SOME CLASSES OF POLYNOMIALS OVER FINITE FIELDS

Thesis submitted for the award of the Degree
of

Doctor of Philosophy

in the Department of Mathematics

by

Mohit Pal
(2018RMA0021)

Under the supervision of

Sartaj Ul Hasan

भारतीय प्रौद्योगिकी
संस्थान जम्मू
INDIAN INSTITUTE OF
TECHNOLOGY JAMMU

Indian Institute of Technology Jammu
Jammu 181221

July 2021

Declaration

I hereby declare that the matter embodied in this thesis entitled **"Some Classes of Polynomials over Finite Fields"** is the result of investigations carried out by me in the Department of Mathematics, Indian Institute of Technology Jammu, India, under the supervision of **Sartaj Ul Hasan** and it has not been submitted elsewhere for the award of any degree or diploma, membership etc. In keeping with the general practice in reporting scientific observations, due acknowledgements have been made whenever the work described is based on the findings of other investigators. Any omission that might have occurred due to oversight or error in judgment is regretted. A complete bibliography of the books and journals referred in this thesis is given at the end of the thesis.

July 2021 — Mohit Pal

Indian Institute of Technology Jammu — (2018RMA0021)

To My Sisters

Acknowledgements

First of all, I wish to express my deepest gratitude to my supervisor Sartaj Ul Hasan for believing in me more than I believe myself. I am lucky and honoured to be his first Ph.D. student. I never expected anyone could help me as much as he did. He worked hard to create plateforms where I can furnish. I will forever appreciate all the discussions, academics and otherwise, we had.

I would like to thank Pantelimon Stănică for giving me an opportunity to work with him. I am grateful to him for suggesting me several problems during my Ph.D. studies. I will also never forget how he helped me when I got stuck at certain points while solving problems. He not only shared his knowledge, experience and wisdom with me, but also taught me to be an active person. I am much indebted to him as my collaborator and mentor. I am very thankful to him for allowing me to include our joint work in my thesis.

I would like to thank Constanza Riera and Neranga Fernando for several helpful discussions and suggestions. I am also thankful to them for allowing me to include our joint works in my thesis.

I also like to thank my SRC committee members Sumit Kumar Pandey and Ajay Kumar for their useful suggestions during my semester progress seminars. In fact special thanks to Sumit Kumar Pandey for helping me at several occasions especially in programming.

I was fortunate to find supporting friends during my Ph.D. studies. I will forever cherish moments shared with Hridesh, Hardeep, Kirpa, Bijender, Mukul, Jay, Uzma, Nitesh, Mehran, Shubham, Satyendra, Abhishek, Gaurav, Ambreen, Shilpa, Sonam, and Rahul. I would also like to thank my other friends from school and college.

Words fail me to discribe my gratitude towards my parents and my sisters for their endless support.

Abstract

Mathematics and cryptography have a long history together. Almost all the modern crypto systems use the notions either from number theory or from finite fields in some way or the other. This thesis is devoted to the study of some mathematical problems arising from cyptography. More precisely, we study cryptographic properties of some classes of polynomials over finite fields.

Substitution boxes (S-boxes) play a very crucial role in the design of secure cryptographic primitives such as block ciphers. Differential attack, introduced by Biham and Shamir [4] in 1991, is one of the most efficient attacks on the S-boxes used in the block ciphers. To quantify the degree of security of a S-box against the differential attacks, Nyberg [45] in 1993 introduced the notion of differential uniformity. In 2020, Ellingsen et. al generalized the notion of differential uniformity and introduced the concept of c-differential uniformity.

There is yet another important attack on block ciphers known as the boomerang attack. This attack was proposed by Wagner [57] in 1999. In 2018, Cid et. al [19] introduced the notion of boomerang connectivity table to analyze the boomerang attack. Further, to quantify the resistance of a function against the boomerang attack, Boura and Canteaut in 2018 introduced the concept of boomerang uniformity. In 2020, Stănică generalized the concept of boomerang uniformity and introduced the notion of c-boomerang uniformity. Now we summarize our contributions in the subsequent paragraphs.

First, we consider optimal functions with respect to differential uniformity over finite fields of odd characteristic known as planar functions. To be more precise, we discuss the problem of classifying Dembowski-Ostrom polynomials from the composition of reversed Dickson polynomials of arbitrary kind and monomials over finite fields of odd characteristic. Moreover, by using a variant of the Weil bound for the number of points of affine algebraic curves over finite fields, we discuss the planarity of all such Dembowski-Ostrom polynomials.

Afterwards, we study the c-differential uniformity of some functions over finite fields of odd characteristic and give several classes of power maps with low c-differential uniformity, for $c = -1$. We also give a necessary and sufficient condition for a linearized polynomial to be a perfect c-nonlinear function and investigate conditions when perturbations of

perfect c-nonlinear (or not) function via an arbitrary Boolean or p-ary function is perfect c-nonlinear. In the process, we obtain a class of polynomials that are perfect c-nonlinear for all $c \neq 1$, in every characteristic.

Next, we consider the c-differential uniformity and boomerang uniformity of two classes of permutation functions over finite fields of even characteristic. One of these classes is in fact a class of involutions, which has been used by Beierle and Leander [3] to construct a class of differentially 4-uniform functions. We shall show that the c-differential uniformity of this involution is 2 for all $c \neq 0, 1$. We also give the boomerang connectivity table entries of this class of involutions. The other class is of differentially 4-uniform permutations given by Tan et. al [55]. We give a bound for its c-differential uniformity and boomerang uniformity.

Further, we consider the boomerang uniformity of an infinite class of power maps over finite fields of even characteristic. We show that for non-permutations, the differential uniformity is not necessarily smaller than the boomerang uniformity, as was the case for permutations.

At the end, we give a complete description of the c-boomerang connectivity table entries for the Gold function over finite fields of even characteristic, by using double Weil sums. In the process we generalize a result of Boura and Canteaut [8] for the classical boomerang uniformity.

List of Abbreviations

APN	:	almost perfect nonlinear
APcN	:	almost perfect c-nonlinear
BCT	:	boomerang connectivity table
BU	:	boomerang uniformity
CCZ	:	Carlet Charpin Zinoviev
cBCT	:	c-boomerang connectivity table
cBU	:	c-boomerang uniformity
cDDT	:	c-difference distribution table
cDU	:	c-differential uniformity
CPP	:	complete permutation polynomial
DO	:	Dembowski-Ostrom
DDT	:	difference distribution table
DU	:	differential uniformity
EA	:	extended affine
HFE	:	hidden field equation
RDP	:	reversed Dickson polynomial
PN	:	perfect nonlinear
PcN	:	perfect c-nonlinear
PP	:	permutation polynomial

Contents

Chapter 1

Introduction

This thesis comprises of a study of some polynomials over finite fields, which have applications in cryptography and coding theory, and it consists of two parts. The first part is devoted to the study of the differential uniformity (DU) and its generalisation called the c-differential uniformity (cDU), of some classes of polynomials over finite fields. The second part of the thesis is dedicated to the study of the boomerang uniformity (BU) and its generalisation called the c-boomerang uniformity (cBU), of some classes of polynomials over finite fields of even characteristic. Chapters 2, 3 and part of Chapter 4 shall form the first part, while the remaining part of Chapter 4 and Chapters 5 and 6 constitute the second part. In the following, we explain some relevant background and give a brief motivated account of the contents of these chapters.

We denote, by $\mathbb{F}_q$ the finite field with $q = p^n$ elements, where p is a prime number and n is a positive integer. By $\mathbb{F}_q^* = \langle g \rangle$, where g is a primitive element of $\mathbb{F}_q$, we denote the multiplicative cyclic group of non-zero elements of $\mathbb{F}_q$. We call a function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ a p-ary function in n variables. For positive integers n and m, any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is called a vectorial p-ary function, or (n, m)-function. When $m = n$, f can be uniquely represented as a univariate polynomial over $\mathbb{F}_q$ of the form $f(X) = \sum_{i=0}^{q-1} a_i X^i$, $a_i \in \mathbb{F}_q$. Therefore in such a scenerio, we often consider f as a polynomial $f \in \mathbb{F}_q[X]$. We recall that a polynomial $f \in \mathbb{F}_q[X]$ is a permutation polynomial (PP) over $\mathbb{F}_q$ if the associated mapping $X \mapsto f(X)$ is a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$.

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 sometimes write this as Tr_1^n). We define the relative trace $\operatorname{Tr}_e^n : \mathbb{F}_{p^n} \to \mathbb{F}_{p^e}, e|n$, by $\operatorname{Tr}_e^n(X) = X + X^{p^e} + X^{p^{2e}} + \cdots + X^{p^{e(\frac{n}{e}-1)}}$. Note that all additive characters of $\mathbb{F}_q$ can be expressed in terms of χ_1 [36, Theorem 5.7].

For each $0 \le k \le q-2$, the k-th multiplicative character is a homomorphism $\psi_k : \mathbb{F}_q^* \to \mathbb{C}$ of the multiplicative group of $\mathbb{F}_q$ defined as follows

$$\psi_k\left(g^\ell\right) = \exp\left(\frac{2\pi i k \ell}{q-1}\right) \quad \text{for } \ell = 0, \ldots, q-2.$$

It is well-known that the group of multiplicative characters of $\mathbb{F}_q$ is a cyclic group of order $q-1$ with identity element ψ_0 [36, Corollary 5.9].

In the theory of finite fields, exponential sums are important tools in the study of number of solutions of equations over finite fields. As a special case, the Gauss' sums are defined as follows

$$G(\psi, \chi) = \sum_{X \in \mathbb{F}_q^*} \psi(X)\chi(X),$$

where χ and ψ are additive and multiplicative characters of $\mathbb{F}_q$, respectively.

A Weil sum is yet another important character sum defined as follows

$$\sum_{X \in \mathbb{F}_q} \chi(f(X)),$$

where χ is an additive character of $\mathbb{F}_q$ and $f(X)$ is a polynomial in $\mathbb{F}_q[X]$. It is well-known that a polynomial $f(X)$ over finite field $\mathbb{F}_q$ is a PP if and only if its Weil sum $\sum_{X \in \mathbb{F}_q} \chi(f(X)) = 0$ for all nontrivial additive characters χ of $\mathbb{F}_q$.

Differential cryptanalysis, introduced by Biham and Shamir [4], is one of the most powerful attacks against block ciphers. To quantify the ability of a given function to resist the differential attack, Nyberg [45] introduced the concept of differential uniformity. For any function $f : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of f in the direction a, denoted by

$D_f(X, a)$, is defined as

$$D_f(X, a) := f(X + a) - f(X) \text{ for all } X \in \mathbb{F}_q.$$

For any $a, b \in \mathbb{F}_q$, the Difference Distribution Table (DDT) entry at point (a, b), denoted by $\Delta_f(a, b)$, is defined as

$$\Delta_f(a, b) := |\{X \in \mathbb{F}_q \mid D_f(X, a) = b\}|.$$

The differential uniformity of f, denoted by Δ_f, is defined as

$$\Delta_f := \max\{\Delta_f(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}.$$

If $\Delta_f = \delta$, we say that the function f is δ-uniform. When $\delta = 1, 2$, we say that the function f is perfect nonlinear (PN) and almost perfect nonlinear (APN), respectively. It is easy to observe that over finite fields of even characteristic, the solutions of the equation $D_f(X, a) = b$ always comes into pairs, i.e., if X is a solution then so is $X + a$. Therefore, the least possible value for the DU of a function over finite fields of even characteristic is two. Thus, APN functions have lowest possible DU over finite fields of characteristic 2. Though PN functions do not exist over finite fields of even characteristic, they do exist over finite fields of odd characteristic where they are often called as planar functions. A polynomial $f \in \mathbb{F}_q[X]$ is called exceptional planar if it is planar over $\mathbb{F}_{p^n}$ for infinitely many n. Planar functions are very important due to their wide range of applications. For example, planar functions are used to construct finite projective planes [24], relative difference sets [30] and error-correcting codes [14].

A Dembowski-Ostrom (DO) polynomial over finite field $\mathbb{F}_q$ is a polynomial that admits the following shape

$$\sum_{i,j} a_{ij} X^{p^i + p^j},$$

where $a_{ij} \in \mathbb{F}_q$. DO polynomials have been used in designing a public key cryptosystem known as HFE [46]. Note that DO polynomials provide a very rich source of planar functions. It was conjectured by Rónyai and Szönyi [49] (see also [43, Conjecture 9.5.19]) that all planar functions are of "DO type". This conjecture is still open except in the case

of characteristic 3 for which a counter example was given by Coulter and Matthews [20].

For any nonnegative integer k, the k-th Dickson polynomial of the first kind $D_k(X, a)$ over $\mathbb{F}_q$ was introduced by Dickson [25] in 1897, and is defined as follows

$$D_k(X,a) := \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-a)^i X^{k-2i},$$

where $a \in \mathbb{F}_q$ is a parameter and $D_0(X, a) = 2$. More than two decades later, Schur [50] introduced a variant of Dickson polynomial of the first kind in 1923, which is now known as Dickson polynomial of the second kind. For any nonnegative integer k, the k-th Dickson polynomial of the second kind $E_k(X, a)$ over $\mathbb{F}_q$ is defined as follows

$$E_k(X,a) := \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} (-a)^i X^{k-2i},$$

where $a \in \mathbb{F}_q$ is a parameter and $E_0(X, a) = 1$. Dickson polynomials of the first and second kind over $\mathbb{F}_q$ have been studied extensively, especially with respect to their permutation behaviour. For a non-zero element a in $\mathbb{F}_q$, Nöbauer [44] proved that the Dickson polynomial of the first kind $D_k(X, a)$ permutes the elements of $\mathbb{F}_q$ if and only if $\gcd(k, q^2-1) = 1$. However, except for a few cases, the permutation behaviour of Dickson polynomials of the second kind $E_k(X, a)$ remains unresolved. One may refer to the monograph [35] for more on Dickson polynomials.

In 2010, Coulter and Matthews [22] classified DO polynomials from the composition of Dickson polynomials of the first and second kind with the monomial X^d, where d is a positive integer, and further discussed the planarity of such DO polynomials. The motivation behind considering this composition actually stemmed from the known fact that the exceptional planar polynomials $X^{10} \pm X^6 - X^2$ are essentially the composition of the Dickson polynomials $D_5(X, \pm 1)$ and the monomial X^2.

The notion of k-th reversed Dickson polynomial (RDP) of the first kind was introduced by Hou, Mullen, Sellers and Yucas [33] by simply reversing the roles of the variable X and the parameter a in the k-th Dickson polynomial of the first kind $D_k(X, a)$. Moreover, the authors showed that the reversed Dickson polynomials of the first kind are closely related to APN functions.

Motivated by the results of Coulter and Matthews [22], Zhang, Wu and Liu [64] classified DO polynomials from RDPs of the first kind in the even characteristic case and they also characterized APN functions among all such DO polynomials.

For any nonnegative integers k and m, the notion of k-th Dickson polynomial of the $(m+1)$-th kind, denoted as $D_{k,m}(X,a)$, was introduced by Wang and Yucas [58], and is defined as follows

$$D_{k,m}(X,a) := \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k-mi}{k-i} \binom{k-i}{i} (-a)^i X^{k-2i}, \tag{1.1}$$

where $0 \leq m \leq p-1$, $a \in \mathbb{F}_q$ and $D_{0,m}(X,a) = 2-m$. The k-th RDP of the $(m+1)$-th kind is also defined in a similar way by just reversing the role of the variable X and the parameter a in (1.1). More precisely, for any nonnegative integers k and m, the k-th RDP of the $(m+1)$-th kind $D_{k,m}(a,X)$ is defined as follows

$$D_{k,m}(a,X) := \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k-mi}{k-i} \binom{k-i}{i} (-X)^i a^{k-2i}, \tag{1.2}$$

where $0 \leq m \leq p-1$, $a \in \mathbb{F}_q$ and $D_{0,m}(a,X) = 2-m$. The k-th RDP of the $(m+1)$-th kind also satisfies the following recurrence relation

$$D_{k,m}(a,X) = mE_k(a,X) - (m-1)D_k(a,X). \tag{1.3}$$

In Chapter 2, we extend the results of Zhang, Wu and Liu [64] to the odd characteristic case, where we give a complete classification of DO polynomials arising from the composition of RDPs of the $(m+1)$-th kind with the monomial X^d, where d is a positive integer. Moreover, by using a variant of the Weil bound for the number of points of affine algebraic curves over finite fields, we discuss the planarity of all such DO polynomials.

Deviating from the usual differentials $(f(X+a), f(X))$, Borisov et. al. [6] introduced the notion of so called multiplicative differentials of the form $(f(cX), f(X))$ and they used this new type of differentials to attack some existing ciphers. Motivated by the multiplicative differentials as discussed in [6], Ellingsen et. al [28] defined a new (output) multiplicative differential in the following way. For any function f from a finite field $\mathbb{F}_q$ to itself and for any $a, c \in \mathbb{F}_q$, the (multiplicative) c-derivative of f with respect to a is

defined as

$$_cD_f(X,a) = f(X+a) - cf(X) \text{ for all } X \in \mathbb{F}_q.$$

For $a, b \in \mathbb{F}_q$, the c-difference distribution table (cDDT) entry of f at point (a,b), denoted by $_c\Delta_f(a,b)$, is given by

$$_c\Delta_f(a,b) = |\{X \in \mathbb{F}_q : \ _cD_f(X,a) = b\}|.$$

The c-differential uniformity (cDU) of f, denoted as $_c\Delta_f$, is then defined as

$$_c\Delta_f := \max\{_c\Delta_f(a,b) : a, b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}.$$

When $_c\Delta_f = \delta$, we say that cDU of f is δ. It is easy to see that when $c = 1$, cDU coincides with the usual notion of DU. If $\delta = 1$ then f is called perfect c-nonlinear (PcN) function and when $\delta = 2$ then f is called almost perfect c-nonlinear (APcN) function. Also it is easy to observe from the definition of PcN function that when $c \neq 1$ and $a = 0$ then $f(X+a) - cf(X) = (1-c)f(X)$ is a permutation polynomial if and only if $f(X)$ is a permutation polynomial. Therefore, we shall consider the perfect c-nonlinearity of permutation polynomials only.

In chapter 3, we establish a relation between the c-derivative of the power map X^d and Dickson polynomial of the first kind over $\mathbb{F}_q$, for $c = -1$. In fact, such a relationship has its origin in [60, Proposition 8], where it was established for the fields of characteristic 3. We extend this result to finite fields of odd characteristic and use it to construct several classes of PcN power maps. We also give a necessary and sufficient condition for a linearized polynomial to be PcN. We also find necessary and sufficient conditions for the sum $f + \gamma F$ to be PcN, where $\gamma \in \mathbb{F}_q$, f is PcN and F is any Boolean function. We also show that in some instances such perturbations do not produce PcN functions. We further discuss the affine, extended affine and CCZ-equivalence as it relates to cDU.

In a block cipher, nonlinearity of the function f is also an important property. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function. The Walsh-Hadamard transform is defined as the integer-valued function

$$\mathcal{W}_F(u) := \sum_{X \in \mathbb{F}_{2^n}} (-1)^{F(X)+\mathrm{Tr}(uX)}, \ u \in \mathbb{F}_{2^n},$$

where $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function. The (vectorial) Walsh transform $\mathcal{W}_f(a,b)$ of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ at $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is the Walsh-Hadamard transform of its component function $\mathrm{Tr}(bf(X))$ at a, that is,

$$\mathcal{W}_f(a,b) := \sum_{X \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(bf(X)+aX)}.$$

The nonlinearity, denoted by $\mathcal{NL}(f)$, of the function f is defined by

$$\mathcal{NL}(f) := 2^{n-1} - \frac{1}{2} \max_{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}} |\mathcal{W}_f(a,b)|.$$

In Chapter 4, the first part deals with the cDU of two classes of permutation polynomials. The first class of permutation polynomials is in fact a class of involutions which has been used by Beierle and Leander [3] to construct a class of differentially 4-uniform functions with trivial nonlinearity. We give the cDDT entries of this class of involutions explicitely, for all $c \neq 0, 1$. The second class of permutations is a class of differentially 4-uniform functions introduced by Tan et. al [55]. We give a bound for the cDU of this class of permutations.

The second part of the thesis is devoted to another cryptographic property of functions over finite fields called Boomerang uniformity (BU). The BU is connected to the boomerang attack against block ciphers introduced by Wagner [57]. The boomerang attack may be thought of as an extension of the differential attack [4]. In order to analyze the boomerang attack in a better way, and analogously to the DDT concerning differential attack, Cid et al. [19] introduced the notion of boomerang connectivity table (BCT). Further, to quantify the resistance of a function against the boomerang attack, Boura and Canteaut [8] introduced the concept of boomerang uniformity (BU), which is the maximum value in the BCT excluding the first row and first column. For effectively computing the entries in the BCT, Li et al. [37] proposed an equivalent formulation as follows. For any $a, b \in \mathbb{F}_q$, the BCT entry of the function f at point (a,b), denoted by $\mathcal{B}_f(a,b)$, is the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the following system of equations

$$\begin{cases} f(X) - f(Y) = b, \\ f(X+a) - f(Y+a) = b. \end{cases}$$

The BU of the function f, denoted by $\mathcal{B}_f$, is given by

$$\mathcal{B}_f = \max\{\mathcal{B}_f(a,b) \mid a,b \in \mathbb{F}_q^*\}.$$

In Chapter 4, the second part is devoted to the BU of the class of involutions given by Beierle and Leander [3] and the class of differentially 4-uniform permutations introduced by Tan et. al [55]. For the class of involutions, we explicitely compute the BCT entries and show that there are only two values for the BCT entries. For the class of differentially 4-uniform permutations, we give bound for its BU.

Cid et al. [19] (see also [42]) showed that for any function f and for any $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$, the BCT entry is greater than or equal to the corresponding DDT entry. In fact, the authors Cid et al. [19] (see also [42, Theorem 1]) showed that for permutation functions f, $\Delta_f \leq \mathcal{B}_f$. Cid et. al [19, Lemma 4] also showed that for APN permutations, the BCT is the same as the DDT, except for the first row and the first column. Thus, APN permutations offer an optimal resistance to both differential and boomerang attacks. However, over finite fields $\mathbb{F}_{2^n}$ with n even, which is the most interesting case in cryptography, the only known example of APN permutation is due to Dillon [10] over $\mathbb{F}_{2^6}$. The existence of APN permutations over $\mathbb{F}_{2^n}$, $n \geq 8$ even, is an open problem and often referred to as the Big APN Problem. Therefore, over $\mathbb{F}_{2^n}$, n even, the functions with DU and BU four offer the best (known) resistance to differential and boomerang attacks. So far, there are six classes of permutations over $\mathbb{F}_{2^n}$, n even, with boomerang uniformity 4 (see [8, 37, 38, 39, 42, 56]).

In Chapter 5, we give a class of power functions (non-permutation) having boomerang uniformity 4. This is the first example of a non-permutation function with boomerang uniformity 4. We also show that for this class of power maps $\Delta_f > \mathcal{B}_f$. To the best of our knowledge this is the first such example of a class of functions (non-permutation).

Recently, Stănică [51] extended the notion of BCT and BU and defined the c-boomerang connectivity table (cBCT) and c-boomerang uniformity (cBU) for an arbitrary polynomial function f over $\mathbb{F}_q$, for any $c \neq 0 \in \mathbb{F}_q$. Let $a, b \in \mathbb{F}_q$, then the entry of the cBCT at $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q$, denoted as ${}_c\mathcal{B}_f(a,b)$, is the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the following system

$$\begin{cases} f(X) - cf(Y) = b \\ f(X+a) - c^{-1}f(Y+a) = b. \end{cases}$$

The cBU of f is defined as

$$_c\mathcal{B}_f = \max \{_c\mathcal{B}_f(a,b) \mid a,b \in \mathbb{F}_q^*\}.$$

In yet another recent paper, Stănică [52] further studied the cBCT and gave an elegant description of the cBCT entries of the power maps 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 $1 \leq k < n$ and p odd.

In Chapter 6, we extend the work of Stănică [52] to the finite fields of characteristic 2. More precisely, we give a complete description of the cBCT for the Gold function over finite fields of even characteristic, by using double Weil sums. In the process we generalize a result of Boura and Canteaut [8] for the classical BU.

Chapter 2

Dembowski-Ostrom Polynomials and Reversed Dickson Polynomials

In this chapter, we give a complete classification of Dembowski-Ostrom (DO) polynomials arising from the composition of reversed Dickson polynomials (RDPs) of the $(m+1)$-th kind and the monomial X^d, where d is a positive integer, in odd characteristic, and we further characterize planar functions among these DO polynomials. DO polynomials do not have any constant term. We shall, therefore, consider the polynomials $\widehat{\mathfrak{D}}_{k,m} := D_{k,m}(a, X^d) - D_{k,m}(a, 0)$ for the purpose of classifying DO polynomials. Notice that $\widehat{\mathfrak{D}}_{k,m}$ is given by

$$\widehat{\mathfrak{D}}_{k,m} = \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} \frac{k-mi}{k-i} \binom{k-i}{i} (-X^d)^i a^{k-2i}.$$

For the sake of simplicity, we shall denote $\widehat{\mathfrak{D}}_{k,0}$, $\widehat{\mathfrak{D}}_{k,1}$, $\widehat{\mathfrak{D}}_{k,2}$, $\widehat{\mathfrak{D}}_{k,3}$, and $\widehat{\mathfrak{D}}_{k,4}$ by $\widehat{\mathfrak{D}}_k$, $\widehat{\mathfrak{E}}_k$, $\widehat{\mathfrak{F}}_k$, $\widehat{\mathfrak{G}}_k$ and $\widehat{\mathfrak{H}}_k$, respectively. This chapter has been organized as follows. In Section 2.1, we state some lemmas that will be used in the subsequent sections. In Sections 2.2, 2.3, 2.4 and 2.5, we classify DO polynomials from $\widehat{\mathfrak{D}}_k$, $\widehat{\mathfrak{E}}_k$, $\widehat{\mathfrak{G}}_k$ and $\widehat{\mathfrak{H}}_k$, respectively. The case $m \geq 5$ has been considered in Section 2.6. In Section 2.7, we consider the planarity of DO polynomials obtained in the previous sections. The complete list of DO polynomials derived from reversed Dickson polynomials is given in Section 2.8.

Throughout this chapter, we always assume that p is an odd prime, d is a positive integer, and $i, j, k, \ell, m, n, s, t, \alpha, \beta, \gamma, \delta$ are nonnegative integers unless specified otherwise.

2.1 Some Useful Lemmas

As alluded earlier, we shall first classify DO polynomials derived from the composition of RDPs of the $(m+1)$-th kind and the monomial X^d, where d is a positive integer. Since DO polynomials are closed under the composition with the monomial X^p, it would be sufficient to consider the cases when $\gcd(d,p)=1$. One may also note that the monomial X^{rd}, where r is positive integer, is a DO monomial if and only if $rd = p^\beta(p^\alpha+1)$ for some nonnegative integers α and β. Here, β is the highest exponent of p such that $p^\beta \mid r$. It is obvious that whenever $\gcd(r,p)=1$, we must have $\beta=0$. In what follows, we shall invoke these assumptions and conventions as and when required.

We now present some lemmas which will be useful in the sequel.

Lemma 2.1.1. *Let d be a positive integer and $p>3$ be a prime such that $\gcd(d,p)=1$. Assume that the coefficients of X^d and X^{2d} in the polynomial $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Then the polynomial $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial.*

Proof. Assume that $p>3$ and the coefficients of X^d and X^{2d} in the polynomial $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Therefore, if $\widehat{\mathfrak{D}}_{k,m}$ is a DO polynomial then $d=p^\alpha+1$ and $2d=p^\beta+1$. Thus, we have $2p^\alpha+1=p^\beta$, which is true if and only if $\alpha=0$, $\beta=1$ and $p=3$. This is a contradiction to our assumption that $p>3$, hence $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial. □

Lemma 2.1.2. *Let d be a positive integer and $p>5$ be a prime such that $\gcd(d,p)=1$. Assume that the coefficients of X^d and X^{3d} in the polynomial $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Then the polynomial $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial.*

Proof. The proof follows using a similar reasoning as in the proof of Lemma 2.1.1. □

Lemma 2.1.3. *Let d be a positive integer and $p>3$ be an odd prime such that $\gcd(d,p)=1$. Assume that the coefficients of X^{3d} and X^{4d} in the polynomial $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Then the polynomial $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial.*

Proof. The proof is along the similar line as in the proof of Lemma 2.1.1. □

Lemma 2.1.4. *Let $p=3$ and d be a positive integer such that $\gcd(d,3)=1$. Assume that the coefficients of X^d and X^{4d} in the polynomial $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Then the polynomial $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial.*

Proof. The proof follows by using a similar argument as in Lemma 2.1.1. □

Now we recall the following lemma from [36, Proposition 6.39], which will be used later.

Lemma 2.1.5. *(Legendre's formula) For any nonnegative integer ω and any prime p, $E_p(\omega!)$ the largest exponent of p that divides $\omega!$ is given by*

$$E_p(\omega!) = \sum_{i=1}^{\infty} \left\lfloor \frac{\omega}{p^i} \right\rfloor = \frac{\omega - \omega_s}{p-1},$$

where ω_s is the sum of the digits in the representation of ω to the base p.

2.2 DO Polynomials from RDPs of the First Kind

Before we begin the classification of DO polynomials from RDPs of the first kind, we shall slightly deviate and prove the following proposition that readily gives DO polynomials arising from RDPs of the $(m+1)$-th kind when the parameter a is zero.

Proposition 2.2.1. *The polynomial $D_{k,m}(0, X^d)$ is DO if and only if k is even, $m \not\equiv 2 \pmod{p}$ and kd is of the form $2p^j(p^i+1)$, where $i, j \geq 0$.*

Proof. We know that

$$D_{k,m}(0, X^d) = \begin{cases} 0 & \text{if } k \text{ is odd;} \\ (2-m)(-X^d)^{\frac{k}{2}} & \text{if } k \text{ is even.} \end{cases}$$

Clearly, $D_{k,m}(0, X^d)$ is a DO polynomial if and only if k is even, $m \not\equiv 2 \pmod{p}$ and $kd = 2p^j(p^i+1)$. □

In view of Proposition 2.2.1, we shall assume that a is non-zero for the rest of the chapter. We now consider RDPs of the first kind. For $a \neq 0$, we write $X = Y(a-Y)$ with an indeterminate $Y \in \mathbb{F}_{q^2}$. Then

$$D_{k,0}(a, X) = Y^k + (a-Y)^k;$$

see [29, Section 2]. Also, we have $D_{k,0}(a,0) = a^k$. Since $D_{kp,0}(a,X) = (D_{k,0}(a,X))^p$ and $D_{kp,0}(a,0) = (D_{k,0}(a,0))^p$, we have $\widehat{\mathfrak{D}}_{kp} = \widehat{\mathfrak{D}}_k^p$, where

$$\widehat{\mathfrak{D}}_k = D_{k,0}(a,X^d) - D_{k,0}(a,0) = \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i}\binom{k-i}{i}(-X^d)^i a^{k-2i}.$$

Since $\widehat{\mathfrak{D}}_{kp} = \widehat{\mathfrak{D}}_k^p$, it would be sufficient to consider the cases when $\gcd(k,p) = 1$. The following theorems give a complete classification of DO polynomials from polynomial $\widehat{\mathfrak{D}}_k$ for k odd and k even, respectively.

Theorem 1. *Let q be a power of an odd prime p, $a \in \mathbb{F}_q^*$ and k odd. The polynomial $\widehat{\mathfrak{D}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$p = 3$, $d = 2p^t$, $k = 5p^\ell, 7p^\ell$, where $\ell, t \geq 0$.*

(ii) *$p > 3$, $d = p^t(p^\alpha + 1)$, $k = 3p^\ell$, where $\ell, t, \alpha \geq 0$.*

Proof. The sufficiency of the theorem is straightforward. It only remains to show the necessity. Notice that when k is odd, then

$$\begin{aligned}\widehat{\mathfrak{D}}_k = -kX^d a^{k-2} + \frac{(k-3)k}{2!}X^{2d}a^{k-4} - \frac{(k-4)(k-5)k}{3!}X^{3d}a^{k-6} + \\ \cdots + (-1)^{\frac{k-3}{2}}\frac{(k-1)k(k+1)}{24}X^{\frac{d(k-3)}{2}}a^3 + (-1)^{\frac{k-1}{2}}kX^{\frac{d(k-1)}{2}}a.\end{aligned} \tag{2.1}$$

Since $\gcd(k,p) = 1$, the first term $-ka^{k-2}X^d$ in $\widehat{\mathfrak{D}}_k$ will always exist. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial then $d = p^j(p^i+1)$. Since $\gcd(d,p) = 1$, we have $j = 0$. Therefore, we shall always take $d = p^i + 1$. Now we consider two cases, $k \not\equiv 3 \pmod p$ and $k \equiv 3 \pmod p$.

Case 1. Let $k \not\equiv 3 \pmod p$. In this case, the coefficient of the second term in (2.1) is non-zero. Therefore, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $2d = p^\beta(p^\alpha+1)$ and $d = p^i + 1$. Since p is odd and $\gcd(d,p) = 1$, $\beta = 0$. Hence, the first equation reduces to $2d = p^\alpha + 1$. Combining these two equations, we obtain $2p^i + 1 = p^\alpha$, which is true if and only if $p = 3$, $\alpha = 1$, $i = 0$ and $d = 2$. Therefore, in this case, we shall always assume that $p = 3$ and $d = 2$. For $k = 5$ and $k = 7$, the polynomials $\widehat{\mathfrak{D}}_5 = a^3X^2 + 2aX^4$ and $\widehat{\mathfrak{D}}_7 = 2a^5X^2 + 2a^3X^4 + 2aX^6$, are clearly DO polynomials. Now we claim that when $p = 3$ and $k > 7$ is odd, $\widehat{\mathfrak{D}}_k$ is never a DO polynomial. Since $\gcd(k,3) = 1$, we have only two cases to consider, namely, $k \equiv 2 \pmod 3$ and $k \equiv 1 \pmod 3$.

