ON BOOLEAN BENT FUNCTIONS AND THEIR GENERALIZATIONS

Ph. D. THESIS

by

BIMAL MANDAL

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (INDIA)
JULY, 2017

ON BOOLEAN BENT FUNCTIONS AND THEIR GENERALIZATIONS

A THESIS

Submitted in partial fulfilment of the
requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

by

BIMAL MANDAL

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247 667 (INDIA)
JULY, 2017

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled "**ON BOOLEAN BENT FUNCTIONS AND THEIR GENERALIZATIONS**" in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the Department of Mathematics of the Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during a period from July, 2013 to July, 2017 under the supervision of Dr. Sugata Gangopadhyay, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other Institution.

(BIMAL MANDAL)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

(Sugata Gangopadhyay)
Supervisor

Date: **July , 2017**

Dedicated

to

My Parents and Sister

Abstract

In this thesis, we investigate and analyze a special class of Boolean functions namely bent functions. Using the existing techniques we derive the lower bounds of second-order nonlinearity and identify the affine inequivalent classes of bent functions. We further construct some classes of *generalized bent functions*. We identify some classes of Boolean functions having maximum possible second-order nonlinearity by using Gowers norm.

A class of cubic Maiorana–McFarland ($\mathcal{M}$) bent functions having no affine derivative was constructed by Canteaut and Charpin [5], thereby solving an open problem posed by Hou [149]. We construct two classes of cubic $\mathcal{M}$ bent functions with no affine derivative and show their mutual affine inequivalence.

Two (so-called $\mathcal{C}, \mathcal{D}$) classes of permutation-based bent Boolean functions were introduced by Carlet [17] two decades ago, but without specifying some explicit construction methods for their construction (apart from the subclass $\mathcal{D}_0$). We look in more detail at the $\mathcal{C}$ class, and derive some existence and nonexistence results concerning the bent functions in the $\mathcal{C}$ class for many of the known classes of permutations over $\mathbb{F}_{2^n}$. Most importantly, the existence results induce generic methods of constructing bent functions in class $\mathcal{C}$ which possibly do not belong to the completed Maiorana–McFarland class. The question whether the specific permutations and related subspaces we identify in this article indeed give bent functions outside the completed Maiorana–McFarland class remains open.

In 1985, Kumar et al. [98] introduced the concept of *generalized bent functions* $f : \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q$ where $q > 1$ is a positive integer and A. C. Ambrosimov [4] proposed another *generalized bent functions* over finite field. We consider functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, and characterize the subspace sum concept (depending upon the derivative) and give many of its properties. In particular, it is shown that the subspace sum is an affine invariant. Further, we construct two new classes of *generalized bent functions* (so-called $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ where $\mathcal{D}_0^p$ is a subclass of $\mathcal{D}^p$). Also, we prove that the generalized Maiorana–McFarland bent functions and $\mathcal{D}^p$ do not contain one another, and derive some existence and nonexistence results concerning the bent functions in the $\mathcal{C}^p$ class for many of the known classes of permutations over $\mathbb{F}_p^n$.

Carlet [28] introduced a recursive lower bound on nonlinearity profile of Boolean functions. We construct a class of cubic Maiorana–McFarland bent-negabent functions by using Feistel functions and then obtain the lower bound of their second-order nonlinearities.

Gowers [126] introduced a new measure of functions which is called Gowers uniformity norm. The Gowers U_3 norm of a Boolean function is the measure of its resistance to quadratic approximations. We compute Gowers U_3 norms for some classes of Maiorana–McFarland bent functions. In particular, we explicitly determine the value of the Gowers U_3 norm of Maiorana–McFarland bent functions obtained by using APN permutations. Further, it is proved that this value is always smaller than the Gowers U_3 norms of Maiorana–McFarland bent functions obtained by using differentially δ-uniform permutations, for all $\delta \geq 4$. We compute the Gowers U_3 norm for a class of cubic monomial functions, not necessarily bent, and show that for $n = 6$, these norm values are less than that obtained for Maiorana–McFarland bent function constructed by using APN permutations. Further, we computationally show that there exist 6-variable functions in this class which are not bent but achieve the maximum second-order nonlinearity for 6 variables.

List of Publications

Journals

1. Gangopadhyay S., Mandal B. and Stănică P., Gowers U_3 norm of some classes of bent Boolean functions, Designs, Codes and Cryptography, DOI: $10.1007/s10623-017-0383-z$.

2. Mandal B., Gangopadhyay S. and Stănică P., Cubic Maiorana–McFarland bent functions with no affine derivative, International Journal of Computer Mathematics: Computer Systems Theory, vol. 2(1), pp. $14-27$, 2017.

3. Mandal B., Stănică P., Gangopadhyay S. and Pasalic E., An analysis of the $\mathcal{C}$ class of bent function, Fundamenta Informaticae, vol. 146(3), pp. $271-292$, 2016.

4. Gangopadhyay S. and Mandal B., Second Order Nonlinearity Bounds of Cubic MMF Bent-Negabent Functions Constructed by Using Feistel Functions, IPSI BgD Transactions on Advanced Research, vol. 11(1), pp. $13-19$, 2015.

Conferences/ Workshops

1. Mandal B., Stănică P. and Gangopadhyay S., New classes of generalized bent functions, Presented in the 2nd International Workshop on Boolean Functions and their Applications (BFA), Norway, July $3-8$, 2017.

Communicated

1. Mandal B., Stănică P., Gangopadhyay S. and Pasalic E., An analysis of the $\mathcal{C}$ class of bent function, IACR Cryptology ePrint Archive, June, 2015; 588.

Acknowledgement

I would like to express my heartfelt gratitude and sincere thanks to my supervisor Dr. Sugata Gangopadhyay, Associate Professor, Department of Computer Science and Engineering, Indian Institute of Technology Roorkee for his guidance, help and encouragement without which it would not have been possible for me to complete this work. It has been a great experience and joy to work with him. I will never forget his encouragement that he had suggested during the course of my research. I wish to thank Dr. Aditi Gangopadhyay, Associate Professor, Department of Mathematics, Indian Institute of Technology Roorkee for the valuable discussions related to research work.

I would like to thank Prof. Pantelimon Stănică, Department of Applied Mathematics, Naval Postgraduate School, Monterey, USA and Prof. Enes Pasalic, Faculty of Mathematics, Natural Sciences and Information Technologies (Famnit), Slovenia for their guidance, constant encouragement throughout my research work.

Most special thanks goes to my parents Mr. Bivash Mandal and Mrs. Ujjawala Mandal for their love, kind affection, moral support and never ending blessing. I express my heartfelt thanks and regards to my sister Lakhi Mandal and bother-in-law Subhankar Sarkar. I would like to thank all my relatives, especially Mr. Narayan Chandra Ray, Mr. Surajit Ray and Mr. Nitai Chandra Biswas for their moral support and never ending blessing.

I am highly obliged to the Department of Mathematics, Indian Institute of Technology Roorkee for providing the departmental facilities for carrying out my research work. Special thanks to my Student Research Committee members for spending their valuable time and suggestion during my research.

I am thankful to the Ministry of Human and Research Development, India for financial support to carry out this research work.

I am thankful to my lab colleagues Avinash Kumar, Nishant Sinha, Pratap Kumar

Behera and Tajender Kumar. My heartfult thanks to my friends Amit Sharma, Alka Arya, Indira P. Debnath, Kalu R. Meena, Neha Singhal, Rangoli Goyal, Ruchi Panwar, Sumit Malik, Sumita Dahiya and Vikram Singh. I would also like to thank Abhishek Banarjee, Ainul Haque, Kiran Kumar Behera, Priyanka Singhal, Sourav Das and Sumana Ghosh. They provided their helping hand with friendly gesture whenever I needed.

Roorkee
July......, 2017 (Bimal Mandal)

List of Tables

Contents

Chapter 1

Introduction

A Boolean function in n variables maps binary string of length n to the set $\{0, 1\}$. These functions are important in combinatorics, cryptography and coding theory, especially for designing substitution boxes (S-boxes) for block ciphers and robust pseudo-random generators for stream ciphers. For more details we refer to [3,8,36,108,117,122,123,135]. Boolean functions that are used as cryptographic primitives must resist affine approximations, which is achieved by having high nonlinearity. The bent functions defined on an even number of variables (although not directly usable as cryptographic primitives due to not being balanced) have the maximum nonlinearity, that is, they offer maximum resistance to affine approximations. Bent functions are of interest among researchers, since they have maximum Hamming distance from the set of all affine Boolean functions and have very nice combinatorial properties. Several classes of bent functions were constructed by Dillon [56], Rothaus [86], Carlet [17], and Dobbertin [49]. Further, we refer to [15, 33, 65, 67, 85, 89, 102, 106, 120, 135].

The idea of first-order nonlinearity, usually referred to as nonlinearity, was introduced by Rothaus [86]. The relationship between nonlinearity and explicit attack on symmetric ciphers was discovered by Matsui [76]. The idea of higher order nonlinearity has been used in cryptanalysis by Courtois, Golic, Iwata-Kurosawa, Knudsen-Robshaw, Maurer and Millan [57, 78, 101, 129, 138, 144]. More results related to nonlinearity of Boolean functions, we refer to [20, 27–29, 31, 40, 44, 46, 50, 58, 81, 95, 99, 110, 113, 114].

In 2001, Gowers [126] used an analytic technique to give a new proof of Szemerédi's Theorem, and in particular, initiates the study of new measure of functions. Gowers introduced Gowers uniformity norm and it is applied in additive combinatorics [132]. The connection between the Gowers uniformity norms and correlation of a function with polynomials with a certain degree bound is described by results obtained by Gowers, Green and Tao [11,126]. For survey we refer to [11,12,139,143].

In 1985, Kumar et al. [98] introduced the concept of *generalized bent functions.* Different approaches for construction of *generalized bent functions* are introduced in [4,24,63,68,69, 82–84,140]. *Generalized bent functions* play an important role in combinatorial objects such as partial difference sets, strongly regular graphs, association schemes (see [10,155,157]) and codes for Code Division Multiple Access (CDMA) [60,133].

The main goal in this thesis is to identify the classes of bent functions with the highest possible second-order nonlinearity, and to analyze the different classes bent functions in a more explicit way. Our techniques involve the use of Walsh–Hadamard transforms and Gowers uniformity norms of Boolean functions. Also, we work on generalized Boolean functions which are defined over finite field.

1.1 Definitions and notations

Let $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{R}$ be the set of integers, positive integers and real numbers respectively, and $\mathbb{F}_2$ be the prime field of characteristic 2. Let $\mathbb{F}_2^n = \{x = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i = 1, \ldots, n\}$. We denote the extension field of degree n over $\mathbb{F}_2$ by $\mathbb{F}_{2^n}$, and the unit group therein by $\mathbb{F}_{2^n}^*$. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be primitive element if α is a generator of the unit group $\mathbb{F}_{2^n}^*$. For any positive integer n, we always get a finite field with degree of extension n over $\mathbb{F}_2$ by taking a primitive polynomial $p(x)$ of degree n. We know that

$$\mathbb{F}_{2^n} = \mathbb{F}_2[x]/\langle p(x)\rangle = \{c_0 + c_1x + \ldots + c_{n-1}x^{n-1} : c_i \in \mathbb{F}_2, i = 0, 1, \ldots, n-1\}.$$

$\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ both are n dimension vector space over $\mathbb{F}_2$. Let $B = \{b_1, b_2, \ldots, b_n\}$ be an $\mathbb{F}_2$ basic of $\mathbb{F}_{2^n}$. Then any element $a \in \mathbb{F}_{2^n}$ can be written as

$$a = x_1b_1 + x_2b_2 + \ldots + x_nb_n$$

where $x_i \in \mathbb{F}_2$, $i = 1, 2, \ldots, n$. Using the following mapping one can check that $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ are vector isomorphism over $\mathbb{F}_2$:

$$x = (x_1, x_2, \ldots, x_n) \longmapsto x_1 b_1 + x_2 b_2 + \ldots + x_n b_n$$

where $\{b_1, b_2, \ldots, b_n\}$ is an $\mathbb{F}_2$ basic of $\mathbb{F}_{2^n}$. With respect to the basic B defined as above, the n-tuple vector $(x_1, x_2, \ldots, x_n)$ is called the coordinates of $x \in \mathbb{F}_{2^n}$.

