_2', b_3$, or b_3'?

- If $b_4 = b_1$ (or b_1'), then they must satisfy both $cb^2 + b + 1 = 0$, $cb^2 + (c^2 + c + 1)b + 1 = 0$, from which we infer $b = 0$ or $c = 0, 1$, an impossibility.

- If $b_4 = b_2$ (or b_2'), then they must satisfy both $b^2 + bc + c = 0$, $cb^2 + (c^2 + c + 1)b + 1 = 0$, implying $b = c + 1$, which does not satisfy $b^2 + bc + c = 0$.

- If $b_4 = b_3$, then they must satisfy both equations $cb^2+(c^2+c+1)b+c^2 = 0, cb^2 + (c^2 + c + 1)b + 1 = 0$, inferring $c = 1$, an impossibility.

- If $b_4 = b_3'(= c^{1/2})$, then $c^2 + c + 1 = 0$ (so, $n \equiv 0 \pmod 2$) and $cb_4^2 + (c + 1)b + (c + 1) = 0$. Thus, $c^2 = (c + 1)c^{1/2}$, which combined with $c^2 + c + 1 = 0$, renders $(c + 1)(c^{1/2} + 1) = 0$, that is, $c = 1$, an impossibility.

Case 5. Assuming now that $x(x+1)(x+\gamma)(x+\gamma+1) \neq 0$, and multiplying the first equation of (8) by $x(x + \gamma)$ and the second by $c(x + 1)(x + \gamma + 1)$ we obtain the new system

$$1 + cx + bx^2 + (c + bx)\gamma = 0$$
$$1 + c + bc + (1 + c)x + bcx^2 + (1 + bc + bcx)\gamma = 0. \tag{9}$$

Observe that $x \neq c/b$ since, otherwise, $c = 0$ (inferred from the first equation), a contradiction. If $x \neq c/b$, then using $\gamma = \dfrac{bx^2 + cx + x}{bx + c}$ found from the first equation and replacing it into the second, we get

$$b^2cx^2 + (b^2c + bc^2 + b + c^2 + 1)x + bc^2 + c^2 + c = 0,$$

or

$$x^2 + \frac{b^2c + bc^2 + b + c^2 + 1}{b^2c}x + \frac{bc + c + 1}{b^2} = 0. \tag{10}$$

If $b^2c + bc^2 + b + c^2 + 1 = 0$, we have a contribution of 1 to $_c\mathcal{B}_F(a, ab)$. If $b^2c + bc^2 + b + c^2 + 1 \neq 0$, by Lemma 8, Equation (9) will have two solutions if and only if

$$\mathrm{Tr}\left(\frac{\frac{bc+c+1}{b^2}}{\left(\frac{b^2c+bc^2+b+c^2+1}{b^2c}\right)^2}\right) = \mathrm{Tr}\left(\frac{b^2c^2(bc + c + 1)}{(b^2c + bc^2 + b + c^2 + 1)^2}\right) = 0. \tag{11}$$

Therefore, under the above trace condition on b for a fixed c, we have a contribution of 2 to $_c\mathcal{B}_F(a, ab)$.

To avoid speaking about an empty condition, we want to argue next that (11) will happen for a fixed $c \neq 0, 1$, so it will be sufficient to find a values of b where the trace above is 0. If $b = 1$ (and so, $1+b+b^2c+c^2+bc^2 \neq 0$), then the trace becomes $\mathrm{Tr}(1) = 0$, which will always happen if the dimension is even, the Equation (10) is then $x^2 + x + 1 = 0$ (with two distinct roots), so in this case we have a contribution of 2 to $_c\mathcal{B}_F(a, ab)$, where b satisfies (11), otherwise there is none.

For the remainder of the proof below we assume that n is odd. Taking, for example, $b = c^2 + c^{-1} \neq 0$ (for this value, $1 + b + b^2 c + c^2 + bc^2 \neq 0$, since otherwise, we would get $c^5 + c^4 + c + 1 = (c+1)^5 = 0$, so $c = 1$, a contradiction), since the dimension is odd and $c \neq 0, 1$, the above trace calculation reduces to

$$\text{Tr}\left(\frac{c(1 + c + c^2)^2}{(1+c)^4}\right) = \text{Tr}\left(\frac{c}{(1+c)^2} + \frac{c^2}{(1+c)^4}\right) = 0,$$

which is obviously true, and so there are two roots x to the Equation (10).

We need to make sure that the solutions x, γ will not satisfy $x(x+1)(x+\gamma)(x+\gamma+1) = 0$, so we go back (replacing $b = c^2 + c^{-1}$) to Equation (10), obtaining

$$x^2 + \frac{c^4 + c^3 + c^2 + c}{(c^2 + c + 1)^2}x + \frac{c^3}{(c^2 + c + 1)^2} = 0$$

If $x = 0$, then $c = 0$, which is not allowed. If $x = 1$, then we get $\frac{1+c}{(c^2+c+1)^2} = 0$, and so, $c = 1$, which is not allowed. If $x = \gamma$, then the system (9) becomes

$$x = 0, (c^3 + c + 1)x + c^3 + c = 0,$$

which is impossible since $c \neq 0, 1$. If $x = \gamma + 1$, the system is now

$$x + 1 = 0, (c^3 + c + 1)x + c^2 = 0,$$

which can only happen if $c^3 + c^2 + c + 1 = (c+1)^3 = 0$, an impossibility.