In the case $k \equiv 2 \pmod 3$, consider the second last term in (2.1) which is given by

$$(-1)^{\frac{k-3}{2}} \frac{(k-1)k(k+1)}{24} a^3 X^{k-3}.$$

If the coefficient of the second last term in (2.1) is non-zero, then we claim that $(k-3)$ cannot be written as $3^i + 3^j$ for some nonnegative integers i and j. On the contrary assume that $k-3 = 3^i + 3^j$, which implies $k-2 = 3^i + 3^j + 1$. Since $k \equiv 2 \pmod 3$, $k-2 = 3^i + 3^j + 1$ if and only if $i = j = 0$. But $i = j = 0$ implies $k = 5$, which is a contradiction to our assumption that $k > 7$. Therefore $\widehat{\mathfrak{D}}_k$ is not a DO polynomial in this case.

Now assume that the coefficient of the second last term in (2.1) is zero. In this case, we shall show that the fourth term always exists. Note that the fourth term contains the monomial X^8 whose exponent cannot be written as $3^i + 3^j$ for some nonnegative integers i and j. The coefficient of the fourth term is given by

$$\frac{k(k-5)(k-6)(k-7)}{24} a^{k-8}. \tag{2.2}$$

Since $\gcd(k, 3) = 1$, we have $3 \nmid k$ and $3 \nmid (k-6)$. Since $k \equiv 2 \pmod 3$, where k is odd and greater than 7, $(k-5)(k-7)$ is a multiple of 24, i.e. $(k-5)(k-7) = 24b$, where b is an integer. Then the coefficient of the fourth term in (2.2) becomes $k(k-6)b$.

Now we show that $3 \nmid b$. On the contrary, assume that $3 \mid b$. Then we have, $(k-5)(k-7) = 72e$ for some integer e. Since $k \equiv 2 \pmod 3$, write $k = 3e_1 - 1$ for some integer e_1. Recall that the second last term in (2.1) vanishes. By substituting $3e_1 - 1$ for k in the coefficient of the second last term, we obtain $e_1 \equiv 0 \pmod 3$. Let $e_1 = 3n_1$ for some integer n_1. Then $k = 3e_1 - 1 = 9n_1 - 1 \equiv -1 \pmod 9$. From $(k-5)(k-7) = 72e$ and $k \equiv -1 \pmod 9$, we have $3 \equiv 0 \pmod 9$, which is a contradiction. Therefore, our assumption that $3 \mid b$ is wrong, and hence the coefficient of X^8 is non-zero. Therefore, when the second last term in (2.1) vanishes, $\widehat{\mathfrak{D}}_k$ is not a DO polynomial.

In the case $k \equiv 1 \pmod 3$, we first look at the fourth term. Recall that the fourth term contains the monomial X^8 whose exponent cannot be written as $3^i + 3^j$ for some nonnegative integers i and j. If the coefficient of the fourth term given in (2.2) is non-zero, then clearly $\widehat{\mathfrak{D}}_k$ is not a DO polynomial. In the case of the coefficient of the fourth term

is zero, we claim that the coefficient of the 7th term, which contains the monomial X^{14}, is non-zero. The coefficient of the 7th term is given by

$$\frac{k(k-8)(k-9)(k-10)(k-11)(k-12)(k-13)}{7!}a^{k-14}.$$

It is clear that the exponent of the monomial X^{14} cannot be written as $3^i + 3^j$ for some nonnegative integers i and j. Since k is odd and $k \equiv 1 \pmod 3$, it is clear that $3 \mid (k-10)$, $6 \mid (k-13)$, $9 \nmid (k-10)$ and $12 \nmid (k-13)$. Also, $3 \nmid k$, $3 \nmid (k-9)$, $3 \nmid (k-12)$, $3 \nmid (k-8)$ and $3 \nmid (k-11)$. Therefore, the coefficient of the 7th term is non-zero. Hence, in the case of the coefficient of the fourth term is zero, $\widehat{\mathfrak{D}}_k$ is not a DO polynomial.

Case 2. Let $k \equiv 3 \pmod p$. In this case, notice that if $p = 3$, then $k \equiv 0 \pmod 3$, which is a contradiction as $\gcd(k, p) = 1$. Therefore we shall assume that $p > 3$. For $k = 3$, the polynomial $\widehat{\mathfrak{D}}_3 = -3aX^d$ is a DO polynomial if and only if $d = p^i + 1$. For $k > 3$, consider the third term in (2.1), which contains the monomial X^{3d}. Since $k \equiv 3 \pmod p$, $k \not\equiv 4, 5 \pmod p$. Hence the coefficient of the third term is non-zero. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $d = p^i + 1$ and $3d = p^j + 1$. Combining these two equations, we have $3p^i + 2 = p^j$, which is true if and only if $i = 0$, $j = 1$, $p = 5$ and $d = 2$. Notice that the coefficient of last term in (2.1), which contains the monomial X^{k-1}, is non-zero. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial then $k - 1 = 5^j(5^i + 1)$. Since $k \equiv 3 \pmod 5$, $k \not\equiv 1 \pmod 5$, and hence $j = 0$. Also, notice that if $i = 0$ then $k = 3$, which is a contradiction as $k > 3$. Therefore $k - 1 = 5^i + 1$ which implies that $k \equiv 2 \pmod 5$, a contradiction as $k \equiv 3 \pmod 5$. Therefore for $k > 3$, $\widehat{\mathfrak{D}}_k$ is never a DO polynomial. This completes the proof. □

Theorem 2. *Let q be a power of an odd prime p, $a \in \mathbb{F}_q^*$ and k even. The polynomial $\widehat{\mathfrak{D}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) $d = p^t(p^\alpha + 1)$, $k = 2p^\ell$, *where* $\ell, t, \alpha \geq 0$.

(ii) $p = 3$, $d = 2p^t$, $k = 4p^\ell$, *where* $\ell, t \geq 0$.

Proof. The sufficiency of the theorem is straightforward. It only remains to show the

necessity. Notice that when k is even, then

$$\widehat{\mathfrak{D}}_k = -ka^{k-2}X^d + \frac{k(k-3)}{2}a^{k-4}X^{2d} - \frac{k(k-4)(k-5)}{6}a^{k-6}X^{3d} + \cdots + (-1)^{\frac{k}{2}-1}\frac{k^2}{4}a^2X^{d(\frac{k}{2}-1)} + (-1)^{\frac{k}{2}} \cdot 2 \cdot X^{\frac{dk}{2}}. \tag{2.3}$$

Since $\gcd(k,p) = 1$, the first term $-ka^{k-2}X^d$ in $\widehat{\mathfrak{D}}_k$ will always exist. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $d = p^j(p^i+1)$. Since $\gcd(d,p) = 1$, we have $j = 0$. Therefore, we shall always take $d = p^i + 1$. When $k = 2$, the polynomials $\widehat{\mathfrak{D}}_2 = -2X^{p^\alpha+1}$ is clearly a DO polynomial. For $k \geq 4$, we consider two cases, $k \not\equiv 3 \pmod p$ and $k \equiv 3 \pmod p$.

Case 1. Let $k \not\equiv 3 \pmod p$. In this case, the coefficient of the second term in (2.3), which contains the monomial X^{2d}, is non-zero. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $2d = p^\beta(p^\alpha+1)$ and $d = p^i + 1$. Since p is odd and $\gcd(d,p) = 1$, we have $\beta = 0$. Combining these two equations, we obtain $p = 3, i = 0, \alpha = 1$ and $d = 2$. Therefore in what follows, we shall take $p = 3$ and $d = 2$. In the case $k = 4$, the polynomial $\widehat{\mathfrak{D}}_4 = 2a^2X^2 + 2X^4$ is clearly DO polynomial.

Now for $k > 4$, even and $k \not\equiv 3 \pmod 3$, we claim that $\widehat{\mathfrak{D}}_k$ is not a DO polynomial. Consider the fourth term, which contains the monomial X^8. It is clear that 8 cannot be written as $3^i + 3^j$ for some nonnegative integers i and j. If the coefficient of the fourth term in (2.2) is non-zero, then $\widehat{\mathfrak{D}}_k$ is not a DO polynomial. Now consider the case where the coefficient of the fourth term is zero. Note that the coefficient of the last term in (2.3), which contains the monomial X^k, is always non-zero. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $k = 3^i + 1$. Clearly, $i \neq 0$, otherwise $k = 2$, a contradiction. If $i > 0$, then $k \equiv 1 \pmod 3$. Now consider the second last term in (2.3), which contains the monomial X^{k-2}. Clearly, the coefficient is non-zero as $\gcd(k,3) = 1$. If $\widehat{\mathfrak{D}}_k$ is a DO polynomial and $k \equiv 1 \pmod 3$, then $k - 2 = 3^j + 1$. If $i = 0$ then $k = 4$, which is a contradiction since $k > 4$. If $i > 0$, then $k = 3^i + 3$. This contradicts the assumption that $\gcd(k,3) = 1$. Thus $\widehat{\mathfrak{D}}_k$ is not a DO polynomial in this case.

Case 2. Let $k \equiv 3 \pmod p$. In this case, if $p = 3$, then $k \equiv 0 \pmod 3$, which is a contradiction as $\gcd(k,p) = 1$. Therefore, we shall always consider $p > 3$. Notice that the coefficient of the last term in (2.3), which contains the monomial $X^{\frac{kd}{2}}$, is non-zero. Thus, if $\widehat{\mathfrak{D}}_k$ is a DO polynomial, then $\frac{kd}{2} = p^\beta(p^\alpha+1)$ and $d = p^i + 1$. Since $\gcd(k,p) = 1$ and $\gcd(d,p) = 1$, $\beta = 0$. Hence, the first equation reduces to $kd = 2p^\alpha + 2$. Combining

these two equations, we get $kp^i + k = 2p^\alpha + 2$. If $i = 0$, then $k = p^\alpha + 1$, which implies $k \equiv 2 \pmod{p}$ or $k \equiv 1 \pmod{p}$ depending on whether $\alpha = 0$ or $\alpha > 0$, respectively, a contradiction. If $i > 0$, then $\alpha > 0$, otherwise $k(p^i + 1) = 4$, which is a contradiction as $p > 3$. Therefore $k \equiv 2 \pmod{p}$, a contradiction. This completes the proof. □

2.3 DO Polynomials from RDPs of the Second Kind

Recall that $D_{k,1}(a, X^d) - D_{k,1}(a, 0)$ is denoted by $\widehat{\mathfrak{E}}_k$, where

$$\widehat{\mathfrak{E}}_k = (1-k)a^{k-2}X^d + \frac{(k-2)(k-3)}{2!}a^{k-4}X^{2d} - \frac{(k-3)(k-4)(k-5)}{3!}a^{k-6}X^{3d} + \cdots . \tag{2.4}$$

The following theorems give necessary and sufficient conditions for RDPs of the second kind to be DO polynomials for $p = 3$ and $p \geq 5$, respectively.

Theorem 3. *Let q be a power of the odd prime $p = 3$ and $a \in \mathbb{F}_q^*$. The polynomial $\widehat{\mathfrak{E}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$k = 2, 3, 5, 6$ and $d = p^t(p^\alpha + 1)$, where $\alpha,\ t \geq 0$.*

(ii) *$k = 4$ and $d = p^t(p^\alpha + 1)/2$, where $\alpha,\ t \geq 0$.*

(iii) *$k = 7, 10, 13, 19$ and $d = 2p^t$, where $t \geq 0$.*

(iv) *$k = 15$ and $d = 4p^t$, where $t \geq 0$.*

Proof. The sufficient part of the theorem is straightforward, therefore, we only prove the necessary part. If the polynomials $\widehat{\mathfrak{E}}_2 = -X^d, \widehat{\mathfrak{E}}_3 = -2aX^d$ and $\widehat{\mathfrak{E}}_5 = 2a^3X^d$ are DO polynomial, then d is of the form $p^\alpha + 1$. Similarly, the polynomial $\widehat{\mathfrak{E}}_4 = X^{2d}$ is a DO polynomial only if d is of the form $(p^\alpha + 1)/2$. If the polynomial $\widehat{\mathfrak{E}}_6 = a^4X^d + 2X^{3d}$ is a DO polynomial, then $d = 3^\alpha + 1$ and $3d = 3^t(3^\beta + 1)$. Since $3^t \mid 3$, $t = 1$. Therefore, $\widehat{\mathfrak{E}}_6$ is a DO polynomial only if d is of the form $p^\alpha + 1$. The polynomial $\widehat{\mathfrak{E}}_7 = a^3X^{2d} + 2aX^{3d}$ is a DO polynomial only if $2d = 3^\alpha + 1$ and $3d = 3^t(3^\beta + 1)$. Since $3^t \mid 3$, $t = 1$. Combining these two equations, we obtain $\beta = 0$, $\alpha = 1$ and $d = 2$. For $k \geq 8$, we shall treat all possible cases depending on the value of k modulo 9.

Case 1. Let $k \equiv 2, 8 \pmod 9$. In this case, $k \equiv 2 \pmod 3$, therefore, $k \not\equiv 1 \pmod 3$ and hence the coefficient of X^d in (2.4), is non-zero. Now, consider the fourth term

$$\frac{(k-4)(k-5)(k-6)(k-7)}{4!}a^{k-8}X^{4d}. \tag{2.5}$$

It is clear that $3 \nmid (k-4)$, $3 \nmid (k-6)$ and $3 \nmid (k-7)$. Also, since $k \equiv 2, 8 \pmod 9$, $k \not\equiv 5 \pmod 9$, and hence the highest exponent of 3 which divides the numerator of the coefficient of fourth term is 1. By Lemma 2.1.5, the highest exponent of 3 which divides 4! is 1. Therefore, coefficient of the fourth term is non-zero and $\widehat{\mathfrak{E}}_k$ is not a DO polynomial by Lemma 2.1.4.

Case 2. Let $k \equiv 0, 3 \pmod 9$. In this case, $k \equiv 0 \pmod 3$ and hence, the coefficient of X^d in (2.4) is non-zero. Now consider the fourth term as given in (2.5) again. Following similar arguments as in the Case 1 above, it is easy to see that the coefficient of the fourth term is nonzero and hence $\widehat{\mathfrak{E}}_k$ is not a DO polynomial by Lemma 2.1.4.

Case 3. Let $k \equiv 1 \pmod 9$. In this case, if the polynomial $\widehat{\mathfrak{E}}_{10} = a^6X^{2d} + a^4X^{3d} + 2X^{5d}$ is a DO polynomial, then $2d = 3^\alpha + 1$, $3d = 3^t(3^\beta + 1)$ and $5d = 3^\gamma + 1$. Since $3^t \mid 3$, $t = 1$. Combining the first two equations, we obtain $\beta = 0$, $\alpha = 1$ and $d = 2$. Now, putting these values in third equation, we have $3^\gamma = 9$ and $\gamma = 2$. Similarly, if the polynomial $\widehat{\mathfrak{E}}_{19} = a^{15}X^{2d} + a^{13}X^{3d} + 2a^9X^{5d} + 2aX^{9d}$ is a DO polynomial, then $2d = 3^\alpha + 1$, $3d = 3^t(3^\beta + 1)$, $5d = 3^\gamma + 1$ and $9d = 3^s(3^\delta + 1)$. Since $3^t \mid 3$ and $3^s \mid 9$, we have $t = 1$ and $s = 2$. Combining first, second and fourth equation, we obtain $\beta = 0$, $\alpha = 1$ and $d = 2$. Now, putting these values in third equation, we have $3^\gamma = 9$ and $\gamma = 2$. For $k \geq 28$, since $k \equiv 1 \pmod 3$, we have $k \not\equiv 0, 2 \pmod 3$, and hence the coefficient of X^{2d} is non-zero. Now, consider the 11th term

$$\frac{(k-11)(k-12)(k-13)\cdots(k-19)(k-20)(k-21)}{11!}a^{k-22}(-X^d)^{11}. \tag{2.6}$$

By Lemma 2.1.5, the highest exponent of 3 that divides 11! is 4. In the numerator of the coefficient of 11th term, $(k-13), (k-16), (k-19) \equiv 0 \pmod 3$ and $(k-13), (k-16) \not\equiv 0 \pmod 9$. Now, if $k \not\equiv 19 \pmod{27}$, then the highest exponent of 3 which divides the numerator is 4. Hence the coefficient of X^{11d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial then $2d = 3^\alpha + 1$ and $11d = 3^\beta + 1$. Combining these equations, we have $11 \cdot 3^\alpha + 9 = 2 \cdot 3^\beta$,

which forces $\alpha = 2$ and $3^\beta = 54$, a contradiction. Therefore, $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $k \equiv 19 \pmod{27}$, we have $k \geq 46$. In this case, consider the 20th term

$$\frac{(k-20)(k-21)(k-22)\cdots(k-37)(k-38)(k-39)}{20!}a^{k-40}X^{20d}. \tag{2.7}$$

The arguments of Case 1 can be invoked here to shows that the coefficient of X^{20d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $2d = 3^\alpha + 1$ and $20d = 3^\beta + 1$. Combining these equations, we have $10 \cdot 3^\alpha + 9 = 3^\beta$, which forces $\alpha = 2$ and $3^\beta = 99$, a contradiction. Therefore, $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case.

Case 4. Let $k \equiv 4 \pmod{9}$. In this case, if the polynomial $\widehat{\mathfrak{E}}_{13} = a^9X^{2d} + a^3X^{5d} + aX^{6d}$ is a DO polynomial, then $2d = 3^\alpha + 1$, $5d = 3^\beta + 1$ and $6d = 3^t(3^\gamma + 1)$. Since $3^t \mid 6$, $t = 1$. Combining these equations, we obtain $\alpha = 1$, $\beta = 2$ and $d = 2$. Now, for $k \geq 22$, since $k \equiv 1 \pmod{3}$, we have $k \not\equiv 0, 2 \pmod{3}$, and hence the coefficient of X^{2d} in (2.4) is non-zero. Now, consider the 11th term as given in (2.6). By Lemma 2.1.5, the highest exponent of 3 that divides 11! is 4. In the numerator of the coefficient of 11th term, $(k-13), (k-16), (k-19) \equiv 0 \pmod{3}$ and $(k-16), (k-19) \not\equiv 0 \pmod{9}$. Now if $k \not\equiv 13 \pmod{27}$, then the highest exponent of 3 which divides the numerator is 4. Hence the coefficient of X^{11d} is non-zero. Thus if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $2d = 3^\alpha + 1$ and $11d = 3^\beta + 1$. Combining these two equations, we have $11 \cdot 3^\alpha + 9 = 2 \cdot 3^\beta$, which forces $\alpha = 2$ and $3^\beta = 54$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $k \equiv 13 \pmod{27}$, $k \geq 22$ is equivalent to $k \geq 40$. In this case, consider the 20th term as given in (2.7). By similar arguments as in the Case 1 one may prove that the coefficient of X^{20d} is non-zero. Therefore, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $2d = 3^\alpha + 1$ and $20d = 3^\beta + 1$. Combining these equations, we have $10 \cdot 3^\alpha + 9 = 3^\beta$, which forces $\alpha = 2$ and $3^\beta = 99$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case.

Case 5. Let $k \equiv 5 \pmod{9}$. In this case, if the polynomial $\widehat{\mathfrak{E}}_{14} = 2a^{10}X^{2d} + a^2X^{6d} + X^{7d}$ is a DO polynomial, then $d = 3^\alpha + 1$, $6d = 3^t(3^\beta + 1)$ and $7d = 3^\gamma + 1$. Since $3^t \mid 6$, $t = 1$. Combining the first two equations, we obtain $\alpha = 0$, $\beta = 1$ and $d = 2$. Now putting these values in third equation, we have $3^\gamma = 13$, a contradiction. Therefore, $\widehat{\mathfrak{E}}_{14}$ is not a DO polynomial. Now, for $k \geq 23$, consider the 10th term

$$\frac{(k-10)(k-11)(k-12)(k-13)\cdots(k-17)(k-18)(k-19)}{10!}a^{k-20}X^{10d}. \tag{2.8}$$

By Lemma 2.1.5, the highest exponent of 3 that divides 10! is 4. In the numerator of the coefficient of 10th term, $(k-11),(k-14),(k-17) \equiv 0 \pmod 3$ and $(k-11),(k-17) \not\equiv 0 \pmod 9$. Now if $k \not\equiv 14 \pmod{27}$, then the highest exponent of 3 which divides the numerator is 4. Hence the coefficient of X^{10d} is non-zero. Thus if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = 3^\alpha + 1$ and $10d = 3^\beta + 1$. Combining these equations, we get $10 \cdot 3^\alpha + 9 = 3^\beta$, which forces $\alpha = 2$ and $3^\beta = 99$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $k \equiv 14 \pmod{27}$, $k \geq 23$ is equivalent to $k \geq 41$. Now, consider the 16th term

$$\frac{(k-16)(k-17)(k-18)\cdots(k-29)(k-30)(k-31)}{16!}a^{k-32}X^{16d}. \tag{2.9}$$

By way of similar arguments as done in Case 1, the coefficient of X^{16d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = 3^\alpha + 1$ and $16d = 3^\beta + 1$. Combining these equations, we get $16 \cdot 3^\alpha + 15 = 3^\beta$, which forces $\alpha = 1$ and $3^\beta = 63$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case.

Case 6. Let $k \equiv 6 \pmod 9$. In this case, if the polynomial $\widehat{\mathfrak{E}}_{15} = a^{13}X^d + 2a^9X^{3d} + aX^{7d}$ is a DO polynomial, then $d = 3^\alpha + 1$, $3d = 3^t(3^\beta + 1)$ and $7d = 3^\gamma + 1$. Since $3^t \mid 3$, $t = 1$. Combining these equations, we obtain $\alpha = 1$, $\gamma = 3$ and $d = 4$. Now, for $k \geq 24$, consider the 10th term as given in (2.8). One may follow the similar arguments of Case 5 above to shows that if $k \not\equiv 15 \pmod{27}$, the coefficient of X^{10d} is non-zero. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $k \equiv 15 \pmod{27}$, $k \geq 24$ is equivalent to $k \geq 42$. In this case, consider the 16th term as given in (2.9). Similar arguments as in the Case 1 show that the coefficient of X^{16d} is non-zero. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case.

Case 7. Let $k \equiv 7 \pmod 9$. In this case $k \geq 8$ is equivalent to $k \geq 16$. Also, since $k \equiv 1 \pmod 3$, we have $k \not\equiv 0$ or $2 \pmod 3$ and hence the coefficient of X^{2d} in (2.4) is non-zero. Now consider the 8th term, which is given by

$$\frac{(k-8)(k-9)(k-10)(k-11)(k-12)(k-13)(k-14)(k-15)}{8!}a^{k-16}X^{8d}. \tag{2.10}$$

By following similar arguments as in the Case 1, it is not difficult to prove that the coefficient of X^{8d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $2d = 3^\alpha + 1$ and

$8d = 3^\beta + 1$. Combining these equations, we have $4 \cdot 3^\alpha + 3 = 3^\beta$, which forces $\alpha = 1$ and $3^\beta = 15$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. This completes the proof. □

Theorem 4. *Let q be a power of an odd prime $p \geq 5$ and $a \in \mathbb{F}_q^*$. The polynomial $\widehat{\mathfrak{E}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$k = 2, 3$ and $d = p^n(p^\alpha + 1)$, where $\alpha,\ n \geq 0$.*

(ii) *$k = 7$, $p = 5$ and $d = 2p^n$, where $n \geq 0$.*

Proof. It is enough to prove the necessary part. If the polynomials $\widehat{\mathfrak{E}}_2 = -X^d$ and $\widehat{\mathfrak{E}}_3 = -2aX^d$ are DO polynomial, then d is of the form $p^\alpha + 1$. By Lemma 2.1.1, the polynomials $\widehat{\mathfrak{E}}_4 = -3a^2X^d + X^{2d}$ and $\widehat{\mathfrak{E}}_5 = -4a^3X^d + 3aX^{2d}$ are not DO polynomials. The polynomial $\widehat{\mathfrak{E}}_6 = -5a^4X^d + 6a^2X^{2d} - X^{3d}$ is a DO polynomial only if $2d = p^\alpha + 1$ and $3d = p^\beta + 1$. Combining these equations, we get $3p^\alpha + 1 = 2p^\beta$, which forces $\alpha = 0$, $p^\beta = 2$, a contradiction. Therefore, $\widehat{\mathfrak{E}}_6$ is not a DO polynomial. For the polynomial $\widehat{\mathfrak{E}}_7 = -6a^5X^d + 10a^3X^{2d} - 4aX^{3d}$, we consider two cases, namely, $p = 5$ and $p > 5$. For $p = 5$, if $\widehat{\mathfrak{E}}_7 = 4a^5X^d + X^{3d}$ is a DO polynomial, then $d = 5^\alpha + 1$ and $3d = 5^\beta + 1$. Combining these equations, we have $3 \cdot 5^\alpha + 2 = 5^\beta$, which forces $\alpha = 0$, $\beta = 1$ and $d = 2$. For $p > 5$, $\widehat{\mathfrak{E}}_7 = -6a^5X^d + 10a^3X^{2d} - 4X^{3d}$. Since the coefficients of X^d and X^{2d} are non-zero, Lemma 2.1.1 confirms that $\widehat{\mathfrak{E}}_7$ is not a DO polynomial. For $k \geq 8$, we shall consider four cases, namely, $k \not\equiv 1, 2, 3 \pmod p$, $k \equiv 1 \pmod p$, $k \equiv 2 \pmod p$ and $k \equiv 3 \pmod p$, respectively.

Case 1. Let $k \not\equiv 1, 2, 3 \pmod p$. In this case, the coefficients of X^d and X^{2d} in (2.4) are non-zero, therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial by Lemma 2.1.1.

Case 2. Let $k \equiv 1 \pmod p$. In this case, we have $(k-2), (k-3), (k-4), (k-5) \not\equiv 0 \pmod p$. Therefore, the coefficients of X^{2d} and X^{3d} in (2.4) are non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $2d = p^\alpha + 1$ and $3d = p^\beta + 1$. Combining these equations, we have $3p^\alpha + 1 = 2p^\beta$, which forces $\alpha = 0$ and $p^\beta = 2$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial.

Case 3. Let $k \equiv 2 \pmod p$. In this case, the coefficient of the first term in (2.4), which contains the monomial X^d, is non-zero. Now we consider two cases, namely, $p = 5$ and $p > 5$. In the case $p = 5$, $k \geq 8$ is equivalent to $k \geq 12$. We now show that if $k \not\equiv 7$

(mod 25), then the sixth term exists whose coefficient is given by

$$\frac{(k-6)(k-7)(k-8)(k-9)(k-10)(k-11)}{6!}a^{k-12}.$$

Since $k \equiv 2 \pmod 5$, we have $(k-6),(k-8),(k-9),(k-10),(k-11) \not\equiv 0 \pmod 5$. Also, if $k \not\equiv 7 \pmod{25}$, then the highest exponent of 5 which divides the numerator is 1. By Lemma 2.1.5, the highest exponent of 5 that divides 6! is 1. Therefore the coefficient of X^{6d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = 5^\alpha + 1$ and $6d = 5^\beta + 1$. Combining these equations, we have $6 \cdot 5^\alpha + 5 = 5^\beta$, which forces $\alpha = 1$ and $5^\beta = 35$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. Now if $k \equiv 7 \pmod{25}$, then the condition $k \geq 12$ is equivalent to $k \geq 32$. In this case, using the similar arguments, we can show that the coefficient of X^{8d} is non-zero. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = 5^\alpha + 1$ and $8d = 5^\beta + 1$. Combining these equations, we have $8 \cdot 5^\alpha + 7 = 5^\beta$, which forces $\alpha = 0$ and $5^\beta = 15$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $p > 5$, since $k \equiv 2 \pmod p$, we have $k \not\equiv 1, 3, 4, 5 \pmod p$. Hence the coefficients of X^d and X^{3d} in (2.4) are non-zero, therefore $\widehat{\mathfrak{E}}_k$ is not DO polynomial by Lemma 2.1.2.

Case 4. Let $k \equiv 3 \pmod p$. In this case, the first term $(1-k)X^d$ in (2.4) does not vanish. Now we consider two cases, namely, $p = 5$ and $p > 5$. In the case $p = 5$, since $k \equiv 3 \pmod 5$, we have $k \not\equiv 0, 1, 2, 4 \pmod 5$, and hence the fourth term as given in (2.5) does not vanish. Therefore, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = 5^i + 1$ and $4d = 5^j + 1$. Combining these equations, we have $4 \cdot 5^i + 3 = 5^j$, which forces $i = 0$ and $5^j = 7$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. In the case $p > 5$, since $k \equiv 3 \pmod p$, we have $(k-1),(k-4),(k-5),(k-6),(k-7),(k-8),(k-9) \not\equiv 0 \pmod p$. Therefore, the fourth term as given in (2.5) and the fifth term whose coefficient is given by

$$\frac{(k-5)(k-6)(k-7)(k-8)(k-9)}{5!}a^{k-10},$$

do not vanish. Thus, if $\widehat{\mathfrak{E}}_k$ is a DO polynomial, then $d = p^\alpha + 1$, $4d = p^\beta + 1$ and $5d = p^\gamma + 1$. Combining the first two equations, we have $4p^\alpha + 3 = p^\beta$, which forces $\alpha = 0$, $\beta = 1$, $p = 7$ and $d = 2$. Now putting these values in third equation, we have $7^\gamma = 9$, a contradiction. Therefore $\widehat{\mathfrak{E}}_k$ is not a DO polynomial in this case. This completes the proof. □

One may recall from [58, Theorem 3.1] that RDPs of the second kind and RDPs of the third kind admit the following relationship

$$D_{k,2}(a, X) = aD_{k-1,1}(a, X).$$

Thus, it is obvious that $\widehat{\mathfrak{F}}_k$ is a DO polynomial whenever $\widehat{\mathfrak{E}}_{k-1}$ is a DO polynomial. Consequently, the classification of DO polynomials from RDPs of the third kind $\widehat{\mathfrak{F}}_k$ follows immediately. In view of this, we shall consider RDPs of the fourth kind in the next section.

2.4 DO Polynomials from RDPs of the Fourth Kind

Recall that $D_{k,3}(a, X^d) - D_{k,3}(a, 0)$ is denoted by $\widehat{\mathfrak{G}}_k$, where

$$\widehat{\mathfrak{G}}_k = (3-k)a^{k-2}X^d + \frac{(k-3)(k-6)}{2}a^{k-4}X^{2d} - \frac{(k-4)(k-5)(k-9)}{3!}a^{k-6}X^{3d} + \cdots . \tag{2.11}$$

Also, from (1.3), it is easy to see that $\widehat{\mathfrak{G}}_k = \widehat{\mathfrak{D}}_k \pmod 3$. Therefore, for $p = 3$, $\widehat{\mathfrak{G}}_k$ is a DO polynomial whenever $\widehat{\mathfrak{D}}_k$ is a DO polynomial and the classification of DO polynomials from $\widehat{\mathfrak{D}}_k$ has already been discussed in Section 2.2. Therefore, throughout this section, we consider $p \geq 5$. The following theorem gives a complete classification of DO polynomials derived from $\widehat{\mathfrak{G}}_k$.

Theorem 5. *Let q be a power of an odd prime $p \geq 5$ and $a \in \mathbb{F}_q^*$. The polynomial $\widehat{\mathfrak{G}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$k = 2$ and $d = p^t(p^\alpha + 1)$, where $\alpha,\ t \geq 0$.*

(ii) *$k = 6, 11$, $p = 5$ and $d = 2p^t$, where $t \geq 0$.*

Proof. It is enough to prove only the necessary part. If the polynomial $\widehat{\mathfrak{G}}_2 = X^d$ is a DO polynomial, then $d = p^\alpha + 1$. The polynomial $\widehat{\mathfrak{G}}_3$ is the zero polynomial and hence it is not a DO polynomial. The polynomials $\widehat{\mathfrak{G}}_4 = -a^2X^d - X^{2d}$, $\widehat{\mathfrak{G}}_5 = -2a^3X^d - aX^{2d}$ and $\widehat{\mathfrak{G}}_7 = -4a^5X^d + 2a^3X^{2d} + 2aX^{3d}$ are not DO polynomials by Lemma 2.1.1. In the case of the polynomial $\widehat{\mathfrak{G}}_6 = -3a^4X^d + X^{3d}$, we consider two cases, namely, $p = 5$ and $p > 5$. In the case $p = 5$, if $\widehat{\mathfrak{G}}_6$ is a DO polynomial, then $d = 5^i + 1$ and $3d = 5^j + 1$. Combining

these equations, we have $3 \cdot 5^i + 2 = 5^j$, which is true if and only if $i = 0$, $j = 1$ and $d = 2$. When $p > 5$, $\widehat{\mathfrak{G}}_6$ is not a DO polynomial by Lemma 2.1.2. For $k \geq 8$, we consider two cases, namely, $p = 5$ and $p > 5$.

Case 1. Let $p > 5$. Note that when $k \not\equiv 3, 6 \pmod{p}$, the coefficients of X^d and X^{2d} in $\widehat{\mathfrak{G}}_k$ are non-zero. Therefore, $\widehat{\mathfrak{G}}_k$ is not a DO polynomial by Lemma 2.1.1. In the case $k \equiv 3 \pmod{p}$, the coefficient of X^{3d} is non-zero and also, the coefficient of X^{4d} in $\widehat{\mathfrak{G}}_k$, given by

$$\frac{(k-5)(k-6)(k-7)(k-12)}{4!}a^{k-8}$$

is non-zero. Therefore, $\widehat{\mathfrak{G}}_k$ is not a DO polynomial by Lemma 2.1.3. When $k \equiv 6 \pmod{p}$, the coefficients of X^d and X^{3d} in $\widehat{\mathfrak{G}}_k$ are non-zero, therefore, $\widehat{\mathfrak{G}}_k$ is not a DO polynomial by Lemma 2.1.2.