Example 1.1.1. *Let $n = 3$ and α be a root of the primitive polynomial $x^3 + x + 1$, that is, $\alpha^2 + \alpha + 1 = 0$. Then the one to one correspondence between $\mathbb{F}_{2^3}$ and $\mathbb{F}_2^3$ is given in Table 1.1 below.*

$\mathbb{F}_{2^3}$	$\mathbb{F}_2^3$
0	$(0, 0, 0)$
1	$(0, 0, 1)$
α	$(0, 1, 0)$
α^2	$(1, 0, 0)$
$\alpha^3 = \alpha + 1$	$(0, 1, 1)$
$\alpha^4 = \alpha^2 + \alpha$	$(1, 1, 0)$
$\alpha^5 = \alpha^2 + \alpha + 1$	$(1, 1, 1)$
$\alpha^6 = \alpha^2 + 1$	$(1, 0, 1)$

Table 1.1: Correspondence between finite fields and vector spaces

For any set S, $|S|$ denotes the cardinality of S. For any $x \in \mathbb{F}_2^n$, the (Hamming) weight of x is the integer sum $wt(x) = \sum_{i=1}^{n} x_i$, that is, the number of 1's it has. The Hamming distance between two vectors $x, y \in \mathbb{F}_2^n$, $d(x, y)$, is defined as

$$d(x, y) = |\{i : x_i \neq y_i, i = 1, 2, \ldots, n\}| = wt(x + y).$$

The Hamming distance is a metric which represents the minimum number of necessary substitutions to transform a vector into another. Let $x = (1, 1, 0, 0, 1, 0), y = (0, 1, 1, 0, 0, 1) \in \mathbb{F}_2^5$. Then $wt(x) = 3$, $wt(y) = 4$ and $d(x, y) = 4$.

1.2 Boolean functions

Any function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (or, equivalently from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) is said to be a Boolean function in n variables. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$ and the cardinality of $\mathcal{B}_n$ is 2^{2^n}. For detailed study of Boolean functions we refer to Carlet [29,31], Cusick and Stănică [135] and Mesnager [120].

There are several representations of a Boolean function. We study three standard representations of Boolean functions, namely truth-table representation, algebraic normal form (ANF) and trace representation. We describe in details these representations below.

Truth-table representation

In the truth-table representation we list the 2^n elements of $\mathbb{F}_2^n$ in lexicographically increasing order along with the corresponding functional values. Thus, any Boolean function $f \in \mathcal{B}_n$ is a 2^n length binary string of $\mathbb{F}_2^{2^n}$ and it can be uniquely represented as

$$[f(0,0,\ldots,0), f(0,0,\ldots,1), f(0,0,\ldots,1,0), \ldots, f(1,1,\ldots,1)].$$

Example 1.2.1. *Let $n = 3$. Suppose $f \in \mathcal{B}_3$ is a Boolean function and $(1,0,0,1,1,0,1,0)$ is the truth-table of f. Since $(1,0,0,1,1,0,1,0)$ is an element of $\mathbb{F}_2^8$. The truth-table of f is written in the right most column in Table 1.2.*

x_3	x_2	x_1	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Table 1.2: Truth-table of a Boolean function in 3 variables

Definition 1.2.2. *The support of a Boolean function $f \in \mathcal{B}_n$, supp(f), is defined by*

$$supp(f) = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}.$$

The weight of a Boolean function $f \in \mathbb{F}_2^n$, $wt(f)$, is the cardinality of $supp(f)$, i.e., the total number of nonzero output.

Definition 1.2.3. *The Hamming distance between two Boolean functions $f, g \in \mathcal{B}_n$, $d(f,g)$, is defined by*

$$\begin{aligned} d(f,g) &= |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}| = wt(f+g) \\ &= \frac{1}{2}\{|(f(x)=g(x))| + |(f(x)\neq g(x))|\} - \frac{1}{2}\{|(f(x)=g(x))| - |(f(x)\neq g(x))|\} \\ &= 2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+g(x)}. \end{aligned} \tag{1.2.1}$$

Example 1.2.4. *Let f, g be two Boolean functions on 3 variables with their truth-tables $(0,1,0,1,1,1,0,1)$ and $(1,1,0,1,1,1,0,1)$,respectively. Then the weights of f and g are 5 and 6, respectively. The Hamming distance of f and g is $d(f,g) = 1$, i.e., changing only one bit in truth-table we can transform one truth-table to another.*

Algebraic normal form

Any Boolean function f in n variables can be expressed as a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n] / \langle x_1^2+x_1, \ldots, x_n^2+x_n\rangle$. This form is called Algebraic normal form (ANF) of f and is written as

$$f(x_1, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \lambda_a \left(\prod_{i=1}^{n} x_i^{a_i}\right)$$

where $\lambda_a \in \mathbb{F}_2$. Each term of the form $\prod_{i=1}^n x_i^{a_i}$ is called a monomial. One can obtain the algebraic normal form of a Boolean function from truth-table and vice-versa. Suppose $x \preceq y$ means $x_i \leq y_i$, for all $i \in \{1, 2, \ldots, n\}$ where $x, y \in \mathbb{F}_2^n$. Then we have

$$\lambda_a = \sum_{x \preceq a} f(x),$$

for all $a \in \mathbb{F}_2^n$ which is the way to get ANF from truth-table of a Boolean function. If we have the ANF of Boolean function then in the same way we get its truth-table as

$$f(x) = \sum_{a \preceq x} \lambda_a,$$

for all $x \in \mathbb{F}_2^n$.

Definition 1.2.5. *The algebraic degree of $f \in \mathcal{B}_n$, denoted by* $\deg(f)$*, is define as*

$$\deg(f) = \max_{a \in \mathbb{F}_2^n} \{wt(a) : \lambda_a \neq 0\}.$$

The degree of a monomial $\prod_{i=1}^n x_i^{a_i}$ is $wt(a)$.

Definition 1.2.6. *Boolean functions with algebraic degree at most 1 are said to be affine functions. Precisely, an affine function $\varphi_{a,\varepsilon} : \mathbb{F}_2^n \to \mathbb{F}_2$ is of the form*

$$\varphi_{a,\varepsilon}(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n + \varepsilon, \text{ for all } x \in \mathbb{F}_2^n \tag{1.2.2}$$

where $a \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$. If $\varepsilon = 0$ then $\varphi_{a,0}$ is a linear function. The total number of n variables affine Boolean functions is 2^{n+1}.

Let $x, y \in \mathbb{F}_2^n$. The inner product of $x, y \in \mathbb{F}_2^n$, $x \cdot y$, is defined as

$$x \cdot y = x_1y_1 + x_2y_2 + \ldots + x_ny_n,$$

and $x \cdot y \in \mathbb{F}_2$. Thus, if we vary a all over $\mathbb{F}_2^n$, we get all 2^n linear function of the form $\varphi_{a,0}$.

Example 1.2.7. *The algebraic normal form of the Boolean function in 3 variables given in Table 1.2 is*

$$\begin{aligned} f(x_1, x_2, x_3) &= (x_1 + 1)(x_2 + 1) + x_1x_2(x_3 + 1) + (x_1 + 1)x_2x_3 \\ &= 1 + x_1 + x_2 + x_2x_3. \end{aligned}$$

Thus, the degree of f is 2. The nonzero coefficients in ANF are $\lambda_{(0,0,0)} = 1 = \lambda_{(0,0,1)} = \lambda_{(0,1,0)} = \lambda_{(1,1,0)}$.

Trace representation

First we discuss some basic definitions and properties of cyclotomic cosets and trace functions. The cyclotomic coset of 2 modulo $2^n - 1$ containing j, $C[j]$, is defined as

$$C[j] = \{j, j2, j2^2, \ldots, j2^{n_j - 1}\}$$

where n_j is the smallest positive integer such that $j \equiv j2^{n_j} \pmod{2^n - 1}$. Conventionally, the smallest element j modulo 2^n-1 in the coset is called the coset leader and the cyclotomic coset is denoted by $C[j]$.

Example 1.2.8. *Let $n = 5$ and $j = 2$. Since $2 \equiv 2 \times 2^5 \pmod{31}$. Then $\{2, 2 \times 2, 2 \times 2^2, 2 \times 2^3, 2 \times 2^4\} = \{2, 4, 8, 16, 1\}$ which is $C[1]$ (operation over modulo 31). All the distinct cyclotomic cosets modulo 31 are given below.*

$$\begin{aligned} C[0] &= \{0\} \\ C[1] &= \{1, 2, 4, 8, 16\} \\ C[3] &= \{3, 6, 12, 24, 16\} \\ C[5] &= \{5, 9, 10, 18, 20\} \\ C[7] &= \{7, 14, 19, 25, 28\} \\ C[11] &= \{11, 13, 21, 22, 26\} \\ C[15] &= \{15, 23, 27, 29, 30\} \end{aligned}$$

Let $j_1, j_2, \ldots, j_r \in \mathbb{Z}_{2^n-1}$ such that $C[j_1], C[j_2], \ldots, C[j_r]$ are all distinct cyclotomic cosets modulo $2^n - 1$. Then $\cup_{i=1}^{r} C[j_i] = \mathbb{Z}_{2^n-1}$. Some basic properties are given below.

- The cardinality of $C[j]$ is either 1 or n.
- For a positive integer j, if $\gcd(j, 2^n - 1) = 1$ then the cardinality of $C[j]$ is n.
- For any two positive integers i and j, $C[i]$ and $C[j]$ are either disjoint or identical.

Definition 1.2.9. *Let $n = kt$, $k \in \mathbb{Z}^+$. The trace function from $\mathbb{F}_{2^n}$ to the subfield $\mathbb{F}_{2^t}$, Tr_t^n, is defined as*

$$\mathrm{Tr}_t^n(x) = x + x^{2^t} + x^{2^{2t}} + \ldots + x^{2^{(k-1)t}}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

If $\mathbb{F}_{2^t}$ is a prime field (i.e., $t = 1$) then the trace is called absolute trace and denoted by Tr_1^n. The inner product of $x, y \in \mathbb{F}_{2^n}$ is denotes by $\mathrm{Tr}_1^n(xy)$. The basic properties of trace function are given as follows:

- For all $x, y \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_1^n(x + y) = \mathrm{Tr}_1^n(x) + \mathrm{Tr}_1^n(y)$.

- For all $c \in \mathbb{F}_2$ and $x \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_1^n(cx) = c\mathrm{Tr}_1^n(x)$.
- For all $c \in \mathbb{F}_2$, $\mathrm{Tr}_1^n(c) = nc$.
- For all $x \in \mathbb{F}_{2^n}$ and for any $r \in \mathbb{Z}^+$, $\mathrm{Tr}_1^n(x^{2^r}) = \mathrm{Tr}_1^n(x)$.
- For $a \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_1^n(a) = 0$ if and only if $a = \alpha^2 + \alpha$ for some $\alpha \in \mathbb{F}_{2^n}$.
- Trace function satisfies transitivity property, i.e., if $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^t}$ is a subfield of $\mathbb{F}_{2^m}$ then

$$\mathrm{Tr}_t^n(x) = \mathrm{Tr}_t^m(\mathrm{Tr}_m^n(x)), \text{ for all } x \in \mathbb{F}_{2^n}.$$

From the first two properties we observe that trace is a linear mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For proof of the above results we refer to [41, 103, 120].

Any function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be uniquely written as a univariate polynomial of degree at most $2^n - 1$ of the form

$$f(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{2^n-1}x^{2^n-1}$$

where $c_i, x \in \mathbb{F}_{2^n}$, $i = 0, 1, \ldots, 2^n - 1$. If $f(x)^2 = f(x)$, for all $x \in \mathbb{F}_{2^n}$ then f is a Boolean function and vice-versa. A function f is a Boolean function if and only if $c_0, c_{2^n-1} \in \mathbb{F}_2$ and $c_{2i \pmod{2^n-1}} = c_i^2$, $i \in \{1, 2, \ldots, 2^n - 2\}$. The univariate representation of any function $f \in \mathcal{B}_n$ is

$$f(x) = \sum_{j \in \Gamma(n)} \mathrm{Tr}_1^{n_j}(\alpha_j x^j) + \varepsilon(1 + x^{2^n-1})$$

where $\Gamma(n)$ is the set of cyclotomic coset leaders modulo $2^n - 1$, n_j is the size of the cyclotomic class containing j, $\alpha_j \in \mathbb{F}_{2^{n_j}}$ and $\varepsilon = \sum_{x \in \mathbb{F}_{2^n}} f(x) \pmod 2$. For every $j \in \mathbb{Z}/(2^n - 1)\mathbb{Z}$, we can write

$$j = \sum_{s \in E} 2^s \text{ where } E \subseteq \{0, 1, \ldots, n - 1\}.$$

The cardinality of E is referred to as the 2-weight of j and written as $w_2(j)$. The algebraic degree of f is $\deg(f) = \max_{j \in \Gamma(n)}\{w_2(j) : \alpha_j \neq 0\}$. Precisely, an affine function $\varphi_{a,\varepsilon} : \mathbb{F}_{2^n} \to$

$\mathbb{F}_2$ is of the form

$$\varphi_{a,\varepsilon}(x) = \mathrm{Tr}_1^n(ax) + \varepsilon, \text{ for all } x \in \mathbb{F}_{2^n}$$

where $a \in \mathbb{F}_{2^n}$ and $\varepsilon \in \mathbb{F}_2$ (if $\varepsilon = 0$ then $\varphi_{a,0}$ is a linear function). In general, it is difficult to compute the algebraic degree of a Boolean function given in univariate form.