Putting together the above cases, we see that, if $n \geq 4$, the only possibility is for at most three solutions of the c-boomerang system: we get three solutions if Case 5 is combined with any of the previous 4 cases (for (iv) we use $c^2 + c = 1 = 0$ to simplify the trace expression), and therefore, the c-boomerang uniformity is ≤ 3, but not higher. Our theorem is shown. $\square$

Remark 3. *From the previous proof, we do get a lot more information about the Boomerang Connectivity Table for the binary inverse function, but we preferred to simply give just the maximum c-BCT entries.*

We now treat the case of the inverse for odd characteristic. We let $[A]^2 = \{x^2 \,|\, x \in A\}$, where A is a set with a defined multiplication on it.

Theorem 13. *Let p be an odd prime, $n \geq 1$ be a positive integer, $0, 1 \neq c \in \mathbb{F}_{p^n}$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the inverse p-ary function defined by $F(x) = x^{p^n - 2}$. For any $a, b \in \mathbb{F}_{p^n}$, the c-BCT entries $_c\mathcal{B}_F(a, ab) \leq 4$. Furthermore,*

(i) If $1 + 2c - 2c^2 + 2c^3 + c^4 = 0$ and $3 - 2c + 3c^2, 1 - 4c, c^2 - 4c \in [\mathbb{F}_{p^n}]^2$, then $\beta_{F,c} = 4$ (e.g., for such c, if $b = \frac{c^2-1}{c^2+1}$, then $_c\mathcal{B}_F(a, ab) = 4$).

(ii) If $1 - 2c - 2c^2 - 2c^3 + c^4 = 0$ and $1 - 6c + c^2, 1 - 4c, c^2 - 4c \in [\mathbb{F}_{p^n}]^2$, then $\beta_{F,c} = 4$ (e.g., for such c, if $b = \frac{c^2-1}{2c}$, then $_c\mathcal{B}_F(a, ab) = 4$).

Proof. For $a = 0$, the corresponding system $(x + \gamma)^{p^n-2} - cx^{p^n-2} = b, (x + \gamma)^{p^n-2} - c^{-1}x^{p^n-2} = b$ has one solution (x, γ). We assume now that $a \neq 0$. Multiplying by a and relabeling, the c-boomerang system becomes

$$(x + \gamma)^{p^n-2} - cx^{p^n-2} = b.$$
$$(x + \gamma + 1)^{p^n-2} - c^{-1}(x+1)^{p^n-2} = b. \tag{12}$$

If $b = 0$, we easily get only one solution, so we may assume below that $b \neq 0$.

Case 1. Let $x = 0$. The c-boomerang system is $\gamma^{p^n-2} = b, (\gamma+1)^{p^n-2}-c^{-1} = b$, so $\gamma = 1/b$, and $(\frac{1}{b} + 1)^{p^n-2} = b + \frac{1}{c}$ (surely, $b + \frac{1}{c} \neq 0$, since, otherwise, $b = -1$, and so, $c = 1$, an impossibility). Thus, $(0, \frac{1}{b})$ is a solution assuming b satisfies $b^2 + \frac{1}{c}b + \frac{1}{c} = 0$. By Lemma 8, a unique b'_1 exists if and only if the discriminant $D_1 = c^{-2} - 4c^{-1} = 0$, that is $c = 4^{-1}$. Again, from Lemma 8, two solutions b_1 (we call these, here and in the next three cases, by the same label, as it will not matter in our argument) exist if and only if $1 - 4c \in [\mathbb{F}_{p^n}]^2$, $c \neq 4^{-1}$. In either case, there is a contribution of 1 to the respective c-BCT entry.

Case 2. If $x = -1$, the c-boomerang system is now $(\gamma - 1)^{p^n-2} + c = b, \gamma^{p^n-2} = b$, so $\gamma = 1/b$, which used in the first equation renders $(\frac{1}{b} - 1)^{p^n-2} = b - c$, which simplified gives $b^2 - bc + c = 0$ (again, $b \neq c$, since otherwise $1/b = 1$, and so, $c = 1$, an impossibility). By Lemma 8, a unique b'_2 exists if and only if the discriminant $D_2 = c^2 - 4c = 0$, so $c = 4$, and two solutions b_2 exist if and only if $D_2 \in [\mathbb{F}_{p^n}]^2$, $c \neq 4$ (thus, $D_2 \in [\mathbb{F}_{p^n}^*]^2$). In either case, there is a contribution of 1 to the respective c-BCT entry.