Case 2. Let $p = 5$. Notice that when $k \not\equiv 1, 3 \pmod 5$, the coefficients of X^d and X^{2d} in $\widehat{\mathfrak{G}}_k$ are non-zero, therefore $\widehat{\mathfrak{G}}_k$ is not a DO polynomial by Lemma 2.1.1. In the case $k \equiv 3 \pmod 5$, the coefficients of X^{3d} and X^{4d} in $\widehat{\mathfrak{G}}_k$ are non-zero, therefore $\widehat{\mathfrak{G}}_k$ is not a DO polynomial by Lemma 2.1.3. For $k \equiv 1 \pmod 5$, if the polynomial $\widehat{\mathfrak{G}}_{11} = 2a^9X^d + a^5X^{3d} + 4aX^{5d}$ is a DO polynomial, then $d = 5^\alpha + 1$, $3d = 5^\beta + 1$ and $5d = 5^t(5^\gamma + 1)$. Since $5^t \mid 5$, $t = 1$. Thus, by combining these equations, we obtain $\alpha = 0$, $\beta = 1$ and $d = 2$. For $k \geq 16$, since $k \equiv 1 \pmod 5$, we have $k \not\equiv 0, 2, 3, 4 \pmod 5$ and hence the coefficient of X^{3d} in $\widehat{\mathfrak{G}}_k$ is non-zero. Now consider the 6th term whose coefficient is given by

$$\frac{(k-7)(k-8)(k-9)(k-10)(k-11)(k-18)}{6!}a^{k-12}.$$

By Lemma 2.1.5, the highest exponent of 5 which divides 6! is 1. Also, if $k \not\equiv 11 \pmod{25}$, then highest exponent of 5 that divides the numerator of coefficient of X^{6d} is 1, hence the coefficient of X^{6d} is non-zero. Thus, if $\widehat{\mathfrak{G}}_k$ is a DO polynomial, then $3d = 5^\alpha + 1$ and $6d = 5^\beta + 1$. Combining these equations, we get $2 \cdot 5^\alpha + 1 = 5^\beta$, which forces $\alpha = 0$ and $5^\beta = 3$, a contradiction. Thus $\widehat{\mathfrak{G}}_k$ is not a DO polynomial in this case. In the case $k \equiv 11 \pmod{25}$, consider the 11th term whose coefficient is given by

$$\frac{(k-12)(k-13)\cdots(k-19)(k-20)(k-21)(k-33)}{11!}a^{k-22}.$$

It is easy to verify that the coefficient of X^{11d} is non-zero. Thus, if $\widehat{\mathfrak{G}}_k$ is a DO polynomial, then $3d = 5^\alpha + 1$ and $11d = 5^\beta + 1$. Combining these equations, we have $11 \cdot 5^\alpha + 8 = 3 \cdot 5^\beta$, which forces $\alpha = 0$ and $3 \cdot 5^\beta = 19$, a contradiction. Thus $\widehat{\mathfrak{G}}_k$ is not a DO polynomial in this case. □

2.5 DO Polynomials from RDPs of the Fifth Kind

Here we consider RDPs of the fifth kind. Recall that $D_{k,4}(a, X^d) - D_{k,4}(a, 0)$ is denoted by $\widehat{\mathfrak{H}}_k$, where

$$\widehat{\mathfrak{H}}_k = (4-k)a^{k-2}X^d + \frac{(k-3)(k-8)}{2}a^{k-4}X^{2d} - \frac{(k-4)(k-5)(k-12)}{3!}a^{k-6}X^{3d} + \cdots . \tag{2.12}$$

It is easy to see from (1.3) that $\widehat{\mathfrak{H}}_k = \widehat{\mathfrak{E}}_k \pmod 3$, thus for $p = 3$, $\widehat{\mathfrak{H}}_k$ is a DO polynomial whenever $\widehat{\mathfrak{E}}_k$ is a DO polynomial. Thus, throughout this section, we take $p \geq 5$.

Theorem 6. *Let q be a power of an odd prime $p \geq 5$ and $a \in \mathbb{F}_q^*$. The polynomial $\widehat{\mathfrak{H}}_k$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$k = 2, 3$ and $d = p^t(p^\alpha + 1)$, where $\alpha,\ t \geq 0$.*

(ii) *$k = 4$ and $d = p^t(p^\alpha + 1)/2$, where $\alpha,\ t \geq 0$.*

Proof. The sufficiency of the theorem is straightforward. It only remains to show the necessity. If the polynomials $\widehat{\mathfrak{H}}_2 = 2X^d$ and $\widehat{\mathfrak{H}}_3 = aX^d$ are DO polynomials, then $d = p^\alpha + 1$. Similarly, if the polynomial $\widehat{\mathfrak{H}}_4 = -2X^{2d}$ is a DO polynomial, then $d = (p^\alpha + 1)/2$. In the case of polynomials $\widehat{\mathfrak{H}}_5 = -a^3X^d - 3aX^{2d}$, $\widehat{\mathfrak{H}}_6 = -2a^4X^d - 3a^2X^{2d} + 2X^{3d}$ and $\widehat{\mathfrak{H}}_7 = -3a^5X^d - 2a^3X^{2d} + aX^{3d}$, the coefficients of X^d and X^{2d} are non-zero. Therefore, $\widehat{\mathfrak{H}}_5$, $\widehat{\mathfrak{H}}_6$ and $\widehat{\mathfrak{H}}_7$ are not DO polynomials by Lemma 2.1.1. The polynomial $\widehat{\mathfrak{H}}_8 = -4a^6X^d + 8a^2X^{3d} - 2X^{4d}$ is not a DO polynomial by Lemma 2.1.3. If the polynomial $\widehat{\mathfrak{H}}_9 = -5a^7X^d + 3a^5X^{2d} + 10a^3X^{3d} - 7aX^{4d}$ is a DO polynomial, then $2d = 5^\alpha + 1$ and $4d = 5^\beta + 1$. Combining these equations, we get $2 \cdot 5^\alpha + 1 = 5^\beta$, which forces $\alpha = 0$, $5^\beta = 3$, a contradiction. Thus $\widehat{\mathfrak{H}}_9$ is not a DO polynomial. For $k \geq 10$, we consider two cases, $p = 5$ and $p > 5$.

Case 1. Let $p = 5$. Notice that when $k \not\equiv 3, 4 \pmod 5$, the coefficients of X^d and X^{2d} in $\widehat{\mathfrak{H}}_k$ are non-zero, therefore, $\widehat{\mathfrak{H}}_k$ is not a DO polynomial by Lemma 2.1.1. In the case $k \equiv 3 \pmod 5$, the coefficients of X^d is clearly non-zero and also, the coefficient of X^{4d} in $\widehat{\mathfrak{H}}_k$ given by

$$\frac{(k-4)(k-5)(k-6)(k-7)}{4!}a^{k-8}$$

is non-zero. Thus, if $\widehat{\mathfrak{H}}_k$ is a DO polynomial, then $d = 5^\alpha + 1$ and $4d = 5^\beta + 1$. Combining these equations, we have $4 \cdot 5^\alpha + 3 = 5^\beta$, which forces $\alpha = 0$ and $5^\beta = 7$, a contradiction. Thus $\widehat{\mathfrak{H}}_k$ is not a DO polynomial in this case. When $k \equiv 4 \pmod 5$, the coefficient of X^{2d} in $\widehat{\mathfrak{H}}_k$ is non-zero. Also, if $k \not\equiv 9 \pmod{25}$, the coefficient of X^{5d} in $\widehat{\mathfrak{H}}_k$ given by

$$\frac{(k-6)(k-7)(k-8)(k-9)(k-20)}{5!}a^{k-10}$$

is non-zero. Thus, if $\widehat{\mathfrak{H}}_k$ is a DO polynomial, then $2d = 5^\alpha + 1$ and $5d = 5^t(5^\beta + 1)$. Since $5^t \mid 5$, $t = 1$ and hence, the second equation reduces to $d = 5^\beta + 1$. Combining these equations, we have $2 \cdot 5^\beta + 1 = 5^\alpha$, which forces $\beta = 0$ and $5^\alpha = 3$, a contradiction. Thus $\widehat{\mathfrak{H}}_k$ is not a DO polynomial. In the case $k \equiv 9 \pmod{25}$, the condition $k \geq 10$ is equivalent to $k \geq 34$. Now consider the 9th term whose coefficient is given by

$$\frac{(k-10)(k-11)(k-12)\cdots(k-16)(k-17)(k-36)}{9!}a^{k-18}.$$

Since $k \equiv 9 \pmod{25}$, we have $k \not\equiv 14 \pmod{25}$. Hence the highest exponent of 5, which divides the numerator is 1. By Lemma 2.1.5, highest exponent of 5, which divides 9! is 1. Therefore, the coefficient of X^{9d} is non-zero. Thus, if $\widehat{\mathfrak{H}}_k$ is a DO polynomial, then $2d = 5^\alpha + 1$ and $9d = 5^\beta + 1$. Combining these two equations, we have $9 \cdot 5^\alpha + 7 = 2 \cdot 5^\beta$, which forces $\alpha = 0$ and $5^\beta = 8$, a contradiction. Thus $\widehat{\mathfrak{H}}_k$ is not a DO polynomial.

Case 2. Let $p > 5$. Notice that when $k \not\equiv 3, 4, 8 \pmod p$, the coefficients of X^d and X^{2d} in $\widehat{\mathfrak{H}}_k$ are non-zero, therefore $\widehat{\mathfrak{H}}_k$ is not a DO polynomial by Lemma 2.1.1. In the case $k \equiv 3, 8 \pmod p$, the coefficients of X^d and X^{3d} in $\widehat{\mathfrak{H}}_k$ are non-zero, therefore $\widehat{\mathfrak{H}}_k$ is not a DO polynomial by Lemma 2.1.2. When $k \equiv 4 \pmod p$, the coefficients of X^{2d} and X^{4d} in $\widehat{\mathfrak{H}}_k$ are non-zero. Thus, if $\widehat{\mathfrak{H}}_k$ is a DO polynomial, $2d = p^\alpha + 1$ and $4d = p^\beta + 1$. Combining these equations, we have $2 \cdot p^\alpha + 1 = p^\beta$, which forces $\alpha = 0$ and $p^\beta = 3$, a contradiction. Thus, $\widehat{\mathfrak{H}}_k$ is not a DO polynomial. This completes the proof. □

2.6 The Case $m \geq 5$

For $m \geq 5$, we shall classify DO polynomials from the polynomial $\widehat{\mathfrak{D}}_{k,m}$, where

$$\begin{aligned}\widehat{\mathfrak{D}}_{k,m} = (m-k)a^{k-2}X^d + \frac{(k-3)(k-2m)}{2}a^{k-4}X^{2d} \\ - \frac{(k-4)(k-5)(k-3m)}{3!}a^{k-6}X^{3d} + \cdots .\end{aligned} \tag{2.13}$$

From (1.3), it is straightforward to see that for $p = 3$, $\widehat{\mathfrak{D}}_{k,m} = \widehat{\mathfrak{D}}_k, \widehat{\mathfrak{E}}_k,$ and $\widehat{\mathfrak{F}}_k$, whenever $m \equiv 0, 1$ and $2 \pmod 3$, respectively. Similarly, for $p \geq 5$, $\widehat{\mathfrak{D}}_{k,m} = \widehat{\mathfrak{D}}_k, \widehat{\mathfrak{E}}_k, \widehat{\mathfrak{F}}_k, \widehat{\mathfrak{G}}_k$ and $\widehat{\mathfrak{H}}_k$, whenever $m \equiv 0, 1, 2, 3$ and $4 \pmod p$, respectively. Thus the only cases that remain to be considered are $p > 5$ and $m \not\equiv 0, 1, 2, 3, 4 \pmod p$ for which we have the following theorem.

Theorem 7. *Let q be a power of an odd prime $p > 5$ and $a \in \mathbb{F}_q^*$. The polynomial $\widehat{\mathfrak{D}}_{k,m}$ where $m \not\equiv 0, 1, 2, 3, 4 \pmod p$ is a DO polynomial over $\mathbb{F}_q$ if and only if one of the following holds.*

(i) *$k = 2, 3$ and $d = p^t(p^\alpha + 1)$, where $\alpha,\ t \geq 0$.*

(ii) *$k = 5$, $m \equiv 5 \pmod p$ and $d = p^t(p^\alpha + 1)/2$, where $\alpha,\ t \geq 0$.*

(iii) *$k = 5$, $2m \equiv 5 \pmod p$ and $d = p^t(p^\alpha + 1)$, where $\alpha,\ t \geq 0$.*

Proof. Only sufficiency of the theorem is required to be proved. If the polynomials $\widehat{\mathfrak{D}}_{2,m} = (m-2)X^d$ and $\widehat{\mathfrak{D}}_{3,m} = (m-3)aX^d$ are DO polynomials, then d is of the form $p^\alpha + 1$. The polynomial $\widehat{\mathfrak{D}}_{4,m} = (m-4)a^2X^d + (2-m)X^{2d}$ is not a DO polynomial by Lemma 2.1.1. In the case of the polynomial $\widehat{\mathfrak{D}}_{5,m} = (m-5)a^3X^d + (5-2m)aX^{2d}$, we consider three cases, namely, $m \equiv 5 \pmod p$, $2m \equiv 5 \pmod p$ and $m, 2m \not\equiv 5 \pmod p$. In the case $m \equiv 5 \pmod p$, if $\widehat{\mathfrak{D}}_{5,m} = -5aX^{2d}$ is a DO polynomial, then d is of the form $(p^\alpha + 1)/2$. When $2m \equiv 5 \pmod p$ and if $\widehat{\mathfrak{D}}_{5,m} = (m-5)a^3X^d$ is a DO polynomial, then d is of the form $p^\alpha + 1$. In the case $m, 2m \not\equiv 5 \pmod p$, $\widehat{\mathfrak{D}}_{5,m} = (m-5)a^3X^d + (5-2m)aX^{2d}$ is not a DO polynomial by Lemma 2.1.1. For $k \geq 6$, we consider four cases, namely, $k \not\equiv 3, m, 2m \pmod p$, $k \equiv 3 \pmod p$, $k \equiv m \pmod p$ and $k \equiv 2m \pmod p$.

Case 1. Let $k \not\equiv 3, m, 2m \pmod p$. In this case, the coefficients of X^d and X^{2d} in $\widehat{\mathfrak{D}}_{k,m}$ are non-zero, and therefore $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial by Lemma 2.1.1.

Case 2. Let $k \equiv 3 \pmod{p}$. In this case, we have $k \not\equiv 4, 5 \pmod{p}$. Also, note that $k \not\equiv m \pmod{p}$, otherwise $m \equiv 3 \pmod{p}$. Similarly, $k \not\equiv 3m \pmod{p}$, otherwise $m \equiv 1 \pmod{p}$. Therefore, the coefficients of X^d and X^{3d} in $\widehat{\mathfrak{D}}_{k,m}$ are non-zero and hence $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial by Lemma 2.1.2.

Case 3. Let $k \equiv m \pmod{p}$. Notice that $k \not\equiv 3, 4 \pmod{p}$. Also, note that $k \not\equiv 2m, 3m \pmod{p}$, otherwise $m \equiv 0 \pmod{p}$. Therefore, the coefficient of X^{2d} in $\widehat{\mathfrak{D}}_{k,m}$ is non-zero. Also, when $k \not\equiv 5 \pmod{p}$, the coefficient of X^{3d} in $\widehat{\mathfrak{D}}_{k,m}$ is non-zero. Thus, if $\widehat{\mathfrak{D}}_{k,m}$ is a DO polynomial, then $2d = p^\alpha + 1$ and $3d = p^\beta + 1$. Combining these equations, we get $3p^\alpha + 1 = 2p^\beta$, which forces $\alpha = 0$ and $p^\beta = 2$, a contradiction. Therefore, $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial in this case. In the case $k \equiv 5 \pmod{p}$, consider the coefficient of the fifth term

$$\frac{(k-6)(k-7)(k-8)(k-9)(k-5m)}{5!}a^{k-10}.$$

Since $k \equiv 5 \pmod{p}$, we have $(k-6), (k-7), (k-8), (k-9) \not\equiv 0 \pmod{p}$. Also, note that $k \not\equiv 5m \pmod{p}$, otherwise $m \equiv 1 \pmod{p}$. Therefore, the coefficients of X^{2d} and X^{5d} in $\widehat{\mathfrak{D}}_{k,m}$ are non-zero. Thus, if $\widehat{\mathfrak{D}}_{k,m}$ is a DO polynomial, then $2d = p^\alpha + 1$ and $5d = p^\beta + 1$. Combining these equations, we get $5p^\alpha + 3 = 2p^\beta$, which forces $\alpha = 0$ and $p^\beta = 4$, a contradiction. Therefore, $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial.

Case 4. Let $k \equiv 2m \pmod{p}$. Notice that $k \not\equiv m \pmod{p}$, otherwise $m \equiv 0 \pmod{p}$. Therefore the coefficient of X^d in $\widehat{\mathfrak{D}}_{k,m}$ is non-zero. Also note that $k \not\equiv 3m \pmod{p}$ and $k \not\equiv 4 \pmod{p}$, otherwise $m \equiv 0 \pmod{p}$ and $m \equiv 2 \pmod{p}$, respectively. When $k \not\equiv 5 \pmod{p}$, the coefficient of X^{3d} in $\widehat{\mathfrak{D}}_{k,m}$ is non-zero and hence $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial by Lemma 2.1.2. In the case $k \equiv 5 \pmod{p}$, the condition $k \geq 6$ is equivalent to $k \geq 13$. Now consider the fifth term again. By similar arguments as done in Case 3 above, it is easy to see that the coefficient of X^{5d} is non-zero. Thus, if $\widehat{\mathfrak{D}}_{k,m}$ is a DO polynomial, then $d = p^\alpha + 1$ and $5d = p^\beta + 1$. Combining these equations, we get $5p^\alpha + 4 = p^\beta$, which forces $\alpha = 0$ and $p^\beta = 9$, a contradiction. Therefore $\widehat{\mathfrak{D}}_{k,m}$ is not a DO polynomial. This completes the proof. □

2.7 Discussion on Planarity

We consider the planarity of DO polynomials obtained from RDPs of the $(m+1)$-th kind as listed in the Section 2.8. First, we shall discuss the tools and techniques that are needed to understand the planarity of DO polynomials. These tools and techniques are similar to the ones used in [22]. Recall that a polynomial function $f : \mathbb{F}_q \to \mathbb{F}_q$ is said to be planar if the difference function $\Delta_f(X, a) = f(X + a) - f(X) - f(a)$ permutes the elements of $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$. If f happens to be a DO polynomial, the difference function $\Delta_f(X, a)$ for each $a \in \mathbb{F}_q^*$, belongs to another well-known class of polynomials called linearized polynomials. Therefore, a DO polynomial f is planar if and only if the linearized polynomial $\Delta_f(X, a)$ is a permutation polynomial for each $a \in \mathbb{F}_q^*$. The permutation behaviour of linearized polynomial is well-known. In fact, [36, Theorem 7.9] tells us that a linearized polynomial is a permutation polynomial over $\mathbb{F}_q$ if and only if its only root in $\mathbb{F}_q$ is 0. Therefore, in order to show that a DO polynomial f is not planar, it is sufficient to show that the difference function $\Delta_f(X, Y) = f(X + Y) - f(X) - f(Y)$ has a root in $\mathbb{F}_q^* \times \mathbb{F}_q^*$.

We recall that a DO polynomial function f from $\mathbb{F}_q$ to itself is called 2-to-1 function if the cardinality of the image set on $\mathbb{F}_q^*$ is $(q-1)/2$. Qiu et al. [47] showed that the size of the image set on $\mathbb{F}_q^*$ of a planar polynomial f over $\mathbb{F}_q$ must be at least $(q-1)/2$. For a DO polynomial f, Weng and Zeng [59, Theorem 2.3] gave the following necessary and sufficient condition for f to be planar.

Lemma 2.7.1. *Let f be a DO polynomial over $\mathbb{F}_q$. Then f is planar if and only if f is 2-to-1.*

Lemma 2.7.1 has further consequences. First, if a DO polynomial f has a root $z \in \mathbb{F}_q^*$, then $-z$ is also a root of f. Therefore, the cardinality of image set of f on $\mathbb{F}_q^*$ is strictly less than $(q-1)/2$ and hence, in such a case, f is not planar.

For the second consequence, we begin with an easy observation that if $f(X)$ is a DO polynomial, then so is $f(X^{p^t})$. We know that X^{p^t} is a linearized permutation polynomial over $\mathbb{F}_{p^n}$. Therefore, the cardinality of the image set of $f(X)$ and $f(X^{p^t})$ on $\mathbb{F}_q^*$ is same. Hence if $f(X)$ is planar, then $f(X^{p^t})$ is also planar. Therefore in such situations, it would be sufficient to consider the planarity of $f(X)$.

Another important tool that we would require to study the planarity of DO polynomials is the following version of Weil bound as stated in [16, Lemma 2.4].

Lemma 2.7.2. *Let $f(X,Y)$ be an absolutely irreducible polynomial in $\mathbb{F}_q[X,Y]$. Then the number N_f of $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ with $f(u,v) = 0$ satisfies*

$$N_f \geq q - (d-1)(d-2)\sqrt{q} - d - 1,$$

where d is the total degree of f.

We now describe the strategy for using the Weil bound to determine the planarity of certain DO polynomials. Let f be a DO polynomial over $\mathbb{F}_q$ and consider the difference function $\Delta_f(X,Y) = f(X+Y) - f(X) - f(Y)$. If this difference function has an absolutely irreducible factor, say $h(X,Y)$, of total degree d_h, then Lemma 2.7.2 gives a lower bound for the cardinality N_h of all the points $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $h(u,v) = 0$. If the degree of the absolutely irreducible factor $h(X,Y)$ is not too large and q is large enough, then we have many $\mathbb{F}_q$-rational points on the affine algebraic curve defined by $h(X,Y) = 0$. Moreover, if N_h is strictly larger than the number of solutions to $h(X,Y) = 0$ with either $X = 0$ or $Y = 0$, then Lemma 2.7.2 yields the existence of a point (u,v) in $\mathbb{F}_q^* \times \mathbb{F}_q^*$ such that $h(u,v) = 0$ and hence, for such a point, we have $\Delta_f(u,v) = 0$, i.e, $\Delta_f(X,Y)$ has a root in $\mathbb{F}_q^* \times \mathbb{F}_q^*$. Thus, in order to show that f is not exceptional planar (i.e., planar over infinitely many extensions of $\mathbb{F}_q$), it is sufficient to show that the difference function of f contains an absolutely irreducible component with a solution in $\mathbb{F}_q^* \times \mathbb{F}_q^*$.

It is straightforward to see that for $b \in \mathbb{F}_q^*$, RDPs of the $(m+1)$-th kind admit the following relationship

$$b^{kd} D_{k,m}(a, X^d) = D_{k,m}(ab^d, (Xb^2)^d). \tag{2.14}$$

In view of (2.14), and due to the fact that the planarity property of a function f remains invariant under linear transformations (i.e. if $f(X)$ is planar so is $\alpha f(\lambda X + \mu) + \beta$ with $\alpha, \lambda \neq 0$), we have the following lemma.

Lemma 2.7.3. *Let $D_{k,m}(a,X)$ be the k-th RDP of the $(m+1)$-th kind. Then $D_{k,m}(a,X^d)$ is planar equivalent over $\mathbb{F}_q$ to $D_{k,m}(ab^d, X^d)$ for any $b \in \mathbb{F}_q^*$.*

Over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, we derive a useful consequence of Lemma 2.7.3. Note that one may always choose $b \in \overline{\mathbb{F}}_q$ that satisfies the equation $aX^d = 1$. In this

way the factorizations of $\Delta_{D_{k,m}(a,X^d)}$ and $\Delta_{D_{k,m}(1,X^d)}$ over $\overline{\mathbb{F}}_q$ are linearly related. As a consequence, the absolutely irreducible factors of $\Delta_{D_{k,m}(a,X^d)}$ are of the same form for all non-zero a. Thus, without loss of generality, one may always take $a = 1$, while checking the absolute irreducibility of certain polynomials.

Now we consider the planarity of the DO polynomials listed in the Section 2.8 in three different cases.

Case 1. Let $p = 3$. The planarity of monomials $\widehat{\mathfrak{D}}_2 = X^{3^\alpha+1}$, $\widehat{\mathfrak{E}}_2 = 2X^{3^\alpha+1}$, $\widehat{\mathfrak{E}}_3 = aX^{3^\alpha+1}$, $\widehat{\mathfrak{E}}_4 = X^{3^\alpha+1}$, and $\widehat{\mathfrak{E}}_5 = 2a^3X^{3^\alpha+1}$ is well-known by [20, Theorem 3.3] and these monomials are planar over $\mathbb{F}_{3^n}$ if and only if $n/(\alpha, n)$ is odd. It is easy to see that $X = a$ is a root of the polynomials $\widehat{\mathfrak{D}}_5 = 2aX^4 + a^3X^2$, $\widehat{\mathfrak{E}}_7 = 2aX^6 + a^3X^4$, $\widehat{\mathfrak{D}}_7 = 2aX^6 + 2a^3X^4 + 2a^5X^2$, $\widehat{\mathfrak{E}}_{13} = aX^{12} + a^3X^{10} + a^9X^4$ and $\widehat{\mathfrak{E}}_{19} = 2aX^{18} + 2a^9X^{10} + a^{13}X^6 + a^{15}X^4$. Therefore, these DO polynomials are not planar. Now we consider the planarity of the rest of the DO polynomials one by one.

(i) In the case of binomial $f(X) = \widehat{\mathfrak{D}}_4 = 2X^4+2a^2X^2$, consider the difference function $\Delta_f(X, Y) = f(X + Y) - f(X) - f(Y) = XYB(X, Y)$, where $B(X, Y) = X^2 + Y^2 - a^2$, which is simply an irreducible conic since a is non-zero. Therefore, by Lemma 2.7.2, the number N_B of $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ with $B(u, v) = 0$ is greater than or equal to $q - 3$. Note that we can obtain at most 4 solutions (u, v) to $B(X, Y) = 0$ by putting either $X = 0$ or $Y = 0$. Therefore, when $q - 3 > 4$, there must exist a root $(u, v) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ of $B(X, Y)$. Therefore, $\widehat{\mathfrak{D}}_4$ is not planar when $q > 7$, i.e., $n \geq 2$. For $n = 1$, $\widehat{\mathfrak{D}}_4 \equiv X^2 \pmod{X^3 - X}$ which is clearly a planar function.

(ii) The DO binomial $\widehat{\mathfrak{E}}_6 = 2X^{3(3^\alpha+1)} + a^4X^{3^\alpha+1}$ can be written as composition of a linearized polynomial and a monomial as $(2X^3 + a^4X) \circ X^{3^\alpha+1}$. Now from [20, Theorem 2.3], $\widehat{\mathfrak{E}}_6$ is planar if and only if $2X^3 + a^4X$ is a permutation polynomial and $X^{3^\alpha+1}$ is planar. Now, since $X = a^2$ is a root of the linearized polynomial $2X^3 + a^4X$, $2X^3 + a^4X$ is not a permutation polynomial. Hence, $\widehat{\mathfrak{E}}_6$ is not planar.

(iii) In the case of the DO polynomial $f(X) = \widehat{\mathfrak{E}}_{10} = 2X^{10} + a^4X^6 + a^6X^4$, consider the difference function $\Delta_f(X, Y) = XY\ h(X, Y)$, where $h(X, Y) = 2(X^8+Y^8)-a^4X^2Y^2+a^6(X^2+Y^2)$. The Magma algebra package [7] reveals that $h(X, Y)$ is absolutely irreducible. Therefore, by Lemma 2.7.2, the number N_h of solutions $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ of $h(X, Y) = 0$ satisfies $N_h \geq q - 42\sqrt{q} - 9$. Now $h(X, 0) = 2X^8 + a^6X^2 = X^2(a + X)^3(a - X)^3$ have in total 8 solutions in $\mathbb{F}_q$. Similarly, $h(0, Y) = 2Y^8a + a^6Y^2 = Y^2(a - Y)^3(a + Y)^3$ have in

total 8 solutions in $\mathbb{F}_q$. Therefore, in total 16 solutions can be obtained either by putting $X = 0$ or $Y = 0$. Now if $q-42\sqrt{q}-9 > 16$, i.e., $q-42\sqrt{q}-25 > 0$ then $h(X,Y)$ possesses a solution $(u,v) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. This is true for $n \geq 7$, therefore, for $n \geq 7$, $\widehat{\mathfrak{E}}_{10}$ is not planar. For $n = 1$ $\widehat{\mathfrak{E}}_{10} = X^2 \pmod{X^3 - X}$, which is clearly a planar polynomial. Computations show that for $2 \leq n \leq 6$, the cardinality of the image set of $\widehat{\mathfrak{E}}_{10}$ on $\mathbb{F}_q^*$ is strictly less than $(3^n - 1)/2$. Therefore, by Lemma 2.7.1, $\widehat{\mathfrak{E}}_{10}$ is not planar in these cases.

(iv) Consider the DO polynomial $f(X) = \widehat{\mathfrak{E}}_{15} = aX^{28} + 2a^9X^{12} + a^{13}X^4 = a(X^7 + 2a^8X^3 + a^{12}X) \circ X^4$. This polynomial is never planar over $\mathbb{F}_{3^n}$ when n is even. Since in this case $4 \mid (q-1)$, the cardinality of image set of $f(X)$ on $\mathbb{F}_q^*$ is at most $(q-1)/4$ and thus, by Lemma 2.7.1, $f(X)$ is not planar. When n is odd, we consider the difference function $\Delta_f(X,Y) = aXY(X^2+Y^2)\ h(X,Y)$, where

$$h(X,Y) = a^{12} + \sum_{i=0}^{12}(-1)^i X^{24-2i}Y^{2i} + \sum_{i=1}^{3}(-1)^i a^8 X^{8-2i}Y^{2i}.$$

Again, the Magma algebra package [7] shows that the polynomial $h'(X,Y)$ obtained from $h(X,Y)$ by putting $a = 1$, is absolutely irreducible. Therefore, by Lemma 2.7.2, the number $N_{h'}$ of solutions $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ of $h'(X,Y) = 0$ satisfies $N_{h'} \geq q - 506\sqrt{q} - 25$. Also, $h'(X,0) = X^{24} + 1$ and this has no root in odd degree extensions of $\mathbb{F}_3$. Similarly, $h'(0,Y) = Y^{24} + 1$ has no root in odd degree extensions of $\mathbb{F}_3$. Therefore, there is no solution to $h'(X,Y) = 0$ corresponding to $XY = 0$. If $q - 506\sqrt{q} - 25 > 0$, then $h'(X,Y)$ has a root $(u,v) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. This holds true for all $n \geq 12$. Therefore, $\widehat{\mathfrak{E}}_{15}$ is not planar over $\mathbb{F}_{3^n}$ for $n \geq 12$. In the case $n = 1$, the polynomial $f(X) = \widehat{\mathfrak{E}}_{15} = aX^2 \pmod{X^3 - X}$ which is clearly a planar function. Computations show that for $n = 5, 7, 9, 11$, the cardinality of the image set of $\widehat{\mathfrak{E}}_{15}$ on $\mathbb{F}_{3^n}^*$ is strictly less than $(3^n - 1)/2$, therefore, $\widehat{\mathfrak{E}}_{15}$ is not planar in these cases. In the case $n = 3$, $\widehat{\mathfrak{E}}_{15}$ is planar for every choice of $a \in \mathbb{F}_{27}^*$.

Case 2. Let $p = 5$. The planarity of DO monomials $\widehat{\mathfrak{D}}_2 = 3X^{5^\alpha+1}$, $\widehat{\mathfrak{D}}_3 = 2aX^{5^\alpha+1}$, $\widehat{\mathfrak{E}}_2 = 4X^{5^\alpha+1}$, $\widehat{\mathfrak{E}}_3 = 3aX^{5^\alpha+1}$, $\widehat{\mathfrak{G}}_2 = X^{5^\alpha+1}$, $\widehat{\mathfrak{H}}_2 = 2X^{5^\alpha+1}$, $\widehat{\mathfrak{H}}_3 = aX^{5^\alpha+1}$, and $\widehat{\mathfrak{H}}_4 = 3X^{5^\alpha+1}$ is well-known by [20, Theorem 3.3] and these monomials are planar over $\mathbb{F}_{5^n}$ whenever $n/(\alpha, n)$ is odd. It is straightforward to see that $X = a$ is a root of the DO binomial $\widehat{\mathfrak{E}}_7 = 4a^5X^2 + aX^6$ and hence, it is not planar. Now we consider the planarity of the rest of the DO polynomials one by one.

(i) For the DO binomial $f(X) = \widehat{\mathfrak{G}}_6 = 2a^4X^2 + X^6$, consider the difference function

$\Delta_f(X,Y) = XYB(X,Y)$, where $B(X,Y) = X^4 + Y^4 - a^4$. It is easy to see that $Y - a \mid Y^4 - a^4$ and $Y^4 - a^4$ has no repeated roots. Therefore, by Eisenstein's criterion, $B(X,Y)$ is absolutely irreducible. Thus, by Lemma 2.7.2, the number of solutions $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ of $B(X,Y) = 0$ satisfies $N_B \geq q - 6\sqrt{q} - 5$. Now, at most 8 roots of $B(X,Y)$ can be obtained by putting either $X = 0$ or $Y = 0$. Therefore, if $q - 6\sqrt{q} - 5 > 8$, $B(X,Y)$ will have a solution $(u,v) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, which holds for all $n \geq 3$. Therefore, $\widehat{\mathfrak{G}}_6$ is not planar over $\mathbb{F}_{5^n}$ for $n \geq 3$. When $n = 1$, $f(X) = 3X^2 (\text{mod } (X^5 - X))$ which is clearly a planar function. For $n = 2$, the number of solutions of the equation $X^4 + Y^4 = a^4$ in $\mathbb{F}_{5^2} \times \mathbb{F}_{5^2}$ is 40, which is greater than 16. Therefore, $\widehat{\mathfrak{G}}_6$ is not planar in this case.