Example 1.2.10. *Let $n = 2t$ and $\alpha \in \mathbb{F}_{2^n}^*$. Then*

- *the degree of $f(x) = \mathrm{Tr}_1^n(\alpha x^{2^t+1})$ is 2;*
- *the degree of $f(x) = \mathrm{Tr}_1^n(\alpha x^{2^t-1})$ is t.*

Suppose $n \in \mathbb{Z}^+$ and $g(x_1, \ldots, x_n) \in \mathbb{F}_2[x_1, \ldots, x_n]$. Then the *n-variate representation* of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is

$$f(x_1, \ldots, x_n) = \mathrm{Tr}_1^n(g(x_1, \ldots, x_n)), \text{ for all } (x_1, \ldots, x_n) \in \mathbb{F}_2^m.$$

1.2.1 Walsh–Hadamard transform

The discrete Fourier transform of Boolean function is called Walsh–Hadamard transform or Walsh transform. For the computation of many cryptographic properties of a Boolean function it is needed to compute their Walsh–Hadamard transform.

Definition 1.2.11. *The Walsh–Hadamard transform of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$ is defined as*

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x}.$$

The multiset $[W_f(a) : a \in \mathbb{F}_2^n]$ is said to be the Walsh–Hadamard spectrum of f. The absolute value of the Walsh–Hadamard spectrum of f is at most 2^n, i.e., $-2^n \leq W_f(a) \leq 2^n$, for all $a \in \mathbb{F}_2^n$. The weight distribution of Walsh–Hadamard spectrum of a Boolean function f is the frequency distribution of the values in the Walsh–Hadamard spectrum of f. It is also defined over the finite field $\mathbb{F}_{2^n}$ as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(ax)}, \text{ for all } a \in \mathbb{F}_{2^n}. \tag{1.2.3}$$

In the bivariate case, where $f : \mathbb{F}_{2^t}^2 \to \mathbb{F}_2$, instead of Equation (1.2.3) we have

$$W_f(a,b) = \sum_{(x,y)\in\mathbb{F}_{2^t}^2} (-1)^{f(x,y)+\mathrm{Tr}_1^t(ax)+\mathrm{Tr}_1^t(by)}, \text{ for all } (a,b) \in \mathbb{F}_{2^t}^2.$$

If $s \in \mathbb{F}_2$ then we know that $(-1)^s = 1 - 2s$. Using the inverse Walsh–Hadamard transform, f can be recovered as below:

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{a\in\mathbb{F}_2^n} W_f(a)(-1)^{x\cdot a}, \text{ for all } x \in \mathbb{F}_2^n.$$

Let $g(x) = \varphi_{a,\varepsilon}(x)$ be an affine function, for all $x \in \mathbb{F}_2^n$. Then from Equation (1.2.1), we get

$$d(f,g) = 2^{n-1} - \frac{(-1)^\varepsilon}{2} \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} = 2^{n-1} - \frac{(-1)^\varepsilon}{2} W_f(a), \tag{1.2.4}$$

which is the relation between distance and Walsh–Hadamard transform of two Boolean functions. One can also compute the Walsh–Hadamard spectrum using the Hadamard matrix. We consider the following recursive definition of Hadamard matrices:

$$H_0 = \begin{pmatrix} 1 \end{pmatrix}; \ H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and

$$H_m = \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}.$$

Here H_m is the tensor product $H_m = H_1 \otimes H_{m-1}$. The walsh-Hadamard spectrum of $f \in \mathcal{B}_n$ can be written as

$$\Big(W_f(\alpha_0), \ \ldots \ , W_f(\alpha_{2^n-1})\Big) = \Big((-1)^{f(\alpha_0)}, \ \ldots \ , (-1)^{f(\alpha_{2^n-1})}\Big) H_n$$

where $\alpha_j \in \mathbb{F}_2^n$, $j = 0, 1, \ldots, 2^n - 1$. The Hadamard matrix H of order m is an $m \times m$ square matrix of all entry ± 1 such that

$$HH^t = mI_m$$

where H^t is the transpose of H and I_n is the identity matrix of order $m \times m$.

Proposition 1.2.12 ([135]). *Any Boolean function f in n variables satisfies the following identity*

$$\sum_{a \in \mathbb{F}_2^n} W_f^2(a) = 2^{2n}.$$

This identity is called Parseval's identity. Using the Parseval's identity one can prove that the absolute value of the Walsh–Hadamard spectrum of $f \in \mathcal{B}_n$ is at least $2^{n/2}$, that is, $\max\{|W_f(a)| : a \in \mathbb{F}_2^n\} \geq 2^{n/2}$.

Theorem 1.2.13 ([100, Theorem 2.6]). *Let E be an arbitrary subspace of $\mathbb{F}_2^n$ and $E^\perp$ be the dual of E, defined as*

$$E^\perp = \{a \in \mathbb{F}_2^n : a \cdot x = 0, \text{ for all } x \in E\}.$$

Then for any $f \in \mathcal{B}_n$, we have

$$\sum_{a \in E} W_f(a) = |E| \sum_{x \in E^\perp} (-1)^{f(x)}.$$

The above equation between W_f and f is called the Poisson Summation Formula. Using the above Theorem one can easily derive the next Corollary.

Corollary 1.2.14. *For any $f \in \mathcal{B}_n$*

$$\sum_{a \preceq b} W_f(a) = 2^{wt(b)} \sum_{a \preceq \bar{b}} (-1)^{f(a)}$$

where $a, b \in \mathbb{F}_2^n$ and $a \preceq b$ means that $a_i \leq b_i$, for all $i \in \{1, 2, \ldots, n\}$.

Definition 1.2.15. *Let E be the subspace of $\mathbb{F}_2^n$ and ϕ_E be a Boolean function in n variables, defined as*

$$\phi_E(x) = \begin{cases} 1, & \text{if } x \in E; \\ 0, & \text{otherwise.} \end{cases}$$

ϕ_E is called the indicator function of the space E.

Let E be a subspace of $\mathbb{F}_2^n$. Then for any $a, b \in \mathbb{F}_2^n$

$$\sum_{x \in b+E} (-1)^{a \cdot x} = |E|(-1)^{a \cdot b} \phi_{E^\perp}(a) \tag{1.2.5}$$

where $E^\perp$ is dual of E. The Walsh–Hadamard transform at any $b \in \mathbb{F}_2^n$ of an affine functions $\varphi_{a,\varepsilon}$ is

$$W_{\varphi_{a,\varepsilon}}(b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\varphi_{a,\varepsilon}(x) + b \cdot x} = \begin{cases} 0, & \text{if } a \neq b; \\ 2^n(-1)^\varepsilon, & \text{if } a = b, \end{cases}$$

where $\varphi_{a,\varepsilon}$ is defined as in Equation (1.2.2).

1.2.2 Cryptographic Boolean functions

In this section we discuss some properties of Boolean functions which have cryptographic significance.

Algebraic Degree

The algebraic degree of Boolean function gives the linear complexity of the pseudo-random generator. To resist the Berlekamp–Messey attack [8, 29, 59] and Rønjom–Helleseth attack [124] of a cryptosystem it is needed that Boolean functions used in pseudo-random generators posses optimal algebraic degree. From algebraic normal form of Boolean function we know that the maximum algebraic degree of a Boolean function in n variables is at most n.

Balancedness

A Boolean function f in n variables is said to be balanced if the truth-table of f has equal number of 1's and 0's, i.e., the cardinality of support of f, $supp(f)$, is 2^{n-1}. There are $\binom{2^n}{2^{n-1}}$ many balanced functions in $\mathcal{B}_n$. Boolean functions used in a cryptosystem must be balanced. Otherwise, cryptosystem unable to prevent the distinguishing attacks [30] as the attacker gain some statistical information between plaintext and ciphertext of stream cipher. If a Boolean function in n variables is balanced then the algebraic degree is at most $n - 1$. It is to be noted that any nonconstant affine functions is balanced.

Example 1.2.16. *Let $h_1, h_2 \in \mathcal{B}_3$ such that the truth-table of h_1 and h_2 be $(1,1,0,0,0,0,1,1)$ and $(0,0,0,0,0,1,0,1)$, respectively. Here h_1 is balanced and h_2 is not balanced.*

Crosscorrelation and Autocorrealtion

Let $f, g \in \mathcal{B}_n$. Then the crosscorrelation between f and g at $\alpha \in \mathbb{F}_2^n$, $\mathcal{C}_{f,g}(\alpha)$, is defined by

$$\mathcal{C}_{f,g}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x+\alpha)}.$$

Two Boolean functions f and g in n variables are called uncorrelated of order r, $0 \leq r \leq n$ if $\mathcal{C}_{f,g}(\alpha) = 0$, for all $\alpha \in \mathbb{F}_2^n$ with $0 \leq wt(\alpha) \leq r$. If for all $\alpha \in \mathbb{F}_2^n$, $\mathcal{C}_{f,g}(\alpha) = 0$ then f and g are perfectly uncorrelated. For details we refer to [96, 120, 135].

Example 1.2.17. *Let $f, g \in \mathcal{B}_3$. Suppose the truth-table of f and g are $(0,0,1,0,1,1,0,0)$ and $(1,1,0,1,1,1,0,0)$, respectively (consider the lexicographic order). Then the crosscorrelation value at $(0,0,1)$ of f and g is $\mathcal{C}_{f,g}(0,0,1) = 4$.*

The relation between crosscorrelatin value and Walsh–Hadamard spectrum of two Boolean function $f, g \in \mathcal{B}_n$ is

$$\left(\mathcal{C}_{f,g}(\alpha_0), \quad \ldots \quad , \mathcal{C}_{f,g}(\alpha_{2^n-1})\right) = \frac{1}{2^n}\left(W_f(\alpha_0)W_g(\alpha_0), \quad \ldots \quad , W_f(\alpha_{2^n-1})W_g(\alpha_{2^n-1})\right) H_n$$

where $\alpha_j \in \mathbb{F}_2^n$, $j = 0, 1, \ldots, 2^n - 1$ and H_n is Hadamard matrix of order 2^n. From Equation (1.2.1), we get

$$d(f,g) = 2^{n-1} - \frac{1}{2}\mathcal{C}_{f,g}(0),$$

which is the relation between Hamming distance and crosscorrelation of two Boolean functions. The autocorrelation of $f \in \mathcal{B}_n$ at $\alpha \in \mathbb{F}_2^n$, $\mathcal{C}_f(\alpha)$, is defined as

$$\mathcal{C}_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\alpha)}.$$

It is obvious that if $\alpha = 0$ then $\mathcal{C}_f(0)$ is equal to 2^n. Moreover, the absolute value of autocorrelation of any Boolean functions in n variables is at most 2^n. If $g = f$ then we get

$$\left(\mathcal{C}_f(\alpha_0), \quad \ldots \quad , \mathcal{C}_f(\alpha_{2^n-1})\right) = \frac{1}{2^n}\left(W_f^2(\alpha_0), \quad \ldots \quad , W_f^2(\alpha_{2^n-1})\right) H_n$$

where $\alpha_j \in \mathbb{F}_2^n$, $j = 0, 1, \ldots, 2^n - 1$ and H_n is Hadamard matrix of order 2^n which is the relation between autocorrelatin value and Walsh–Hadamard spectrum of a Boolean function $f \in \mathcal{B}_n$.

Nonlinearity

Nonlinearity of a Boolean function is one of the most important criterion as it measures the distance between the Boolean function and the set of affine functions. From cryptographic point of view this quantity must be as large as possible to resist the affine approximation attacks [32].

Definition 1.2.18. *Let $f \in \mathcal{B}_n$. The nonlinearity of f, $nl(f)$, is defined as*

$$nl(f) = \min\{d(f, l) : l \in \varphi_{a,\varepsilon}\}.$$

From Equation (1.2.4), we get the relation between Walsh–Hadamard spectrum and nonlinearity of a Boolean function f in n variables as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|. \tag{1.2.6}$$

Using Parseval's identity, we can calculate the upper bound of nonlinearity. The nonlinearity of an n-variable Boolean function is at most $2^{n-1} - 2^{\frac{n}{2}-1}$. Rothaus [86] introduced the idea of nonlinearity and Matsui [76] discovered the relationship between nonlinearity and explicit attack on symmetric ciphers. For results on constructions of Boolean functions with high nonlinearity we refer to [29, 31, 40, 58, 75, 81, 86, 95, 113, 114].

Definition 1.2.19. *Suppose $f \in \mathcal{B}_n$. For every $r \in \mathbb{Z}$, $0 < r \leq n$, the minimum Hamming distance of f from all the functions having algebraic degree at most r is said to be the rth-order nonlinearity of the Boolean function f, i.e.,*

$$nl_r(f) = \min\{d(f, g) : g \in \mathcal{B}_n \textit{ and } \deg(g) \leq r\}.$$

The sequence of values $nl_r(f)$, for r ranging from 1 to $n-1$, is said to be the nonlinearity profile of f. To construct a good cryptosystem, the rth-order nonlinearity of Boolean function is must be optimal. Thus, a cryptosystem is secure against different low order approximations attacks [57, 62, 71, 130, 138, 144] when the Boolean functions used in it possess high nonlinearity profile.

Following are some of the results proved by Carlet [28].