Case 3. Let $x = -\gamma$. The c-boomerang system is now $c\gamma^{p^n-2} = b, 1-c^{-1}(1-\gamma)^{p^n-2} = b$. Thus, $\gamma = c/b$ (if $b = 0$, then $\gamma = 0$, and the second equation gives us, $c^{-1} = b = 0$, an impossibility). Using $\gamma = c/b$ (observe that $b \neq 1$) in the second equation we obtain $b^2 - b\frac{c^2+c-1}{c} + c = 0$, which has a unique solution b'_3 if and only if $D_3 = \frac{1-2c-c^2-2c^3+c^4}{c^2} = \frac{(1-3c+c^2)(1+c+c^2)}{c^2} = 0$. There are two roots b_3 if and only if $D_3 \in [\mathbb{F}_{p^n}^*]^2$, or equivalently, $(1 - 3c + c^2)(1 + c + c^2) \in [\mathbb{F}_{p^n}^*]^2$.

Case 4. Let $x = -\gamma - 1$. The c-boomerang system becomes $-1 - cx^{p^n-2} = b, -c^{-1}(x+1)^{p^n-2} = b$. Then $x = -\frac{c}{b+1}$ (if $b = -1$, then $x = 0$, and using the

23

second equation, we get $-c^{-1} = b$, that is, $c = 1$, an impossibility), which used in the second equation gives $b^2 - b\frac{c^2-c-1}{c} + \frac{1}{c} = 0$. This equation has a root b_4' if and only if $D_4 = \frac{1-2c-c^2-2c^3+c^4}{c^2} = \frac{(1-3c+c^2)(1+c+c^2)}{c^2} = 0$, and two roots b_4 if and only if $D_4 \in [\mathbb{F}_{p^n}^*]^2$, or equivalently, $(1-3c+c^2)(1+c+c^2) \in [\mathbb{F}_{p^n}^*]^2$.

We now need to check if overlaps exist among the b's of various cases, and therefore the contributions to the c-BCT entries will be added.

- If b_1 (or b_1') equals b_2 (or b_2'), then these must satisfy both $b^2 + \frac{1}{c}b + \frac{1}{c} = 0$, $b^2 - bc + c = 0$, that is, $b = \frac{c^2-1}{c^2+1}$, which when used in the first equation gives $1 + 2c - 2c^2 + 2c^3 + c^4 = 0$. Observe that $c = 4, 4^{-1}$ vanish this expression if and only if $p = 19$. So, we have a contribution of 2 to the respective c-BCT entry if and only if $1 + 2c - 2c^2 + 2c^3 + c^4 = 0$ (this includes the cases $c = 4, 4^{-1}$).

- If b_1 (or b_1') equals b_3 (or b_3'), then these must satisfy both $b^2 + \frac{1}{c}b + \frac{1}{c} = 0$, $b^2 - \frac{c^2+c-1}{c}b + c = 0$, giving $b = \frac{c-1}{c}$, which when used in the first equation implies $1 = 0$, an impossibility.

- If b_1 (or b_1') equals b_4 (or b_4'), then these must satisfy both $b^2 + \frac{1}{c}b + \frac{1}{c} = 0$, $b^2 - \frac{c^2-c-1}{c}b + \frac{1}{c} = 0$, implying that either $c = 0, 1$, or $b = 0$, none of which will work.

- If b_2 (or b_2') equals b_3 (or b_3'), then these must satisfy both $b^2 - bc + c = 0$, $b^2 - \frac{c^2+c-1}{c}b + c = 0$, which will not work (same argument as in the previous item).

- If b_2 (or b_2') equals b_4 (or b_4'), then these must satisfy both $b^2 - bc + c = 0$, $b^2 - \frac{c^2-c-1}{c}b + \frac{1}{c} = 0$, so $b = c - 1$, which when replaced into the first equation gives $1 = 0$, an impossibility.

- If b_3 (or b_3') equals b_4 (or b_4'), then these must satisfy both $b^2 - \frac{c^2+c-1}{c}b + c = 0$, $b^2 - \frac{c^2-c-1}{c}b + \frac{1}{c} = 0$, and so, $b = \frac{c^2-1}{2c}$, which implies $1 - 2c - 2c^2 - 2c^3 + c^4 = 0$.

Observe that other combinations cannot occur above.

Case 5. Assume now that $x \neq 0, 1, \gamma, \gamma + 1$. Multiplying the first equation by $x(x + \gamma)$ and the second by $c(x + 1)(x + \gamma + 1)$ renders

$$x - c(x + \gamma) = bx(x + \gamma)$$
$$c(x + 1) - (x + \gamma + 1) = bc(x + 1)(x + \gamma + 1).$$

Solving for γ in the first equation, we get $\gamma = \frac{x - cx - bx^2}{c + bx}$ (observe that $x \neq -c/b$), which used in the second equation gives us the equation

$$x^2 + \frac{bc^2 + b^2c + b + 1 - c^2}{b^2 c} x + \frac{bc - c + 1}{b^2} = 0,$$

with a unique root x if and only if

$$\begin{aligned}
b^4 c^2 D_5 &= 1 + 2b + b^2 + 2b^2 c + 2b^3 c - 2c^2 - 2b^2 c^2 \\
&\quad + b^4 c^2 + 2b^2 c^3 - 2b^3 c^3 + c^4 - 2bc^4 + b^2 c^4 \\
&= (1 + b - c)(1 - c + bc)(1 + b + 2c + b^2 c + c^2 - bc^2) = 0,
\end{aligned}$$

and two distinct roots x if and only if

$$(1 + b - c)(1 - c + bc)(1 + b + 2c + b^2 c + c^2 - bc^2) \in [\mathbb{F}_{p^n}^*]^2.$$

Putting together our discussion, we see that the largest c-BCT entry can only be 4; we do get that value if Case 5 is combined with combinations of the other cases c-BCT namely, both Case 1 and Case 2, or both Case 3 and Case 4.