(ii) In the case of the DO trinomial $f(X) = \widehat{\mathfrak{G}}_{11} = -aX^{10} + a^5X^6 + 2a^9X^2$, consider the difference function $\Delta_f(X,Y) = XY\ h(X,Y)$, where $h(X,Y) = 3aX^4Y^4 + a^5X^4 + a^5Y^4 + 4a^9$. The Magma algebra package [7] shows that $h(X,Y)$ is absolute irreducible. Therefore, by Lemma 2.7.2, the number N_h of solutions $(u,v) \in \mathbb{F}_q \times \mathbb{F}_q$ of $h(X,Y) = 0$ satisfies $N_h \geq q - 42\sqrt{q} - 9$. Now, $h(X,0) = X^4 - a^4 = 0$ can have at most 4 solutions. Similarly, $h(0,Y) = Y^4 - a^4 = 0$ can have at most 4 solutions. Therefore, at most 8 solutions can be obtained by putting either $X = 0$ or $Y = 0$. Now, if $q - 42\sqrt{q} - 9 > 8$, i.e., $q - 42\sqrt{q} - 17 > 0$ then $h(X,Y)$ will have a solution $(u,v) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$. This is true for $n \geq 5$, therefore, for $n \geq 5$, $\widehat{\mathfrak{G}}_{11}$ is not planar. For $n = 1$, $\widehat{\mathfrak{G}}_{11} = 2aX^2$ is clearly a planar function. For $n = 2, 4$, computations show that the cardinality of the image set of $\widehat{\mathfrak{G}}_{11}$ on $\mathbb{F}_{5^n}^*$ is strictly less than $(5^n - 1)/2$. Therefore, $\widehat{\mathfrak{G}}_{11}$ is not planar in these cases. For $n = 3$, computations show that $\widehat{\mathfrak{G}}_{11}$ is planar for every choice of $a \in \mathbb{F}_{125}^*$.

Case 3. Let $p > 5$. In this case, the only DO polynomials we are getting are the monomials of the form $bX^{p^\alpha+1}$ where $b \in \mathbb{F}_q^*$ and by [20, Theorem 3.3], these monomials are planar over $\mathbb{F}_{p^n}$ whenever $n/(\alpha, n)$ is odd.

In view of the foregoing discussion, the following theorem gives the list of planar DO polynomials arising from RDPs of arbitrary kind.

Theorem 8. *Let* $\widehat{\mathfrak{D}}_{k,m} = \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} \frac{k-mi}{k-i} \binom{k-i}{i} (-X^d)^i a^{k-2i}$ *as defined in the Introduction. Then the following are the only planar DO polynomials arising from* $\widehat{\mathfrak{D}}_{k,m}$.

(i) X^2 *over* $\mathbb{F}_{p^n}$.

(ii) $X^{p^\alpha+1}$ *over* $\mathbb{F}_{p^n}$ *with* $\frac{n}{(\alpha,n)}$ *odd.*

(iii) $2a^9X^{12} + a^{13}X^4 + aX^2$ *over* $\mathbb{F}_{27}$ *with* $a \in \mathbb{F}_{27}^*$.

(iv) $-aX^{10} + a^5X^6 + 2a^9X^2$ *over* $\mathbb{F}_{125}$ *with* $a \in \mathbb{F}_{125}^*$.

2.8 The Complete List of DO Polynomials

Here, we present the complete list of DO polynomials obtained from polynomial $\widehat{\mathfrak{D}}_{k,m}$ over a finite field of odd characteristic.

1. The case $p = 3$.
   (a) When $m \equiv 0 \pmod 3$
      i. $k = 2 \cdot 3^\ell$, $X^{3^{t+\ell}(3^\alpha+1)}$ for nonnegative integers α, t and ℓ.
      ii. $k = 4 \cdot 3^\ell$, $2a^2X^{2\cdot 3^{t+\ell}} + 2X^{4\cdot 3^{t+\ell}}$ for nonnegative integers t and ℓ.
      iii. $k = 5 \cdot 3^\ell$, $a^3X^{2\cdot 3^{t+\ell}} + 2aX^{4\cdot 3^{t+\ell}}$ for nonnegative integers t and ℓ.
      iv. $k = 7 \cdot 3^\ell$, $2a^5X^{2\cdot 3^{t+\ell}} + 2a^3X^{4\cdot 3^{t+\ell}} + 2aX^{2\cdot 3^{t+\ell+1}}$ for nonnegative integers t and ℓ.
   (b) When $m \equiv 1 \pmod 3$
      i. $k = 2$, $2X^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.
      ii. $k = 3$, $aX^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.
      iii. $k = 4$, $X^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.
      iv. $k = 5$, $2a^3X^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.
      v. $k = 6$, $a^4X^{3^t(3^\alpha+1)} + 2X^{3^{t+1}(3^\alpha+1)}$ for nonnegative integers α and t.
      vi. $k = 7$, $a^3X^{4\cdot 3^t} + 2aX^{2\cdot 3^{t+1}}$ for nonnegative integer t.
      vii. $k = 10$, $a^6X^{4\cdot 3^t} + a^4X^{2\cdot 3^{t+1}} + 2X^{10\cdot 3^t}$ for nonnegative integer t.
      viii. $k = 13$, $a^9X^{4\cdot 3^t} + a^3X^{10\cdot 3^t} + aX^{4\cdot 3^{t+1}}$ for nonnegative integer t.
      ix. $k = 15$, $a^{13}X^{4\cdot 3^t} + 2a^9X^{4\cdot 3^{t+1}} + aX^{28\cdot 3^t}$ for nonnegative integer t.
      x. $k = 19$, $a^{15}X^{4\cdot 3^t} + a^{13}X^{2\cdot 3^{t+1}} + 2a^9X^{10\cdot 3^t} + 2aX^{2\cdot 3^{t+2}}$ for nonnegative integer t.
   (c) When $m \equiv 2 \pmod 3$
      i. $k = 3$, $2aX^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.

ii. $k = 4$, $a^2X^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.

iii. $k = 5$, $aX^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.

iv. $k = 6$, $2a^4X^{3^t(3^\alpha+1)}$ for nonnegative integers α and t.

v. $k = 7$, $a^5X^{3^t(3^\alpha+1)} + 2aX^{3^{t+1}(3^\alpha+1)}$ for nonnegative integers α and t.

vi. $k = 8$, $a^4X^{4\cdot3^t} + 2a^2X^{2\cdot3^{t+1}}$ for nonnegative integer t.

vii. $k = 11$ $a^7X^{4\cdot3^t} + a^5X^{2\cdot3^{t+1}} + 2aX^{10\cdot3^t}$ for nonnegative integer t.

viii. $k = 14$, $a^{10}X^{4\cdot3^t} + a^4X^{10\cdot3^t} + a^2X^{4\cdot3^{t+1}}$ for nonnegative integer t.

ix. $k = 16$, $a^{14}X^{4\cdot3^t} + 2a^{10}X^{4\cdot3^{t+1}} + a^2X^{28\cdot3^t}$ for nonnegative integer t.

x. $k = 20$, $a^{16}X^{4\cdot3^t} + a^{14}X^{2\cdot3^{t+1}} + 2a^{10}X^{10\cdot3^t} + 2a^2X^{2\cdot3^{t+2}}$ for nonnegative integer t.

2. The case $p = 5$.

(a) When $m \equiv 0 \pmod 5$

i. $k = 2 \cdot 5^\ell$, $3X^{5^{t+\ell}(5^\alpha+1)}$ for non negative integers α, t and ℓ.

ii. $k = 3 \cdot 5^\ell$, $2aX^{5^{t+\ell}(5^\alpha+1)}$ for non negative integers α, t and ℓ.

(b) When $m \equiv 1 \pmod 5$

i. $k = 2$, $4X^{5^t(5^\alpha+1)}$ for nonnegative integers α and t.

ii. $k = 3$, $3aX^{5^t(5^\alpha+1)}$ for nonnegative integers α and t.

iii. $k = 7$, $4a^5X^{2\cdot5^t} + aX^{6\cdot5^t}$ for nonnegative integer t.

(c) When $m \equiv 2 \pmod 5$

i. $k = 3$, $4aX^{5^t(5^\alpha+1)}$ for nonnegative integers α and t.

ii. $k = 4$, $3a^2X^{5^t(5^\alpha+1)}$ for nonnegative integer t.

iii. $k = 8$, $4a^6X^{2\cdot5^t} + a^2X^{6\cdot5^t}$ for nonnegative integer t.

(d) When $m \equiv 3 \pmod 5$

i. $k = 2$, $2X^{5^t(5^\alpha+1)}$ for nonnegative integers α and t.

ii. $k = 6$, $2a^4X^{2\cdot5^t} + X^{6\cdot5^t}$ for nonnegative integer t.

iii. $k = 11$, $2a^9X^{2\cdot5^t} + a^5X^{6\cdot5^t} + 4aX^{2\cdot5^{t+1}}$ for nonnegative integer t.

(e) When $m \equiv 4 \pmod 5$

i. $k = 2$, $2X^{5^t(5^\alpha+1)}$ for nonnegative integers α and t.

ii. $k = 3$, $aX^{5^t(5^\alpha+1)}$ for nonnegative integer t.

iii. $k = 4$, $3X^{5^t(5^\alpha+1)}$ for nonnegative integer t.

3. The case $p > 5$.

   In this case, we are getting DO polynomials of the form $bX^{p^\alpha+1}$ where $b \in \mathbb{F}_q^*$.

Chapter 3

On the c-Differential Uniformity of Certain Maps over Finite Fields

In this chapter, we shall consider the c-differential uniformity (cDU) of several classes of functions over finite fields of odd characteristic. This chapter has been arranged as follows. In Section 3.1, we establish a relation between the c-derivative of the power map X^d and Dickson polynomial of the first kind over finite field of odd characteristic, for $c = -1$. As a consequence, we shall show that $X^{\frac{p^\ell+1}{2}}$ is PcN for $c = -1$ over $\mathbb{F}_{p^n}$ if and only if $\ell = 0$ or $\frac{\ell}{\gcd\ (\ell, n)}$ is even. In Section 3.2, we give four classes of power maps whose cDU for $c = -1$ is $2, 3, 6$ and 7. In Section 3.3, we give all values of d for which X^d is PcN over the finite fields $\mathbb{F}_{3^5}$, $\mathbb{F}_{5^5}$ and $\mathbb{F}_{7^5}$, respectively, for $c = -1$. Following the pattern of the computational results, we propose a conjecture about the plausible values of d for which X^d is PcN over $\mathbb{F}_{p^5}$ for $c = -1$. Similarly in Section 3.4, we give all values of d for which X^d is PcN over the finite fields $\mathbb{F}_{3^7}$, $\mathbb{F}_{5^7}$ and $\mathbb{F}_{7^7}$, respectively, for $c = -1$. Following the pattern of the computational results, we propose another conjecture about the plausible values of d for which X^d is PcN over $\mathbb{F}_{p^7}$ for $c = -1$. In Section 3.5, for $c \neq 1$, we give a necessary and sufficient condition for a linearized polynomial to be PcN. We also find necessary and sufficient conditions for the sum $f + \gamma F$ to be PcN, where $\gamma \in \mathbb{F}_{p^n}$, f is PcN and F is any Boolean function. We also show that in some instances such perturbations do not produce PcN functions. We further discuss the affine, extended affine and CCZ-equivalence as it relates to cDU.

3.1 PcN Power Maps and Dickson Polynomials

Before we begin, we recall the definition of Walsh transform. 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 defined as

$$\mathcal{W}_f(a,b) = \sum_{X \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_m(bf(X)) - \mathrm{Tr}_n(aX)},$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is a pth root of unity and $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the absolute trace function, given by $\mathrm{Tr}(X) = \sum_{i=0}^{n-1} X^{p^i}$. We also say that $\alpha \in \mathbb{F}_{p^n}^*$ is a β-linear structure for f, if $f(X+\alpha) - f(X) = \beta$, for all $X \in \mathbb{F}_{p^n}$.

Also, recall that for $c = -1$, a polynomial function $f(X)$ is called PcN over $\mathbb{F}_{p^n}$ if the corresponding mapping $X \to f(X+a) + f(X)$ is a permutation of $\mathbb{F}_{p^n}$ for each $a \in \mathbb{F}_{p^n}$. Therefore, a power map X^d is PcN if and only if $(X+a)^d + X^d$ is a permutation of $\mathbb{F}_{p^n}$ for each $a \in \mathbb{F}_{p^n}$. Now, we present some lemmas that will be useful in the sequel. Throughout this section, we shall assume that $c = -1$, whenever we refer to PcN functions.

Lemma 3.1.1. *A monomial X^d is perfect (-1)-nonlinear in $\mathbb{F}_{p^n}$ if and only if X^d and $(X+1)^d + (X-1)^d$ are permutations of $\mathbb{F}_{p^n}$.*

Proof. Let $f(X) = X^d$; then, by definition, f is a PcN function if and only if $(X+a)^d + X^d$ is a permutation of $\mathbb{F}_{p^n}$ for all $a \in \mathbb{F}_{p^n}$. For $a = 0$, we have $(X+a)^d + X^d = 2X^d$, and $2X^d$ is clearly a permutation of $\mathbb{F}_{p^n}$ if and only if X^d is a permutation of $\mathbb{F}_{p^n}$. For $a \neq 0$, we have

$$\begin{aligned}
& (X+a)^d + X^d \text{ is a permutation of } \mathbb{F}_{p^n} \\
\iff\ & a^d \left[\left(\frac{X}{a} + 1 \right)^d + \left(\frac{X}{a} \right)^d \right] \text{ is a permutation of } \mathbb{F}_{p^n} \\
\iff\ & \left(\frac{X}{a} + 1 \right)^d + \left(\frac{X}{a} \right)^d \text{ is a permutation of } \mathbb{F}_{p^n} \\
\iff\ & (Y+1)^d + Y^d \text{ is a permutation of } \mathbb{F}_{p^n};\ \text{where } aY = X \\
\iff\ & \left(\frac{2Y+1+1}{2} \right)^d + \left(\frac{2Y+1-1}{2} \right)^d \text{ is a permutation of } \mathbb{F}_{p^n} \\
\overset{Z := 2Y+1}{\iff}\ & \left(\frac{1}{2} \right)^d \left[(Z+1)^d + (Z-1)^d \right] \text{ is a permutation of } \mathbb{F}_{p^n}
\end{aligned}$$

$$\iff \quad (Z+1)^d + (Z-1)^d \quad \text{is a permutation of } \mathbb{F}_{p^n}.$$

This completes the proof of the lemma. □

In what follows, we shall adopt this definition of PcN function for power maps, when $c = -1$. One of the motivations behind considering this definition is that we can establish a connection between $(X+1)^d + (X-1)^d$ and d-th Dickson polynomial of the first kind. We recall the Dickson's original approach of defining the Dickson polynomial $D_d(X, a)$, which was essentially based on the relationship between the sum of d-th powers and elementary symmetric functions. In fact, the d-th Dickson polynomial of the first kind $D_d(X, a) \in \mathbb{F}_q[X]$ admits the following representation

$$\begin{aligned} U_1^d + U_2^d &= \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-U_1U_2)^i (U_1+U_2)^{d-2i} \\ &= D_d(U_1+U_2, U_1U_2), \end{aligned} \tag{3.1}$$

where U_1, U_2 are indeterminates and $D_d(X, a) = \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i X^{d-2i}$.

We will be using in some places Hilbert's Theorem 90 (see [9]), 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 the relative trace $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(X) = \sum_{i=0}^{|\mathrm{Gal}(\mathbb{K}/\mathbb{F})|-1} \sigma^i(X) = 0$, $X \in \mathbb{K}$, if and only if $X = \sigma(Y) - Y$, for some $Y \in \mathbb{K}$.

We now recall a result of Nöbauer [44], which we shall often use, regarding the permutation behavior of Dickson polynomial of the first kind over the finite field $\mathbb{F}_{p^n}$.

Lemma 3.1.2. *[44] Let $a \in \mathbb{F}_{p^n}^*$. The d-th Dickson polynomial of the first kind $D_d(X, a)$ permutes the elements of finite field $\mathbb{F}_{p^n}$ if and only if* $\gcd\ (d, p^{2n}-1) = 1$.

The following lemma will be used throughout.

Lemma 3.1.3. *[28, Lemma 9] Let p be a prime number and ℓ, n be positive integers such that $\ell \leq n$. Then:*

(1) *If p is odd, then* $\gcd(p^\ell + 1, p^n - 1) = 2$ *if* $\dfrac{n}{\gcd(\ell, n)}$ *is odd.*

(2) *If p is odd, then* $\gcd(p^\ell + 1, p^n - 1) = p^{\gcd(\ell,n)} + 1$ *if* $\dfrac{n}{\gcd(\ell, n)}$ *is even.*

(3) *If* $p = 2$, *then* $\gcd(2^\ell + 1, 2^n - 1) = \dfrac{2^{\gcd(n,2\ell)} - 1}{2^{\gcd(n,\ell)} - 1}$.

The following lemma gives a nice connection between the difference function of the power map X^d and the Dickson polynomial for first kind over $\mathbb{F}_{3^n}$, for $c = -1$.

Lemma 3.1.4. *[60, Proposition 8] For a positive odd integer* n *with* $n \geq 3$, *if* $d \equiv -1 \pmod 3$ *and gcd* $(d, 3^{2n} - 1) = 1$, *then*

$$(X+1)^d + (X-1)^d = 2D_d(X, 1) \tag{3.2}$$

is a permutation of $\mathbb{F}_{3^n}$, *where* $D_d(X, 1)$ *is the Dickson polynomial of the first kind.*

As alluded to in Introduction, the sufficient conditions in the above lemma do not hold, and the counterexamples can be found using easy computer searches. For instance, when $n = 5$ and $d = 17$, d clearly satisfies the conditions of Lemma 3.1.4, but $(X+1)^{17} + (X-1)^{17} \neq 2D_d(X, 1)$. Bartoli and Timpanella [1, Theorem 6.1] provided the correct conditions on d for which (3.2) holds over finite fields of odd characteristic. However, it appears that there is a missing case ($k = 0$) in [1, Theorem 6.1], which we shall include here. The following theorem provides a relationship between the difference function of the power map X^d and the Dickson polynomial of first kind over $\mathbb{F}_{p^n}$, for $c = -1$.

Theorem 9. *Let* p *be an odd prime,* d *be a positive integer such that* $d = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$ *for some* $k \geq 0$, *where* $a_i \in \{0, 1, \cdots, p-1\}$ *and* $a_0, a_k \neq 0$, *then* $(X+1)^d + (X-1)^d = 2D_d(X, \epsilon)$ *for some* $\epsilon \in \mathbb{F}_p^*$ *if and only if either*

(1) $d = 1, 2, 3$; *or*

(2) $a_0 = \dfrac{p+1}{2}$ *and* $a_j = \dfrac{p-1}{2}$ $\forall j \in \{1, 2, \ldots, k\}$ $\left(\textit{thus}, d = \dfrac{p^{k+1}+1}{2}\right)$.

Proof. The necessity of the theorem has already been proved in [1] for all k except for the case $k = 0$. Here we shall prove the necessity for the case $k = 0$. In this case, we have $d = a_0 \in \{1, \ldots, p-1\}$. We now consider two cases, namely, $p = 3$ and $p > 3$. If $p = 3$, the only possible values for d are 1 and 2 and we are done. If $p > 3$ (hence, we can assume $d \geq 4$, since the values $d = 1, 2, 3$ were already covered in Condition (1)), we shall show that the only possible value of a_0 is $\dfrac{p+1}{2}$. It is given that

$$(X+1)^d + (X-1)^d = 2D_d(X, \epsilon)$$

for some $\epsilon \in \mathbb{F}_p^*$. By using binomial expansion on the left in the above equation, and by comparing the coefficients on both sides, we have

$$\binom{d}{2i} \equiv \frac{d}{d-i}\binom{d-i}{i}(-\epsilon)^i \pmod{p},$$

for all $i \in \left\{0, 1, \ldots, \lfloor \frac{d}{2} \rfloor\right\}$.

Surely, for $i = 0$, the previous claim is obviously true. For $i = 1$, we have

$$\frac{a_0(a_0-1)}{2} \equiv -\epsilon \cdot a_0 \pmod{p},$$

which is true if and only if $\epsilon \equiv \dfrac{1-a_0}{2} \pmod{p}$.

For $i = 2$, we have

$$\frac{a_0(a_0-1)(a_0-2)(a_0-3)}{24} \equiv \frac{a_0(a_0-1)^2(a_0-3)}{8} \pmod{p}. \tag{3.3}$$

Now since $a_0 \in \{4, \ldots, p-1\}$, the congruence (3.3) reduces to $2a_0 \equiv 1 \pmod{p}$ which is true if and only if $a_0 = \dfrac{p+1}{2}$. Therefore for $k = 0$ and $d \geq 4$, $\dfrac{p+1}{2}$ is the only possible value for a_0. Hence, the necessity of the theorem for the case $k = 0$ is established. Next, we shall proceed to prove the sufficiency of the theorem. When $d = 1$, then $(X+1)^d+(X-1)^d = 2X = 2D_d(X, \epsilon)$ for any $\epsilon \in \mathbb{F}_p^*$. When $d = 2$, then $(X+1)^d+(X-1)^d = 2(X^2+1) = 2D_d\left(X, -\dfrac{1}{2}\right)$. When $d = 3$, then $(X+1)^d + (X-1)^d = 2(X^3+3X) = 2D_d(X, -1)$. For $d \geq 4$, we shall show that

$$(X+1)^d + (X-1)^d = 2D_d\left(X, \frac{1}{4}\right).$$

Since we evaluate Dickson's polynomial over some extension of the involved prime field, $\mathbb{F}_p$, we assume that the variables take values in the extension $\mathbb{F}_q$ of $\mathbb{F}_p$. Now, for $\alpha \in \mathbb{F}_q$, we let $U_1 = \dfrac{U}{2} \in \mathbb{F}_{q^2}$ and $U_2 = \dfrac{U^{-1}}{2} \in \mathbb{F}_{q^2}$, where U, U^{-1} are the roots of the polynomial $Z^2-2\alpha Z+1 \in \mathbb{F}_q[Z]$. Then, the sum of the roots is $2\alpha = U+U^{-1} \in \mathbb{F}_q$, and Equation (3.1)

reduces to

$$D_d\left(\frac{U+U^{-1}}{2},\frac{1}{4}\right)=\left(\frac{U}{2}\right)^d+\left(\frac{U^{-1}}{2}\right)^d$$
$$D_d\left(\alpha,\frac{1}{4}\right)=\left(\frac{U}{2}\right)^d+\left(\frac{U^{-1}}{2}\right)^d.$$

One may note that when $d=a_0+a_1p+a_2p^2+\cdots+a_kp^k$ for some $k\geq 0$ and $a_0=\frac{p+1}{2}$ and $a_j=\frac{p-1}{2}$, for all $j\in\{1,2,\ldots,k\}$, then

$$d=\frac{p+1}{2}+\frac{p-1}{2}\sum_{j=1}^{k}p^j=\frac{p+1}{2}+\frac{p-1}{2}\,p\,\frac{p^k-1}{p-1}=\frac{p^{k+1}+1}{2}.$$

Now, we have (with $\ell=k+1$)

$$\begin{aligned}
(\alpha+1)^{\frac{p^\ell+1}{2}}+(\alpha-1)^{\frac{p^\ell+1}{2}} &= \left(\frac{U+U^{-1}}{2}+1\right)^{\frac{p^\ell+1}{2}}+\left(\frac{U+U^{-1}}{2}-1\right)^{\frac{p^\ell+1}{2}}\\
&= \left(\frac{1}{2}\right)^{\frac{p^\ell+1}{2}}\left((U+U^{-1}+2)^{\frac{p^\ell+1}{2}}+(U+U^{-1}-2)^{\frac{p^\ell+1}{2}}\right)\\
&= \left(\frac{1}{2U}\right)^{\frac{p^\ell+1}{2}}\left((U^2+2U+1)^{\frac{p^\ell+1}{2}}+(U^2-2U+1)^{\frac{p^\ell+1}{2}}\right)\\
&= \left(\frac{1}{2U}\right)^{\frac{p^\ell+1}{2}}\left((U+1)^{p^\ell+1}+(U-1)^{p^\ell+1}\right)\\
&= \left(\frac{1}{2U}\right)^{\frac{p^\ell+1}{2}}\left(2U^{p^\ell+1}+2\right)\\
&= 2\left(\frac{1}{2}\right)^{\frac{p^\ell+1}{2}}\left(U^{\frac{p^\ell+1}{2}}+(U^{-1})^{\frac{p^\ell+1}{2}}\right)\\
&= 2\left(\left(\frac{U}{2}\right)^{\frac{p^\ell+1}{2}}+\left(\frac{U^{-1}}{2}\right)^{\frac{p^\ell+1}{2}}\right)\\
&= 2D_{\frac{p^\ell+1}{2}}\left(\frac{U+U^{-1}}{2},\frac{1}{4}\right)\\
&= 2D_{\frac{p^\ell+1}{2}}\left(\alpha,\frac{1}{4}\right).
\end{aligned}$$

Hence, the theorem is proved. □

Remarks 3.1.5. Theorem 9 above completes Theorem 6.1 of [1]. Proposition 8 of [60] is a particular case of the above theorem with $p=3$. Also, the above theorem provides a

simpler proof of [1, Proposition 4.1] in the particular case of $\ell = 2$.

Our focus is now to study the perfect c-nonlinearity of the power map $X^{\frac{p^\ell+1}{2}}$ over $\mathbb{F}_{p^n}$, where $\ell \geq 0$ and $n > 1$ (note that this has been also investigated in [48]). As alluded to in Introduction, we shall consider the perfect c-nonlinearity of permutation polynomials only. In view of this, we shall first examine the permutation behaviour of the power map $X^{\frac{p^\ell+1}{2}}$. We may impose a restriction of $\ell < n$, so as to ensure that the exponent $\frac{p^\ell+1}{2}$ does not exceed $p^n - 1$. The following theorem gives the necessary and sufficient conditions on ℓ and n for which the power map $X^{\frac{p^\ell+1}{2}}$ is a permutation of $\mathbb{F}_{p^n}$. Surely, we can find it as a particular case of existing permutation classes, but our proof is short enough to warrant an inclusion here.

Theorem 10. *The power map $X^{\frac{p^\ell+1}{2}}$ is a permutation of $\mathbb{F}_{p^n}$ if and only if any one of the following conditions hold*:

(1) $\ell = 0$;

(2) *ℓ is even and n is odd*;

(3) *ℓ is even and n is even together with $t_2 \geq t_1$, where $n = 2^{t_1}u$ and $\ell = 2^{t_2}v$ such that $2 \nmid u, v$*;

(4) *ℓ is odd, n is odd and $p \equiv 1 \pmod 4$.*

Proof. The case $\ell = 0$ is trivial. In the case of $\ell \neq 0$, if the exponent $\dfrac{p^\ell+1}{2}$ is even, $\gcd\left(\dfrac{p^\ell+1}{2}, p^n - 1\right) \geq 2$ and thus, the power map $X^{\frac{p^\ell+1}{2}}$ is not a permutation of $\mathbb{F}_{p^n}$. We shall, therefore, consider the case when $\dfrac{p^\ell+1}{2}$ is odd. It is easy to see that $\dfrac{p^\ell+1}{2}$ is odd if and only if ℓ is even or ℓ is odd and $p \equiv 1 \pmod 4$. If we assume that $\dfrac{p^\ell+1}{2}$ is odd, then a direct application of Lemma 3.1.3 shows that $X^{\frac{p^\ell+1}{2}}$ is a permutation of $\mathbb{F}_{p^n}$ if and only if $\gcd\left(\dfrac{p^\ell+1}{2}, p^n - 1\right) = 1$, that is, $\gcd\left(p^\ell + 1, p^n - 1\right) = 2$, which is equivalent to $\dfrac{n}{\gcd(\ell, n)}$ is odd. Further, under the assumption that $\dfrac{p^\ell+1}{2}$ is odd, we observe that $\dfrac{n}{\gcd(\ell, n)}$ is odd if and only if one of later three conditions of the statement of the theorem holds and hence, the theorem is proved. □

Although the map $X^{\frac{p^\ell+1}{2}}$ is a permutation of $\mathbb{F}_{p^n}$ when both ℓ, n are odd and $p \equiv 1 \pmod 4$, the following theorem tells that it ceases to be perfect (-1)-nonlinear over $\mathbb{F}_{p^n}$ (compare with [48, Theorem 8]).

Theorem 11. *If both ℓ, n are odd and $p \equiv 1 \pmod 4$, then the power map $X^{\frac{p^\ell+1}{2}}$ is not perfect (-1)-nonlinear over $\mathbb{F}_{p^n}$.*

Proof. Since ℓ is odd and $p \equiv 1 \pmod 4$, $\dfrac{p^\ell+1}{2}$ is odd. Now, by a direct application of Lemma 3.1.1, Theorem 9 and Lemma 3.1.2 at the appropriate places, we obtain the following equivalence

$$
\begin{aligned}
& X^{\frac{p^\ell+1}{2}} \text{ is P}c\text{N over } \mathbb{F}_{p^n} \\
\iff & (X+1)^{\frac{p^\ell+1}{2}} + (X-1)^{\frac{p^\ell+1}{2}} \text{ is a permutation of } \mathbb{F}_{p^n} \\
\iff & D_{\frac{p^\ell+1}{2}}\left(X, \frac{1}{4}\right) \text{ is a permutation of } \mathbb{F}_{p^n}, \forall\ 1 \leq \ell < n \\
\iff & \gcd\ \left(\frac{p^\ell+1}{2}, p^{2n}-1\right) = 1 \\
\iff & \gcd\ \left(p^\ell+1, p^{2n}-1\right) = 2 \\
\iff & \frac{2n}{\gcd\ (\ell, 2n)} \text{ is odd.}
\end{aligned}
$$

But since ℓ and n are odd, $\dfrac{2n}{\gcd\ (\ell, 2n)}$ is never odd and we are done. □

In view of Theorem 11, it remains to check perfect (-1)-nonlinearity of the map $X^{\frac{p^\ell+1}{2}}$ only under the first three conditions of Theorem 10 which essentially make it a permutation of $\mathbb{F}_{p^n}$. Notice that the first three conditions of Theorem 10 have a common property that ℓ is even. Thus, it makes sense to assume that ℓ is even and prove the following theorem that gives necessary and sufficient conditions on ℓ and n for which the power map $X^{\frac{p^\ell+1}{2}}$ is perfect (-1)-nonlinear over $\mathbb{F}_{p^n}$ (compare with [48, Theorem 8], which also investigates the map).

Theorem 12. *The power map $X^{\frac{p^\ell+1}{2}}$ is perfect (-1)-nonlinear over $\mathbb{F}_{p^n}$ if and only if any one of the following conditions holds*:

(1) $\ell = 0$;

(2) *ℓ even and n odd*;

(3) *ℓ even and n even together with $t_2 \geq t_1 + 1$, where $n = 2^{t_1}u$ and $\ell = 2^{t_2}v$ such that $2 \nmid u, v$.*

Proof. From Theorem 10 and Theorem 11, it is clear that we need to check the perfect (-1)-nonlinearity of the map $X^{\frac{p^\ell+1}{2}}$ only when ℓ is even. The case $\ell = 0$ is trivial. Suppose $\ell \neq 0$. Since ℓ is even, $\dfrac{p^\ell+1}{2}$ is odd. Now by the similar arguments as in the proof of Theorem 11 based on Lemma 3.1.1, Theorem 9 and Lemma 3.1.2 , we arrive at the following

$$X^{\frac{p^\ell+1}{2}} \text{ is P}c\text{N over } \mathbb{F}_{p^n} \text{ if and only if } \frac{2n}{\gcd\ (\ell, 2n)} \text{ is odd.}$$

It is easy to see that $\dfrac{2n}{\gcd\ (\ell, 2n)}$ is odd if and only if one of the latter two conditions of the statement of the theorem is true and thus, we are done. □

Remarks 3.1.6. Observe that Theorem 12 gives a simpler proof of [61, Theorem 5], which, in turn, provides a simpler proof of a conjecture of Bartoli and Timpanella [1, Conjecture 4.7], already settled in [61].

3.2 Power Maps with Low (-1)-Differential Uniformity

Due to their wide range of applications in symmetric key cryptography, functions with low differential uniformity are very important objects. In this section, we give some classes of power maps (monomials) with low cDU for $c = -1$. We first recall a useful lemma [40] related to the Dickson polynomial of the first kind, which is more general than Lemma 3.1.2 (see [44]).

Lemma 3.2.1. *[40, Proposition 41] Let $a \in \mathbb{F}_{p^n}^*$, and let $D_d(X, a)$ be the Dickson polynomial of the first kind. Then $D_d(X, a)$ is an m-to-1 function over $\mathbb{F}_{p^n}$ if and only if* $\gcd\left(d, p^{2n} - 1\right) = m$.

Now, we shall prove the following theorem that gives (-1)-differential uniformity of the map $X^{\frac{p^\ell+1}{2}}$ over $\mathbb{F}_{p^n}$ under certain restrictions. Riera et al. [48] found the (-1)-uniformity of this map in its generality, but with much more effort, so we thought that

the following simpler approach in the next theorem is worth including here, albeit the result being weaker.