Proposition 1.2.20 ([28, Proposition 2]). *Let $f \in \mathcal{B}_n$, $r \in \mathbb{Z}^+$ such that $r < n$ and i be a non-negative integer smaller than r. Then*

$$nl_r(f) \geq \frac{1}{2^i} \max_{a_1,\dots,a_i \in \mathbb{F}_2^n} nl_{r-i}(D_{a_1} \dots D_{a_i} f).$$

In particular, for $r = 2$,

$$nl_2(f) \geq \frac{1}{2} \max_{a \in \mathbb{F}_2^n} nl(D_a f).$$

Proposition 1.2.21 ([28, Proposition 3]). *Let $f \in \mathcal{B}_n$ and $r \in \mathbb{Z}^+$ such that $r < n$. We have*

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_2^n} nl_{r-1}(D_a f)}.$$

If some lower bound on $nl(D_a f)$ is known for all $a \in \mathbb{F}_2^n$, we have the following corollary.

Corollary 1.2.22 ([28, Corollary 2]). *Let $f \in \mathcal{B}_n$ and $r \in \mathbb{Z}^+$ such that $r < n$. Assume that, for some non-negative integers M and m, $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_2^n$. Then*

$$nl_r(f) \quad \geq \quad 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n - 1)M2^{m+1} + 2^n}.$$

It is known that any first derivative of a cubic Boolean function has algebraic degree at most 2 and the Walsh–Hadamard spectrum of a quadratic Boolean function (degree 2 Boolean function) is completely characterized by the dimension of the kernel of the bilinear form associated with it. Therefore, Propositions 1.2.20, 1.2.21 and Corollary 1.2.22 are required for computation of the lower bounds of the second-order nonlinearities of cubic Boolean functions.

Some results on higher-order nonlinearity are listed below.

Theorem 1.2.23 ([110, Theorem 1]). *Let $n = 6r$ and $d = 2^{2r} + 2^r + 1$. Suppose $f_\lambda(x) = \mathrm{Tr}_1^n(\lambda x^d)$, for all $x \in \mathbb{F}_{2^n}$ where $\lambda \in \mathbb{F}_{2^n}^*$. Then*

$$nl_2(f_\lambda) \geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{\frac{n}{2}+2r} + 2^n} \approx 2^{n-1} - 2^{\frac{3n+4r-4}{4}}.$$

Theorem 1.2.24 ([110, Theorem 2]). *Let $n = 2t$ with $n \geq 6$. Suppose $f(x,y) = \mathrm{Tr}_1^t(xy^{2^i+1})$, for all $x, y \in \mathbb{F}_{2^t}$ and $i \in \mathbb{Z}$ such that $1 \leq i < t$, $\gcd(i,t) = e$ and $\gcd(2^t-1, 2^i+1) = 1$. Then*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n}{2}+e} - 2^{\frac{3n}{4}+\frac{e}{2}} + 2^n(2^{\frac{n}{4}+\frac{e}{2}} - 2^e + 1)}.$$

Lemma 1.2.25 ([45, Lemma 5]). *Let $n = 4r$ and $d = 2^{2r} + 2^r + 1$. Suppose $f_\lambda(x) = \mathrm{Tr}_1^n(\lambda x^d)$, for all $x \in \mathbb{F}_{2^n}$ where $\lambda \in \mathbb{F}_{2^n}^*$. Then*

$$nl(D_a f) \geq \begin{cases} 0, & \text{if } a \in \mathbb{F}_{2^r}; \\ 2^{4r-1} - 2^{3r-1}, & \text{if } a \notin \mathbb{F}_{2^r}. \end{cases}$$

Theorem 1.2.26 ([45, Theorem 1]). *Let $n = 4r$ and $d = 2^{2r} + 2^r + 1$. Suppose $f_\lambda(x) = \mathrm{Tr}_1^n(\lambda x^d)$, for all $x \in \mathbb{F}_{2^n}$ where $\lambda \in \mathbb{F}_{2^n}^*$. Then*

$$nl_2(f_\lambda) \geq 2^{4r-1} - 2^{2r-1}\sqrt{2^{3r} + 2^r - 1}.$$

Let $n = 2t$ and $f \in \mathcal{B}_n$ be a bent function belongs to $\mathcal{PS}$ class of the form

$$f(x,y) = \mathrm{Tr}_1^t\left(\frac{\lambda x}{y}\right), \tag{1.2.7}$$

for all $(x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ where $\lambda \in \mathbb{F}_{2^t}^*$ and $\mathrm{Tr}_1^t(0) = 0$ with convention that $\frac{\lambda x}{0} = 0$. Suppose

$$k_t = \max\{|t_1| : t_1 \in [-2^{\frac{t}{2}+1} + 1, 2^{\frac{t}{2}+1} + 1] \text{ and } t_1 \equiv 0 \pmod 4\}. \tag{1.2.8}$$

Clearly, $k_t = 2^{\frac{t}{2}+1}$ when t is even.

Lemma 1.2.27 ([37, Lemma 4]). *Let $f \in \mathcal{B}_n$ be defined as in Equation (1.2.7) and $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. Then*

$$nl(D_{(a,b)} f) = \begin{cases} 0, & \text{if } a = 0, b = 0; \\ 2^{n-1} - 2^{t-s+1}, & \text{if } a \in \mathbb{F}_{2^t}, b \in \mathbb{F}_{2^t}^*; \\ 2^{n-1} - k_t 2^{t-1}, & \text{if } a \in \mathbb{F}_{2^t}^*, b = 0, \end{cases}$$

where $s \equiv t \pmod 2$ and k_t is defined as in Equation (1.2.8).

Theorem 1.2.28 ([37, Theorem 1]). *Let $n = 2t$ and $f \in \mathcal{B}_n$ be a bent function defined as in Equation* (1.2.7)*. Then*

$$nl_2(f) \geq \begin{cases} 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n}{2}+1} - 2^n + k_t(2^n - 2^{\frac{n}{2}})}, & \text{if } t \equiv 1 \pmod 2; \\ 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n}{2}+2} - 3 \cdot 2^n + 2^{\frac{5n}{4}+1} - 2^{\frac{3n}{4}+1}}, & \text{if } t \equiv 0 \pmod 2, \end{cases}$$

where k_t is defined as in Equation (1.2.8)*.*

Theorem 1.2.29 ([37, Theorem 3]). *Let $n = 2t$. Suppose $g \in \mathcal{B}_t$ and ϕ is an APN (t,t)-function which is a permutation on $\mathbb{F}_2^t$. Then the second-order nonlinearity of the bent function $f(x, y) = x \cdot \phi(y) + g(y)$ satisfies*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} + 2^{n+2} - 2^{\frac{3n}{2}+2} - 2 \sum_{\alpha \in \mathbb{F}_2^t, \alpha \neq 0} nl(\alpha \cdot \phi)}.$$

Corollary 1.2.30 ([37, Corollary 1]). *Let $n = 2t$ where t be an odd integer. Suppose g is an arbitrary Boolean function on $\mathbb{F}_2^t$ and ϕ is an AB (t,t)-function which is a permutation on $\mathbb{F}_2^t$. Then the second-order nonlinearity of the bent function $f(x, y) = x \cdot \phi(y) + g(y)$ satisfies*

$$nl_2(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{\frac{3n}{2}+1} + 2^{\frac{5n+2}{4}} - 2^{\frac{3n+2}{4}} - 2^n}.$$

Algebraic Immunity

The measure of resistance against algebraic attacks is called the algebraic immunity of Boolean functions. Algebraic attack was proposed by Courtois et al. [79, 80]. For cryptographic primitives algebraic immunity of Boolean function should be large. For further details we refer to [21, 22, 25, 35, 42].

Definition 1.2.31. *Let $f \in \mathcal{B}_n$. A nonzero Boolean function $h \in \mathcal{B}_n$ is said to be an annihilator of f if $f(x)h(x) = 0$, for all $x \in \mathbb{F}_2^n$ and their set is denoted by $\mathcal{AN}(f)$.*

Definition 1.2.32. *The algebraic immunity of $f \in \mathcal{B}_n$, $\mathcal{AI}(f)$, is defined as*

$$\mathcal{AI}(f) = \min\{\deg(h) : h \in \mathcal{AN}(f) \cup \mathcal{AN}(f + 1)\}.$$

It is easy to see that $\mathcal{AI}(f) \leq \deg(f)$, for all $f \in \mathcal{B}_n$ as $f(x)(1 + f(x)) = 0$, $x \in \mathbb{F}_2^n$.

Example 1.2.33. *Let $f, h \in \mathcal{B}_4$ such that $f(x) = x_1x_2x_3x_4$ and $h(x) = x_1 + x_2 + x_3 + x_4$. Since for all $x \in \mathbb{F}_2^4$,*

$$f(x)h(x) = x_1x_2x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_4 = 0.$$

Thus, the algebraic immunity of f is equal to $\mathcal{AI}(f) = 1$ as h is an annihilator of f with degree 1.

We discuss some known results related to the bounds of algebraic immunity and relations with the nonlinearity of Boolean function. Let $f \in \mathcal{B}_n$ and $s \in \mathbb{Z}^+$, $1 \leq r \leq n-1$. Then the following conditions holds:

- From [80, Theorem 6.0.1], we have

$$\mathcal{AI}(f) \leq \min\{\deg(f), \lceil \frac{n}{2} \rceil\}.$$

- If $\mathcal{AI}(f) \leq r$ and f is balanced then [21, Proposition 1]

$$nl_r(f) \leq 2^{n-1} - 2^{n-r}.$$

- If $\mathcal{AI}(f) \geq r+1$ then [22, Theorem 1]

$$nl_r(f) \geq 2 \sum_{j=0}^{\mathcal{AI}(f)-r-1} \binom{n-r}{j}.$$

- Let $\deg(f)$ be d. If $nl(f) \leq \sum_{j=0}^{d} \binom{n}{j}$ then [25, Theorem]

$$\mathcal{AI}(f) \leq d+1.$$

Correlation Immune and Resiliency

Correlation immunity of Boolean function can be defined in two equivalent ways.

Definition 1.2.34. *A Boolean function in n variables is said to be correlation immune of order r if any function obtain from it by fixing at most r variables is balanced. Equivalently,*

$f \in \mathcal{B}_n$ is said to be correlation immune of order r if

$$W_f(\beta) = 0, \text{ for all } \beta \in \mathbb{F}_2^n \text{ with } 1 \leq wt(\beta) \leq r.$$

Definition 1.2.35. *A balanced Boolean function in n variables with correlation immune of order r is said to be resilient of order r.*

For details we refer to [6,13,52,74,77,90,122,131,141,142,145,153]. Siegenthaler [131] derived the relation between algebraic degree and correlation immunity of Boolean functions. Let $f \in \mathcal{B}_n$ such that algebraic degree be d and correlation immunity be r. Then from [131], we have $r + d \leq n$. Maitra amd Sarkar [115] proved that

$$nl(f) \leq 2^{n-1} - 2^{r+1}$$

where $f \in \mathcal{B}_n$ with algebraic immunity r. This nonlinearity bound of Boolean function is called Sarkar and Maitra's bound.

1.2.3 Affine equivalence and Derivatives of Boolean functions

The general linear group of degree n over $\mathbb{F}_2$, $GL(n, \mathbb{F}_2)$, is the group of invertible linear transformations acting on $\mathbb{F}_{2^n}$. For any $A \in GL(n, \mathbb{F}_2)$ and $x \in \mathbb{F}_{2^n}$ we denote the action of A on x by $x \mapsto xA$. The affine general linear group, $AGL(n, \mathbb{F}_2)$, is the set of all transformations of the form $x \mapsto xA + b$ where $b \in \mathbb{F}_{2^n}$. This group can be thought of as the semidirect product $GL(n, \mathbb{F}_2) \ltimes \mathbb{F}_{2^n}$, but we will not need that here.

Definition 1.2.36. *Two Boolean functions $f, g \in \mathcal{B}_n$ are said to be affine equivalent if there exists $(A, b) \in AGL(n, \mathbb{F}_2)$ such that $g(x) = f(xA + b)$, for all $x \in \mathbb{F}_{2^n}$.*

For Boolean functions used as cryptographic primitives the notion of equivalence is further generalized as follows.

Definition 1.2.37. *Two Boolean functions $f, g \in \mathcal{B}_n$ are said to be extended affine equivalent (EA-equivalent) if there exist $(A, b) \in AGL(n, \mathbb{F}_2)$, $a \in \mathbb{F}_{2^n}$ and $\varepsilon \in \mathbb{F}_2$ such that $g(x) = f(xA + b) + \varphi_{a,\varepsilon}(x)$, for all $x \in \mathbb{F}_{2^n}$ where $\varphi_{a,\varepsilon}(x) = \mathrm{Tr}_1^n(ax) + \varepsilon$.*

The computational complexity for direct verification of affine equivalence between given two Boolean functions is $\mathcal{O}(2^{n^2})$, which is computationally infeasible for $n \geq 7$. If two

Boolean functions $f, g \in \mathcal{B}_n$ have different algebraic degrees then they are EA-inequivalent. Therefore, the algebraic degree serves as an EA-invariant. The multiset consisting of absolute values of Walsh–Hadamard transforms of a function f is said to be its absolute Walsh–Hadamard spectrum. If the absolute Walsh–Hadamard spectra of two Boolean functions are different, which is possible even if their algebraic degrees are same, then we know that they are EA-inequivalent. Thus, the absolute Walsh–Hadamard spectrum serves as a more sophisticated EA-invariant. In fact, the autocorrelation spectrum which is another invariant is also connected to Walsh–Hadamard spectra. For bent functions the absolute Walsh–Hadamard spectrum is unique and flat, set to $2^{\frac{n}{2}}$ where n is the number of variables. Thus, the invariants dependent on Walsh–Hadamard spectra are unable to decide EA-inequivalence of bent functions.