The proof of the theorem is done. □

Remark 4. *From the previous proof, we do get a lot more information about the c-Boomerang Connectivity Table for the p-ary inverse function, but, as for the binary case, we preferred to just give the maximum c-BCT entries.*

8 Concluding remarks

We defined a new concept, we call c-boomerang uniformity based upon a previously defined multiplicative differential. We characterized the new concept in terms of the Walsh transforms and investigated the properties of some perfect nonlinear functions, as well as the inverse function in all characteristics via this new concept.

It would certainly be interesting to see how other perfect nonlinear, as well as almost perfect nonlinear functions behave under this new c-boomerang uniformity.

References

[1] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10 (1967), 553–564.

[2] E. Biham, O. Dunkelman, N. Keller, *New results on boomerang and rectangle attacks*, In: Daemen J., Rijmen V. (eds.), Fast Software Encryption, FSE 2002, LNCS 2365, 2002, pp. 1–16, Springer, Berlin, Heidelberg.

[3] A. Biryukov, D. Khovratovich, *Related-key cryptanalysis of the full AES-192 and AES-256*, In: Matsui M. (ed.), Advances in Cryptology – ASIACRYPT 2009, LNCS 5912, 2009, pp. 1–18, Springer, Berlin, Heidelberg.

[4] A.W. Bluher, *On $x^{q+1} + ax + b$*, Finite Fields Appl. 10 (3) (2004), 285–305.

[5] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative Differentials*, In: Daemen J., Rijmen V. (eds.), Fast Software Encryption, FSE 2002, LNCS 2365, pp. 17–33, Springer, Berlin, Heidelberg, 2002.

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

[7] C. Boura, L. Perrin, S. Tian, *Boomerang Uniformity of Popular S-box Constructions*, Workshop on Cryptography and Coding, Paper 15, `https://www.lebesgue.fr/sites/default/files/proceedings_WCC/WCC_2019_paper_15.pdf`.

[8] N. Bourbaki, Elements of Mathematics, Algebra II (translated by P. M. Cohn and J. Howie), Springer, Berlin, 1990.

[9] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[10] L. Budaghyan, C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inform.Theory 54:5 (2008), 2354–2357.

[11] M. Calderini, I.Villa, *On the Boomerang Uniformity of some Permutation Polynomials*, `https://eprint.iacr.org/2019/881.pdf`.

[12] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[13] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[14] C. Carlet, *Characterizations of the Differential Uniformity of Vectorial Functions by the Walsh Transform*, IEEE Trans. Inf. Theory 64:9 (2018), 6443–6453.

[15] F. Chabaud, S. Vaudenay, *Links between differential and linear cryptanalysis*, In: A. De Santis (ed.), Adv. in Crypt – EUROCRYPT '94, LNCS 950, pp. 356–365, 1995, Springer.

[16] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, *Boomerang Connectivity Table: A new cryptanalysis tool*, In: J. B. Nielsen and V. Rijmen (eds.), Adv. in Crypt. – EUROCRYPT '18, pp. 683–714, Cham, 2018. Springer.

[17] R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.

[18] R. S. Coulter, R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class* II, Des. Codes Cryptogr. 10 (1997), 167–184.

[19] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

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

[21] P. Ellingsen, P. Felke, C. Riera P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, to appear in IEEE Trans. Inf. Theory, 2020, DOI: 10.1109/TIT.2020.2971988.

[22] J. Kelsey, T. Kohno and B. Schneier, *Amplified boomerang attacks against reduced-round MARS and Serpent*, In: Goos G., Hartmanis J., van Leeuwen J., Schneier B. (eds,), Fast Software Encryption, FSE 2000. LNCS 1978. Springer, Berlin, Heidelberg.

[23] J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, *Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis*, IEEE Trans. Inf. Theory 58(7) (2012), 4948–4966.

[24] 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.

[25] N. Li, Z. Hu, M. Xiong, X. Zeng, *4-uniform BCT permutations from generalized butterfly structure*, `https://arxiv.org/abs/2001.00464`.

[26] J. Liang, *On the solutions of trinomial equations over finite fields*, Bull. Cal. Math. Soc. 70 (1978), 379–382.

[27] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[28] S. Mesnager, C. Tang, M. Xiong, *On the boomerang uniformity of quadratic permutations*, `https://eprint.iacr.org/2019/277.pdf`.

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

[30] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.

[31] Z. Tu, N. Li, X. Zeng, J. Zhou, A class of quadrinomial permutation with boomerang uniformity four, to appear in IEEE Trans. Inf. Theory.

[32] D. Wagner, *The boomerang attack*, In: L. R. Knudsen (ed.), Fast Software Encryption, FSE '99, LNCS 1636, pages 156–170, 1999, Springer, Heidelberg.