Theorem 13. *Let $X^{\frac{p^\ell+1}{2}}$ be a power map from $\mathbb{F}_{p^n}$ to itself and $\gcd(\ell, 2n) = 1$, p an odd prime. If $p \equiv 1 \pmod 4$, or $p \equiv 3 \pmod 8$, then the (-1)-differential uniformity of $X^{\frac{p^\ell+1}{2}}$ over $\mathbb{F}_{p^n}$ is $\frac{p+1}{2}$.*

Proof. Since $\gcd(\ell, 2n) = 1$, ℓ is odd. Thus, $p \equiv 1 \pmod 4$ implies that $p^\ell + 1 \equiv 2 \pmod 4$, i.e, $\frac{p^\ell+1}{2}$ is odd (we will only show the first claim as the second is rather similar: we, however, use that if $p \equiv 3 \pmod 8$ implies that $p^\ell + 1 \equiv 4 \pmod 8$, that is, $\frac{p^\ell+1}{4}$ is odd). Now we will show that for all $a, b \in \mathbb{F}_{p^n}$, the following equation

$$(X + a)^{\frac{p^\ell+1}{2}} + X^{\frac{p^\ell+1}{2}} = b \tag{3.4}$$

has at most $\frac{p+1}{2}$ solutions in $\mathbb{F}_{p^n}$. We first consider the case when $a = 0$. In this case, Equation (3.4) can have at most $\gcd\left(\frac{p^\ell+1}{2}, p^n - 1\right)$ roots. By Lemma 3.1.3, if n is odd, then $\gcd\left(p^\ell + 1, p^n - 1\right) = 2$ and if n is even, then $\gcd\left(p^\ell + 1, p^n - 1\right) = p+1$. Therefore, $\gcd\left(\frac{p^\ell+1}{2}, p^n - 1\right) = 1$ for n odd and $\gcd\left(\frac{p^\ell+1}{2}, p^n - 1\right) = \frac{p+1}{2}$ for n even. Thus, for $a = 0$, Equation (3.4) can have at most $\frac{p+1}{2}$ solutions. We can be more precise: for $a = 0$, then Equation (3.4) has one solution for n odd and exactly $\frac{p+1}{2}$ solutions for n even for some b, and we argue that below. Let α be a primitive root in $\mathbb{F}_{p^n}$ and $\frac{b}{2} = \alpha^k$, for some k. With $X = \alpha^Y$, Equation (3.4) becomes $\alpha^{\frac{p^\ell+1}{2}Y} = \alpha^k$. We are reduced to the equation

$$\frac{p^\ell+1}{2}Y \equiv k \pmod{p^n - 1}. \tag{3.5}$$

If $\gcd\left(\frac{p^\ell+1}{2}, p^n - 1\right) = m \in \left\{1, \frac{p+1}{2}\right\}$, then Equation (3.5) has solutions if and only if $m \mid k$, and under that assumption, using elementary number theory, there are exactly m solutions Y for Equation (3.5), and they are $Y_0, Y_0 + \frac{p^n-1}{m}, Y_0 + 2\frac{p^n-1}{m}, \ldots, Y_0 + (m-1)\frac{p^n-1}{m}$, where $Y_0 \equiv \frac{k}{m}\left(\frac{p^\ell+1}{2m}\right)^{-1} \pmod{\frac{p^n-1}{m}}$, thus inferring our claim (those b for which we have the claim are of the form $b = 2\alpha^k$, with $k \equiv 0 \pmod m$).

In the case of $a \neq 0$, we can take $a = 1$ in (3.4). After relabelling, it is equivalent to

find the maximum number of solutions of the equation

$$(X+1)^{\frac{p^\ell+1}{2}} + (X-1)^{\frac{p^\ell+1}{2}} = b' \tag{3.6}$$

in $\mathbb{F}_{p^n}$, where $b' \in \mathbb{F}_{p^n}$. By Theorem 9, the above equation can be re-written as

$$D_{\frac{p^\ell+1}{2}}\left(X, \frac{1}{4}\right) = b'. \tag{3.7}$$

Now, by Lemma 3.1.3, we have $\gcd\left(p^\ell+1, p^{2n}-1\right) = p+1$ and therefore we have $\gcd\left(\dfrac{p^\ell+1}{2}, p^{2n}-1\right) = \dfrac{p+1}{2}$. Therefore, by Lemma 3.2.1, Equation (3.7) can have at most $\dfrac{p+1}{2}$ roots, however, with the bound being attained, otherwise $D_{\frac{p^\ell+1}{2}}\left(X, \frac{1}{4}\right)$ would not be m-to-1. This completes the proof. □

The following are immediate corollaries to Theorem 13.

Corollary 3.2.2. *Let $\tilde{f}(X) = X^{\frac{5^\ell+1}{2}}$ be a power function on $\mathbb{F}_{5^n}$, $\tilde{g}(X) = X^{\frac{13^\ell+1}{2}}$ on $\mathbb{F}_{13^n}$, and gcd $(\ell, 2n) = 1$. Then for $c = -1$, the c-differential uniformity of the function $\tilde{f}$ is 3 and the one of $\tilde{g}$ is 7.*

Corollary 3.2.3. *Let $\tilde{f}(X) = X^{\frac{3^\ell+1}{2}}$ be a power function on $\mathbb{F}_{3^n}$, $\tilde{g}(X) = X^{\frac{11^\ell+1}{2}}$ on $\mathbb{F}_{11^n}$, and* gcd $(\ell, 2n) = 1$. *Then for $c = -1$, $\tilde{f}$ is an APcN function (see also* [28, Thm. 10]*), and the (-1)-differential uniformity of $\tilde{g}$ is* 6.

3.3 PcN Power Functions over $\mathbb{F}_{p^5}$ with $c = -1$

In this section, first we shall prove four propositions, which will be useful in the sequel.

Proposition 3.3.1. *Let $c \in \mathbb{F}_p^*$ then the cDU of the power functions X^d and $X^{dp^j}, j \in \{0, 1, \ldots, n-1\}$ over $\mathbb{F}_{p^n}$ is the same.*

Proof. For $a, b \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned}(X+a)^d - cX^d = b &\iff X^{p^j} \circ \left((X+a)^d - cX^d\right) = X^{p^j}(b) \\ &\iff (X+a)^{dp^j} - cX^{dp^j} = e, \text{ where } X^{p^j}(b) = e \in \mathbb{F}_{p^n}.\end{aligned}$$

Since X^{p^j} is a permutation, if b runs over $\mathbb{F}_{p^n}$ then so does e. This completes the proof. □

Proposition 3.3.2. *Let $c = \pm 1$ and gcd $(d, p^n - 1) = 1$, then the cDU of the power functions X^d and $X^{d^{-1}}$ over $\mathbb{F}_{p^n}$ is the same, where d^{-1} is the inverse of d modulo $p^n - 1$.*

Proof. For any $a, b \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned}
(X+a)^d - cX^d = b &\iff (X+a)^d = (cX^d + b) \\
&\iff X + a = (cX^d + b)^{d^{-1}} \\
&\iff a = (cX^d + b)^{d^{-1}} - X \\
&\iff a = (Y+b)^{d^{-1}} - \frac{Y^{d^{-1}}}{c^{d^{-1}}}, \text{ where } Y = cX^d \\
&\iff a = (Y+b)^{d^{-1}} - cY^{d^{-1}}
\end{aligned}$$

Therefore, for $c = \pm 1$, the cDU of X^d and $X^{d^{-1}}$ over $\mathbb{F}_{p^n}$ is the same. □

Proposition 3.3.3. *Let p be an odd prime and $d' = p^4 + (p-2)p^2 + (p-1)p + 1$. Then for $c = -1$, the map $X^{d'}$ is PcN over $\mathbb{F}_{p^5}$.*

Proof. From Theorem 12, we know that for $c = -1$, $X^{\frac{p^2+1}{2}}$ is PcN over $\mathbb{F}_{p^5}$. Now since gcd $\left(\frac{p^2+1}{2}, p^5 - 1\right) = 1$, its multiplicative inverse modulo $p^5 - 1$ exists and is equal to $p^4 + (p-2)p^2 + (p-1)p + 1$. Therefore, by Proposition 3.3.2, $X^{d'}$ is a PcN over $\mathbb{F}_{p^5}$ for $c = -1$. □

In view of Proposition 3.3.1, Proposition 3.3.2 and Theorem 12, the following proposition immediately follows from the fact, stated in [61], that over $\mathbb{F}_{p^n}^*$ with n odd, $p\left(\frac{p^n+1}{p+1}\right)$ is the inverse of $\frac{p^{n-1}+1}{2}$.

Proposition 3.3.4. *Let p be an odd prime and $d = \frac{p^5+1}{p+1}$. Then for $c = -1$, X^d is PcN over $\mathbb{F}_{p^5}$.*

As an empirical support for these results, and in search of more PcN power functions for $c = -1$, we performed an exhaustive search of all possible exponents d for which X^d is PcN for $c = -1$ over the finite fields $\mathbb{F}_{3^5}$, $\mathbb{F}_{5^5}$, and $\mathbb{F}_{7^5}$, respectively. The result of this search was that d is of the form

$$p^j \left\{1, \frac{p^2+1}{2}, p^4 + (p-2)p^2 + (p-1)p + 1, \frac{p^4+1}{2}, \frac{p^5+1}{p+1}\right\}$$

for all $0 \leq j \leq 4$, for $p = 3, 5, 7$, respectively.

Based on this empirical evidence, we propose the following conjecture.

Conjecture 3.3.5. *Let p be an odd prime. Then, for $c = -1$, and for all $0 \leq j \leq 4$,*

$$p^j \left\{ 1, \frac{p^2+1}{2}, p^4 + (p-2)p^2 + (p-1)p + 1, \frac{p^4+1}{2}, \frac{p^5+1}{p+1} \right\}$$

are the only values of d for which X^d is PcN on $\mathbb{F}_{p^5}$.

3.4 PcN Power Functions over $\mathbb{F}_{p^7}$ with $c = -1$

Proposition 3.4.1. *Let p be an odd prime and $d_1 = (p-1)p^6 + p^5 + (p-2)p^3 + (p-1)p^2 + p$. Then for $c = -1$, the map X^{d_1} is a PcN map over $\mathbb{F}_{p^7}$.*

Proof. From Theorem 12, we know that for $c = -1$, $X^{\frac{p^2+1}{2}}$ is PcN map over $\mathbb{F}_{p^7}$. Now since gcd $\left(\frac{p^2+1}{2}, p^7 - 1\right) = 1$, its multiplicative inverse modulo $p^7 - 1$ exists and is equal to $(p-1)p^6 + p^5 + (p-2)p^3 + (p-1)p^2 + p$. Thus, by Proposition 3.3.2, the map X^{d_1} is PcN function over $\mathbb{F}_{p^7}$ for $c = -1$. □

Proposition 3.4.2. *Let p be an odd prime and $d_2 = (p-2)p^6 + (p-2)p^5 + (p-1)p^4 + p^3 + p^2 + p$. Then for $c = -1$, the map X^{d_2} is a PcN function over $\mathbb{F}_{p^7}$.*

Proof. From Theorem 12, we know that for $c = -1$, the power function $X^{\frac{p^4+1}{2}}$ is PcN over $\mathbb{F}_{p^7}$. Now since gcd $\left(\frac{p^4+1}{2}, p^7 - 1\right) = 1$, its multiplicative inverse modulo $p^7 - 1$ exists and is equal to $(p-2)p^6 + (p-2)p^5 + (p-1)p^4 + p^3 + p^2 + p$. Therefore. by Proposition 3.3.2, the map X^{d_2} is PcN function over $\mathbb{F}_{p^7}$ for $c = -1$. □

In view of Proposition 3.3.1, Proposition 3.3.2 and Theorem 12, the following proposition is a direct consequence of the fact that over $\mathbb{F}_{p^n}^*$ with n odd, $p\left(\frac{p^n+1}{p+1}\right)$ is the inverse of $\frac{p^{n-1}+1}{2}$.

Proposition 3.4.3. *Let p be an odd prime and $d_3 = \frac{p^7+1}{p+1}$. Then for $c = -1$, the power function X^{d_3} is PcN over $\mathbb{F}_{p^7}$.*

As an empirical support for these results, and in search of more PcN power functions for $c = -1$, we performed an exhaustive search of all possible exponents d for which X^d

is PcN for $c = -1$ over the finite fields $\mathbb{F}_{3^7}$, $\mathbb{F}_{5^7}$, and $\mathbb{F}_{7^7}$, respectively. The result of this search was that d is of the form

$$p^j\left\{1, \frac{p^2+1}{2}, ((p-1)p^6+p^5+(p-2)p^3+(p-1)p^2+p), \frac{p^4+1}{2}, \right.$$
$$\left. \frac{p^6+1}{2}, (p-2)p^6+(p-2)p^5+(p-1)p^4+p^3+p^2+p, \frac{p^7+1}{p+1}\right\}$$

for all $0 \leq j \leq 6$, for $p = 3$, 5, 7, respectively.

Conjecture 3.4.4. *Let p be an odd prime. Then for $c = -1$ and for all $0 \leq j \leq 6$,*

$$p^j\left\{1, \frac{p^2+1}{2}, ((p-1)p^6+p^5+(p-2)p^3+(p-1)p^2+p), \frac{p^4+1}{2}, \right.$$
$$\left. \frac{p^6+1}{2}, (p-2)p^6+(p-2)p^5+(p-1)p^4+p^3+p^2+p, \frac{p^7+1}{p+1}\right\}$$

are the only values of d for which X^d is PcN over $\mathbb{F}_{p^7}$.

Remarks 3.4.5. The pattern in [1, Conjecture 5.3], Conjecture 4.19 and Conjecture 4.20 appears to suggest that over a finite field $\mathbb{F}_{p^n}$, where n is odd, the positive integers in the following set

$$\left\{p^j\left\{1, \frac{p^2+1}{2}, \frac{p^4+1}{2}, \ldots, \frac{p^{n-1}+1}{2}\right\}\right\}_{j=0,1,2,\ldots,r-1}$$

and their multiplicative inverse modulo $(p^n - 1)$ are the only possible exponents d for which the power function X^d is PcN for $c = -1$. However, this is not true in general and the smallest example is $d = 29$ over the finite field $\mathbb{F}_{3^9}$. Therefore, the question about the exponents d, for which the power functions X^d are PcN over finite field $\mathbb{F}_{p^n}$, where n is odd, is not clear, even conjecturally.

3.5 Perturbations of PcN and Other Functions

After linear functions and power functions, linearized polynomials are another special class containing permutation polynomials. The following proposition gives a necessary and sufficient condition for a linearized polynomial to be PcN, similar to [20, Proposition 2.4].

Proposition 3.5.1. *Let $c \neq 1$. A linearized polynomial L is PcN over $\mathbb{F}_{p^n}$ if and only if L is a permutation polynomial if and only if its only root in $\mathbb{F}_{p^n}$ is zero.*

Proof. Recall that a linearized polynomial $L(X)$ over finite field $\mathbb{F}_{p^n}$ is a polynomial of the form $\sum_{i=0}^{n-1} a_i X^{p^i}$. Now consider the difference function

$$\begin{aligned} {}_cD_L(X,a) &= L(X+a) - cL(X) \\ &= \sum_{i=0}^{n-1} a_i (X+a)^{p^i} - c \cdot \sum_{i=0}^{n-1} a_i X^{p^i} \\ &= (1-c) \cdot \sum_{i=0}^{n-1} a_i X^{p^i} + \sum_{i=0}^{n-1} a_i a^{p^i}. \end{aligned}$$

Now, if the only root of $L(X)$ in $\mathbb{F}_{p^n}$ is zero, then $L(X)$ is a permutation polynomial. Now since $c \neq 1$, the difference function ${}_cD_L$ being an affine linearized polynomial is also a permutation polynomial and hence $L(X)$ is PcN. □

Corollary 3.5.2. *Let $c \neq 1$. The binomial $f(X) = X^{p^j} - aX^{p^i}$, $0 \leq i < j$, is a PcN function over $\mathbb{F}_{p^n}$ if and only if a is not a $(p^{j-i}-1)$-st power in $\mathbb{F}_{p^n}$ and $c \neq 1$.*

Proof. If a is not a $(p^{j-i}-1)$-th power in $\mathbb{F}_{p^n}$ then the only root of $f(X)$ in $\mathbb{F}_{p^n}$ is 0 and hence $f(X)$ is a linearized permutation polynomial and the result follows from Proposition 3.5.1. □

It is not a simple matter to characterize when a perturbation of a function with some specific property is preserved. We can, however, characterize when the sum of a PcN and an arbitrary p-ary function is also PcN (for $1 \neq c \in \mathbb{F}_p$), thus extending in some direction the previous corollary.

Theorem 14. *Let $1 \neq c \in \mathbb{F}_p$ be fixed, p odd. Let f be a PcN function, and F be an arbitrary p-ary function, both on $\mathbb{F}_{p^n}$. Then, $f + \gamma F$ is PcN if and only if for any $\lambda \in \mathbb{F}_{p^n}$ with $\mathrm{Tr}(\gamma\lambda) = \beta \in \mathbb{F}_p^*$, the following is true*

$$\mathcal{W}_{R_a}(-\lambda, \beta) = \sum_{Y \in \mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}(\beta R_a(Y) + \lambda Y)} = 0,$$

where ζ is a p-root of unity, $R_a = H_a \circ G^{-1}$, ${}_cD_F(X,a) = \mathrm{Tr}(H_a(X))$ (H_a is non-unique) and G^{-1} is the compositional inverse of $G = {}_cD_f(X,a)$.

Proof. Certainly, $f + \gamma F$ is PcN if and only if

$$\begin{aligned} & f(X+a) + \gamma F(X+a) - cf(X) - c\gamma F(X) \\ &= f(X+a) - cf(X) + \gamma(F(X+a) - cF(X)) \\ &= {}_cD_f(X,a) + \gamma \cdot {}_cD_F(X,a) \end{aligned}$$

is a permutation polynomial.

We now write ${}_cD_F(X,a) = \mathrm{Tr}(H_a(X))$, for some (non-unique) function H_a on $\mathbb{F}_{p^n}$ (since $c \in \mathbb{F}_p$, if F is p-ary, then ${}_cD_F(X,a)$ is p-ary, and such H_a does exists). We then use [18, Theorem 2], which states that if G is a permutation and H is arbitrary, then $G(X) + \gamma\mathrm{Tr}(H(X))$ is a permutation polynomial if and only if for any $\lambda \in \mathbb{F}_{p^n}$ with $\mathrm{Tr}(\gamma\lambda) = \beta \in \mathbb{F}_p^*$ then $\sum_{Y \in \mathbb{F}_{p^n}} \zeta^{\mathrm{Tr}(\beta R(Y) + \lambda Y)} = 0$, where $R = H \circ G^{-1}$. Our theorem is shown. □

What can we say about a Boolean perturbation of a non-permutation? Let $f = L + \gamma F$. From [18, Proposition 3], we know that if f is a PP then the linearized polynomial L on $\mathbb{F}_{p^n}$ must be a permutation or a p-to-1 map (surely, in general a linearized polynomial can have a kernel with dimension higher than 1, but the quoted result shows that if L is a p^s-to-1 ($s > 1$) function, then f cannot be a PP). We denote by $\mathrm{Im}(L) = \{L(X) \,|\, X \in \mathbb{F}_{p^n}\}$, the image of the map L. If L is a permutation polynomial, then Theorem 14 applies, so we consider the case of a p-to-1 linearized polynomial.

Theorem 15. *Let $1 \neq c \in \mathbb{F}_p$, L be a p-to-1 linearized polynomial on $\mathbb{F}_{p^n}$ and F an arbitrary p-ary function, and let $f = L + \gamma F$ be a permutation polynomial. Then $f = L + \gamma F$ is PcN if and only if both of the following conditions are satisfied for all $a \in \mathbb{F}_{p^n}^*$:*

(i) $\gamma \notin \mathrm{Im}(L)$*;*

(ii) ${}_cD_F(X+\epsilon, a) - {}_cD_F(X,a) \neq 0$*, for all* $X \in \mathbb{F}_{p^n}$*,* $\epsilon \in \mathrm{Ker}(L)^*$*.*

Proof. Let $a \in \mathbb{F}_{p^n}^*$ and $1 \neq c \in \mathbb{F}_p$. Notice that

$$\begin{aligned} {}_cD_L(X,a) &= L(X+a) - cL(X) \\ &= (1-c)L(X) + L(a) \\ &= L((1-c)X + a). \end{aligned}$$

Therefore, $\mathrm{Im}({}_cD_L) \subseteq \mathrm{Im}(L)$. Further, as we know, f is PcN if and only if

$$ {}_cD_f(X,a) = {}_cD_L(X,a) + \gamma\, {}_cD_F(X,a) = L((1-c)X+a) + \gamma(F(X+a) - cF(X)) $$

is a permutation polynomial.

We now slightly modify the proof of [18, Theorem 4], since, as it is, it cannot be applied directly for our case. Further, observe that

$$ {}_cD_f(X,a) = \begin{cases} L((1-c)X+a) & \text{if } F(X+a)-cF(X) = 0; \\ L((1-c)X+a) + \gamma d & \text{if } F(X+a)-cF(X) = d \in \mathbb{F}_p^*. \end{cases} $$

If $\gamma \in \mathrm{Im}(L)$, then $\gamma = L(\alpha)$, $\alpha \in \mathbb{F}_{p^n}$, and for $d \in \mathbb{F}_p^*$, $\gamma d = dL(\alpha) = L(d\,\alpha)$. Therefore, the image set of ${}_cD_f(X,a)$ is contained in the image set of L. Consequently, ${}_cD_f(X,a)$ cannot be a permutation as L is a p-to-1 function. Thus, we can assume that $\gamma \notin \mathrm{Im}(L)$. For any $\epsilon \in \mathrm{Ker}(L)^*$, we have

$$ \begin{aligned} &{}_cD_f(X+\epsilon,a) - {}_cD_f(X,a) \\ &= L((1-c)(X+\epsilon)+a) - L((1-c)X+a) + \gamma({}_cD_F(X+\epsilon,a) - {}_cD_F(X,a)) \\ &= L((1-c)\epsilon) + \gamma({}_cD_F(X+\epsilon,a) - {}_cD_F(X,a)) \\ &= \gamma({}_cD_F(X+\epsilon,a) - {}_cD_F(X,a)) \end{aligned} $$

Thus, if ${}_cD_f$ is a permutation, then ${}_cD_F(X+\epsilon,a) - {}_cD_F(X,a)$ has to be non-zero for all $X \in \mathbb{F}_{p^n}$ and $\epsilon \in \mathrm{Ker}(L)^*$.

Conversely, we assume that (i) and (ii) hold. Let $Y, Z \in \mathbb{F}_{p^n}$ such that ${}_cD_f(Y,a) = {}_cD_f(Z,a)$. Thus

$$ \begin{aligned} {}_cD_f(Y,a) - {}_cD_f(Z,a) &= 0 \\ L((1-c)(Y-Z)) + \gamma({}_cD_F(Y,a) - {}_cD_F(Z,a)) &= 0. \end{aligned} $$

Let $Y - Z = \epsilon$, then the above equation reduces to

$$ (1-c)L(\epsilon) + \gamma\,({}_cD_F(Z+\epsilon,a) - {}_cD_F(Z,a)) = 0. $$

If $\epsilon \in \mathrm{Ker}(L)$, then by condition (ii), $\epsilon = 0$, forcing $Y = Z$. If $\epsilon \notin \mathrm{Ker}(L)$, then ${}_cD_F(Y,a) - {}_cD_F(Z,a) = \tilde{d} \in \mathbb{F}_p^*$, so $0 = (1-c)L(Y-Z) + \gamma\tilde{d}$, contradicting the fact that $\gamma \notin \mathrm{Im}(L)$. □

We shall use below some results of [17, Theorem 3] and [18, Corollary 1].

Theorem 16. *Let p be a prime number, $\beta, \gamma \in \mathbb{F}_{p^n}$ and $H \in \mathbb{F}_{p^n}[X]$. Then the polynomial*

$$f(X) = X + \gamma \mathrm{Tr}(H(X^p - \gamma^{p-1}X) + \beta X)$$

is a permutation polynomial if and only if $\mathrm{Tr}(\beta\gamma) \neq -1$.

(Surely, if $p = 2$, the trace condition is $\mathrm{Tr}(\beta\gamma) = 0$.) We are now ready to show the next result, where we construct a class of (linearized) polynomials that are PcN for every $c \neq 1$, in all characteristics.

Proposition 3.5.3. *Let p be a prime number, $\alpha, \gamma \in \mathbb{F}_{p^n}$. Then $f(X) = X + \gamma \mathrm{Tr}(X^p - \alpha X)$ is PcN for all $c \neq 1$ if and only if* $\mathrm{Tr}(\gamma(1-\alpha)) \neq -1$.

Proof. The c-differential of f at a is now

$$\begin{aligned} {}_cD_f(X,a) &= f(X+a) - cf(X) \\ &= X + a + \gamma \mathrm{Tr}\left(X^p + a^p - \alpha X - \alpha a\right) - cX - \gamma c \mathrm{Tr}(X^p - \alpha X) \\ &= (1-c)X + (1-c)\gamma \mathrm{Tr}(X^p - \alpha X) + a + \gamma \mathrm{Tr}(a^p - \alpha a). \end{aligned}$$

Thus, f is PcN if and only if $(1-c)X + (1-c)\gamma \mathrm{Tr}(X^p - \alpha X) + a + \gamma \mathrm{Tr}(a^p - \alpha a)$ is PP for all a, which is equivalent to $(1-c)X + (1-c)\gamma \mathrm{Tr}(X^p - \alpha X)$ being a PP, and further, $X + \gamma \mathrm{Tr}(X^p - \alpha X)$ being a PP. Now, we re-write the previous function as $X + \mathrm{Tr}\left(X^p - \gamma^{p-1}X + (\gamma^{p-1} - \alpha)X\right)$. Using Theorem 16 with $\beta = \gamma^{p-1} - \alpha$, we see that the last claim will hold if and only if $\mathrm{Tr}\left(\gamma\left(\gamma^{p-1} - \alpha\right)\right) = \mathrm{Tr}\left(\gamma^p\right) - \mathrm{Tr}\left(\gamma\alpha\right) = \mathrm{Tr}(\gamma(1-\alpha)) \neq -1$. □

We saw that some modifications of PcN functions preserve their perfect c-nonlinearity. It surely makes sense to ask whether the cDU is preserved through affine, extended affine or CCZ-equivalence [13]. Given a function f, we call the set $\{\beta_{f,c} \,|\, c \in \mathbb{F}_{p^n}\}$, the differential

spectrum of f. We ask here the question of whether that the c-differential uniformity spectra is preserved under the A-equivalence, EA-equivalence, or CCZ-equivalence. Our guess was that it is not preserved by EA, nor CCZ-equivalence, and an easy computation via SageMath confirmed it: while X^3 has c-differential spectrum $[1, 2, 3]$, the EA-equivalent function $X^3 + X^4$ has c-differential spectrum $[1, 2, 3, 4]$, both on $\mathbb{F}_{2^4}$.

It is not difficult to show that the differential spectrum is invariant under the (restricted to input) affine-equivalence (A-equivalence) (recall that f, f' on $\mathbb{F}_{p^n}$ are restricted to input A-equivalent if $f'(X) = f \circ \mathcal{L}(X)$, where $\mathcal{L}$ is an affine permutation on $\mathbb{F}_{p^n}$), and we provide the argument next. The equation $f'(X + a) - cf'(X) = b$ is equivalent to $(f \circ \mathcal{L})(X + a) - c(f \circ \mathcal{L})(X) = b$, that is $f(\mathcal{L}(X) + \mathcal{L}(a)) - cf(\mathcal{L}(X)) = b$. Setting $\mathcal{L}(X) = Y, \mathcal{L}(a) = \alpha$, the previous equation becomes $f(Y + \alpha) - cf(Y) = b$. Surely, any solution of $f'(X + a) - cf'(X) = b$ is in one-to-one correspondence to a solution of $f(Y + \alpha) - cf(Y) = b$, since $\mathcal{L}$ is invertible.

Since the CCZ-equivalence is more general than EA-equivalence, we shall concentrate on it. Recall that two (n, m)-functions f, f' from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ are CCZ-equivalent if and only if their graphs $G_f = \{(X, f(X)) \,|\, X \in \mathbb{F}_{p^n}\}$, $G_{f'} = \{(X, f'(X)) \,|\, X \in \mathbb{F}_{p^n}\}$ are affine equivalent, that is, there exists an affine permutation $\mathcal{A}$ on $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ such that $\mathcal{A}(G_f) = G_{f'}$.

As in [13], we use the identification of the elements in $\mathbb{F}_{p^n}$ with the elements in $\mathbb{F}_p^n$, and denote by X both an element in $\mathbb{F}_{p^n}$ and the corresponding element in $\mathbb{F}_p^n$. We first decompose the affine permutation $\mathcal{A}$ as an affine block-matrix, $\mathcal{A}\mathbf{u} = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \mathbf{u} + \begin{pmatrix} c \\ d \end{pmatrix}$, for an input vector $\mathbf{u}$, where $\mathcal{A}_{11}, \mathcal{A}_{21}, \mathcal{A}_{12}, \mathcal{A}_{22}$ are $n \times n$ matrices with entries in $\mathbb{F}_p$, and $\begin{pmatrix} c \\ d \end{pmatrix}$ is a column vector in $\mathbb{F}_{p^{2n}}$ (just a reminder to the reader that EA-equivalence means that $\mathcal{A}_{12} = 0$ and (full-fledged) A-equivalence means that $\mathcal{A}_{12} = \mathcal{A}_{21} = 0$). Fix $c \in \mathbb{F}_{p^n}$, and let the c-differential system be written as $Y - X = a, f(Y) - cf(X) = b$.

Applying the affine permutation $\mathcal{A}$ to $\binom{a}{b}$ we get

$$\begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} Y - X \\ f(Y) - cf(X) \end{pmatrix}$$

$$= \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} Y \\ f(Y) \end{pmatrix} - \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} X \\ cf(X) \end{pmatrix}$$
$$= \begin{pmatrix} Y' \\ f'(Y') \end{pmatrix} - \begin{pmatrix} \mathcal{A}_{11} & c \cdot \mathcal{A}_{12} \\ \mathcal{A}_{21} & c \cdot \mathcal{A}_{22} \end{pmatrix} \begin{pmatrix} X \\ f(X) \end{pmatrix}.$$

We see that it is not obvious how the second term can be transformed into a pair $\binom{X'}{c^* f'(X')}$ of the graph $G_{f'}$, unless f and f' are also CCZ-equivalent also via an affine transformation whose linear part is a constant multiple of $\begin{pmatrix} \mathcal{A}_{11} & c \cdot \mathcal{A}_{12} \\ \mathcal{A}_{21} & c \cdot \mathcal{A}_{22} \end{pmatrix}$.

We summarize this discussion in the next theorem.

Theorem 17. *Let f, f' be CCZ-equivalent via an affine transformation $\mathcal{A} = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix}$ and also via $\begin{pmatrix} \frac{1}{c^*} \cdot \mathcal{A}_{11} & \frac{c}{c^*} \cdot \mathcal{A}_{12} \\ \frac{1}{c^*} \cdot \mathcal{A}_{21} & \frac{c}{c^*} \cdot \mathcal{A}_{22} \end{pmatrix}$. Then the c-differential uniformity of f is the same as the c^*-differential uniformity of f'.*

With the above discussion, we see that the cDU may change under EA or CCZ-equivalence. Keeping that in mind, we now switch directions a bit and ask whether we can perturb some APcN functions, via a linear/linearized map, thereby obtaining a PcN function. This is in line with the long standing open question on whether some of the known PN or APN functions can be transformed into PN or APN permutation functions by perturbing them via some linear mapping. We will only treat here the Gold case, $f(X) = X^{p^k+1}$. From [28] we know that f is PcN only for $c = 1$ (under $\frac{n}{\gcd(n,k)}$ odd), when $p > 2$, and it is never PcN for $c \neq 1$. The case of $p = 2$ was treated in [48].

Theorem 18. *Let $k \geq 1, n \geq 2$ be integers, p prime, $c \neq 1$ in $\mathbb{F}_{p^n}$. The following are true:*

(i) If $G_1(X) = X^{p^k+1} + \gamma \mathrm{Tr}(X)$ is PcN for $\gamma \in \mathbb{F}_{p^n}^*$, then

$$\gamma \notin \left\{ -\frac{a^{p^k+1}}{\mathrm{Tr}\left(\frac{a}{1-c}\right)(1-c)^2}, \,\middle|\, a \in \mathbb{F}_{p^n}^*, \mathrm{Tr}\left(\frac{a}{1-c}\right) \neq 0 \right\}.$$

(ii) The function $G_2(X) = X^{p^k+1} + \gamma X^{p^k}$ is never PcN, regardless of the value of $\gamma \in \mathbb{F}_{p^n}^*$.

Proof. (i) We first perturb f in the following way $G_1(X) = f(X) + \gamma \mathrm{Tr}(X)$, $\gamma \neq 0$, and attempt to find some condition on γ such that G_1 can potentially be PcN. We look at the c-differential equation of G_1, namely

$$(1-c)X^{p^k+1} + a\,X^{p^k} + a^{p^k}X + a^{p^k+1} + \gamma(1-c)\mathrm{Tr}(X) + \gamma\mathrm{Tr}(a) = b,$$

that is,

$$X^{p^k+1} + \frac{a}{1-c}X^{p^k} + \frac{a^{p^k}}{1-c}X + \gamma\mathrm{Tr}(X) = \frac{b - \gamma\mathrm{Tr}(a) - a^{p^k+1}}{1-c}.$$

By relabeling (since the free term is linear in b), it will be sufficient to investigate the equation

$$X^{p^k+1} + \frac{a}{1-c}X^{p^k} + \frac{a^{p^k}}{1-c}X + \gamma\mathrm{Tr}(X) = b.$$

We argue now that in many instances the equation has more than one solution. We let $b = 0$. Surely, $X = 0$ is one such solution. We write (for $a \neq 0$)

$$X^{p^k}\left(X + \frac{a}{1-c}\right) + \frac{a^{p^k}}{1-c}\left(X + \frac{\gamma(1-c)}{a^{p^k}}\mathrm{Tr}(X)\right) = 0.$$

Now, $X = -\frac{a}{1-c} \neq 0$ is another solution if $\frac{\gamma(1-c)}{a^{p^k}}\mathrm{Tr}\left(-\frac{a}{1-c}\right) = \frac{a}{1-c}$, or, equivalently, $\mathrm{Tr}\left(\frac{a}{1-c}\right) = -\frac{a^{p^k+1}}{\gamma(1-c)^2}$. We obviously need $\frac{a^{p^k+1}}{\gamma(1-c)^2} \in \mathbb{F}_p^*$, for some a, which is equivalent to the first claim.