The problem of deciding EA-inequivalence is completely solved for Boolean functions having algebraic degrees at most 2, that is, for affine and quadratic Boolean functions. We refer to MacWilliams and Sloane [41, Chapter 15] for detailed discussion on quadratic Boolean functions including their affine inequivalence. In the absence of a general theory for functions having algebraic degree three and above we address the problem by considering derivatives of these functions.

Definition 1.2.38. *The derivative of $f \in \mathcal{B}_n$ with respect to an m-dimensional $\mathbb{F}_2$-subspace V of $\mathbb{F}_{2^n}$, or the mth-(order) derivative, is the function $D_V f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by*

$$D_V f(x) = \sum_{a \in V} f(x+a), \text{ for all } x \in \mathbb{F}_{2^n}.$$

The algebraic degree to $D_V f$ is at most $\deg(f) - m$. If V is one-dimensional then $D_V f(x) = f(x+a) + f(x)$ where $a \in V \setminus \{0\}$, which is usually denoted by $D_a f(x)$. If V is a 2-dimensional subspace of $\mathbb{F}_{2^n}$ we choose any pair of distinct elements $a, b \in V \setminus \{0\}$ and write

$$D_V f(x) = D_{a,b} f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b),$$

for all $x \in \mathbb{F}_{2^n}$. Obviously the choice of (a, b) does not change the function $D_V f$.

Dillon [56] proposed proving inequivalence of Boolean functions by considering their mth-order derivatives over all distinct m-dimensional subspaces of $\mathbb{F}_{2^n}$.

Theorem 1.2.39 ([56, Theorem 2.1])**.** *For any function $f \in \mathcal{B}_n$; let $\mathcal{D}_k(f)$ denotes the* *multiset of all k-dimensional derivatives of f. If $f, g \in \mathcal{B}_n$ are affinely equivalent then so are $\mathcal{D}_k(f)$ and $\mathcal{D}_k(g)$. If the nonsingular affine transformation A (operating on $\mathcal{B}_n$) maps f onto g then it also maps $\mathcal{D}_k(f)$ onto $\mathcal{D}_k(g)$.*

Dillon proved the following corollary to Theorem 1.2.39.

Corollary 1.2.40. *If $\mathcal{P}$ is any affine invariant for $\mathcal{B}_n$ then $f \longrightarrow \mathcal{P}\{\mathcal{D}_n(f)\}$ is also an affine invariant for $\mathcal{B}_n$.*

One can solve the affine inequivalent problem partially using the above invariant [109, 111].

1.2.4 Quadratic Boolean functions

Let V be the vector space of dimension n over $\mathbb{F}_{2^r}$ where $r \in \mathbb{Z}^+$. A function $Q : V \to \mathbb{F}_{2^r}$ is said to be a quadratic form [7] on V if

- $Q(\gamma x) = \gamma^2 Q(x)$, for all $x \in V$ and $\gamma \in \mathbb{F}_{2^r}$.
- $B(x, y) = Q(0) + Q(x) + Q(y) + Q(x + y)$ is bilinear on V.

Let $\mathcal{E}_Q$ be the kernel of $B(x, y)$, bilinear form of Q. Then $\mathcal{E}_Q$ is a subspace of V defined by

$$\mathcal{E}_Q = \{x \in V : B(x, y) = 0, \text{ for all } y \in V\}.$$

Suppose $f \in \mathcal{B}_n$ is a quadratic function. The bilinear form associated with f is defined by $B(x, y) = f(0) + f(x) + f(y) + f(x + y)$. The kernel [7, 41] of $B(x, y)$ is the subspace of $\mathbb{F}_{2^n}$ defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x, y) = 0, \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

Lemma 1.2.41 ([7, Proposition 1])**.** *Let V be a vector space over a field $\mathbb{F}_q$ of characteristic 2 and $Q : V \longrightarrow \mathbb{F}_q$ be a quadratic form. Then the dimension of V and the dimension of the kernel of Q have the same parity.*

Lemma 1.2.42 ([7, Lemma 1])**.** *Let f be any quadratic Boolean function. The kernel, $\mathcal{E}_f$, is the subspace of $\mathbb{F}_{2^n}$ consisting of those a such that the derivative $D_a f$ is constant. That is,*

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} : D_a f = \text{ constant } \}.$$

The Walsh–Hadamard spectrum of any quadratic function $f \in \mathcal{B}_n$ is given below.

Lemma 1.2.43 ([7, 41]). *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $B(x, y)$ is the quadratic form associated with it then the Walsh–Hadamard Spectrum of f depends only on the dimension of the kernel of $B(x, y)$. Let the dimension of the kernel of $B(x, y)$ is $\dim(\mathcal{E}_f) = s$. Then the weight distribution of the Walsh–Hadamard spectrum of f is*

$W_f(\beta)$	*Number of* β
0	$2^n - 2^{n-s}$
$2^{(n+s)/2}$	$2^{n-s-1} + (-1)^{f(0)} 2^{(n-s-2)/2}$
$-2^{(n+s)/2}$	$2^{n-s-1} - (-1)^{f(0)} 2^{(n-s-2)/2}$

1.2.5 Reed–Muller Code

In 1954, Muller and Reed introduced Reed–Muller codes. The problem of constructing Boolean functions in n variables with highest possible rth-order nonlinearity is connected to the covering radius problem of rth-order Reed–Muller codes. For more details we refer to [27, 41, 43, 88]. In this section we discuss some basic definitions and properties of Reed–Muller codes.

Definition 1.2.44. *Suppose that $\mathbb{F}$ is a finite field and $V = \mathbb{F}^n$ is an n dimensional vector space of $\mathbb{F}$. Any subspace C of V of dimension k is said to be an $[n, k]$-linear code. Here n and k are said to be the length and the dimension of the code, respectively.*

Definition 1.2.45. *The covering radius of code C of V is the smallest integer r such that for each vector $x \in V$ is covered by at least one codeword of C, that is,*

$$\rho = \max_{x \in V} d(x, C) = \max_{x \in V} \min_{c \in C} d(x, c).$$

In other words the covering radius is the distance between the code and maximum distance away vectors in the space.

Definition 1.2.46. *Let $0 \leq r \leq n$. The set of all Boolean functions in n variables having algebraic degree at most r is called rth-order Reed–Muller code of length 2^n, and denoted by $\mathcal{R}(r, n)$.*

The Reed–Muller code of order r, $\mathcal{R}(r,n)$, is a linear code of length $m = 2^n$ with dimension $t = \sum_{j=0}^{r} \binom{n}{j}$. Reed–Muller code $\mathcal{R}(r,n)$ satisfies the following properties.

- $\mathcal{R}(r-1,n) \subset \mathcal{R}(r,n)$, i.e., the Reed–Muller codes are nested.
- Minimum distance of $\mathcal{R}(r,n)$ is 2^{n-r}.
- For $0 \leq r \leq n-1$, $\mathcal{R}(n-r-1,n)$ is the dual of $\mathcal{R}(r,n)$.
- Reed–Muller code is an extended cyclic code.

Example 1.2.47. *Let $f \in \mathcal{B}_5$. Then all possible linear combinations of monomials in 5 variables namely x_1, x_2, x_3, x_4, x_5 having degree at most 1 is $\mathcal{R}(1,5)$. Thus, the cardinality of $\mathcal{R}(1,5)$ is 2^6 and any codeword $\mathcal{R}(1,5)$ can be expressed as*

$$b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 + b_5x_5, \textit{ for all } b_i \in \mathbb{F}_2, i = 0, 1, \ldots, 5.$$

The rth-order nonlinearity of Boolean function $f \in \mathcal{B}_n$ can be defined as

$$nl_r(f) = \min_{g \in \mathcal{R}(r,n)} d(f,g) = 2^{n-1} - \frac{1}{2} \max_{g \in \mathcal{R}(r,n)} | \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x)} |.$$

Thus, the covering radius of $\mathcal{R}(r,n)$ can be obtained from rth-order nonlinearity of $f \in \mathcal{B}_n$ as

$$\rho_{r,n} = \max_{f \in \mathcal{B}_n} \min_{g \in \mathcal{R}(r,n)} d(f,g) = \max_{f \in \mathcal{B}_n} nl_r(f).$$

The bounds of covering radius for different Reed–Muller codes [43, page 252] are given in Table 1.3. For s and t we refer to [147, 148].

1.2.6 Bent functions

Boolean functions used as cryptographic primitives must resist affine approximation, which is achieved by having high nonlinearity. The bent functions defined on an even number of variables have the maximum nonlinearity, that is, they offer maximum resistance to affine approximations. In this section we always consider $n = 2t$.

Definition 1.2.48. *A Boolean function $f \in \mathcal{B}_n$ is said to be bent if its Walsh–Hadamard spectrum consists of values of the set $\{-2^{n/2}, 2^{n/2}\}$, that is, $|W_f(a)| = 2^{n/2}$, for all $a \in \mathbb{F}_2^n$.*

$r\backslash m$	1	2	3	4	5	6	7	8	9
1	0	1	2	6	12	28	56	120	$240-244$
2		0	1	2	6	18^i	40^s-44^t	84^s-100	171^c-220
3			0	1	2	8	20^s-23^t	43^c-67	111^c-167
4				0	1	2	8	22^s-31	58^c-98
5					0	1	2	10	23^c-41
6						0	1	2	10
7							0	1	2
8								0	1
9									0

Table 1.3: Bounds on the covering radius of Reed–Muller codes

From Equation (1.2.6), $f \in \mathcal{B}_n$ is said to be bent if and only if its nonlinearity is maximum, that is,

$$nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Example 1.2.49. *Let f be a Boolean function in 4 variables of the form $f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_2 + x_1x_3 + x_2x_4 + x_3x_4$. Then f is a bent function as $|W_f(a)| = 4$, for all $a \in \mathbb{F}_2^4$ and $nl(f) = 6$.*

An equivalent definition by using their autocorrelation spectra [54] is given below.

Definition 1.2.50. *An n variables Boolean function f is said to be bent if and only if for any nonzero $\alpha \in \mathbb{F}_2^n$,*

$$\mathcal{C}_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\alpha)} = 0.$$

Definition 1.2.51. *A class of bent functions is complete if it is globally invariant under the action of the general affine group and under the addition of affine functions.*

Using fast Walsh–Hadamard transform one can efficiently compute it up to certain variables as the complexity of fast Walsh–Hadamard transform [51] is $\mathcal{O}(n2^n)$. The properties of bent functions are listed below.

- Let f be a bent function in n variables. Then n must be an even positive integer.

- For $n = 2$, the degree of bent function is 2 and for $n \geq 4$, the degree of bent functions is at most $\frac{n}{2}$ [54, Theorem 4.5].

- Bent functions is invariant under the action of general affine group and addition of affine functions, that is, if $f(x) = h(xA+b)$, for all $x \in \mathbb{F}_2^n$ where $(A, b) \in AGL(n, \mathbb{F}_2)$ then f is bent if and only if h is bent. Also if $f = h + g$ where g is an n variables affine function then f is bent if and only if h is bent.

- Let $f \in \mathcal{B}_n$ be a bent function. Then for all $\alpha \in \mathbb{F}_2^n$,

  $$W_f(\alpha) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\alpha)}$$

  where $\tilde{f}$ is also an n variables bent function, is called dual of f.

- The Hamming weight of a bent function $f \in \mathcal{B}_n$ is $2^{n-1} \pm 2^{\frac{n}{2}-1}$. Therefore, bent functions are not balanced.

- Let $f \in \mathcal{B}_n$. Then $f^{-1}(0) = \{x \in \mathbb{F}_{2^n} : f(x) = 0\}$ or $f^{-1}(1) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$ is a Hadamard difference set in $\mathbb{F}_2^n$.

- Let $f \in \mathcal{B}_n$ and $g \in \mathcal{B}_m$ be bent function, and $h \in \mathcal{B}_{n+m}$ such that $h(x, y) = f(x) + g(y)$, for all $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^m$. Then h is bent.

Compared to the set of Boolean functions, bent functions set are small. Langevin and Leander [93] enumerated all the 8 variables bent functions and classified then under affine equivalence. The number of 8 variables bent functions is

$$99270589265934370305785861242880$$

which is approximately equal to $2^{106.3}$. The number of n, $2 \leq n \leq 8$, variables bent function is given in the Table 1.4. Roughly, the number of bent functions in n variables is bounded above by

$$2^{1+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{n/2}} = 2^{2^{n-1}-1/2\binom{n}{n/2}}.$$

Let r_n be the number of bent function in n variables.