9 Appendix

We list all the uniformity values for the considered functions in the paper, for $2 \leq n \leq 4$, and some values of the parameter k, if involved, computed via SageMath. Below, α denotes a primitive root in the respective field. For $p = 2$, to construct $\mathbb{F}_{2^n}$, $2 \leq n \leq 4$, we take the primitive polynomials, $x^2 + x + 1, x^3 + x + 1, x^4 + x + 1$, respectively. If $p = 3$, to construct $\mathbb{F}_{3^n}$, $2 \leq n \leq 5$, we take the primitive polynomials, $x^2 + 2x + 2, x^3 + 2x + 1, x^4 + 2x^3 + 2, x^5 + 2x + 1$, respectively. If $p = 5$, to construct $\mathbb{F}_{5^n}$, $2 \leq n \leq 4$, we take the primitive polynomials, $x^2 + 4x + 2, x^3 + 3x + 3, x^4 + 4x^2 + 4x + 2$.

We will only mention the nonzero entries (surely, for some parameters, a, b, c, $_c\mathcal{B}_F(a, b) = 0$, but we are not concerned with that). First, if $f(x) = x^2$, the possible c-BCT entries $(c \neq 0, 1)$ for $f(x) = x^2$, $2 \leq n \leq 4$, are $[1, 2]$ for $n = 2$, respectively, $[1, 2, 3, 4]$ for $n = 3, 4$.

p	n	possible values of $_c\mathcal{B}_F(a,b)$
2	2	$[1]$
	3	$[1,2]$
	4	$[1,2,3]$
3	2	$[1,2]$
	3	$[1,2,3]$
	4	$[1,2,3,4]$

Table 1: Possible c-BCT entries for the inverse $f(x) = x^{p^n-2}$, $2 \leq n \leq 4$, $p = 2, 3$, $c \neq 0, 1$

k	n	possible values of $_c\mathcal{B}_F(a,b)$
1	2	$[1,2,4,6,9]$
	3	$[1,2,3]$
	4	$[1,2,3,4,5,6,7,8,9]$
2	2	$[1,2]$
	3	$[1,2,3]$
	4	$[1,2,4,72,73,81,82,90,91,100]$
3	2	$[1,2,4,6,9]$
	3	$[1,2,3,4]$
	4	$[1,2,3,4,5,6,7,8,9]$

Table 2: Possible c-BCT entries for the Gold $f(x) = x^{3^k+1}$, $2 \leq n \leq 4$, $1 \leq k \leq 3$, $c \neq 0, 1$

k	n	possible values of $_c\mathcal{B}_F(a,b)$
1	2	$[1,2]$
	3	$[1,2,3,4]$
	4	$[1,2,3,4]$
2	2	$[1,2]$
	3	$[1,2,3,4]$
	4	$[1,2,3,4,5,6,7,8,9,10,12,18]$
3	2	$[1,2]$
	3	$[1,2,3,4,6,7,8]$
	4	$[1,2,3,4,5]$

Table 3: Possible c-BCT entries for $f(x) = x^{\frac{3^k+1}{2}}$, $2 \leq n \leq 4$, $1 \leq k \leq 3$, $c \neq 0, 1$

Let $f(x) = x^{10} - x^6 - x^2$ on $\mathbb{F}_{3^2}$. We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 2 (all c-BCT entries of $[1,2]$ occur): $(2, 2\alpha), (\alpha+2, \alpha+2), (2\alpha, 2\alpha), (\alpha+2, 2\alpha), (2\alpha+1, 2\alpha), (2\alpha+1, \alpha+2), (\alpha, 2\alpha), (2, 2), (2, \alpha+2), (2\alpha, \alpha+2), (\alpha, \alpha+2)$.

Let $f(x) = x^{10} - x^6 - x^2$ on $\mathbb{F}_{3^3}$. We list all values of (c, b), for which the

c-DDT entry (for some a) equals the c-boomerang uniformity of 4 (all c-BCT entries of $[1, 2, 3, 4]$ occur): $(2\alpha, \alpha^2), (\alpha^2 + \alpha, \alpha^2 + \alpha + 1), (\alpha^2 + 2, \alpha^2), (2\alpha + 1, \alpha^2 + \alpha + 1), (2\alpha + 2, \alpha^2 + 2\alpha + 1), (\alpha^2 + 2\alpha, \alpha^2 + 2\alpha + 1)$.

Let $f(x) = x^{10} - x^6 - x^2$ on $\mathbb{F}_{3^4}$. We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 6 (all c-BCT entries of $[1, 2, 3, 4, 5, 6]$ occur): $(2, 2\alpha^3 + 2\alpha^2), (2, \alpha^3 + \alpha^2 + 2)$.