(ii) Next, we perturb f as $G_2(X) = f(X) + \gamma\, X^{p^k}$, $\gamma \neq 0$. As before, the c-differential equation of G_2 is then

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

or, by relabeling $\frac{b - a^{p^k+1} - \gamma a^{p^k}}{1-c} \mapsto b$

$$X^{p^k+1} + \frac{a + \gamma(1-c)}{1-c}\,X^{p^k} + \frac{a^{p^k}}{1-c}X = b.$$

If $b = 0$, then $X = 0$ is a solution. Assuming $b = 0, X \neq 0, a \neq 0$, factoring out X, and

using $Y = \frac{1}{X}$, we get

$$Y^{p^k} + \frac{a + \gamma(1-c)}{a^{p^k}} Y + \frac{1-c}{a^{p^k}} = 0.$$

It is easy to show that taking $a = \gamma(c-1)$, then $Y = \left(\frac{c-1}{a^{p^k}}\right)^{p^{-k}}$ (which always exists, since $\gcd(p^k, p^n - 1) = 1$) is a solution of the above equation, and hence $X = \left(\frac{a^{p^k}}{c-1}\right)^{p^{-k}}$ is a solution of the original equation in X. Hence ${}_cD_{G_2}(X, a)$ is not a permutation, and therefore, G_2 is not PcN, for $c \neq 1$. □

Surely, the question is whether $G_1(X) = X^{2^k+1} + \gamma \mathrm{Tr}(X)$ is ever PcN over $\mathbb{F}_{2^n}$. We quickly took some small examples of $\mathbb{F}_{2^n}$, $2 \leq n \leq 4$, determined by the primitive polynomials $X^2 + X + 1$, $X^3 + X + 1$, $X^4 + X + 1$ over $\mathbb{F}_2$, all with some primitive root α. We then checked that $G_1(X) = X^{2^k+1} + \gamma \mathrm{Tr}(X)$ is never PcN on $\mathbb{F}_{2^n}$, for $2 \leq k < n \leq 4$. If $k = n$, we can get PcN functions. For the considered cases, if $(k, n) = (2, 2)$, G_1 is PcN when $(c, \gamma) = (0, 1), (\alpha, 1), (\alpha^2, 1)$; if $(k, n) = (3, 3)$, G_1 is PcN when $(c, \gamma) = (c, \alpha), (c, \alpha^2), (c, \alpha^4)$, since the function G_1 becomes a linearized polynomial (via $X^{2^n+1} = X^2$ on $\mathbb{F}_{2^n}$). We do not have other examples for small dimensions. The computation was done via SageMath.

Chapter 4

The c-Differential Uniformity and Boomerang Uniformity of Some Permutation Polynomials

In this chapter, we consider the cDU and BU of two classes of PPs over finite fields of even characteristic, introduced by Beierle and Leander [3], respectively, Tan et al. [55]. First, we shall recall some definitions and results, which will be used throughout this chapter, in Section 4.1. In Section 4.2, we shall consider cDU of an involution over finite field $\mathbb{F}_{2^n}$, which has been used to construct a class of differentially 4-uniform function in [3] and shall show that it is APcN for all $c \in \mathbb{F}_{2^n}$, $c \neq 0, 1$. Moreover, we shall also give the cDDT entries of this involution, for all $c \in \mathbb{F}_q$, $c \neq 0, 1$, using the Weil sum technique used in [54, 52]. In Section 4.3, we shall give a complete description of the BCT entries of the involution and show that there are only two entries in the BCT. The cDU of the differentially 4-uniform function studied by Tan et al. [55], has been considered in Section 4.4. A bound for the BU of this function will be given in Section 4.5.

4.1 Preliminaries

In the study of finite fields, PPs are very important objects as they are used in variety of theoretical and practical applications. Therefore, construction of infinite classes of PPs over finite fields is an interesting problem and a lot of research has been done in this

direction in recent years. A PP $f(X)$ is called complete permutation polynomial (CPP) if both $f(X)$ and $f(X) + X$ are permutations. In view of the definition of CPP, an interesting problem is to add some simple functions in a given PP and to check for its permutation behaviour.

Recently, Beierle and Leander [3] considered the perturbation of a linear function by a trace function and showed that it is an involution. More precisely, authors showed that the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where $\mathrm{Tr}(\alpha) = 1$ and $\gcd(k, n) = 1$ is an involution of finite field $\mathbb{F}_{2^n}$, $n \geq 3$ odd. Here, Tr is the absolute trace function. Recall that the power function $f(X) = X^{2^k+1}$ over $\mathbb{F}_{2^n}$, $0 \leq k < n$ is the Gold function [31] and if $\gcd(k, n) = \gcd(2k, n)$, it is a permutation of $\mathbb{F}_{2^n}$. Nyberg [45] showed that when $\gcd(k, n) = s$, the Gold function is differentially 2^s-uniform. Thus, when $\gcd(k, n) = 1$ and n odd, the Gold function is an APN permutation. Beierle and Leander [3] considered the composition of the involution $G(X)$ with the monomial X^ℓ, where $\ell = (2^k + 1)^{-1} \pmod{2^n - 1}$ with $\gcd(k, n) = 1$, and showed that it is a differentially 4-uniform permutation with trivial nonlinearity 0. More precisely, authors proved the following result.

Lemma 4.1.1. *[3, Proposition 1] Let $n \geq 3$ is odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$ and $\ell = (2^k+1)^{-1} \pmod{2^n-1}$ with $\gcd(k, n) = 1$. Then the function $G_{\alpha,\ell}(X) = X^\ell + \mathrm{Tr}(\alpha X^\ell + X)$ is a differentially 4-uniform permutation with null nonlinearity over $\mathbb{F}_{2^n}$.*

We explicitly determine the cDDT entries of the involution $G(X)$ for all $c \in \mathbb{F}_{2^n}$ in Section 4.2. Moreover, we compute BCT entries of the involution $G(X)$ in Section 4.3.

We shall now turn our focus towards another interesting function. A systematic study of permutation behaviour of the functions of the form $f(X) = g(X) + \gamma \mathrm{Tr}(h(X))$ has been done by Charpin and Kyureghyan [18] where authors gave necessary conditions on $\gamma \in \mathbb{F}_{2^n}$, $g, h \in \mathbb{F}_{2^n}[X]$ for which $g(X) + \gamma \mathrm{Tr}(h(X))$ is a permutation polynomial. More precisely, authors gave the following two classes of permutation polynomials.

Lemma 4.1.2. *[18, Corollary 1] For any $\beta, \gamma \in \mathbb{F}_{2^n}$ and $h(X) \in \mathbb{F}_{2^n}[X]$, the polynomials*

(1) $f_1(X) = X + \gamma \mathrm{Tr}(h(X^2 + \gamma X) + \beta X)$; *and*

(2) $f_2(X) = X + \gamma \mathrm{Tr}(h(X) + h(X + \gamma) + \beta X)$

are permutation polynomials if and only if $\mathrm{Tr}(\beta\gamma) = 0$.

From the above lemma, it is easy to see that if $\beta = 0, \gamma = 1$ and $h(X) = X^{-1}$, the function $f_1'(X) = X + \mathrm{Tr}\left(\frac{1}{X^2+X}\right)$ is a permutation of $\mathbb{F}_{2^n}$. Tan et al. [55] showed that when n is even, the permutation polynomial $H(X) = f_1'(X) \circ X^{-1} = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ is differentially 4-uniform. Recall that when n is even, the inverse mapping X^{-1} is a differentially 4-uniform permutation of $\mathbb{F}_{2^n}$ (see [45, Proposition 6]). Thus, the permutation behaviour and DU remain the same even after adding the term $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ in the inverse mapping X^{-1}. The cDU of the inverse function has been studied by Ellingsen et al. [28]. In Section 4.4, we shall consider the cDU of the function $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$ for $1 \neq c \in \mathbb{F}_{2^n}$, to see the effect of the addition of the trace term $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ on cDU. We shall also consider the BU of the function $H(X)$ in Section 4.5.

We shall later use the following result [28, Lemma 11].

Lemma 4.1.3. *Let n be a positive integer. 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.*

With regard to inverses of elements in the finite field, we shall use the convention that for any non-zero $a \in \mathbb{F}_{2^n}$, $a^{-1} := \frac{1}{a}$ and $0^{-1} := 0$ in the rest of the paper.

4.2 The c-Differential Uniformity of a Class of Involutions

In this section, first we shall consider the cDU of the involution $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$ over $\mathbb{F}_{2^n}$, where $n \geq 3$ is odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$ and $\gcd(k, n) = 1$. Let $f(X) = \mathrm{Tr}(X^{2^k+1})$ be the trace of the Gold function. For $c \in \mathbb{F}_q$, $c \neq 0, 1$, the following theorem gives the cDDT entries of the involution $G(X)$.

Theorem 19. *Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$ and let $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$ with $\gcd(k, n) = 1$. Then for any $a, b, c \in \mathbb{F}_{2^n}$, $c \neq 0, 1$, the cDDT entry ${}_c\Delta_G(a, b)$ of $G(X)$ at (a, b) is given by*

$$
{}_c\Delta_G(a,b) = \begin{cases} 0 & \text{if } \mathrm{Tr}\left(\frac{(a+b)(a^{2^{-k}}+a^{2^k})}{1+c} + \alpha a + a^{2^k+1}\right) = 1 \text{ and } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right) = 1 \\ 1 & \text{if } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right) = 0 \\ 2 & \text{if } \mathrm{Tr}\left(\frac{(a+b)(a^{2^{-k}}+a^{2^k})}{1+c} + \alpha a + a^{2^k+1}\right) = 0 \text{ and } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right) = 1. \end{cases}
$$

Proof. Recall that the cDDT entry ${}_c\Delta_G(a,b)$ at the point (a,b) of the function $G(X)$ is given by the number of solutions of the following equation

$$\begin{aligned} b &= G(X+a) + cG(X) \\ &= X + a + \mathrm{Tr}\left(\alpha(X+a) + (X+a)^{2^k+1}\right) + c\left(X + \mathrm{Tr}(\alpha X + X^{2^k+1})\right) \\ &= (1+c)\left(X + \mathrm{Tr}(\alpha X + X^{2^k+1})\right) + a + \mathrm{Tr}(\alpha a + a^{2^k+1}) + \mathrm{Tr}(X^{2^k}a + Xa^{2^k}), \end{aligned}$$

which can be further written as

$$(1+c)G(X) + \mathrm{Tr}(X^{2^k}a + Xa^{2^k}) + G(a) + b = 0. \tag{4.1}$$

It is straightforward to observe that the number of solutions of the above Equation (4.1) is given by

$$\begin{aligned} {}_c\Delta_G(a,b) &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(\beta\left((1+c)G(X)+\mathrm{Tr}(X^{2^k}a+Xa^{2^k})+G(a)+b\right)\right)} \\ &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(\beta(1+c)G(X)+\beta\mathrm{Tr}(X^{2^k}a+Xa^{2^k})\right)} \\ &= \frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\ &= \frac{1}{2^n}(M_0+M_1), \end{aligned}$$

where M_0 and M_1 are the sums corresponding to $\mathrm{Tr}(\beta)=0$ and $\mathrm{Tr}(\beta)=1$, respectively. We shall now compute M_0 and M_1, separately. The first sum M_0 is given by

$$\begin{aligned} M_0 &= \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta(G(a)+b))}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\ &= \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta(G(a)+b))}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))} \\ &= 2^n + \sum_{\substack{\beta\in\mathbb{F}_q^* \\ \mathrm{Tr}(\beta)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))}\sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))} \\ &= 2^n, \end{aligned}$$

where the last equality holds because $\beta(1+c)\neq 0$ and $G(X)$ is a permutation of $\mathbb{F}_{2^n}$,

which makes the inner sum zero. Similarly, we can compute the second sum M_1 which is given by

$$\begin{aligned}
M_1 &= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)G(X))+\mathrm{Tr}(\beta)\mathrm{Tr}(X^{2^k}a+Xa^{2^k})} \\
&= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)X+\beta(1+c)\mathrm{Tr}(\alpha X+X^{2^k+1}))+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}))} \\
&= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)X)+\mathrm{Tr}(\beta(1+c))\mathrm{Tr}(\alpha X+X^{2^k+1})+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}))} \\
&= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c))\mathrm{Tr}(\alpha X+X^{2^k+1})+\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))}.
\end{aligned}$$

Now we shall consider two cases, namely, $\mathrm{Tr}(\beta(1+c))=0$ and $\mathrm{Tr}(\beta(1+c))=1$, respectively. Equivalently, $\mathrm{Tr}(\beta c)=1$ and $\mathrm{Tr}(\beta c)=0$, respectively. We shall denote the sums corresponding to $\mathrm{Tr}(\beta c)=1$ and $\mathrm{Tr}(\beta c)=0$ by $M_{1,1}$ and $M_{1,0}$, respectively.

Case 1. Let $\mathrm{Tr}(\beta c)=1$. In this case,

$$\begin{aligned}
M_{1,1} &= \sum_{\substack{\mathrm{Tr}(\beta)=1\\ \mathrm{Tr}(\beta c)=1}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\
&= \sum_{\substack{\mathrm{Tr}(\beta)=1\\ \mathrm{Tr}(\beta c)=1}} (-1)^{\mathrm{Tr}((a+b)\beta+\beta\mathrm{Tr}(\alpha a+a^{2^k+1}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\
&= \sum_{\substack{\mathrm{Tr}(\beta)=1\\ \mathrm{Tr}(\beta c)=1}} (-1)^{\mathrm{Tr}((a+b)\beta)+\mathrm{Tr}(\beta)\mathrm{Tr}(\alpha a+a^{2^k+1})} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))} \\
&= \sum_{\substack{\mathrm{Tr}(\beta)=1\\ \mathrm{Tr}(\beta c)=1}} (-1)^{\mathrm{Tr}((a+b)\beta+\alpha a+a^{2^k+1})} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}+\beta(1+c)))}.
\end{aligned}$$

Notice that the inner sum will have a contribution if and only if $\beta(1+c)=a^{2^{-k}}+a^{2^k}$. Therefore, we have

$$M_{1,1} = \begin{cases} 0 & \text{if } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right)=0 \\ 2^n\cdot(-1)^{\mathrm{Tr}\left(\frac{(a+b)(a^{2^{-k}}+a^{2^k})}{1+c}+\alpha a+a^{2^k+1}\right)} & \text{if } \mathrm{Tr}\left(\frac{a^{2^{-k}}+a^{2^k}}{1+c}\right)=1. \end{cases}$$

Case 2. Let $\mathrm{Tr}(\beta c) = 0$. In this case,

$$\begin{aligned} M_{1,0} &= \sum_{\substack{\mathrm{Tr}(\beta)=1 \\ \mathrm{Tr}(\beta c)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}\left(X^{2^k+1}+X(a^{2^{-k}}+a^{2^k}+\beta(1+c)+\alpha)\right)} \\ &= \sum_{\substack{\mathrm{Tr}(\beta)=1 \\ \mathrm{Tr}(\beta c)=0}} (-1)^{\mathrm{Tr}(\beta(G(a)+b))} \mathcal{W}_f(u), \end{aligned}$$

where $u = a^{2^{-k}} + a^{2^k} + \beta(1+c) + \alpha$. We now apply an old result of Gold [31] (see also [34, Theorem 4]) which states that when n is odd and $\gcd(k, n) = 1$, the Walsh coefficient of the Gold function f is given by

$$\mathcal{W}_f(u) = \begin{cases} 0 & \text{if } \mathrm{Tr}(u) = 0 \\ (-1)^{Tr(\gamma^{2^k+1})} \mathcal{W}_f(1) & \text{if } \mathrm{Tr}(u) = 1, \end{cases}$$

where γ is the unique element in $\mathbb{F}_{2^n}$ of trace 0 such that $u = \gamma^{2^k} + \gamma^{2^{-k}} + 1$, completed with one of Dillon and Dobbertin's results [26] (see also [34, Theorem 5]), which gives the Walsh-Hadamard coefficient

$$\mathcal{W}_f(1) = \begin{cases} +2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 1 \pmod 8 \\ -2^{\frac{n+1}{2}} & \text{if } n \equiv \pm 3 \pmod 8. \end{cases}$$

It is easy to see that $\mathrm{Tr}(u) = \mathrm{Tr}(a^{2^{-k}} + a^{2^k} + \beta(1+c) + \alpha) = 0$. Therefore $M_{1,0} = 0$. This completes the proof. □

The case $c = 0$ is considered in the following remark.

Remarks 4.2.1. Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then for $c = 0$, the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where $\gcd(k, n) = 1$, is PcN.

The following theorem gives the DU (the case $c = 1$) of the function $G(X)$.

Theorem 20. *Let $n \geq 3$ be odd, $\alpha \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha) = 1$. Then the DDT entries $\Delta_G(a, b)$ at point $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ of the function $G(X) = X + \mathrm{Tr}(\alpha X + X^{2^k+1})$, where*

$\gcd(k,n)=1$, *is given by*

$$\Delta_G(a,b)=\begin{cases}2^n & \text{if } (a,b)=(1,1)\\ 2^{n-1} & \text{if } (a,b)\neq(1,1) \text{ and } G(a)=b \text{ or } b+1\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Recall that the DDT entry $\Delta_G(a,b)$ at the point $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}$ of the function $G(X)=X+\mathrm{Tr}(\alpha X+X^{2^k+1})$ is given by the number of solutions of the following equation

$$\begin{aligned}
&G(X+a)+G(X)=b\\
\iff\ &X+a+\mathrm{Tr}\left(\alpha(X+a)+(X+a)^{2^k+1}\right)+X+\mathrm{Tr}(\alpha X+X^{2^k+1})=b\\
\iff\ &a+\mathrm{Tr}(\alpha a+a^{2^k+1})+\mathrm{Tr}(X^{2^k}a+Xa^{2^k})=b\\
\iff\ &\mathrm{Tr}(X^{2^k}a+Xa^{2^k})=G(a)+b\\
\iff\ &\mathrm{Tr}(X(a^{2^{-k}}+a^{2^k}))=G(a)+b
\end{aligned}$$

Notice that when $a=1$, then $G(a)=1$ and in this case the above equation has 2^n solutions if $b=1$ and no solution otherwise. For $a\neq 1$, $a^{2^{-k}}+a^{2^k}\neq 0$ as $\gcd(k,n)=1$ and n is odd. In this case the above equation has 2^{n-1} solutions if either $G(a)=b$ or $G(a)=b+1$ and has no solution, otherwise. □

4.3 The Boomerang Uniformity of a Class of Involutions

In this section, we shall consider the BU of the involution $G(X)$. The following theorem gives the BCT entries of the involution $G(X)$ over finite field $\mathbb{F}_{2^n}$.

Theorem 21. *Let $n\geq 3$ be odd and $\alpha\in\mathbb{F}_{2^n}$ with $\mathrm{Tr}(\alpha)=1$. Then the BCT entry $\mathcal{B}_G(a,b)$ at point $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$ of the function $G(X)=X+\mathrm{Tr}(\alpha X+X^{2^k+1})$, where $\gcd(k,n)=1$, is given by*

$$\mathcal{B}_G(a,b)=\begin{cases}2^n & \text{if } \mathrm{Tr}((a^k+a^{-k})b)=0\\ 0 & \text{if } \mathrm{Tr}((a^k+a^{-k})b)=1.\end{cases}$$

Proof. Recall that the BCT entry of $G(X)$ at point $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$ is the number of solutions in $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of the following system

$$\begin{cases} G(X) + G(Y) = b \\ G(X + a) + G(Y + a) = b, \end{cases}$$

that is,

$$\begin{cases} X + Y + \mathrm{Tr}(\alpha(X + Y)) + \mathrm{Tr}(X^{2^k+1} + Y^{2^k+1}) = b \\ X + Y + \mathrm{Tr}(\alpha(X + Y)) + \mathrm{Tr}((X + a)^{2^k+1} + (Y + a)^{2^k+1}) = b. \end{cases} \tag{4.2}$$

Now adding both the equations in the above system (4.2), we have

$$\begin{aligned} 0 &= \mathrm{Tr}\left((X + a)^{2^k+1} + X^{2^k+1} + (Y + a)^{2^k+1} + Y^{2^k+1}\right) \\ &= \mathrm{Tr}\left(X^{2^k}a + Xa^{2^k} + Y^{2^k}a + Ya^{2^k}\right) \\ &= \mathrm{Tr}\left((X + Y)^{2^k}a + (X + Y)a^{2^k}\right). \end{aligned}$$

Therefore, the system (4.2) is equivalent to the following system

$$\begin{cases} X + Y + \mathrm{Tr}\left(\alpha(X + Y) + X^{2^k+1} + Y^{2^k+1}\right) = b \\ \mathrm{Tr}\left((X + Y)^{2^k}a + (X + Y)a^{2^k}\right) = 0, \end{cases}$$

and so,

$$\begin{cases} X + Y + \mathrm{Tr}\left(\alpha(X + Y) + (X + Y)^{2^k+1}\right) + \mathrm{Tr}\left(X^{2^k}Y + XY^{2^k}\right) = b \\ \mathrm{Tr}\left((X + Y)^{2^k}a + (X + Y)a^{2^k}\right) = 0. \end{cases} \tag{4.3}$$

Taking $Y = X + Z$, the above system (4.3) becomes

$$\begin{cases} Z + \mathrm{Tr}\left(\alpha Z + Z^{2^k+1}\right) + \mathrm{Tr}\left(X^{2^k}Z + XZ^{2^k}\right) = b \\ \mathrm{Tr}\left(Z^{2^k}a + Za^{2^k}\right) = 0, \end{cases}$$

which can be written as

$$\begin{cases} G(Z) + \mathrm{Tr}\left(X(Z^{2^{-k}} + Z^{2^k})\right) = b \\ \mathrm{Tr}\left(a(Z^{2^{-k}} + Z^{2^k})\right) = 0. \end{cases} \tag{4.4}$$

Our aim is to compute the number of solutions of the above system (4.4). We shall now use the techniques given in [52] to find this number, i.e., to compute the BCT entries of $G(X)$. Recall that the number of solutions of the above system (4.4), denoted as $\mathcal{B}_G(a,b)$, is given by

$$\begin{aligned} \mathcal{B}_G(a,b) &= \frac{1}{2^{2n}} \sum_{X,Z\in\mathbb{F}_{2^n}} \sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(Z)+\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))+b))} \sum_{\gamma\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\gamma\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k})))} \\ &= \frac{1}{2^{2n}} \sum_{X,Z\in\mathbb{F}_{2^n}} \sum_{\beta\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(G(Z)+b))+\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad \cdot \sum_{\gamma\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= \frac{1}{2^{2n}} \sum_{\beta,\gamma\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta b)} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad \cdot \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= \frac{1}{2^{2n}}(S_0 + S_1), \end{aligned} \tag{4.5}$$

where S_0 and S_1 are the sums corresponding to $\mathrm{Tr}(\beta) = 0$ and $\mathrm{Tr}(\beta) = 1$, respectively. We shall now compute S_0 and S_1 separately. We first consider the sum S_0 given by

$$\begin{aligned} S_0 &= \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\qquad \cdot \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^n \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^n \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)}(S_{0,0} + S_{0,1}), \end{aligned} \tag{4.6}$$

where $S_{0,0}$ and $S_{0,1}$ are the sums corresponding to $\mathrm{Tr}(\gamma) = 0$ and $\mathrm{Tr}(\gamma) = 1$, respectively.

We shall now compute $S_{0,0}$ and $S_{0,1}$, separately. Consider

$$\begin{aligned} S_{0,0} &= \sum_{\mathrm{Tr}(\gamma)=0} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= \sum_{\mathrm{Tr}(\gamma)=0} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))}. \end{aligned}$$

Similarly,

$$\begin{aligned} S_{0,1} &= \sum_{\mathrm{Tr}(\gamma)=1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= \sum_{\mathrm{Tr}(\gamma)=1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta Z+\beta\mathrm{Tr}(\alpha Z+Z^{2^k+1}))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta Z)+\mathrm{Tr}(\beta)\mathrm{Tr}(\alpha Z+Z^{2^k+1})+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta Z)+\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))}. \end{aligned}$$

Now putting the values of $S_{0,0}$ and $S_{0,1}$ into Equation (4.6), we have

$$\begin{aligned} S_0 &= 2^{2n-1} \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)} \left(\sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))} + \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))} \right) \\ &= 2^{2n-1} \left(2^n + \sum_{\substack{\mathrm{Tr}(\beta)=0 \\ \beta\neq 0}} (-1)^{\mathrm{Tr}(\beta b)} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))} \right. \\ &\qquad \left. + \sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))} \right) \\ &= 2^{3n-1} + 2^{2n-1} \left(\sum_{\mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta b)} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(Z(a^{2^{-k}}+a^{2^k}+\beta))} \right) \\ &= 2^{3n-1} + 2^{3n-1} \cdot (-1)^{\mathrm{Tr}(b(a^{2^{-k}}+a^{2^k}))}, \end{aligned}$$

where the second last equality holds because $G(Z)$ is permutation of $\mathbb{F}_{2^n}$. The last equality holds as the inner sum will contribute if and only if $\beta = a^{2^{-k}} + a^{2^k}$.

Now, we shall calculate S_1 which is given by

$$\begin{aligned} S_1 &= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\quad \cdot \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta b)} \sum_{\gamma\in\mathbb{F}_{2^n}} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \\ &\quad \cdot \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta b)} (S_{1,0} + S_{1,1}), \end{aligned} \tag{4.7}$$

where $S_{1,0}$ and $S_{1,1}$ are the sum corresponding to $\mathrm{Tr}(\gamma) = 0$ and $\mathrm{Tr}(\gamma) = 1$, respectively. We shall now compute $S_{1,0}$ and $S_{1,1}$ separately. Consider

$$\begin{aligned} S_{1,0} &= \sum_{\mathrm{Tr}(\gamma)=0} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= \sum_{\mathrm{Tr}(\gamma)=0} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\ &= 2^{n-1} \left(\sum_{\substack{Z\in\mathbb{F}_{2^n} \\ Z\neq 0,1}} (-1)^{\mathrm{Tr}(\beta G(Z))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \right) + 2^{2n-1} + 2^{2n-1} \cdot (-1)^{\mathrm{Tr}(\beta G(1))} \\ &= 2^{2n-1} + 2^{2n-1} \cdot (-1)^{\mathrm{Tr}(\beta(1+\mathrm{Tr}(\alpha+1))} \\ &= 2^{2n-1} + 2^{2n-1} \cdot (-1)^{\mathrm{Tr}(\beta)}, \end{aligned}$$

where the second identity holds because $Z^{2^{-k}} + Z^{2^k} = 0$, or equivalently, $Z^{2^{2k}} + Z = 0$ if and only if $Z = 0, 1$. For $Z \in \mathbb{F}_{2^n}\backslash\{0, 1\}$, $Z^{2^{-k}} + Z^{2^k} \neq 0$ and as a consequence, the inner sum will be equal to zero. The last equality holds because $\mathrm{Tr}(\alpha) = 1$. Similarly,

$$S_{1,1} = \sum_{\mathrm{Tr}(\gamma)=1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))}$$

$$
\begin{aligned}
&= \sum_{\mathrm{Tr}(\gamma)=1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\
&=2^{n-1} \sum_{Z\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\
&=2^{2n-1} + 2^{2n-1}\cdot(-1)^{\mathrm{Tr}(\beta G(1))} \\
&\quad + 2^{n-1} \sum_{\substack{Z\in\mathbb{F}_{2^n} \\ Z\neq 0,1}} (-1)^{\mathrm{Tr}(\beta G(Z))+\mathrm{Tr}(a(Z^{2^{-k}}+Z^{2^k}))} \sum_{X\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(X(Z^{2^{-k}}+Z^{2^k}))} \\
&=2^{2n-1} + 2^{2n-1}\cdot(-1)^{\mathrm{Tr}(\beta+\beta\mathrm{Tr}(\alpha+1))} \\
&=2^{2n-1} + 2^{2n-1}\cdot(-1)^{\mathrm{Tr}(\beta)}.
\end{aligned}
$$

Now putting the values of $S_{1,0}$ and $S_{1,1}$ in the Equation (4.7), we have

$$S_1 = \sum_{\mathrm{Tr}(\beta)=1} (-1)^{\mathrm{Tr}(\beta b)}(2^{2n} + 2^{2n}\cdot(-1)^{\mathrm{Tr}(\beta)}) = 0.$$

Now putting the values of S_0 and S_1 into Equation (4.5), we have

$$\mathcal{B}_G(a,b) = 2^{n-1} + 2^{n-1}\cdot(-1)^{\mathrm{Tr}(b(a^{2^{-k}}+a^{2^k}))}.$$

This completes the proof. □

4.4 The c-Differential Uniformity of a Perturbed Inverse Function

In this section, we shall consider the cDU of the function $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$, for all positive integers n and $1 \neq c \in \mathbb{F}_q$. We shall first recall the following lemma (we have slightly modified the statement as per our requirements), which gives the cDU of the inverse mapping.

Lemma 4.4.1. *[28, Theorem 12] Let n be a positive integer and $c \in \mathbb{F}_{2^n}\backslash\{0,1\}$. For any $a, b \in \mathbb{F}_{2^n}$, the number of solutions of the equation $(X+a)^{-1} + cX^{-1} = b$ are given as*

follows.

$$\begin{cases} \{\frac{ac}{1+c}\} & \text{if } b=0; \\ \{0\} & \text{if } ab=1 \text{ and } \mathrm{Tr}(1/c)=1 \\ \{0, \text{ two more solutions}\} & \text{if } ab=1 \text{ and } \mathrm{Tr}(1/c)=0 \\ \{a\} & \text{if } ab=c \text{ and } \mathrm{Tr}(c)=1 \\ \{a, \text{ two more solutions}\} & \text{if } ab=c \text{ and } \mathrm{Tr}(c)=0 \\ \{\left(\frac{ac}{b}\right)^{2^{n-1}}\} & \text{if } ab=1+c \\ \{\text{two solutions}\} & \text{if } ab\neq 1, c, 1+c \text{ and } \mathrm{Tr}\left(\frac{abc}{(ab)^2+c^2+1}\right)=0 \\ \text{no solution} & \text{otherwise.} \end{cases}$$

The following theorem gives bound for the cDU of the function $H(X)$ over $\mathbb{F}_{2^n}$, for all positive integers n and $1 \neq c \in \mathbb{F}_q$.

Theorem 22. *Let* $1 \neq c \in \mathbb{F}_{2^n}$ *and* $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *is defined by* $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. *We have*:

(i) If $c = 0$, *then* $H(X)$ *is PcN;*

(ii) If $\mathrm{Tr}(c) = 1 = \mathrm{Tr}(1/c)$, *then* ${}_c\Delta_H \leq 8$;

(iii) Otherwise, ${}_c\Delta_H \leq 9$.

Proof. For any fixed $1 \neq c \in \mathbb{F}_{2^n}$, the cDU of the function $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ equals the maximum number of solutions of the following equation

$$(X+a)^{-1} + \mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) + cX^{-1} + c\mathrm{Tr}\left(\frac{X^2}{X+1}\right) = b, \tag{4.8}$$

where $a, b \in \mathbb{F}_{2^n}$. Notice that when $c = 0$, the above Equation (4.8) reduces to

$$(X+a)^{-1} + \mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) = b,$$

which has exactly one solution for each pair $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ as the left hand side is a

PP. Let $c \neq 0, 1$. For any fixed $c \neq 0, 1$, if $a = 0$, Equation (4.8) reduces to

$$X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right) = b(1+c)^{-1},$$

which has exactly one solution for each $b \in \mathbb{F}_{2^n}$ as the left hand side is a PP. Now for any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, to find the solutions of Equation (4.8) we shall split the analysis into four cases.

Case 1. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) = 0 = \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. In this case, Equation (4.8) reduces to

$$(X+a)^{-1} + cX^{-1} = b. \tag{4.9}$$

Notice that if 0 is a solution of Equation (4.8) then either $ab = 1$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 0$ or $a(b+1) = 1$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 1$. Similarly, if a is a solution of Equation (4.8) then either $ab = c$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 0$ or $a(b+c) = c$ and $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 1$. From Lemma 4.4.1, we know that if $ab = 1$ and $\mathrm{Tr}(1/c) = 0$, then the Equation (4.9) has three solutions and one among them is zero. Similarly, if $ab = c$ and $\mathrm{Tr}(c) = 0$, then the Equation (4.9) has three solutions and one among them is a. In rest of the cases Equation (4.9) can have atmost two solutions. From here we conclude that for any fixed $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$, Equation (4.8) can have at most three solutions if either $\mathrm{Tr}(1/c) = 0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 0$ and $ab = 1$, or $\mathrm{Tr}(c) = 0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right) = 0$ and $ab = c$. Otherwise, there can be at most two solutions of Equation (4.8) from this case.

Case 2. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) = 1 = \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$. In this case, Equation (4.8) reduces to

$$(X+a)^{-1} + cX^{-1} = b + c + 1. \tag{4.10}$$

Again, by Lemma 4.4.1, if $a(b+c+1) = 1$ and $\mathrm{Tr}(1/c) = 0$, then the Equation (4.10) has three solutions and one among them is zero. It is easy to see that when $X = 0$, $\mathrm{Tr}\left(\frac{X^2}{X+1}\right) = 0$. Therefore 0 can not be a solution of Equation (4.8). Similarly, if $a(b+c+1) = c$ and $\mathrm{Tr}(c) = 0$, then Equation (4.10) has three solutions and one among them is a. Notice that, when $X = a$, $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) = 0$. Therefore a can not be a solution of Equation (4.8). Thus, we can get at most two solutions of Equation (4.8) from this case.

Case 3. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right) = 0$ and $\mathrm{Tr}\left(\frac{X^2}{X+1}\right) = 1$. Then Equation (4.8) reduces

to

$$(X+a)^{-1}+cX^{-1}=b+c. \tag{4.11}$$

From Lemma 4.4.1, we know that if $a(b+c)=1$ and $\mathrm{Tr}(1/c)=0$, then the Equation (4.11) has three solutions and one among them is 0. As we are in the case $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=1$, the solution $X=0$ of Equation (4.11) will not be a solution of Equation (4.8). Similarly, if $a(b+c)=c$ and $\mathrm{Tr}(c)=0$, then the Equation (4.11) has three solutions and one among them is a. It is easy to see that the solution $X=a$ of (4.11) will be a solution of Equation (4.8) if and only if $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. Thus, for any fixed $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$, if $\mathrm{Tr}(c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$ and $a(b+c)=c$, then there can be at most 3 solutions of Equation (4.8) from this case, otherwise there can be at most 2 solutions.