Constructions of bent functions

In this section we focus on primary and some secondary constructions of bent functions. For more details one may refer to [120, 135]. Rothaus studied these functions in the 1960's,

n	2	4	6	8
r_n	8	896	5425430528	99270589265934370305785861242880
$\approx$			$2^{32.3}$	$2^{106.3}$

Table 1.4: Numbers of bent functions in n variables, $2 \leq n \leq 8$

although his paper was not published until ten years later [86]. In print, bent functions appear in a preprint authored by Dillon in 1972, and in his Ph.D. thesis [56]. The class of bent functions found by Dillon is known as Partial Spread ($\mathcal{PS}$) class, and a subclass known as $\mathcal{PS}_{ap}$ allows an explicit mathematical description. The Maiorana–McFarland ($\mathcal{M}$) class introduced in [102] and further investigated in [56] is the other generic class of bent functions discovered around the same time. Dobbertin [49] proposed another set of bent functions which includes both $\mathcal{M}$ and $\mathcal{PS}$. These three classes are also referred to as the primary constructions, whereas the classes $\mathcal{C}$ and $\mathcal{D}$ were introduced by Carlet [17] belong to secondary constructions obtained by modifying the class $\mathcal{M}$.

Rothaus Construction:

In [86], Rothaus identified two large general classes of bent functions on $\mathbb{F}_2^n$. Let $x = (x_1, x_2, \dots, x_t), y = (y_1, y_2, \dots, y_t) \in \mathbb{F}_2^n$. Then

$$f(x_1, y_1, x_2, y_2, \dots, x_t, y_t) = \sum_{i=1}^{t} x_i y_i + p(x)$$

is a bent function where $p(x)$ is an arbitrary polynomial on $\mathbb{F}_2^t$. Rothaus constructed another type of bent functions of the form

$$\begin{aligned} g(x_1, x_2, \dots, x_t, x_{t+1}, y_{t+1}) = f_1(x)f_2(x) + f_2(x)f_3(x) + f_1(x)f_3(x) + [f_1(x) + f_2(x)]y_{t+1} \\ + [f_1(x) + f_3(x)]x_{t+1} + x_{t+1}y_{t+1} \end{aligned}$$

where f_1, f_2 and f_3 are bent functions such that $f_1 + f_2 + f_3$ is bent. The dual of f, $\tilde{f}$, is defined as

$$\tilde{f}(x_1, y_1, x_2, y_2, \dots, x_t, y_t) = \sum_{i=1}^{t} x_i y_i + p(y).$$

Maiorana and McFraland Construction:

Let $\pi : \mathbb{F}_2^t \to \mathbb{F}_2^t$ be a permutation polynomial. Rothaus [86] proved that any function of the form

$$\begin{aligned} &f : \mathbb{F}_2^t \times \mathbb{F}_2^t \to \mathbb{F}_2 \\ &f(x, y) = x \cdot \pi(y) + g(y), \text{ for all } (x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^t, \end{aligned} \tag{1.2.9}$$

is bent where $g \in \mathcal{B}_t$. These bent functions are said to be Maiorana–McFarland bent functions [55, 102], and their set is denoted by $\mathcal{M}$. The dual of f, $\tilde{f}$, is defined as

$$\tilde{f}(x, y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x)), \text{ for all } (x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^t$$

where π^{-1} is inverse of π and f is defined as in Equation (1.2.9). For $f \in \mathcal{M}$ with $g = 0$, the algebraic degree is $\deg(f) = \deg(\pi) + 1$. Maiorana–McFarland construction provides a natural connection between permutations over finite fields and functions in $\mathcal{M}$. Permutations having algebraic degree 1 are said to be linearized permutations. Each linearized permutation on $\mathbb{F}_2^t$ generates a quadratic function in $\mathcal{M}$. The complete Maiorana–McFarland class is denoted by $\mathcal{M}^*$. The completed class of $\mathcal{M}$ contains all the quadratic bent functions.

Proposition 1.2.52 ([55]). *A bent function $f \in \mathcal{B}_n$ belongs to the completed class of Maiorana–MaFarland then there exists an $\frac{n}{2}$ dimensional subspace U in $\mathbb{F}_2^n$ such that all second derivatives are vanish, i.e., for any nonzero $u, v \in U$ with $u \neq v$*

$$D_{u,v} f(x, y) = f(x) + f(x + u) + f(x + v) + f(x + u + v) = 0.$$

Dillon Construction:

Dillon constructed an important class of bent functions referred to as the partial spreads class. It is known that there are functions in the partial spreads class which are not $\mathcal{M}$. The partial Spreads class of bent functions is denoted by $\mathcal{PS}$. $\mathcal{PS}$ is divided by two disjoint classes, so-called $\mathcal{PS}^+$ and $\mathcal{PS}^-$. We first define the meaning of spreads and partial spreads. In this section we takes $n = 2t$, $t \in \mathbb{Z}^+$.

Definition 1.2.53. *Let $\{E_1, E_2, \ldots, E_r\}$ be the set of subspace of $\mathbb{F}_2^n$ over $\mathbb{F}_2$. The set $\{E_1, E_2, \ldots, E_r\}$ is said to be a partial spread of F_2^n if*

- *$E_i \cap E_j = \{0\}$, for all $i \neq j$,*
- *$\dim(E_i) = t$, for all $i \in \{1, 2, \ldots, r\}$,*

i.e., the set of pairwise supplementary t-dimensional subspace of $\mathbb{F}_2^n$. *If* $\cup_{i=1}^{r} E_i = \mathbb{F}_2^n$ *then it is called a spread of* $\mathbb{F}_2^n$ *over* $\mathbb{F}_2$.

A Boolean function $f \in \mathcal{B}_n$ belongs to $\mathcal{PS}^-$ class if $f(0) = 0$ and its support along with 0 is the union of 2^{t-1} elements of a partial spread of $\mathbb{F}_2^n$, that is,

$$supp(f) \cup \{0\} = \cup_{i=1}^{2^{t-1}} E_i \tag{1.2.10}$$

where $\{E_1, E_2, \ldots, E_{2^{t-1}}\}$ is a partial spread. Dillon proved that the Boolean function defined as in Equation (1.2.10) is a bent function with algebraic degree t. Dillon constructed another class of bent function so-called $\mathcal{PS}_{ap}$, a subclass of $\mathcal{PS}^-$. Let $\mathbb{F}_2^n$ be identified as $\mathbb{F}_2^t \times \mathbb{F}_2^t$. A Boolean function $f \in \mathcal{B}_n$ on $\mathbb{F}_2^t \times \mathbb{F}_2^t$ belongs to $\mathcal{PS}_{ap}$ if for all $x, y \in \mathbb{F}_2^t$

$$f(x, y) = g\left(\frac{x}{y}\right)$$

where $g \in \mathcal{B}_n$ is Balanced such that $g(0) = 0$ with convention that $\frac{x}{0} = 0$. The dual of $f \in \mathcal{PS}_{ap}$ is $\tilde{f}(x, y) = g(\frac{y}{x})$.

A Boolean function $f \in \mathcal{B}_n$ belongs to $\mathcal{PS}^+$ class if $f(0) = 1$ and its support is the union of $2^{t-1} + 1$ elements of partial spreads of $\mathbb{F}_2^n$, that is,

$$supp(f) = \cup_{i=1}^{2^{t-1}+1} E_i \tag{1.2.11}$$

where $\{E_1, E_2, \ldots, E_{2^{t-1}+1}\}$ is a partial spread. Dillon also proved that the Boolean function defined as in Equation (1.2.11) is a bent function with algebraic degree t. For, more details and an new construction we refer to [14, 23, 24, 94, 119, 150].

Dobbertin Construction:

Let $g \in \mathcal{B}_t$ be balanced and $\eta, \psi : \mathbb{F}_2^t \to \mathbb{F}_2^t$ such that η be one-to-one and ψ be arbitrary. Suppose f is a Boolean function on $\mathbb{F}_2^t \times \mathbb{F}_2^t$ of the form

$$f_{g,\eta,\psi}(x, \eta(y)) = \begin{cases} g(\frac{x+\psi(y)}{y}), & \text{if } y \neq 0; \\ 0, & \text{if } otherwise. \end{cases}$$

Dobbertin [49] proved that $f_{g,\eta,\psi}$ ia a bent function which includes both $\mathcal{M}$ and $\mathcal{PS}$. Dobbertin also proved that if g is an affine function then the above function $f_{g,\eta,\psi}$ is belong to

$\mathcal{M}$, and $f_{g,\phi_{\mathbb{F}_2^t},0}$ is belong to Dillon's classes where $\phi_{\mathbb{F}_2^t}$ is the identity on $\mathbb{F}_2^t$.

Carlet Construction:

Two new classes of bent functions were introduced by Carlet [17, 18]. Let E be a subspace of $\mathbb{F}_2^t$. The class $\mathcal{D}$ consists of bent functions of the form

$$f(x,y) = x \cdot \pi(y) + \phi_{E_1}(x)\phi_{E_2}(y) \tag{1.2.12}$$

with π a permutation on $\mathbb{F}_2^n$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^t$ such that $\pi(E_2) = E_1^{\perp}$ (ϕ_E is the indicator function of the space E defined as in Definition 1.2.15).

An explicit subclass of $\mathcal{D}$, denoted by $\mathcal{D}_0$, contains all elements of the form

$$x \cdot \pi(y) + \delta_0(x)$$

where $\delta_0(x)$ is the Dirac symbol, which is 1 if $x = 0$, and 0, otherwise. It has been shown that $\mathcal{D}_0$ strictly includes the $\mathcal{M}$ and $\mathcal{PS}$ classes [17, 49].

The second Carlet class $\mathcal{C}$ of bent functions (one we will concentrate on) contains all functions of the form

$$f(x,y) = x \cdot \pi(y) + \phi_{L^{\perp}}(x) \tag{1.2.13}$$

where L is any linear subspace of $\mathbb{F}_2^t$ and π is any permutation on $\mathbb{F}_2^t$ such that $\phi(a + L)$ is a flat (affine subspace), for all $a \in \mathbb{F}_2^t$ where $\phi := \pi^{-1}$. If $L = \mathbb{F}_2^t$ then the function belongs to $\mathcal{C}$ is same as in $\mathcal{D}_0$. Thus, the class $\mathcal{C}$ contains $\mathcal{D}_0$, and so is not included in classes $\mathcal{M}$ and $\mathcal{PS}$.

1.2.7 Generalized Boolean functions

Let $\mathbb{F}_p$, $\mathbb{F}_{p^n}$, and $\mathbb{F}_p^n$ be the prime field of characteristic p, the extension field of degree n over $\mathbb{F}_p$ and the set of all n-tuples of elements of $\mathbb{F}_p$, respectively. For any $x \in \mathbb{F}_{p^n}$ can be written as

$$x = c_1x_1 + c_2x_2 + \ldots + c_nx_n$$

where $x_i \in \mathbb{F}_p$, $i = 1, 2, \ldots, n$ and $c = \{c_1, c_2, \ldots, c_n\}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ (or, equivalently $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$) is called a *generalized Boolean function* in n variables whose set is denoted by $\mathcal{B}_n^p$. For $p = 2$, we obtain the classical Boolean functions whose set is denoted by $\mathcal{B}_n$. Any $f \in \mathcal{B}_n^p$ can be uniquely expressed [151] as a polynomial in $\mathbb{F}_p[x_1, \ldots, x_n]/\langle x_1^p - x, \ldots, x_n^p - x\rangle$ of the form

$$f(x_1, x_2, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_p^n} \mu_a \left(\prod_{i=1}^{n} x_i^{a_i}\right)$$

where $\mu_a \in \mathbb{F}_p$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_p^n$. The algebraic degree of f, denoted by $\deg(f)$, is defined as

$$\deg(f) = \max_{a\in\mathbb{F}_p^n} \left\{\sum_{i=1}^{n} a_i : \mu_a \neq 0\right\}$$

where $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$, the sum is over $\mathbb{Z}$. For details we refer to [4, 82, 83]. Let $\zeta = e^{\frac{2\pi\imath}{p}}$ be the complex p^{th} root of unity where $\imath^2 = -1$. The generalized Walsh–Hadamard transform of $f \in \mathcal{B}_n^p$ at $a \in \mathbb{F}_p^n$ is defined by

$$\mathcal{H}_f(a) = \sum_{x\in\mathbb{F}_p^n} \zeta^{f(x)-a\cdot x}$$

where $a \cdot x$ denotes an inner product on $\mathbb{F}_p^n$. According to [98], a function $f \in \mathcal{B}_n^p$ is called a *generalized bent function* if

$$|\mathcal{H}_f(a)| = p^{\frac{n}{2}}, \text{ for all } a \in \mathbb{F}_p^n.$$

Equivalently, a function $f \in \mathcal{B}_n^p$ is said to be *generalized bent function* if for any nonzero $a \in \mathbb{F}_p^n$,

$$\sum_{x\in\mathbb{F}_p^n} \zeta^{f(x+a)-f(x)} = 0.$$

A bent function f is said to be regular if for any $a \in \mathbb{F}_p^n$, $\mathcal{H}_f(a) = p^{\frac{n}{2}}\zeta^{\tilde{f}(a)}$ where $\tilde{f} \in \mathcal{B}_n^p$ is called dual of f.