Let $f(x) = x^{10} - x^6 - x^2$ on $\mathbb{F}_{3^5}$ (the complexity of this computation is about 2^{32}, and if we were to go up to $n = 6$, it would be 2^{40} operations, so we stopped at $n = 5$). We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 6 (all c-BCT entries of $[1, 2, 3, 4, 5, 6]$ occur):

$(\alpha^4 + \alpha^3 + \alpha^2 + 2\alpha, \alpha^4 + \alpha^2 + 2\alpha + 1), (2\alpha^2 + 2\alpha, \alpha^4 + 2\alpha^3 + \alpha^2 + 1),$

$(\alpha^4 + \alpha^2 + 2, 2\alpha^3 + 2\alpha), (2\alpha^4 + \alpha^3 + \alpha^2 + 2\alpha + 2, \alpha^3 + \alpha^2 + \alpha),$

$(2\alpha^3 + \alpha^2 + \alpha + 2, \alpha^4 + 2\alpha^3 + 2\alpha + 1), (2\alpha + 1, 2\alpha^4 + \alpha^2 + 2\alpha + 2),$

$(\alpha^3 + \alpha^2 + \alpha, \alpha^4 + 2\alpha^3 + 1), (\alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 2, \alpha^4 + 2\alpha^3 + 2\alpha + 1),$

$(2\alpha^4 + \alpha^3 + \alpha^2 + 2, 2\alpha^4 + \alpha^3 + \alpha^2 + 2\alpha + 2), (\alpha^4 + 2\alpha^2, \alpha^4 + \alpha^3 + 2\alpha^2 + \alpha + 1),$

$(2\alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 1, 2\alpha^4 + \alpha^3 + 2\alpha^2 + \alpha + 2), (2\alpha^2 + 2, \alpha^4 + 2\alpha^2 + 2\alpha + 1),$

$(\alpha^4 + \alpha^3 + 1, 2\alpha^4 + \alpha^3 + \alpha^2 + 2), (\alpha^3 + 2\alpha, \alpha^4 + 2\alpha^2 + 2\alpha + 1),$

$(\alpha^4 + 2\alpha + 2, \alpha^4 + \alpha^3 + 2\alpha^2 + \alpha + 1), (\alpha^4 + \alpha^3 + \alpha^2 + \alpha, 2\alpha^4 + \alpha^2 + 2\alpha + 2),$

$(2\alpha^3 + 1, 2\alpha^4 + \alpha^3 + 2\alpha + 2), (2\alpha^4 + 2\alpha^3 + \alpha + 2, \alpha^4 + \alpha + 1),$

$(2\alpha^3 + \alpha + 2, 2\alpha^4 + \alpha^3 + \alpha^2 + 2), (\alpha^4 + \alpha^3 + 2\alpha^2 + 1, \alpha^4 + \alpha^2 + 2\alpha + 1),$

$(2\alpha^4 + 2\alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha), (2\alpha^3 + 2\alpha^2 + 2, 2\alpha^4 + \alpha^3 + 2\alpha + 2),$

$(\alpha^4 + 2\alpha^3 + 1, \alpha^4 + \alpha^3 + 1), (\alpha^3 + \alpha^2 + 2\alpha + 2, \alpha^4 + \alpha^3 + 1),$

$(\alpha^3 + 2\alpha^2 + \alpha + 2, \alpha^4 + 2\alpha^3 + \alpha^2 + 1), (\alpha^4 + \alpha^3 + \alpha, 2\alpha^3 + 2\alpha),$

$(2\alpha^2 + \alpha + 2, \alpha^4 + \alpha + 1), (2\alpha^3 + 2\alpha^2 + \alpha, 2\alpha^4 + \alpha^3 + 2\alpha^2 + \alpha + 2),$

$(\alpha^2 + \alpha + 2, 2\alpha^4 + \alpha^3 + \alpha^2 + 2\alpha + 2), (\alpha^4 + \alpha^3 + 2\alpha, \alpha^4 + 2\alpha^3 + 1).$

Let $f(x) = x^{10} + x^6 - x^2$ on $\mathbb{F}_{3^2}$. We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 2 (all c-BCT entries of $[1, 2]$ occur): $(2, 2\alpha + 1), (2\alpha + 1, \alpha), (2\alpha, 2\alpha + 1), (\alpha, \alpha), (\alpha + 2, 2\alpha + 1), (2\alpha + 1, 2\alpha + 1), (2, 1), (2\alpha, \alpha), (2, \alpha), (\alpha, 2\alpha + 1), (\alpha + 2, \alpha)$.

Let $f(x) = x^{10} + x^6 - x^2$ on $\mathbb{F}_{3^3}$. We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 3 (all c-BCT entries of $[1, 2, 3]$ occur):

$(\alpha^2 + \alpha + 2, \alpha^2 + 2\alpha + 2), (2\alpha^2 + 2\alpha, \alpha^2 + 2\alpha + 2), (\alpha^2 + \alpha + 2, \alpha + 1), (\alpha^2 + 2, 2), (\alpha^2 + 1, \alpha),$

$(2\alpha^2, \alpha + 1), (2\alpha^2 + \alpha + 2, \alpha), (\alpha^2 + 2\alpha + 2, \alpha), (\alpha, \alpha^2 + \alpha + 2), (2\alpha + 1, 2\alpha^2 + 2), (\alpha^2 + \alpha, 2),$

$(\alpha^2 + \alpha, 2\alpha^2 + 2), (2\alpha + 1, 2), (2\alpha, 2), (\alpha^2 + \alpha + 2, \alpha + 2), (\alpha^2 + \alpha + 1, 2\alpha^2 + 2\alpha + 1),$