Case 4. Let $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)=1$ and $\mathrm{Tr}\left(\frac{X^2}{X+1}\right)=0$. Then Equation (4.8) reduces to

$$(X+a)^{-1}+cX^{-1}=b+1. \tag{4.12}$$

Again, by Lemma 4.4.1, if $a(b+1)=1$ and $\mathrm{Tr}(1/c)=0$, then the Equation (4.12) has three solutions and one among them is 0. Notice that the solution $X=0$ of Equation (4.12) will be a solution of Equation (4.8) if and only if $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$. Similarly, if $a(b+1)=c$ and $\mathrm{Tr}(c)=0$, then the Equation (4.12) has three solutions and one among them is a. Notice that solution $X=a$ of (4.12) will not be a solution of Equation (4.8) as $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1}\right)\neq 1$. Thus, for any fixed $c\in\mathbb{F}_{2^n}\backslash\{0,1\}$, if $\mathrm{Tr}(1/c)=0$, $\mathrm{Tr}\left(\frac{a^2}{a+1}\right)=1$ and $a(b+1)=1$ then there can be at most 3 solutions of Equation (4.8) from this case, otherwise there can be at most 2 solutions. This completes the proof. □

The following Table 4.1 gives the maximum possible value of ${}_c\Delta_H$, where $c\neq 0,1$, of the function $H(X)$ over $\mathbb{F}_{2^n}$ for some small values of n.

4.5 The Boomerang Uniformity of a Perturbed Inverse Function

Boura and Canteaut [8] studied the BCT entries of the inverse mapping and proved the following lemma. We are also including the proof here (however, our technique is slightly different from the one given in [8]), for the convenience of the reader.

n	when $\mathrm{Tr}(c) = 0 = \mathrm{Tr}(\frac{1}{c})$ or $\mathrm{Tr}(c) + \mathrm{Tr}(\frac{1}{c}) = 1$	when $\mathrm{Tr}(c) = 1 = \mathrm{Tr}(\frac{1}{c})$
2	1	1
3	3	1
4	5	4
5	6	6
6	7	6
7	7	6
8	8	7

Table 4.1: Maximum value of ${}_c\Delta_H$ over finite field $\mathbb{F}_{2^n}$.

Lemma 4.5.1. *[8, Proposition 6] Let $f(X) = X^{-1}$ be a map from $\mathbb{F}_{2^n}$ to itself with n even. Then for any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, the boomerang system*

$$\begin{cases} X^{-1} + Y^{-1} = b \\ (X + a)^{-1} + (Y + a)^{-1} = b. \end{cases} \tag{4.13}$$

has the following solutions if $n \equiv 2 \pmod 4$

$$\begin{cases} \{(0, a), (a, 0), (a\omega, a\omega^2), (a\omega^2, a\omega)\} & \text{if } ab = 1 \\ \{(0, a\omega^2), (a\omega^2, 0), (a, a\omega), (a\omega, a)\} & \text{if } ab = \omega \\ \{(0, a\omega), (a\omega, 0), (a, a\omega^2), (a\omega^2, a)\} & \text{if } ab = \omega^2 \\ \{(X_1, X_1 + a), (X_1 + a, X_1)\},\ X_1^2 + aX_1 + \frac{a}{b} = 0 & \text{if } \mathrm{Tr}(\frac{1}{ab}) = 0,\ \textit{and } ab \neq 1, \omega, \omega^2 \\ \textit{no solution} & \textit{otherwise.} \end{cases}$$

When $n \equiv 0 \pmod 4$, then there are the following additional solutions

$$\begin{cases} \{(X_2, X_2 + a), (X_2 + a, X_2)\},\ X_2^2 + aX_2 + a^2\omega^2 = 0 & \text{if } ab = \omega \\ \{(X_3, X_3 + a), (X_3 + a, X_3)\},\ X_3^2 + aX_3 + a^2\omega = 0 & \text{if } ab = \omega^2. \end{cases}$$

Proof. It is easy to see that $(0, 0)$ and (a, a) can not be a solution of the Equation (4.13) as $b \neq 0$. Now we shall divide our discussion into the following different cases.

Case 1. Let $X = 0$. In this case, the system (4.13) reduces to

$$\begin{cases} Y = b^{-1} \\ (b^{-1} + a)^{-1} = b + a^{-1}. \end{cases} \tag{4.14}$$

It is easy to see that if $ab = 1$ then $(0, a)$ is the solution of above system (4.14). If $ab \neq 1$ then the system (4.14) reduces to

$$\begin{aligned} 0 &= (b^{-1} + a)(b + a^{-1}) + 1 \\ &= 1 + a^{-1}b^{-1} + ab \\ &= (ab)^2 + ab + 1. \end{aligned}$$

Thus $ab \neq 1$ is a root of $\omega^3 + 1 = 0$, hence a primitive root of $\mathbb{F}_{2^2}$, say ω, ω^2. When $ab = \omega$, Equation (4.14) has exactly one solution $(0, a\omega^2)$. Similarly, when $ab = \omega^2$, Equation (4.14) has exactly one solution $(0, a\omega)$. If $ab \neq 1, \omega, \omega^2$, then system (4.14) has no solution.

Case 2. Let $X = a$. In this case, the system (4.13) reduces to

$$\begin{cases} Y = (b + a^{-1})^{-1} \\ ((b + a^{-1})^{-1} + a)^{-1} = b. \end{cases} \tag{4.15}$$

It is easy to see that if $ab = 1$ then $(a, 0)$ is the solution of above system (4.15). Also notice that if $ab \neq 1$ then $(b+a^{-1})^{-1}+a \neq 0$ as $b \neq 0$. Thus, for $ab \neq 1$ the system (4.15) reduces to

$$\begin{aligned} (b + a^{-1})^{-1} &= a + b^{-1} \\ (a + b^{-1})(a^{-1} + b) &= 1 \\ (ab)^2 + ab + 1 &= 0. \end{aligned}$$

Thus $ab \neq 1$ is a root of $\omega^3 + 1 = 0$, hence a primitive root of $\mathbb{F}_{2^2}$. When $ab = \omega$, Equation (4.15) has exactly one solution $(a, a\omega)$. Similarly, when $ab = \omega^2$, Equation (4.15) has exactly one solution $(a, a\omega^2)$. If $ab \neq 1, \omega, \omega^2$, then system (4.15) has no solution.

Case 3. Let $Y = 0$. Since the system (4.13) is symmetric in the variables X and Y, this case directly follows from the Case 1. Thus, the system (4.13) has exactly one solution $(a, 0), (a\omega^2, 0)$ and $(a\omega, 0)$ when $ab = 1, \omega$ and ω^2, respectively. If $ab \neq 1, \omega, \omega^2$, then system (4.13) has no solution with $Y = 0$.

Case 4. Let $Y = a$. Since the system (4.13) is symmetric in the variables X and Y, this case directly follows from the Case 2. Thus, the system (4.13) has exactly one solution $(0, a), (a\omega, a)$ and $(a\omega^2, a)$ when $ab = 1, \omega$ and ω^2, respectively. If $ab \neq 1, \omega, \omega^2$, then system (4.13) has no solution with $Y = a$.

Case 5. Let $X \neq 0, a$ and $Y \neq 0, a$. Now, the system (4.13) becomes

$$\begin{cases} X + Y = bXY \\ X + Y = b(XY + aX + aY + a^2), \end{cases} \tag{4.16}$$

which is equivalent to

$$\begin{cases} X + a = Y \\ X^2 + aX + \frac{a}{b} = 0. \end{cases} \tag{4.17}$$

Now if $ab = 1$, then the second equation of (4.17) reduces to $X^2 + aX + a^2 = 0$, which is equivalent to $X(X^3 + a^3) = 0$, which has only two solutions $a\omega, a\omega^2$ (since $X \neq 0, a$). Thus, Equation (4.16) has two solutions, namely $(a\omega, a\omega^2)$ and $(a\omega^2, a\omega)$. If $ab = \omega$, then the second equation of (4.17) becomes $X^2 + aX + a^2\omega^2 = 0$, which has two solutions if and only if $\mathrm{Tr}(\omega^2) = \mathrm{Tr}(\omega) = 0$. Here, one may note that $\mathrm{Tr}(\omega) = 0$ if and only if $n \equiv 0 \pmod 4$. Similarly, if $ab = \omega^2$, the second equation of the system (4.17) becomes $X^2 + aX + a^2\omega = 0$, which has two solutions if and only if $\mathrm{Tr}(\omega) = 0$. Again, $\mathrm{Tr}(\omega) = 0$ if and only if $n \equiv 0 \pmod 4$. When $X, Y \neq 0, a$ and $ab \neq 1, \omega, \omega^2$, then Equation (4.17) has two solutions if and only if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$. □

The following is an immediate corollary to Lemma 4.5.1.

Corollary 4.5.2. *Let $f(X) = X^{-1}$ be a map from $\mathbb{F}_{2^n}$ to itself with n even. Then the boomerang uniformity of f is given by*

$$\mathcal{B}_f = \begin{cases} 4 & \text{if } n \equiv 2 \pmod 4 \\ 6 & \text{if } n \equiv 0 \pmod 4. \end{cases}$$

Now we shall consider the boomerang uniformity of the differentially 4-uniform permutation $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ over $\mathbb{F}_{2^n}$ with n even in the following theorem.

Theorem 23. *Let n be even and $H(X) = X^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1}\right)$ be a map from $\mathbb{F}_{2^n}$ to itself. Then the boomerang uniformity of H is less or equal to* 12.

Proof. For any $a, b \in \mathbb{F}_{2^n}^*$, the BCT entry $\mathcal{B}_H(a,b)$ of H at point (a,b) is the number of solutions of the following system

$$\begin{cases} X^{-1} + Y^{-1} + \mathrm{Tr}\left(\frac{X^2}{X+1} + \frac{Y^2}{Y+1}\right) = b; \\ (X+a)^{-1} + (Y+a)^{-1} + \mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1} + \frac{Y^2+a^2}{Y+a+1}\right) = b. \end{cases} \tag{4.18}$$

We shall split the analysis of solutions of the above system into the following four cases.
Case 1. Let $\mathrm{Tr}\left(\frac{X^2}{X+1} + \frac{Y^2}{Y+1}\right) = 0 = \mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1} + \frac{Y^2+a^2}{Y+a+1}\right)$. In this case, the system (4.18) reduces to

$$\begin{cases} X^{-1} + Y^{-1} = b \\ (X+a)^{-1} + (Y+a)^{-1} = b. \end{cases} \tag{4.19}$$

From Lemma 4.5.1, we know that the above system (4.19) has four solutions if $ab = 1$; four solutions if $ab = \omega, \omega^2$ and $n \equiv 2 \pmod 4$; six solutions if $ab = \omega, \omega^2$ and $n \equiv 0 \pmod 4$; two solutions if $\mathrm{Tr}(\frac{1}{ab}) = 0$ and $ab \neq 1, \omega, \omega^2$; and no solutions, otherwise.
Case 2. Let $\mathrm{Tr}\left(\frac{X^2}{X+1} + \frac{Y^2}{Y+1}\right) = 1 = \mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1} + \frac{Y^2+a^2}{Y+a+1}\right)$. In this case, the system (4.18) reduces to

$$\begin{cases} X^{-1} + Y^{-1} = b + 1 \\ (X+a)^{-1} + (Y+a)^{-1} = b + 1. \end{cases} \tag{4.20}$$

Again, from Lemma 4.5.1, we know that the above system (4.20) has four solutions if $a(b+1) = 1$; four solutions if $a(b+1) = \omega, \omega^2$ and $n \equiv 2 \pmod 4$; six solutions if $a(b+1) = \omega, \omega^2$ and $n \equiv 0 \pmod 4$; two solutions if $\mathrm{Tr}(\frac{1}{a(b+1)}) = 0$ and $a(b+1) \neq 1, \omega, \omega^2$ and no solutions, otherwise.

We shall now compute maximum number of solutions of Equation (4.18) that can be

obtained from Case 1 and Case 2.

(i) Let $ab = 1$. In this subcase, if $ab + a = 1$, $a = 0$ which is not possible as $a \neq 0$. If $ab + a = \omega$, we have $(a, b) = (\omega^2, \omega)$. For $(a, b) = (\omega^2, \omega)$, four solutions of the system (4.19) are $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$. It is easy to verify that all these four solutions are solutions of system (4.18). For $(a, b) = (\omega^2, \omega)$, the system (4.20) has four solutions $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ when $n \equiv 2 \pmod 4$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. A simple calculation shows that none of these four solutions satisfy system (4.18). If $ab + a = \omega^2$, we have $(a, b) = (\omega, \omega^2)$. For $(a, b) = (\omega, \omega^2)$, four solutions of the system (4.19) are $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ and one can easily verify that these four solutions are solutions of system (4.18). For $(a, b) = (\omega, \omega^2)$, we have four solutions of (4.20), when $n \equiv 2 \pmod 4$, which are given by $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. A routine calculation shows that none of these four solutions are solutions of system (4.18) as in all these cases $\mathrm{Tr}\left(\frac{X^2}{X+1} + \frac{Y^2}{Y+1}\right) \neq 1$. If $ab + a \neq 1, \omega, \omega^2$, system (4.20) has two solutions if $\mathrm{Tr}\left(\frac{1}{1+a}\right) = 0$ and no solution, otherwise.

(ii) Let $ab = \omega$. In this subcase, if $ab + a = 1$ then $(a, b) = (\omega^2, \omega^2)$. For $(a, b) = (\omega^2, \omega^2)$, the system (4.19) has four solutions $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ if $n \equiv 2 \pmod 4$ and there are two additional solutions if $n \equiv 2 \pmod 4$. A simple calculation shows that all these four solutions are also a solution of equation (4.18). For $(a, b) = (\omega^2, \omega^2)$, four solutions of the system (4.20) are $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$. A simple calculation shows that none of these four solutions satisfy system (4.18). If $ab + a = \omega$ then $a = 0$ which is not possible as $a \neq 0$. Now if $ab + a = \omega^2$, $(a, b) = (1, \omega)$. For $(a, b) = (1, \omega)$, system (4.19) has four solutions $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$ if $n \equiv 2 \pmod 4$ and there will be two additional solutions if $n \equiv 0 \pmod 4$. A simple calculation yields that all these four solutions are solutions of system (4.18). For $(a, b) = (1, \omega)$, four solutions of (4.20), when $n \equiv 2 \pmod 4$, are $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. It is easy to verify that none of these four solutions are solutions of system (4.18). If $ab + a \neq 1, \omega, \omega^2$, the system (4.20) has two solutions if $\mathrm{Tr}\left(\frac{1}{a+\omega}\right) = 0$ and no solution, otherwise.

(iii) Let $ab = \omega^2$. In this subcase, if $ab + a = 1$, $(a, b) = (\omega, \omega)$. For $(a, b) = (\omega, \omega)$, system (4.19) has four solutions $\{(0, \omega^2), (\omega^2, 0), (\omega, 1), (1, \omega)\}$ if $n \equiv 2 \pmod 4$ and there

are two additional solutions if $n \equiv 0 \pmod 4$. It can be easily shown that all these four solutions are solutions of system (4.18). For $(a, b) = (\omega, \omega)$, four solutions of the system (4.20) are $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ and a routine calculation shows that none of these four solutions satisfy system (4.18). If $ab + a = \omega$, $(a, b) = (1, \omega^2)$. Now for $(a, b) = (1, \omega^2)$, system (4.19) has four solutions $\{(0, \omega), (\omega, 0), (1, \omega^2), (\omega^2, 1)\}$ if $n \equiv 2 \pmod 4$ and there are two additional solutions if $n \equiv 0 \pmod 4$. It is easy to verify that all these four solutions are solutions of system (4.18). For $(1, \omega^2)$, four solutions of (4.20), when $n \equiv 2 \pmod 4$, are $\{(0, \omega^2), (\omega^2, 0), (1, \omega), (\omega, 1)\}$ and there will be two additional solutions when $n \equiv 0 \pmod 4$. One can easily verify that none of these four solutions are solutions of the system (4.18). If $ab + a = \omega^2$, $a = 0$ which is not possible as $a \neq 0$. Now, if $ab + a \neq 1, \omega, \omega^2$, the system (4.20) has two solutions if $\mathrm{Tr}\left(\frac{1}{a+\omega^2}\right) = 0$ and no solution, otherwise.

From the above discussion, we infer the following:

- If $ab = 1, a + 1$, we can get at most 6 solutions of system (4.18) from Case 1 and Case 2.
- If $ab = \omega, \omega^2, a + \omega, a + \omega^2$, we can get at most 6 (respectively 8) solutions of system (4.18) from Case 1 and Case 2, if $n \not\equiv 2 \pmod 4$ (respectively $n \equiv 0 \pmod 4$).
- If $ab \neq 1, \omega, \omega^2, a + 1, a + \omega, a + \omega^2$, we can get at most 4 solutions of system (4.18) from Case 1 and Case 2.

Case 3. Let $\mathrm{Tr}\left(\frac{X^2}{X+1} + \frac{Y^2}{Y+1}\right) = 0$ and $\mathrm{Tr}\left(\frac{X^2+a^2}{X+a+1} + \frac{Y^2+a^2}{Y+a+1}\right) = 1$. In this case, the system (4.18) reduces to

$$\begin{cases} X^{-1} + Y^{-1} = b \\ (X + a)^{-1} + (Y + a)^{-1} = b + 1. \end{cases} \tag{4.21}$$

It is easy to see that when $b = 1$, the system (4.21) is inconsistent, as in this case, second equation of the system (4.21) would imply $X = Y$ and first equation of the system (4.21) cannot have solutions of this type as $b \neq 0$. Now, we shall calculate the number of solutions of the above system (4.21) in following cases.

Subcase 3.1. Let $X = 0$. In this case the system (4.21) reduces to

$$\begin{cases} Y = b^{-1} \\ (Y + a)^{-1} = a^{-1} + b + 1. \end{cases} \tag{4.22}$$

Solving the above equations in system (4.22), we have

$$(b^{-1} + a)^{-1} = a^{-1} + b + 1$$

Notice that if $ab = 1$ or $a(b + 1) = 1$ then the equation above is inconsistent. If $ab \neq 1, a$ then $(0, b^{-1})$ will be a solution of system (4.21) if and only if $a^2b^2 + a^2b + ab + a + 1 = 0$.

Subcase 3.2. Let $X = a$. In this case the system (4.21) reduces to

$$\begin{cases} Y = (a^{-1} + b)^{-1}; \\ (Y + a)^{-1} = b + 1. \end{cases} \tag{4.23}$$

Solving the above equations in system (4.23), we have

$$((a^{-1} + b)^{-1} + a)^{-1} = a^{-1} + b + 1$$

Notice that if $ab = 1$ then the equation above is inconsistent. If $ab \neq 1$ then $(a, (a^{-1}+b)^{-1})$ will be a solution of system (4.21) if and only if $a^2b^2 + a^2b + ab + 1 = 0$.

Subcase 3.3. Let $Y = 0$. As the system (4.21) is symmetric in the variables X and Y, this subcase directly follow from the Subcase 3.1. Therefore system (4.21) has no solution if $ab = 1$ or $a(b + 1) = 1$ and if $ab \neq 1, a$ then $(b^{-1}, 0)$ is a solution of the system (4.21) if and only if $a^2b^2 + a^2b + ab + a + 1 = 0$.

Subcase 3.4. Let $Y = a$. This subcase directly follows from the Subcase 3.2. Therefore system (4.21) has no solution if $ab = 1$ and if $ab \neq 1$ then $(b^{-1}, 0)$ is a solution of the system (4.21) if and only if $a^2b^2 + a^2b + ab + 1 = 0$.

Subcase 3.5. Let $X \neq 0, a$ and $Y \neq 0, a$. In this case, the system (4.21) reduces to

$$\begin{cases} X + Y = bXY \\ X + Y = (b + 1)(X + a)(Y + a). \end{cases} \tag{4.24}$$

Now adding the first and the second equation of the above system, we have

$$\begin{aligned} XY + (ab+a)(X+Y+a) &= 0 \\ bXY + (ab^2+ab)(X+Y+a) &= 0 \\ (ab^2+ab+1)(X+Y) + a^2b^2 + a^2b &= 0, \end{aligned}$$

when $ab^2 + ab + 1 = 0$, then the above equation will be inconsistent, as $a^2b^2 + a^2b \neq 0$ (since $b \neq 0, 1$). When $ab^2 + ab + 1 \neq 0$, we let $X + Y = t$, where $t = \dfrac{a^2b^2 + a^2b}{ab^2 + ab + 1}$. Now putting $Y = X + t$, the first equation of the system (4.24) transforms into

$$X^2 + tX + \frac{t}{b} = 0. \tag{4.25}$$

The above equation has two solutions if and only if $\mathrm{Tr}\left(\frac{1}{tb}\right) = 0$, namely $(X_1, X_1 + t)$ and $(X_1 + t, X_1)$, where X_1 is a root of Equation (4.25).

Case 4. Let $\mathrm{Tr}\left(\dfrac{X^2}{X+1} + \dfrac{Y^2}{Y+1}\right) = 1$ and $\mathrm{Tr}\left(\dfrac{X^2+a^2}{X+a+1} + \dfrac{Y^2+a^2}{Y+a+1}\right) = 0$. In this case, the system (4.18) reduces to

$$\begin{cases} X^{-1} + Y^{-1} = b + 1 \\ (X+a)^{-1} + (Y+a)^{-1} = b, \end{cases} \tag{4.26}$$

It is obvious that if (X, Y) is a solution of the system (4.21) then $(X + a, Y + a)$ will be a solution of the system (4.26). Also it is easy to observe that if solution (X, Y) of system (4.21) is a solution of system (4.18) then solution $(X + a, Y + a)$ of system (4.26) will also be a solution of system (4.18).

We shall now investigate, for any fixed $a, b \in \mathbb{F}_{2^n}^*$, the overlap between the solutions from the Case 3 and Case 4, and the solutions of Equation (4.18). We shall divide our discussion in the following cases.

(i) When $ab = 1$, then there will be no solution from Subcase 3.1 3.2, 3.3 and 3.4 as $a^2b^2 + a^2b + ab + a + 1 = 0$ implies $1 = 0$, a contradiction, and $a^2b^2 + a^2b + ab + 1 = 0$ implies $a = 1$, also a contradiction. Now in the Subcase 3.5, we get two solutions of Equation (4.21), if and only if $\mathrm{Tr}\left(\frac{1}{a+1}\right) = 0$. Thus, there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(ii) When $ab = \omega$, again we get two solutions of Equation (4.21), if and only if $\mathrm{Tr}\left(\frac{\omega^2}{a+\omega}\right) = 0$. Thus, there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(iii) When $ab = \omega^2$, then we get two solutions of Equation (4.21) if and only if $\mathrm{Tr}\left(\frac{\omega}{a+\omega^2}\right) = 0$. Thus, there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(iv) When $ab = a + 1$, then we get two solutions of Equation (4.21) if and only if $\mathrm{Tr}\left(\frac{1}{a+1}\right) = 0$. Thus there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(v) When $ab = a + \omega$, then we get two solutions of Equation (4.21) if and only if $\mathrm{Tr}\left(\frac{\omega(a+1)}{a^2+\omega^2}\right) = 0$. Thus there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(vi) When $ab = a + \omega^2$, then we get two solutions of Equation (4.21) if and only if $\mathrm{Tr}\left(\frac{\omega^2(a+1)}{a^2+\omega}\right) = 0$. Thus there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.

(vii) It is easy to see that for any fixed $a, b \in \mathbb{F}_{2^n}^*$ with $ab \neq 1, \omega, \omega^2, 1+a, a+\omega, a+\omega^2$, there can be at most two solutions of Equation (4.21) from Subcase 3.1, 3.2, 3.3 and 3.4 as $a^2b^2 + a^2b + ab + a + 1 = a^2b^2 + a^2b + ab + 1$ implies $a = 0$, a contradiction. As we have seen earlier that Subcase 3.5 can contribute atmost two solutions. Thus, we can get at most 8 solutions of Equation (4.18) from Case 3 and Case 4.

From the above discussion, we infer the following:

- When $ab = 1, \omega, \omega^2, a + 1, a + \omega, a + \omega^2$, there can be at most four solutions of Equation (4.18) from Case 3 and Case 4.
- When $ab \neq 1, \omega, \omega^2, 1 + a, a + \omega, a + \omega^2$, there can be at most eight solutions of Equation (4.18) from Case 3 and Case 4.

This completes the proof. □

Chapter 5

Boomerang Uniformity of a Class of Power Maps

In this chapter, we consider the BU of an infinite class of power function $f(X) = X^{2^m-1}$ over the finite field $\mathbb{F}_{2^n}$, where $n = 2m$ with $m > 1$. In Section 5.1, we recall some results concerning the DU of f. Section 5.2 will be devoted on the BU of this power map and we shall show that the power map f is boomerang 2-uniform when $n \equiv 0 \pmod 4$ (i.e. when m is even) and boomerang 4-uniform when $n \equiv 2 \pmod 4$ (i.e. when m is odd), respectively. Cid et al. [19] (see also [42, Theorem 1]) showed that for permutation functions f, $\Delta_f \leq \mathcal{B}_f$. We show that for non-permutations, this is not necessarily true.

5.1 Differential Uniformity of X^{2^m-1}

The differential properties of the power maps of the form X^{2^t-1} over $\mathbb{F}_{2^n}$, $1 < t < n$, have been considered in [5] where authors computed DDT entries $\Delta_f(1, b)$ by determining roots of linearized polynomials of the form $X^{2^t} + bX^2 + (b + 1)X = 0$. In fact, in [5] authors introduced a new type of functions, called locally-APN functions, defined as follows.

Definition 24. Let f be a power map from $\mathbb{F}_{2^n}$ to itself. Then the function f is said to be locally-APN if

$$\Delta_f(1, b) \leq 2, \text{ for all } b \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2.$$

In [5] authors gave an infinite class of locally-APN functions by showing that the power map X^{2^m-1} over $\mathbb{F}_{2^{2m}}$ is locally-APN.

The following lemma concerning the DDT entries of the power map X^{2^m-1} over $\mathbb{F}_{2^{2m}}$ has already been proved in [5, Theorem 7]. However, we reproduce its proof here for the sake of convenience of the readers, as it will be used in computing the BCT entries in Section 5.2.

Lemma 5.1.1. *Let $f(X) = X^{2^m-1}$ be a power map defined on the finite field $\mathbb{F}_{2^{2m}}$. Then $\Delta_f(1,0) = 2^m - 2$, $\Delta_f(1,b) \leq 2$ for all $b \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$ and*

$$\Delta_f(1,1) = \begin{cases} 2 & \text{if } m \text{ is even,} \\ 4 & \text{if } m \text{ is odd.} \end{cases}$$

Proof. For any $b \in \mathbb{F}_{2^{2m}}$, consider the DDT entry at point $(1,b)$, which is given by the number of solutions in $\mathbb{F}_{2^{2m}}$ of the following equation

$$(X+1)^{2^m-1} + X^{2^m-1} = b. \tag{5.1}$$

We shall now split the analysis to find the number of solutions of the above equation in the following cases.

Case 1. Let $b = 0$. It is easy to observe that $X = 0, 1$ are not solutions of the above Equation (5.1). For $X \neq 0, 1$, Equation (5.1) reduces to

$$\left(\frac{X+1}{X}\right)^{2^m-1} = 1.$$

If we let $Y = 1 + X^{-1}$, then the above equation reduces to $Y^{2^m-1} = 1$. Since $\gcd(2^m - 1, 2^{2m} - 1) = 2^m - 1$, this equation has exactly $2^m - 2$ solutions in $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$ and hence $\Delta_f(1,0) = 2^m - 2$.

Case 2. Let $b = 1$. Notice that in this case, $X = 0$ and $X = 1$ are solutions of Equation (5.1). For $X \neq 0, 1$, Equation (5.1) is equivalent to

$$\frac{X^{2^m}+1}{X+1} + \frac{X^{2^m}}{X} = 1 \iff X^{2^m} + X^2 = 0.$$

With $X^2 = Y$, the above equation becomes

$$Y(Y^{2^{m-1}-1} + 1) = 0. \tag{5.2}$$

Notice that when $m > 1$ is odd then $\gcd(m-1, 2m) = 2$ and the above equation (5.2) can have at most 4 solutions, namely $0, 1, \omega, \omega^2$, where ω is a primitive cubic root of unity. Hence $\Delta_f(1,1) = 4$. When $m > 1$ is even then $\gcd(m-1, 2m) = 1$, thus $0, 1$ are only solutions of the Equation (5.2). Hence in this case $\Delta_f(1,1) = 2$.

Case 3. Let $b \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$. It is easy to see that in this case $X = 0$ and $X = 1$ are not solutions of Equation (5.1). Therefore, the DDT entry at $(1, b)$ is the number of solutions in $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$ of the following equivalent equation

$$X^{2^m} + bX^2 + (b+1)X = 0. \tag{5.3}$$

Now, raising the above equation to the power 2^m, we have

$$X^{2^{2m}} + b^{2^m} X^{2^{m+1}} + (b^{2^m} + 1)X^{2^m} = 0. \tag{5.4}$$

Combining (5.3) and (5.4), we have

$$b^{2^m+2}X^4 + (b^{2^m+2} + b^{2^m+1} + b^{2^m} + b)X^2 + (b^{2^m+1} + b^{2^m} + b)X = 0.$$

We note that the above equation can have at most 4 solutions in $\mathbb{F}_{2^{2m}}$, two of which are 0 and 1 and thus it can have at most two solutions in $\mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$. Therefore for $b \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$, $\Delta_f(1, b) \leq 2$. This completes the proof. □

5.2 Boomerang Uniformity of X^{2^m-1}

In this section, we shall discuss the BU of the locally-APN functions given in the previous section. The BU of the power maps of the type X^{2^t-1} over $\mathbb{F}_{2^n}$ has been considered in [62], where the authors give bounds on the BU in terms of the DU under the condition $\gcd(n, t) = 1$ and also show that the power permutation X^7 has BU 10 over $\mathbb{F}_{2^n}$, where $n \geq 8$ is even and $\gcd(3, n) = 1$. The following theorem gives the BU of the power map $f(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m}}$ where $m > 1$ is odd.

Theorem 25. *Let $f(X) = X^{2^m-1}$, $m > 1$ odd, be a power map from the finite field $\mathbb{F}_{2^{2m}}$ to itself. Then, the BU of f is* 4.

Proof. Recall that for any $b \in \mathbb{F}_q^*$, $q = 2^{2m}$, the BCT entry $\mathcal{B}_f(1, b)$ at point $(1, b)$ of f, is given by the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the following system of equations

$$\begin{cases} X^{2^m-1} + Y^{2^m-1} = b, \\ (X+1)^{2^m-1} + (Y+1)^{2^m-1} = b. \end{cases} \tag{5.5}$$

Notice that the above system (5.5) cannot have solutions of the form (X_1, Y_1) with $X_1 = Y_1$ as $b \neq 0$. Also it is easy to observe that if (X_1, Y_1) is a solution of the above system (5.5), then so are $(Y_1, X_1), (X_1 + 1, Y_1 + 1)$ and $(Y_1 + 1, X_1 + 1)$. We shall split the analysis of the solutions of the system (5.5) in the following five cases.

Case 1. Let $X = 0$. In this case, the system (5.5) reduces to

$$\begin{cases} Y^{2^m-1} = b, \\ (Y+1)^{2^m-1} + Y^{2^m-1} = 1. \end{cases} \tag{5.6}$$

From Lemma 5.1.1, we know that the second equation of the above system has four solutions, namely $Y = 0, 1, \omega$ and ω^2. Also, since m is odd, we have $2^m - 1 \equiv 1 \pmod 3$. Since $b \neq 0$, $Y = 0$ cannot be a solution of the system (5.6) and $Y = 1, \omega$ and ω^2 will be a solution of the system (5.6) when $b = 1, \omega$ and ω^2, respectively. Equivalently, when $b = 1, \omega, \omega^2$ then $(0, 1), (0, \omega), (0, \omega^2)$ are solutions of the system (5.5), respectively. When $b \in \mathbb{F}_q \backslash \mathbb{F}_{2^2}$ then there is no solution of the system (5.5) of the form $(0, Y)$.

Case 2. Let $X = 1$. In this case, the system (5.5) reduces to

$$\begin{cases} Y^{2^m-1} = b + 1, \\ (Y+1)^{2^m-1} + Y^{2^m-1} = 1. \end{cases} \tag{5.7}$$

Similar to the previous case, the second equation of the above system (5.7) has four solutions, namely $Y = 0, 1, \omega$ and ω^2. Since $b \neq 0$, $Y = 1$ cannot be a solution of (5.7) and $Y = 0, \omega$ and ω^2 will be a solution of (5.7), when $b = 1, \omega^2$ and ω, respectively. Equivalently, when $b = 1, \omega, \omega^2$ then $(1, 0), (1, \omega^2), (1, \omega)$ are solutions of the system (5.5), respectively. When $b \in \mathbb{F}_q \backslash \mathbb{F}_{2^2}$ then there is no solution of the system (5.5) of the form $(1, Y)$.

Case 3. Let $Y = 0$. Since the system (5.5) is symmetric in the variables X and Y,

this case directly follows from Case 1. That is, when $b = 1, \omega, \omega^2$ then $(1, 0), (\omega, 0), (\omega^2, 0)$ are solutions of the system (5.5), respectively. When $b \in \mathbb{F}_q \backslash \mathbb{F}_{2^2}$ then there is no solution for (5.5) of the form $(X, 0)$.

Case 4. Let $Y = 1$. This case directly follows from Case 2. That is, when $b = 1, \omega, \omega^2$ then $(0, 1), (\omega^2, 1), (\omega, 1)$ are solutions of the system (5.5), respectively. When $b \in \mathbb{F}_q \backslash \mathbb{F}_{2^2}$ then there is no solution for (5.5) of the form $(X, 1)$.