The group of all invertible $\mathbb{F}_p$-linear transformations on $\mathbb{F}_p^n$ is denoted by $GL(n, \mathbb{F}_p)$. Two *generalized Boolean functions* $f, g \in \mathcal{B}_n^p$ are said to be affine equivalent if and only if there exist $A \in GL(n, \mathbb{F}_p)$ and $b \in \mathbb{F}_p^n$ such that

$$g(x) = f(xA + b), \text{ for all } x \in \mathbb{F}_p^n.$$

The affine general linear group $AGL(n, \mathbb{F}_p)$ consists of all the elements of the form $(A, b) \in$

$GL(n,\mathbb{F}_p) \ltimes \mathbb{F}_p^n$. Two *generalized Boolean functions* $f, g \in \mathcal{B}_n^p$ are said to be *equivalent* if and only if there exist $(A,b) \in AGL(n,\mathbb{F}_p)$, $u \in \mathbb{F}_p^n$ and $\epsilon \in \mathbb{F}_p$ such that

$$g(x) = f(xA+b) + u \cdot x + \epsilon, \text{ for all } x \in \mathbb{F}_p^n.$$

The derivative of $f \in \mathcal{B}_n^p$ with respect to $a \in \mathbb{F}_p^n$, D_af, is the function $D_af : \mathbb{F}_p^n \to \mathbb{F}_p$ defined as

$$D_af(x) = f(x+a) - f(x), \text{ for all } x \in \mathbb{F}_p^n.$$

The kth-order derivative of $f \in \mathcal{B}_n^p$ with respect to $u_1, u_2, \ldots, u_k \in \mathbb{F}_p^n$ is defined by

$$D_{u_1,u_2,\ldots,u_k}f(x) = D_{u_1}D_{u_2}\ldots D_{u_k}f(x), \text{ for all } x \in \mathbb{F}_p^n.$$

1.3 Group ring

Let $\mathcal{A}$ be a group algebra of $\mathbb{F}_p^n$ over $\mathbb{F}_p$. An element $x \in \mathcal{A}$ can be written as

$$x = \sum_{g \in \mathbb{F}_p^n} x_g X^g \text{ where } x_g \in \mathbb{F}_p.$$

For any $x, y \in \mathcal{A}$ and $c \in \mathbb{F}_p$, addition and scalar multiplication can be defined as

$$x + y = \sum_{g \in \mathbb{F}_p^n} x_g X^g + \sum_{g \in \mathbb{F}_p^n} y_g X^g = \sum_{g \in \mathbb{F}_p^n} z_g X^g \text{ where } z_g = x_g + y_g \in \mathbb{F}_p,$$

$$\text{and} \qquad cx = c\sum_{g \in \mathbb{F}_p^n} x_g X^g = \sum_{g \in \mathbb{F}_p^n} (cx_g) X^g = \sum_{g \in \mathbb{F}_p^n} w_g X^g \text{ where } w_g = cx_g \in \mathbb{F}_p.$$

Using the polynomial multiplication $X^gX^h = X^{g+h}$, the multiplication in the group algebra $\mathcal{A}$ is defined by

$$xy = \sum_{g \in \mathbb{F}_p^n} x_g X^g \sum_{h \in \mathbb{F}_p^n} y_h X^h = \sum_{\ell \in \mathbb{F}_p^n} \left(\sum_{g \in \mathbb{F}_p^n} x_g y_{\ell - g} \right) X^\ell.$$

Note that X^0 is the multiplicative unit of $\mathcal{A}$ as $X^0a = aX^0 = a$, for all $a \in \mathcal{A}$. Consider the mapping $\psi : \mathcal{A} \longrightarrow \mathbb{F}_p$ of the form

$$x = \sum_{g\in\mathbb{F}_p^n} x_g X^g \longmapsto \sum_{g\mathbb{F}_p^n} x_g, \quad \text{for all } \ x \in \mathcal{A}.$$

Then the set

$$\mathcal{P} = \{x \in \mathcal{A} : \psi(x) = 0\} = \{x \in \mathcal{A} : \sum_{g\in\mathbb{F}_p^n} x_g = 0\} \tag{1.3.1}$$

is the unique maximal ideal of $\mathcal{A}$, and

$$\mathcal{A} = \mathcal{P}^0 \supset \mathcal{P} \supset \mathcal{P}^2 \supset \ldots \supset \mathcal{P}^{n(p-1)} = \mathbb{F}_p$$

where $\mathcal{P}^i\mathcal{P}^j = \mathcal{P}^{i+j}$ and $\mathcal{P}^{n(p-1)+1} = \{0\}$. For more details we refer to [1, 39].

A *generalized Boolean function* $f \in \mathcal{B}_n^p$ can be identified with the codeword $\Omega_f = \sum_{g\in\mathbb{F}_p^n} f(g)X^g$ of length p^n consisting of all values of $f(x), x \in \mathbb{F}_p^n$. The support of $f \in \mathcal{B}_n^p$, denoted by $supp(\Omega_f)$, is defined by

$$supp(\Omega_f) = \{x \in \mathbb{F}_p^n : f(x) \neq 0\}.$$

The generalized Reed–Muller code, $\mathcal{R}_p(r, n)$, is the set of codewords Ω_f where $f \in \mathcal{B}_n^p$ with $\deg(f) \leq r$, $0 \leq r \leq n(p-1)$. Let $1 \in \mathbb{F}_p^n$ be a vector contains all 1's. Then $\mathcal{R}_p(0, n) = 1\mathbb{F}_p = \langle 1\rangle$ and $\mathcal{R}_p(n(p-1), n) = \mathbb{F}_p^{p^n}$. The dimension of $\mathcal{R}_p(r, n)$, denoted by $\dim(\mathcal{R}_p(r, n))$, is defined as

$$\dim(\mathcal{R}_p(r, n)) = \sum_{i=0}^{r}\sum_{j=0}^{n}(-1)^j \binom{n}{j}\binom{i - jp + n - 1}{i - jp},$$

for all $0 \leq r \leq n(p-1)$. For example, $\dim(\mathcal{R}_p(1, n))$ is equal to $1 + n$. For further details we refer to [38, 92].

1.4 Overview of the thesis

Chapter wise brief description of this thesis is given below:

Chapter 1. In this chapter, we give the introductory matter, some basic definitions, notations, representation of Boolean functions, Walsh–Hadamard transform, cryptographic significant properties, Reed–Muller code and *generalized Boolean functions*. We further discuss affine equivalence and derivatives of Boolean functions. Also we give a literature survey on construction of bent Boolean function and the existence results on nonlinearity profile of the Boolean functions. We provide some basic on finite fields and group ring which is useful to our work.

Chapter 2. In this chapter, we construct two subclasses of cubic bent functions in $\mathcal{M}$, f_i and g, of the form

1. $f_i(x,y) = \mathrm{Tr}_1^t(xy^{2^i+1} + \alpha xy^{2^{t-i}+1})$
2. $g(x,y) = \mathrm{Tr}_1^t(xy\mathrm{Tr}_l^t(y) + \beta xy^2)$,

for all $(x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ by using two quadratic permutations which were introduced by Blockhuis et al. [2]. We show that the functions in each of these classes have no affine derivative. We prove that the functions in the different subclasses are affine inequivalent by considering their second-derivative weight distributions. Thus, we extend the number of known cubic bent functions in $\mathcal{M}$ with no affine derivative.

Chapter 3. The aim of this chapter is to obtain explicit construction of several subclasses of bent functions in $\mathcal{C}$ for the first time. We are able to identify permutations corresponding to which there are no $\mathcal{C}$ class bent functions. We investigate the choice of linear subspaces L which may potentially give rise to bent functions in $\mathcal{C}$ for some specific permutations π and later we extend the derived conditions for arbitrary π. The analysis uses more general bent conditions (without requesting that the initial function is in $\mathcal{M}$) given in [17, Theorem]. We consider

$$f^*(x,y) = x \cdot \pi(y) + \phi_L(x,y)$$

where $\pi(y) = yA$ is a linear permutation over $\mathbb{F}_2^n$, $L = E \times \mathbb{F}_2^n$ for some k-dimensional linear subspace E, for $0 \leq k \leq n$, and A is an invertible matrix over $\mathbb{F}_2$ of size $n \times n$ (that is $A \in GL(n, \mathbb{F}_2)$). It is shown that f^* is always bent regardless the choice of E, but nevertheless f^* is in the completed class $\mathcal{M}^*$. Further, we consider those permutation polynomials which can be factored (split) into linearized polynomials namely k-linear split permutation, and look at $\mathcal{C}$ type bent functions associated to k-linear split permutations. The main contribution of this chapter can be summarized as follows:

- A classification of linear subspaces that may potentially give rise to bent functions in the $\mathcal{C}$ class is given.

- A theoretical analysis related to the conditions that a permutation π and a linear subspace $L = E \times \mathbb{F}_2^n \subset \mathbb{F}_2^{2n}$ satisfy the bent conditions is presented.

- It is shown that for several classes of permutations π there does not exist 2-dimensional subspace L satisfying the bent conditions. For instance, $\mathcal{C}$ class bent functions associate to Hou's permutations [152, Theorem B] and certain trilinear split permutations.

- The existence of 2-dimensional linear subspaces satisfying the bent conditions have been confirmed for certain classes of bilinear split permutations. Thus, some infinite classes of bent functions in $\mathcal{C}$ have been specified.

Chapter 4. In this chapter, we consider the *generalized Boolean functions* from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ where p is an odd prime integer and the set of all n variables *generalized Boolean function* is denoted by $\mathcal{B}_n^p$. We further characterize the subspace sum concept (depending upon the derivative) and give many of its properties; in particular, we show that it is an affine invariant of *generalized Boolean functions*. First, we define the subspace sum of $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$, $\mathcal{S}_V f$, as

$$\mathcal{S}_V f(x) = \sum_{s \in V} f(x+s), \text{ for all } x \in \mathbb{F}_p^n.$$

We prove that

$$\mathcal{S}_V f(x) = \underbrace{D_a D_a \dots D_a}_{(p-1)-\text{times}} f(x), \text{ for all } x \in \mathbb{F}_p^n$$

where $V = \langle a \rangle$ is an one dimensional subspace of $\mathbb{F}_p^n$. We also prove that if $f, h \in \mathcal{B}_n^p$ are affine equivalent then so are $\mathcal{S}_k[f]$ and $\mathcal{S}_k[h]$ where $\mathcal{S}_k[f]$ denotes the multiset of all subspace sum of f with respect to k-dimensional subspaces of $\mathbb{F}_p^n$, and we generalize a result of Dillon [56]. We derive a necessary condition for generalized Maiorana-McFarland bent functions.

Chapter 5. In this chapter, we consider $m = 2n$ and construct two new classes of *generalized bent functions* (so-called $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ where $\mathcal{D}_0^p$ is a subclass of $\mathcal{D}^p$). We observe that if $f \in \mathcal{D}_0^p$ is an m-variable *generalized Boolean function* then $m \equiv 0 \pmod 4$ and

$$f(x,y) = x \cdot \pi(y) + \epsilon \phi_{E_0}(x,y) = x \cdot \pi(y) + \epsilon \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j)$$

where $(x,y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ and $E_0 = \{0\} \times \mathbb{F}_p^n$, is a regular *generalized bent function.* We prove that $\mathcal{M}^p$ and $\mathcal{D}_0^p \subseteq \mathcal{D}^p$ are overlapping classes, but in general not included in one another. For construction of $\mathcal{C}^p$ bent functions, it is needed to consider a permutation polynomial π on $\mathbb{F}_p^n$ such that $\pi^{-1}(a+L)$ is a flat for any $a \in \mathbb{F}_p^n$ where L is a linear subspace of $\mathbb{F}_p^n$. We investigate these conditions for many classes of permutations and suitable linear subspaces of the dimension less than and equal to 2 for $p = 3$.