$(2\alpha^2 + 2\alpha + 2, \alpha), (\alpha^2 + 2, 2\alpha^2 + \alpha + 1), (2\alpha^2 + 1, \alpha^2 + \alpha + 2), (\alpha^2 + 2\alpha + 1, 2\alpha^2 + \alpha + 1),$

$(2\alpha, 2\alpha^2 + \alpha + 1), (2\alpha + 2, 2\alpha^2 + 2\alpha + 1), (\alpha + 1, \alpha^2 + 1), (2\alpha^2, \alpha + 2), (2\alpha^2 + 2, 2\alpha^2 + \alpha + 1),$

$(\alpha^2, 2\alpha^2 + 2), (\alpha^2 + 2\alpha, 2\alpha^2 + 2\alpha + 1), (\alpha^2 + 2\alpha + 2, \alpha^2 + 1), (\alpha + 2, \alpha^2 + 2\alpha + 2), (2\alpha + 2, 2),$

$(2\alpha^2, \alpha^2 + 2\alpha + 2), (2\alpha^2 + \alpha + 2, \alpha^2 + \alpha + 2), (2\alpha^2 + 2\alpha + 2, \alpha + 1), (\alpha^2 + 2\alpha + 2, \alpha + 1),$

$(2\alpha^2 + \alpha + 1, 2\alpha^2 + 2\alpha + 1), (2\alpha^2 + \alpha + 2, \alpha + 2), (\alpha^2 + 1, \alpha + 2), (\alpha^2 + 2\alpha, 2),$

$(\alpha^2 + 1, \alpha^2 + \alpha + 2), (2\alpha^2 + \alpha, \alpha^2 + 1), (2\alpha^2 + 2\alpha + 1, 2\alpha^2 + 2), (2\alpha^2 + 2\alpha + 2, \alpha^2 + 1).$

Let $f(x) = x^{10} + x^6 - x^2$ on $\mathbb{F}_{3^4}$. We list all values of (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 7 (all c-BCT entries of $[1, 2, 3, 4, 5, 6, 7]$ occur): $(\alpha^2 + 2\alpha + 1, 2\alpha^3 + 2\alpha^2 + 1), (\alpha^2 + \alpha + 2, \alpha^3 + \alpha^2), (\alpha^3 + 2\alpha + 1, \alpha^3 + \alpha^2), (2\alpha^3 + \alpha^2 + \alpha, 2\alpha^3 + 2.$

Let $f(x) = x^{10} + x^6 - x^2$ on $\mathbb{F}_{3^5}$. There are 160 pairs (c, b), for which the c-DDT entry (for some a) equals the c-boomerang uniformity of 5 (all c-BCT entries of $[1, 2, 3, 4, 5]$ occur). We shall list here only the 140 different values of c:

$2\alpha + \alpha^3 + \alpha^4, 2 + 2\alpha^2 + \alpha^3, 1 + 2\alpha^3, 1 + \alpha + \alpha^2, 2 + \alpha^2 + \alpha^4, 1 + \alpha + 2\alpha^3, \alpha + \alpha^2, 2\alpha + \alpha^2, 1 + 2\alpha, 1 + 2\alpha + \alpha^2,$

$1 + 2\alpha + \alpha^2 + 2\alpha^3, \alpha^2, 1 + \alpha + \alpha^3, \alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha + \alpha^2 + \alpha^4, 1 + 2\alpha + 2\alpha^2 + 2\alpha^4, 1 + 2\alpha + \alpha^3 + \alpha^4,$

$2 + \alpha + \alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha, \alpha^2 + \alpha^3, 2 + 2\alpha + \alpha^2 + 2\alpha^3 + \alpha^4, \alpha^4, \alpha + 2\alpha^2 + 2\alpha^3 + \alpha^4, 1 + \alpha + \alpha^3 + \alpha^4, \alpha^3 + 2\alpha^4,$

$1 + \alpha^3, 2 + \alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 2\alpha + 2\alpha^2 + \alpha^3 + \alpha^4, 2\alpha + 2\alpha^2 + \alpha^3, 1 + 2\alpha + 2\alpha^2 + 2\alpha^3, 2\alpha + 2\alpha^2 + \alpha^4, 2\alpha + \alpha^2 + \alpha^3,$

$1 + \alpha^2 + 2\alpha^4, 1 + \alpha^2 + 2\alpha^3 + 2\alpha^4, 1 + \alpha + \alpha^2 + \alpha^4, \alpha^2 + \alpha^4, \alpha^2 + \alpha^3 + 2\alpha^4, 2 + 2\alpha^4, 2 + 2\alpha + 2\alpha^4, 2\alpha + \alpha^2 + \alpha^4,$

$\alpha + \alpha^3 + 2\alpha^4, 2 + 2\alpha + 2\alpha^2 + \alpha^4, 1 + \alpha, 2 + 2\alpha^2 + \alpha^3 + 2\alpha^4, \alpha^2 + 2\alpha^3 + \alpha^4, 2 + \alpha^2 + \alpha^3, \alpha + \alpha^2 + 2\alpha^4, \alpha^2 + 2\alpha^3,$