Case 5. Let $X, Y \neq 0, 1$. In this case, the system (5.5) reduces to

$$\begin{cases} X^{2^m}Y + XY^{2^m} = bXY, \\ (X+Y)^{2^m} + (b+1)(X+Y) + b = 0. \end{cases} \tag{5.8}$$

Let $Y = X + Z$. Then, the above system becomes

$$\begin{cases} X^{2^m}Z + XZ^{2^m} = bX(X+Z), \\ Z^{2^m} + (b+1)Z + b = 0. \end{cases} \tag{5.9}$$

Now, raising the second equation of the above system to the power 2^m, we have

$$(b^{2^m} + 1)Z^{2^m} + Z + b^{2^m} = 0. \tag{5.10}$$

Combining the second equation of (5.9) and Equation (5.10), we obtain

$$((b+1)^{2^m+1} + 1)(Z+1) = 0. \tag{5.11}$$

Therefore, the system (5.9) reduces to

$$\begin{cases} X^{2^m}Z + XZ^{2^m} = bX(X+Z), \\ ((b+1)^{2^m+1} + 1)(Z+1) = 0. \end{cases} \tag{5.12}$$

Now, we shall consider following two cases

Subcase 5.1. Let $(b+1)^{2^m+1} \neq 1$. In this case, the first equation of (5.12) reduces to

$$X^{2^m} + bX^2 + (b+1)X = 0,$$

which is equivalent to

$$b^{2^m+2}X^4 + (b^{2^m+2} + b^{2^m+1} + b^{2^m} + b)X^2 + (b^{2^m+1} + b^{2^m} + b)X = 0. \tag{5.13}$$

When $b = 1$, the above equation becomes $X^4 + X = 0$, which has four solutions $X = 0, 1, \omega, \omega^2$. Since we assumed $X, Y \neq 0, 1$, the only solutions we consider are $X = \omega$ and ω^2. Thus for $b = 1$, (ω, ω^2) and (ω^2, ω) are solutions of the system (5.9). When $b \in \mathbb{F}_q \backslash \mathbb{F}_2$ with $(b+1)^{2^m+1} \neq 1$, by Lemma 5.1.1, Equation (5.13) can have at most two solutions.

Subcase 5.2. Let $(b+1)^{2^m+1} = 1$. It is more convenient, now, to work with (5.8). We then raise the first equation of the system (5.8) to the 2^m-th power obtaining

$$X^{2^{2m}}Y^{2^m} + Y^{2^{2m}}X^{2^m} = b^{2^m}X^{2^m}Y^{2^m},$$

which is equivalent to

$$XY^{2^m} + YX^{2^m} = b^{2^m}X^{2^m}Y^{2^m}.$$

Combining this with the first equation of (5.8), we get

$$b^{2^m}X^{2^m}Y^{2^m} = bXY,$$

and so, $bXY = \alpha \in \mathbb{F}_{2^m}^*$. Using $Y = \frac{\alpha}{bX}$ in the first equation of (5.8), we obtain

$$X^{2^m-1}\frac{1}{b} + X^{1-2^m}\frac{1}{b^{2^m}} = 1. \tag{5.14}$$

Label $T = X^{2^m-1}$. Then the above equation reduces to

$$\begin{aligned} &\frac{T}{b} + \frac{T^{-1}}{b^{2^m}} = 1 \\ \iff &\frac{T^2}{b} + \frac{1}{b^{2^m}} = T \\ \iff &T^2b^{2^m} + b = Tb^{2^m+1}. \end{aligned}$$

Since, $(b+1)^{2^m+1} = 1$, by expansion, we get $b^{2^m+1} + b^{2^m} + b = 0$, and so, $b^{2^m+1} = b^{2^m} + b$. The previous equation becomes

$$T^2b^{2^m} + b = Tb^{2^m} + Tb \iff (Tb^{2^m} + b)(T+1) = 0.$$

If $T = 1$, then $X \in \mathbb{F}_{2^m}$ and so, $bY \in \mathbb{F}_{2^m}$. Taking this back into (5.8), we then obtain

$$\begin{cases} Y^{2^m} + (b+1)Y = 0, \\ Y^{2^m} + (b+1)Y = (X+1)b \end{cases}$$

which is inconsistent with $X \neq 1$ and $b \in \mathbb{F}_q^*$. If $Tb^{2^m} + b = 0$, then we have

$$\begin{aligned} & Tb^{2^m} + b = 0 \\ \iff & Tb^{2^m-1} + 1 = 0 \\ \iff & (bX)^{2^m-1} = 1. \end{aligned}$$

Therefore $bX \in \mathbb{F}_{2^m}$ and hence $\frac{\alpha}{bX} = Y \in \mathbb{F}_{2^m}$. Taking this back into (5.8), we then obtain

$$\begin{cases} X^{2^m} + (b+1)X = 0, \\ X^{2^m} + (b+1)X = (Y+1)b \end{cases}$$

which is inconsistent with $Y \neq 1$ and $b \in \mathbb{F}_q^*$. This completes the proof. □

Example 5.2.1. As an example, we checked by SageMath that the DU of the non-permutation power map X^7 over $\mathbb{F}_{2^6}$ is 6, whereas its BU is 4.

The following theorem gives the BU of the power map $f(X) = X^{2^m-1}$ over $\mathbb{F}_{2^{2m}}$, where $m > 1$ is even.

Theorem 26. *Let $f(X) = X^{2^m-1}$, $m > 1$ even, be a power map from the finite field $\mathbb{F}_{2^{2m}}$ to itself. Then, the BU of f is 2.*

Proof. Following similar arguments as in the proof of Theorem 25, it is straightforward to see that when $b = 1$, $(0, 1)$ and $(1, 0)$ are the only solutions of the system (5.5) with either of the coordinates X, Y being 0 or 1. On the other hand, when $b \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$, there is no solution of the system (5.5) with either of the coordinates $X, Y \in \{0, 1\}$.

We now consider the case when $X, Y \neq 0, 1$. In this case, the system (5.5) reduces to

$$\begin{cases} X^{2^m}Y + XY^{2^m} = bXY, \\ (X+Y)^{2^m} + (1+b)(X+Y) + b = 0. \end{cases} \tag{5.15}$$

Let $Y = X + Z$. Now, raising the second equation of the above system to the power 2^m and adding it to the second equation of the above system, we have

$$\begin{cases} X^{2^m}Z + XZ^{2^m} = bX(X+Z), \\ ((b+1)^{2^m+1} + 1)(Z+1) = 0. \end{cases} \tag{5.16}$$

Now, we shall consider the following two cases.

Case 1. Let $(b+1)^{2^m+1} \neq 1$. In this case, the system (5.16) reduces to

$$X^{2^m} + bX^2 + (b+1)X = 0,$$

which is equivalent to

$$b^{2^m+2}X^4 + (b^{2^m+2} + b^{2^m+1} + b^{2^m} + b)X^2 + (b^{2^m+1} + b^{2^m} + b)X = 0. \tag{5.17}$$

When $b = 1$, the above equation becomes $X^4 + X = 0$, which has two solutions $X = 0, 1$, as m is even. Since we assumed $X, Y \neq 0, 1$, we do not get any solution of the system (5.17) in this case. When $b \in \mathbb{F}_{2^{2m}} \backslash \mathbb{F}_2$ with $(b+1)^{2^m+1} \neq 1$, by Lemma 5.1.1, Equation (5.17) can have at most two solutions.

Case 2. Let $(b+1)^{2^m+1} = 1$, the argument is similar to Subcase 5.2 of Theorem 25 and in this case the system (5.5) will have no solution. □

Example 5.2.2. The DU of the non-permutation power map X^{15} over $\mathbb{F}_{2^8}$ is 14, whereas its BU is 2.

Chapter 6

The Binary Gold Function and its c-Boomerang Connectivity Table

In this chapter, we give a complete description of the cBCT entries for the Gold function over finite fields of even characteristic, by using double Weil sums. The chapter is structured as follows. Section 6.1 contains some preliminary results that will be used across the sections. Section 6.2 contains the characterization of cBCT entries in terms of double Weil sums. For $c = 1$, we further simplify this expression in Section 6.3. In fact, Theorem 28 generalizes previously known results of Boura and Canteaut [8]. In Section 6.4, we consider the case when $c \in \mathbb{F}_{2^e} \backslash \mathbb{F}_2$, where $e = \gcd(k, n)$. In Section 6.5, we discuss the general case.

6.1 Preliminaries

First, we shall state a theorem which gives a nice connection between cBCT and cDDT entries of the power map X^d over $\mathbb{F}_{2^n}$ and is a "binary" analogue of [52, Theorem 1].

Theorem 27. *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 cBCT 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

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

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 6.1.1. *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 [21], 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 6.1.2. *[21, 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 [21]. In what follows, we shall denote, by $\mathfrak{S}(u,v)$, the Weil sum $\sum_{X\in\mathbb{F}_q}\chi(uX^{2^k+1}+vX)$. The following lemma gives the explicit expression for $\mathfrak{S}(u,0)$.

Lemma 6.1.3. *[21] Let χ 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 6.1.1, 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 6.1.4. *[21, Theorem 4.2] Let $v \neq 0$ and n/e is 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 6.1.5. *[21, Theorem 5.3] Let $u, v \in \mathbb{F}_q^*$ and n/e is 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*

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

6.2 The Binary Gold Function

In this section, we shall give the explicit expression for the cBCT entries of the Gold function X^{2^k+1} over $\mathbb{F}_{2^n}$, for all $c \neq 0$. Recall that the cBU 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

$$\begin{cases} X^d + cY^d = b \\ (X+1)^d + c^{-1}(Y+1)^d = b. \end{cases} \tag{6.1}$$

As done in [52], for $b \neq 0$ and fixed $c \neq 0$, the number of solutions $(X,Y) \in \mathbb{F}_q^2$ of the system (6.1) is given by

$$\begin{aligned} {}_c\mathcal{B}_f(1,b) &= \frac{1}{q^2} \sum_{X,Y \in \mathbb{F}_q} \sum_{\alpha \in \mathbb{F}_q} \chi_1\left(\alpha\left(X^d + cY^d + b\right)\right) \sum_{\beta \in \mathbb{F}_q} \chi_1\left(\beta\left((X+1)^d + c^{-1}(Y+1)^d + b\right)\right) \\ &= \frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q} \chi_1\left(b(\alpha+\beta)\right) \sum_{X \in \mathbb{F}_q} \chi_1\left(\alpha X^d + \beta(X+1)^d\right) \\ &\quad \sum_{Y \in \mathbb{F}_q} \chi_1\left(c\alpha Y^d + c^{-1}\beta(Y+1)^d\right) \\ &= \frac{1}{q^2} \sum_{\alpha,\beta \in \mathbb{F}_q} \chi_1\left(b(\alpha+\beta)\right) S_{\alpha,\beta} S_{c\alpha,c^{-1}\beta}, \end{aligned}$$

where $S_{\alpha,\beta} = \sum_{X \in \mathbb{F}_q} \chi_1\left(\alpha X^d + \beta(X+1)^d\right)$. Therefore, the problem of computing the cBCT 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:

$$S_{\alpha,\beta} = \sum_{X \in \mathbb{F}_q} \chi_1\left(\alpha X^{2^k+1} + \beta(X+1)^{2^k+1}\right)$$

$$
\begin{aligned}
&= \chi_1(\beta) \sum_{X\in\mathbb{F}_q} \chi_1((\alpha+\beta)X^{2^k+1})\ \chi_1(\beta X^{2^k}+\beta X)\\
&= \chi_1(\beta) \sum_{X\in\mathbb{F}_q} \chi_1((\alpha+\beta)X^{2^k+1})\ \chi_1((\beta^{2^{n-k}}X)^{2^k}+\beta X)\\
&= \chi_1(\beta) \sum_{X\in\mathbb{F}_q} \chi_1((\alpha+\beta)X^{2^k+1})\ \chi_1((\beta^{2^{n-k}}+\beta)X)\\
&= \chi_1(\beta) \sum_{X\in\mathbb{F}_q} \chi_1((\alpha+\beta)X^{2^k+1}+(\beta^{2^{n-k}}+\beta)X)\\
&= \chi_1(\beta) \sum_{X\in\mathbb{F}_q} \chi_1(AX^{2^k+1}+BX),
\end{aligned}
$$

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 6.1.4 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 6.1.3 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 6.1.2, 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 6.1.5, 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 6.1.5 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 6.1.5, $S_{\alpha,\beta} = 0$.

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 α and β, respectively. We shall now explicitly compute the cBCT entry ${}_c\mathcal{B}_f(1,b)$ for $c = 1$, $c \in \mathbb{F}_{2^e} \backslash \mathbb{F}_2$ and $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ in the forthcoming sections.

6.3 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 cBCT entry is given by,

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

Let us denote $T_b = S^2_{\alpha,\beta}$. 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 [45, Proposition 3] showed that the DU 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 [19], we know that the BU of the APN function equals 2. Boura and Canteaut [8, Proposition 8] proved that when n/e is odd and $n \equiv 2 \pmod 4$, then the DU as well as the BU 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 BU of the Gold function for any parameters, when $\frac{n}{e}$ is odd.

Theorem 28. *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 cBCT 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 α, β, 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,

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

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 $\beta \in \mathbb{F}_{2^e}$, $Y_\beta = \mathbb{F}_{2^n}$)

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

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 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_β 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 ϕ, 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 $e \,|\, k$. 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 [15, Corollary 8.9] and [23, 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 $\dim S$,

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

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)

$$\begin{aligned}
{}_1\mathcal{B}_f(1,b) &= 2^e + \frac{2^e}{2^n} \sum_{\substack{\beta \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^e}, \gamma \in \mathbb{F}_{2^n} \\ \mathrm{Tr}_e\left((\beta^{2^{-k}}+\beta)\gamma^{-1}\right)=1}} \chi_1\left(b\gamma^{2^k+1}\right) \\
&= 2^e + \frac{2^e}{2^n} \sum_{\beta \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^e}} \sum_{\gamma^{-1} \in Y_\beta} \chi_1\left(b\gamma^{2^k+1}\right) \\
&= 2^e + \frac{2^e}{2^n} \sum_{\beta \in \mathbb{F}_{2^n}} \sum_{X \in (\beta^{2^{-k}}+\beta)^{-1} + \langle \beta^{2^{-k}}+\beta \rangle^{\perp_e}} \chi_1\left(bX^{-2^k-1}\right)
\end{aligned}$$

(we used here that $Y_\beta = (\beta^{2^{-k}}+\beta)^{-1} + T_\beta$; we also added $\beta \in \mathbb{F}_{2^e}$, as it contributes 0 to the inner sum)

$$= 2^e + \frac{2^e}{2^n} \sum_{\beta \in \mathbb{F}_{2^n}} 2^{-\dim S} \sum_{u \in \left(\langle \beta^{2^{-k}} + \beta \rangle^{\perp_e}\right)^{\perp}} \mathcal{W}_{g_\beta}(u)(-1)^{\mathrm{Tr}\left(u(\beta^{2^{-k}}+\beta)^{-1}\right)}$$

(by Poisson summation with $S^{\perp} = \langle \beta^{2^{-k}} + \beta \rangle^{\perp_e}$, and $g_\beta(X) = \chi_1\big(bX^{-2^k-1}\big)$).

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,

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

$$= 2^e + \frac{2^e}{2^n} 2^{n-e} \sum_{d' \in \mathbb{F}_{2^e}^*, X \in \mathbb{F}_{2^e}} \chi_1(bX^{-2} + d')$$
$$= 2^e - 2^e \delta_0 \left(\mathrm{Tr}_e \left(b^{\frac{1}{2}} \right) \right),$$

where δ_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. □

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 29. *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 cBCT entry ${}_1\mathcal{B}_f(1, b)$ of f at $(1, b)$ is given by*

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

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

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

This completes the proof. □

Corollary 6.3.1. *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 cBU of f satisfies*

$$
{}_c\mathcal{B}_f \le 2^e + 2^{-n}|\mathcal{G}\cup\mathcal{I}\cup\mathcal{K}| + 2^{2e-n}|\mathcal{H}\cup\mathcal{L}|.
$$

6.4 The Case $c \in \mathbb{F}_{2^e}\backslash\mathbb{F}_2$.

Since the case $c = 1$ has already been considered in the previous section, throughout this section we assume that $c \neq 1$. 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 $b \neq 0$, the cBCT entry is given by,

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

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 $A' \neq 0, B' = 0$, 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 30. *Let $f(X) = X^{2^k+1}$, $1 \leq k < n$ be a function on $\mathbb{F}_{2^n}$, $n \geq 2$. Let $c \in \mathbb{F}_{2^e}\backslash\mathbb{F}_2$ and n/e be odd, where $e = \gcd(k,n)$. Then the cBCT entry ${}_c\mathcal{B}_f(1,b)$ of f at $(1,b)$ is given by*

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

where

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

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

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

Then,

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

This completes the proof. □

Corollary 6.4.1. *Let $f(X) = X^{2^k+1}$, $1 \le k < n$, be a function on $\mathbb{F}_q$, $n \ge 2$. Let $c \in \mathbb{F}_{2^e} \setminus \mathbb{F}_2$ and n/e be odd, where $e = \gcd(k,n)$. With the notations of the previous theorem, the cBU of f satisfies*

$$
{}_c\mathcal{B}_f \le 1 + 2^{e-n}|\mathcal{F}\cap\mathcal{F}'|.
$$

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

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

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

Then,

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

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

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

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

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

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

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

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

Then,

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

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 31. *Let $f(X)=X^{2^k+1}$, $1\le k<n$ be a function on $\mathbb{F}_{2^n}$, $n\ge 2$. Let $c\in\mathbb{F}_{2^e}\backslash\mathbb{F}_2$ and n/e be even, where $e=\gcd(k,n)$. With the previous notations, the cBCT entry ${}_c\mathcal{B}_f(1,b)$ of f at $(1,b)$ is given by*

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

$$+\sum_{(\alpha,\beta)\in\mathcal{H}\cap\mathcal{H}'}\chi_1(b(\alpha+\beta))T_b^{[3(b)]}++\sum_{(\alpha,\beta)\in(\mathcal{I}\cup\mathcal{K})\cap(\mathcal{I}'\cup\mathcal{K}')}\chi_1(b(\alpha+\beta))T_b^{[4(b)]}$$
$$+\sum_{(\alpha,\beta)\in(\mathcal{I}\cup\mathcal{K})\cap\mathcal{L}'}\chi_1(b(\alpha+\beta))T_b^{[4(b)]}+\sum_{(\alpha,\beta)\in\mathcal{L}\cap(\mathcal{I}'\cup\mathcal{K}')}\chi_1(b(\alpha+\beta))T_b^{[4(b)]}$$
$$+\sum_{(\alpha,\beta)\in\mathcal{L}\cap\mathcal{L}'}\chi_1(b(\alpha+\beta))T_b^{[4(b)]}\Bigg).$$

6.5 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 $c\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^e}$. Recall that for any fixed $b\neq 0$, the cBCT entry is given by,

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

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

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

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

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

   (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

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

We now summarize the above discussion in the following theorem.

Theorem 32. *Let $f(X) = X^{2^k+1}$, $1 \leq k < n$ be a function on $\mathbb{F}_{2^n}$, $n \geq 2$. Let $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ and n/e be odd, where $e = \gcd(k, n)$. Then the cBCT entry ${}_c\mathcal{B}_f(1, b)$ of f at $(1, b)$ is given by*

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

Proof.

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

□

Corollary 6.5.1. *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 cBU of f satisfies*

$${}_c\mathcal{B}_f \le 1 + \left(\frac{2}{n/e}\right)^e \cdot 2^{\frac{e-n}{2}} |(\mathcal{A}\cap\mathcal{F}')\cup(\mathcal{A}'\cap\mathcal{F})| + 2^{e-n}|\mathcal{F}\cap\mathcal{F}'|.$$

Case 2: n/e is even.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 33. *Let $f(X) = X^{2^k+1}$, $1 \leq k < n$ be a function on $\mathbb{F}_{2^n}$, $n \geq 2$. Let $c \in \mathbb{F}_{2^n} \backslash \mathbb{F}_{2^e}$ and n/e be even, where $e = \gcd(k, n)$. With the prior notations, the cBCT 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\mathcal{A}\cap\mathcal{A}'} \chi_1(b(\alpha+\beta))T_b^{[1(a)]} + \sum_{(\alpha,\beta)\in\mathcal{A}\cap(\mathcal{I}'\cup\mathcal{K}')} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{A}\cap\mathcal{L}'} \chi_1(b(\alpha+\beta))T_b^{[1(b)]} + \sum_{(\alpha,\beta)\in\mathcal{G}\cap\mathcal{G}'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{G}\cap\mathcal{H}'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + \sum_{(\alpha,\beta)\in\mathcal{H}\cap\mathcal{G}'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{H}\cap\mathcal{H}'} \chi_1(b(\alpha+\beta))T_b^{[3(b)]} + \sum_{(\alpha,\beta)\in\mathcal{G}\cap(\mathcal{I}'\cup\mathcal{K}')} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{G}\cap\mathcal{L}'} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} + \sum_{(\alpha,\beta)\in\mathcal{H}\cap(\mathcal{I}'\cup\mathcal{K}')} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{H}\cap\mathcal{L}'} \chi_1(b(\alpha+\beta))T_b^{[3(c)]} + \sum_{(\alpha,\beta)\in\mathcal{A}'\cap(\mathcal{I}\cup\mathcal{K})} \chi_1(b(\alpha+\beta))T_b^{[4(a)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{A}'\cap\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(a)]} + \sum_{(\alpha,\beta)\in\mathcal{G}'\cap(\mathcal{I}\cup\mathcal{K})} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{G}'\cap\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(c)} + \sum_{(\alpha,\beta)\in\mathcal{H}'\cap(\mathcal{I}\cup\mathcal{K})} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{H}'\cap\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(c)]} + \sum_{(\alpha,\beta)\in(\mathcal{I}\cup\mathcal{K})\cap(\mathcal{I}'\cup\mathcal{K}')} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \\
& + \sum_{(\alpha,\beta)\in(\mathcal{I}\cup\mathcal{K})\cap\mathcal{L}'} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} + \sum_{(\alpha,\beta)\in(\mathcal{I}'\cup\mathcal{K}')\cap\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \\
& + \sum_{(\alpha,\beta)\in\mathcal{L}'\cap\mathcal{L}} \chi_1(b(\alpha+\beta))T_b^{[4(d)]} \Bigg).
\end{aligned}$$

Chapter 7

Conclusion

In this chapter, we shall give a brief summary of the problems considered in this thesis and give some future directions related to the these problems.

In Chapter 2, we classified planar DO polynomials from the composition of the reversed Dickson polynomials of arbitrary kind and monomials X^d, where d is a positive integer, over finite fields of odd characteristic. The permutation behaviour of reversed Dickson polynomials is also an interesting problem. The classification of permutation polynomials from reversed Dickson polynomials is not known even for the prime fields $\mathbb{F}_p$, p odd. Therefore, it is an interesting problem to classify permutation polynomials from the reversed Dickson polynomials.

In Chapter 3, we used Dickson polynomials techniques to compute the cDU of certain power maps over finite fields of odd characteristic. We also found that recently published necessary conditions, which give a relationship between the difference function of a monomial and the Dickson polynomial of first kind, are also sufficient. Next, for $c = -1$, we gave several classes of PcN functions and functions with low cDU, and we proposed two conjectures based upon some computational data. We also obtained a class of polynomials that are PcN for all $c \neq 1$, in every characteristic. Further, we discussed the affine, extended affine and CCZ-equivalence as it relates to cDU. We then concentrated on perturbation of a PcN function to also be PcN and gave necessary and sufficient conditions in some cases. We also showed that in some instances such perturbations do not produce PcN functions. It would be very interesting to find other perturbations, linear or not, that may decrease the cDU.

In Chapter 4, we considered the cDDT entries, as well as, the BCT entries for an involution which has been used to construct a class of differentially 4-uniform permutations, by Beierle and Leander [3]. We also considered the cDU and BU of another differentially 4-uniform function given by Tan et al. [55] and gave bounds for its cDU and BU. The cDU concept, introduced barely a year ago, has proven quite interesting and attractive, mathematically. It would be interesting to construct more function with low cDU over finite fields.

In Chapter 5, we computed the BU of the power map X^{2^m-1} over $\mathbb{F}_{2^{2m}}$. As an immediate consequence, we found that the DU is not necessarily smaller than the BU (for non-permutations), as it was previously shown for permutations and assumed to hold for non-permutations, as well. It would be interesting to construct more functions for which DU is strictly greater than BU.

In Chapter 6, we computed the cBCT entries for the Gold functions over finite fields of even characteristic, for all $c \in \mathbb{F}_{2^n}^*$, using product of Weil sums. In the process, we generalised a result of Boura and Canteaut [8]. It would be interesting to construct more function with low cBU over finite fields.

Bibliography

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

[2] D. Bartoli, M. Calderini, *On construction and (non)existence of c-(almost) perfect nonlinear functions*, Finite Fields Appl., 72 (2021), 101835.

[3] C. Beierle, G. Leander, 4-*uniform permutations with null nonlinearity*, Cryptogr. Commun. 12 (2020), 1133–1141.

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

[5] C. Blondeau, A. Canteaut, P. Charpin, *Differential properties of* $X \mapsto X^{2^t-1}$, IEEE Trans. Inf. Theory 57(12) (2011), 8127–8137.

[6] N. Borisov, M. Chew, R. Johnson, D. Wagner, *Multiplicative differentials*. In: J. Daemen and V. Rijmen (eds.) Proceedings of Fast Software Encryption - FSE 2002. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol. 2365 (2002), 17–33.

[7] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language, J. Symbolic Comput. 24 (1997), 235–265.

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

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

[10] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, *An APN permutation in dimension six*. In: McGuire, G. et al. (eds.) Proceedings of the 9th international conference on finite fields and applications, Contemporary Mathematics, 518 (2010), 33–42.

[11] L. Budaghyan, C. Carlet, G. Leander, *Constructing new APN functions from known ones*, Finite Fields Appl. 15 (2009), 150–159.

[12] M. Calderini, I. Villa, *On the boomerang uniformity of some permutation polynomials*, Cryptogr. Commun. 12 (2020), 1161–1178.

[13] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. 15 (1998), 125–156.

[14] C. Carlet, C. Ding, J. Yuan, *Linear codes from perfect nonlinear mappings and their secret sharing schemes*, IEEE Trans. Inform. Theory, 51 (6) (2005), 2089–2102.

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

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

[17] P. Charpin, G. Kyureghyan, *On a class of permutation polynomials over* $\mathbb{F}_{2^n}$ In: Golomb S.W., Parker M.G., Pott A., Winterhof A. (eds) Proceedings of Sequences and Their Applications - SETA 2008. Lecture Notes in Comput. Sci., Springer, Berlin, Heidelberg, vol 5203 (2008), 368–376.

[18] P. Charpin, G. Kyureghyan, *When does* $G(X) + \gamma Tr(H(X))$ *permute* $\mathbb{F}_{p^n}$, Finite Fields Appl. 15(5) (2009), 615–632.

[19] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song, *Boomerang connectivity table: a new cryptanalysis tool*. In: Nielsen J., Rijmen V. (eds.), Advances in

Cryptology-EUROCRYPT 2018, LNCS 10821, Springer, Cham, (2018), 683–714.

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

[21] R. S. Coulter, *On the evaluation of a class of Weil sums in characteristic 2*, New Zealand J. of Math., vol. 28 (1999), 171–184.

[22] R. S. Coulter, R. W. Mattews, *Dembowski-Ostrom polynomials from Dickson polynomials*, Finite Fields Appl., 16 (2010), 369–379.

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

[24] P. Dembowski, T. G. Ostrom, *Planes of order n with collineation groups of order* n^2, Math. Z., 103 (1968), 239–258.

[25] L. E. Dickson, *The analytic presentation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. 11 (1897), 65–120.

[26] J. F. Dillon, H. Dobbertin, *New cyclic difference sets with Singer parameters*, Finite Fields Appl. 10 (2004), 342–389.

[27] Y. Edel, G. Kyureghyan, A. Pott, *A new APN funciton which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory 52:2 (2006), 744–747.

[28] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inform. Theory 66:9 (2020), 5781–5789.

[29] N. Fernando, *Reversed Dickson polynomials of the* $(k+1)$*-th kind over finite fields*, J. Number Theory, 172 (2017), 234–255.

[30] M.J. Ganley, E. Spence, *Relative difference sets and quasiregular collineation groups,* J. Combin. Theory Ser. A, 19 (1975), 134–153.

[31] R. Gold, *Maximal recursive sequences with 3-valued recursive cross-correlation functions*, IEEE Trans. Inform. Theory 14 (1968), 154–156.

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

[33] X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl., 15 (2009), 748-773.

[34] J. Lahtonen, G. McGuire, H.N. Ward, *Gold and Kasami-Welch functions, quadratic forms and bent functions,* Adv. Math. Commun. 1 (2) (2007), 243–250.

[35] R. Lidl, G.L. Mullen, G. Turnwald, *Dickson Polynomials*, Pitman Monogr. Surveys Pure Appl. Math., vol. 65, Longman Scientific and Technical, Essex, England, 1993.

[36] R. Lidl, H. Niederreiter, *Finite Fields. Encyclopedia of Mathematics and Its Applications*, vol. 20. Addison-Wesley Publishing Company, Reading (1983).

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

[38] K. Li, C. Li, T. Helleseth, L. Qu, *Cryptographically strong permutations from the butterfly structure*, Des. Codes Cryptogr. 89 (2021), 737–761.

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

[40] S. Mesnager, L. Qu, *On two-to-one mappings over finite fields*, IEEE Trans. Inf. Theory 65:12 (2019), 7884–7895.

[41] S. Mesnager, C. Riera, P. Stănică, H. Yan and Z. Zhou, *Investigations on c-(almost) perfect nonlinear functions*, IEEE Trans. Inform. Theory (2021), `https://doi.org/10.1109/TIT.2021.3081348`.

[42] S. Mesnager, C. Tang, M. Xiong, *On the boomerang uniformity of quadratic permutations*, Des. Codes Cryptogr. 88(10) (2020), 2233–2246.

[43] G.L. Mullen, D. Panario, *Handbook of Finite Fields. Series: Discrete Mathematics and Its Applications*, CRC Press (2013).

[44] W. Nöbauer, *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math., 231 (1968), 215–219.

[45] K. Nyberg, *Differentially uniform mappings for cryptography.* In: Helleseth T. (eds.), Advances in Cryptology–EUROCRYPT 1993, LNCS 765, Springer, Berlin, Heidelberg, (1994), 55–64.

[46] J. Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new familiees of asymmetric algorithms*, Advances in Cryptology - Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Comput. Sci., vol. 1070 (1996), 33–48.

[47] W. Qiu, Z. Wang, G. Weng, Q. Xiang, *Pseudo-Paley graphs and skew Hadamard difference sets from presemifields*, Des. Codes Cryptogr., 44 (2007), 49–62.

[48] C. Riera, P. Stănică, *Some c-(almost) perfect nonlinear functions*, `https://arxiv.org/abs/2004.02245`.

[49] L. Rónyai, T. Szönyi, *Planar functions over finite fields*, Combinatorica, Vol. 9 (1989), 315–320.

[50] I. Schur, *Über den Zusammenhang zwischen einemem Problem der Zahlentheorie und einem Satz üiber algebraische Funktionen*, Sitzungsber. Akad. Wiss. Berlin (1923), 123–134.

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

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

[53] P. Stănică, A. Geary, *The c-differential behaviour of the inverse function under the EA-equivalence*, Cryptogr. Commun. 13 (2021), 295–306.

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

[55] Y. Tan, L. Qu, C.H. Tan, C. Li, *New families of differentially* 4*-uniform permutations over* $\mathbb{F}_{2^{2k}}$, in: T. Helleseth, J. Jedwab (Eds.), SETA 2012, in: Lect. Notes Comput. Sci., vol. 7280, Springer, Heidelberg, (2012), 25–39.

[56] Z. Tu, N. Li, X. Zeng, J. Zhou, *A class of quadrinomial permutation with boomerang uniformity four*, IEEE Trans. Inf. Theory 66(6) (2020), 3753–3765.

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

[58] Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl., 18 (2013), 814–831.

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

[60] X. Xu, C. Li, X. Zeng, T. Helleseth, *Constructions of complete permutation polynomials*, Des. Codes Cryptogr. 86 (2018), 2869–2892.

[61] H. Yan, S. Mesnager, and Z. Zhou *Power Functions over Finite Fields with Low c-Differential Uniformity*, https://arxiv.org/abs/2003.13019.

[62] Z. Zha, L. Hu, *The Boomerang Uniformity of Power Permutations* X^{2^k-1} *over* $\mathbb{F}_{2^n}$, 2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA), (2019), 1–4.

[63] Z. Zha, L. Hu, *Some classes of power functions with low c-differential uniformity over finite fields*, Des. Codes Cryptogr. (2021), https://doi.org/10.1007/s10623-021-00866-8.

[64] X. Zhang, B. Wu, Z. Liu, *Dembowski-Ostrom polynomials from reversed Dickson polynomials*, J. Syst. Sci. Complex., 29 (2016), 259–271.

List of Publications/Preprints

The thesis is based on the following papers/preprints.

1. N. Fernando, S. U. Hasan, M. Pal, *Dembowski-Ostrom polynomials and reversed Dickson polynomials.* Discret. Appl. Math. 298 (2021), 66–79.

2. S. U. Hasan, M. Pal, C. Riera, P. Stănică, *On the c-differential uniformity of certain maps over finite fields.* Des. Codes Cryptogr. 89(2) (2021), 221–239.

3. S. U. Hasan, M. Pal, P. Stănică, *The c-differential uniformity and boomerang uniformity of some permutation polynomials.* (submitted)

4. S. U. Hasan, M. Pal, P. Stănică, *Boomerang uniformity of a class of power maps.* (submitted)

5. S. U. Hasan, M. Pal, P. Stănică, *The c-boomerang connectivity table for the Gold function in even characteristic.* (submitted)