$\alpha + 2\alpha^4, 1 + \alpha^3 + \alpha^4, 2 + 2\alpha + 2\alpha^3 + 2\alpha^4, 1 + \alpha^2, 2\alpha + \alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha + \alpha^4, 2 + \alpha + \alpha^2 + 2\alpha^3 + \alpha^4,$

$1 + \alpha + \alpha^2 + \alpha^3 + 2\alpha^4, \alpha + 2\alpha^2 + \alpha^3 + 2\alpha^4, 2 + \alpha + \alpha^3, 1 + \alpha + \alpha^3 + 2\alpha^4, \alpha^3, 2 + \alpha + 2\alpha^2 + 2\alpha^4, 2 + \alpha^2 + \alpha^3 + 2\alpha^4,$

$1 + 2\alpha + \alpha^2 + \alpha^3, 2\alpha + \alpha^2 + 2\alpha^3, 2\alpha + \alpha^4, 1 + \alpha + 2\alpha^2 + \alpha^3 + 2\alpha^4, 2 + 2\alpha^2 + 2\alpha^3 + \alpha^4, 1 + 2\alpha + \alpha^2 + 2\alpha^3 + \alpha^4,$

$1 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha^2 + 2\alpha^3, 1 + 2\alpha^2 + \alpha^3 + 2\alpha^4, 2 + \alpha^2 + 2\alpha^4, 2 + 2\alpha^3, 1 + \alpha + \alpha^2 + 2\alpha^3 + \alpha^4, \alpha + \alpha^2 + \alpha^3 + \alpha^4,$

$1 + 2\alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + \alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + \alpha + 2\alpha^2 + \alpha^4, \alpha + \alpha^2 + \alpha^3, 2\alpha + 2\alpha^4,$

$\alpha + \alpha^2 + 2\alpha^3, 2\alpha^2, 2 + \alpha + \alpha^2 + 2\alpha^3, 1 + 2\alpha + 2\alpha^2 + 2\alpha^3 + \alpha^4, 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4, 2 + \alpha^3 + \alpha^4, \alpha + 2\alpha^2 + \alpha^3,$

$2 + \alpha^2 + 2\alpha^3, \alpha + 2\alpha^2, \alpha, 1 + 2\alpha + \alpha^2 + \alpha^3 + \alpha^4, \alpha + 2\alpha^2 + 2\alpha^4, 2 + 2\alpha + 2\alpha^2 + \alpha^3 + \alpha^4, \alpha + \alpha^3 + \alpha^4,$

$2\alpha^2 + \alpha^4, 1 + \alpha + 2\alpha^2 + 2\alpha^4, 2\alpha^2 + 2\alpha^3, 2\alpha + \alpha^2 + 2\alpha^3 + \alpha^4, 1 + 2\alpha + 2\alpha^4, 2\alpha^3 + 2\alpha^4, 2\alpha + \alpha^2 + \alpha^3 + 2\alpha^4,$

$1 + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + \alpha + 2\alpha^3 + \alpha^4, \alpha + 2\alpha^2 + \alpha^4, 2 + \alpha + \alpha^4, 2\alpha^2 + 2\alpha^3 + \alpha^4, 1 + 2\alpha + 2\alpha^3 + 2\alpha^4, 2 + \alpha + 2\alpha^3,$

$2 + \alpha + 2\alpha^4, 2\alpha^2 + \alpha^3 + 2\alpha^4, \alpha + 2\alpha^3, 2 + 2\alpha + 2\alpha^2 + \alpha^3, 2 + \alpha + \alpha^2 + 2\alpha^4, \alpha + \alpha^2 + \alpha^4, 2 + 2\alpha^3 + \alpha^4, \alpha + \alpha^4,$

$1 + 2\alpha^2 + \alpha^4, \alpha^2 + \alpha^3 + \alpha^4, 2 + 2\alpha + 2\alpha^2 + 2\alpha^3, \alpha + 2\alpha^3 + \alpha^4, 2 + \alpha + 2\alpha^2 + 2\alpha^3 + \alpha^4, 1 + 2\alpha^3 + \alpha^4,$

$2 + 2\alpha + \alpha^2 + \alpha^3 + 2\alpha^4, \alpha + \alpha^2 + 2\alpha^3 + 2\alpha^4, 2 + 2\alpha + 2\alpha^2 + \alpha^3 + 2\alpha^4, 1 + 2\alpha^4, 2 + \alpha + \alpha^2, 2 + \alpha^2 + 2\alpha^3 + \alpha^4,$

$1 + \alpha + \alpha^2 + \alpha^3, 1 + \alpha + \alpha^2 + 2\alpha^4, 2 + 2\alpha^2 + 2\alpha^4, 2 + 2\alpha + \alpha^2 + \alpha^3, 1 + \alpha^3 + 2\alpha^4, 2 + 2\alpha + \alpha^3 + \alpha^4,$

$\alpha^2 + 2\alpha^3 + 2\alpha^4, 2\alpha^2 + 2\alpha^4, 2 + 2\alpha + 2\alpha^2 + 2\alpha^3 + 2\alpha^4, 1 + 2\alpha + \alpha^2 + 2\alpha^3 + 2\alpha^4, , 2\alpha + 2\alpha^2 + 2\alpha^3 + \alpha^4.$