Chapter 6. The main focus of this chapter is to compute the weights of their second derivatives along with a lower bound of their second-order nonlinearities of cubic Maiorana–McFarland bent-negabent functions constructed by using Feistel functions. We take $m = 4t$, $t \geq 3$ and construct a class of cubic Maiorana–McFarland bent-negabent functions by using Feistel functions of the form

$$f_i((x_1,x_2),(y_1,y_2)) = \mathrm{Tr}_1^t(x_1y_2 + x_2y_1 + x_2y_2^{2^i+1}),$$

for all $x_j, y_j \in \mathbb{F}_{2^t}$, $j = 1,2$ where $\gcd(2^i+1, 2^t-1) = 1$, $1 \leq i < t$. We calculate that the number of distinct 2-dimensional subspaces of $\mathbb{F}_{2^t}^4$ corresponding to constant second-derivatives of f_i is

$$\frac{(2^t-1)(2^{5t+e-1}(2^e+1) + (2^t+1)(2^{4t-1} - 2^{2t} - 1))}{3},$$

which depends on $e = \gcd(i,t)$. Thus, by using an invariant proposed by Dillon [56], we identify subclasses of inequivalent bent functions within this class. Further, we prove that the second-order nonlinearity of f_i, $nl_2(f_i)$, satisfies the following inequality:

$$nl_2(f) \geq 2^{m-1} - \frac{1}{2}\sqrt{2^{7t+e} - 2^{\frac{11t+e}{2}} + 2^{6t}(2^{\frac{t+e}{2}} - 2^e + 1)}.$$

Chapter 7. The purpose of this chapter is to locate some functions with low Gowers U_3 norms, since this is also a measure of resistance to second-order approximation of Boolean functions. First, we derive formula to calculate the kth dimensional Gowers norm associated to a Boolean function from the Fourier transform using derivatives. Further, we prove that the Gowers U_3 norms of a bent and its dual are equal and therefore they provide equal "resistance" to quadratic approximations. We compute Gowers U_3 norms of the character form of some classes of Maiorana–McFarland bent functions of the form

$$F_i(x, y) = \mathrm{Tr}_1^n(yx^{2^i+1}),$$

for all $x, y \in \mathbb{F}_{2^n}$. In particular, we explicitly determine the value of the Gowers U_3 norm of the character form of Maiorana–McFarland bent functions obtained by using APN permutations of the form

$$F(x, y) = \mathrm{Tr}_1^n(\phi(x) \cdot y) + h(x),$$

for all $x, y \in \mathbb{F}_{2^n}$ where $h \in \mathcal{B}_n$ and ϕ is an APN permutation on $\mathbb{F}_{2^n}$. We further prove that this value is always smaller than the Gowers U_3 norms of Maiorana–McFarland bent functions obtained by using differentially δ-uniform permutations, for all $\delta \geq 4$. Also we compute the Gowers U_3 norm of the character form of a class of cubic monomial Boolean functions of the form

$$F_r(x) = \mathrm{Tr}_1^n(\lambda x^{2^{2r}+2^r+1}),$$

for all $x \in \mathbb{F}_{2^{3r}}$ and $\lambda \in \mathbb{F}_{2^r}^*$, and show that for $n = 6$ its value is less than that obtained for Maiorana–McFarland bent function constructed by using APN permutations. We then computationally show that the corresponding function has higher second-order nonlinearity that Maiaorana–McFarland bent functions. In fact the 6-variable function identified by us has the maximum possible second-order nonlinearity.

Chapter 8. This chapter contains conclusion of the thesis and some open problems for future work.

Chapter 2

Affine inequivalence of cubic Maiorana–McFarland bent functions with no affine derivative

2.1 Introduction

A class of cubic Maiorana–McFarland ($\mathcal{M}$) bent functions having no affine derivatives was constructed by Canteaut and Charpin [5], thereby solving an open problem posed by Hou [149]. In [91], Charpin et al. derived a relation between polynomials with linear structures and Maiorana–McFarland functions with an affine derivative. The experimental evidences [110, Section 3] suggest that cubic bent functions having no affine derivatives might be possessing higher second-order nonlinearity than the rest. Derivatives have been used for this purpose by Carlet [17] and Canteaut and Charpin [5]. Second derivatives have been used by Gangopadhyay [111] extensively to demonstrate affine inequivalence between cubic bent functions in $\mathcal{M}$ which are in many ways similar to each other. The technique can be summarized as follows:

1. For $f \in \mathcal{B}_n$, construct the set

$$S_f = \{wt(D_V f) : V \text{ varies over all distinct two dimensional subspaces of } \mathbb{F}_2^n\}.$$

2. Construct the frequency distribution of the weights in S_f. We refer to S_f as the

second-derivative weight distribution of f.

3. For any two $f, g \in \mathcal{B}_n$, if the second-derivative weight distributions of f and g are different then f and g are affine inequivalent.

In this chapter our goal is not only to identify some more classes of cubic bent functions in $\mathcal{M}$ having no affine derivatives but also to prove affine inequivalence between the classes of functions so obtained. We use Theorem 2.2.2 almost exclusively for that purpose.

2.2 Preliminary results

Recall the following well known facts from elementary number theory, which we use frequently in this chapter. Suppose that $ax \equiv b \pmod{n}$ where $a, b, n \in \mathbb{Z}$ and $d = \gcd(a, n)$. Then

1. if d does not divide b, the congruence has no solution;

2. if d divides b then all solutions of the congruence are $x_0 + k\frac{n}{d}$, $0 \leq k < d$ where x_0 is the unique solution to $(\frac{a}{d})x \equiv (\frac{b}{d}) \pmod{\frac{n}{d}}$.

Let t be a positive integer and $\gcd(t, i) = e$. Then [105, page 2]

$$\gcd(2^{2i} - 1, 2^t - 1) = 2^{\gcd(2i,t)} - 1 = \begin{cases} 2^e - 1, & \text{if } \frac{t}{e} \text{ is odd;} \\ 2^{2e} - 1, & \text{if } \frac{t}{e} \text{ is even.} \end{cases}$$

Theorem 2.2.1 ([105, Theorem 3.1]). *Let ζ be a primitive element of $\mathbb{F}_{2^t}$ and $\gcd(t, i) = e$. For any $a \in \mathbb{F}_{2^t}^*$, consider the equation $a^{2^i} x^{2^{2i}} + ax = 0$ over $\mathbb{F}_{2^t}$. Then:*

1. *If $\frac{t}{e}$ is odd then there are 2^e solutions to this equation for any choice of $a \in \mathbb{F}_{2^t}^*$.*

2. *If $\frac{t}{e}$ is even then there are two possible cases:*

   (*a*) *if $a = \zeta^{s(2^e+1)}$ for some s then there are 2^{2e} solutions to the equation.*

   (*b*) *if $a \neq \zeta^{s(2^e+1)}$ for any s then there exists one solution only, namely $x = 0$.*

Gangopadhyay [111] identified subclasses of inequivalent bent functions within this class, by using an invariant proposed by Dillon [56].

Theorem 2.2.2 ([111, Theorem 4])**.** *Let $n = 2t$. If $f_i(x, y) = \mathrm{Tr}_1^t(xy^{2^i+1})$ where $x, y \in \mathbb{F}_{2^t}$, $n \geq 6$, $i \in \mathbb{Z}$ such that $1 \leq i < t$ and $\gcd(2^i + 1, 2^t - 1) = 1$ then the number of constant functions among $D_V f_i$ is*

$$\frac{(2^t - 1)(2^{t+e-1}(2^e + 1) - (2^t + 1))}{3}$$

where $\gcd(t, i) = e$.

Using this result, Gangopadhyay [111, Corollary 5] proved that if $\gcd(t, i) \neq \gcd(t, j)$ then f_i and f_j are not affine equivalent.

2.3 Maiorana–McFarland bent functions

Suppose $n = 2t$ where $t \in \mathbb{Z}^+$. Any permutation $\pi : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ can be represented by a polynomial $\pi(x) = \sum_{j=0}^{2^t-1} \alpha_j x^j$ where $\alpha_j \in \mathbb{F}_{2^t}$, for all $0 \leq j \leq 2^t - 1$. The algebraic degree of π is $\deg(\pi) = \max\{w_2(j) : \alpha_j \neq 0\}$. Rothaus [86] proved that any function of the form

$$\begin{aligned} &f : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_2 \\ &f(x, y) = \mathrm{Tr}_1^t(x\pi(y)) + g(y), \text{ for all } (x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \end{aligned} \tag{2.3.1}$$

where $g \in \mathcal{B}_t$, is bent. These bent functions are said to be Maiorana–McFarland bent functions and their set is denoted by $\mathcal{M}$. In this chapter we assume g to be identically zero. For $f \in \mathcal{M}$ with $g = 0$ the algebraic degree is $\deg(f) = \deg(\pi) + 1$.

Suppose that $\gcd(t, i) = e$ with $\frac{t}{e}$ is an odd positive integer. Let $\alpha \in \mathbb{F}_{2^t}$ such that $\alpha \neq \zeta^{m(2^e-1)}$ for any $m \in \mathbb{Z}$, ζ be any primitive element of $\mathbb{F}_{2^t}$. Blokhuis et al. [2] mentioned that σ_j, $j \in \{1, 2, 3\}$, listed below are linearized permutations on $\mathbb{F}_{2^t}$.

$$\begin{aligned} \sigma_1(x) &= x^{2^i} + \alpha x, \\ \sigma_2(x) &= x^{2^{2i}} + \alpha^{2^i} x, \\ \sigma_3(x) &= x^{2^i} + \alpha^{2^i} x. \end{aligned}$$

Some other linearized polynomials over $\mathbb{F}_{2^t}$ which will be used in the chapter are as follows:

$$\begin{aligned}
\sigma_4(y) &= y^{2^{2i}} + \alpha^{2^{2i}} y, \\
\sigma_5(y) &= y^{2^{2i}} + \alpha y, \\
\sigma_6(y) &= y + \alpha^{2^i} y^{2^i}, \\
\sigma_7(y) &= y + \alpha^{2^{2i}} y^{2^{2i}}, \\
\sigma_8(y) &= y + \alpha^{2^{2i}} y^{2^i}.
\end{aligned}$$

The linearized function $\sigma_4(y) = 0$ if and only if $y = 0$ or $y^{2^{2i}-1} = \alpha^{2^{2i}}$. If $y^{2^{2i}-1} = \alpha^{2^{2i}}$ then $\left(\alpha^{\frac{2^t-1}{2^e-1}}\right)^{2^{2i}} = 1$, since $e \,|\, i$, which implies $\alpha^{\frac{2^t-1}{2^e-1}} = 1$. This is a contradiction, since $\alpha^{\frac{2^t-1}{2^e-1}} \neq 1$. Thus, σ_4 is a linearized permutation. Similarly, it can be proved that σ_j, $j = 5, 6, 7, 8$ are linearized permutations.

Each function $f(x, y) = \mathrm{Tr}_1^t(x\sigma_j(y))$, $1 \leq j \leq 8$, is a quadratic bent in $\mathcal{M}$. Moreover, the following two quadratic permutations were constructed by Blockhuis et al. [2]:

$$\begin{aligned}
\pi_1(y) &= y^{2^i+1} + \alpha y^{2^{t-i}+1}, \\
\pi_2(y) &= y(\mathrm{Tr}_\ell^t(y) + \alpha y)
\end{aligned} \tag{2.3.2}$$

where $t = k\ell$, k is an odd integer and $\ell > 1$ is any positive integer (discussed later in details in Section 2.4 on the parameter α). In this chapter, we use the functions of the form $f_j(x, y) = \mathrm{Tr}_1^t(x\pi_j(y))$, $1 \leq j \leq 2$ as a source of cubic bent functions and consider their differential properties.

2.4 Cubic bent functions in $\mathcal{M}$

Two subclasses of cubic bent functions in $\mathcal{M}$ are constructed by using the permutations in Equation (2.3.2). We show that the functions in each of these classes have no affine derivatives. We prove that the functions in the different subclasses are affine inequivalent by considering their second-derivative weight distributions. Thus, we extend the number of known cubic bent functions in $\mathcal{M}$ with no affine derivatives.

2.4.1 Subclass associated to $\pi_1(y) = y^{2^i+1} + \alpha y^{2^{t-i}+1}$

Let $n = 2t$, $t \geq 3$ and ζ be a primitive element of $\mathbb{F}_{2^t}$. Blokhuis et al. [2] proved that the function $\pi_1 : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ defined by

$$\pi_1(y) = y^{2^i+1} + \alpha y^{2^{t-i}+1},$$

for all $y \in \mathbb{F}_{2^t}$ where $i \in \mathbb{Z}$ such that $1 \leq i < t$ is a permutation if the following conditions are satisfied:

1. $\gcd(i, t) = e$ and $\frac{t}{e}$ is odd;
2. $\alpha \neq \zeta^{s(2^e-1)}$ for any $s \in \mathbb{Z}$.

Lemma 2.4.1. *Under the above conditions, the cubic Maiorana–McFarland bent function $f_i : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_2$ defined by*

$$f_i(x, y) = \mathrm{Tr}_1^t(xy^{2^i+1} + \alpha xy^{2^{t-i}+1}), \ \textit{for all } (x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}, \tag{2.4.1}$$

does not possess any affine derivative.

Proof. Let $a, b \in \mathbb{F}_{2^t}$. Then the first derivative of f_i at $(a, b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ is

$$\begin{aligned} D_{(a,b)} f_i(x, y) &= \mathrm{Tr}_1^t \left(a\pi_1(y) + (x + a)D_b\pi_1(y)\right) \\ &= \mathrm{Tr}_1^t \Big(a \left(y^{2^i+1} + \alpha y^{2^{t-i}+1}\right) \\ &\quad +(x + a) \left(y^{2^i} b + yb^{2^i} + b^{2^i+1} + \alpha y^{2^{t-i}} b + \alpha yb^{2^{t-i}} + \alpha b^{2^{t-i}+1}\right)\Big), \end{aligned}$$

for all $(x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. If $a \neq 0$ then $D_{(a,b)} f_i(x, y)$ is a quadratic function. If $a = 0$ and $b \neq 0$ then

$$D_{(0,b)} f_i(x, y) = \mathrm{Tr}_1^t \left(x \left(y^{2^i} b + yb^{2^i} + \alpha y^{2^{t-i}} b + \alpha yb^{2^{t-i}}\right) + x(b^{2^i+1} + \alpha b^{2^{t-i}+1})\right)$$

is an affine function if and only if

$$p(y) = y^{2^i} b + yb^{2^i} + \alpha y^{2^{t-i}} b + \alpha yb^{2^{t-i}}$$

is constant, for all $y \in \mathbb{F}_{2^t}$. Since $p(0) = 0$, then (simplifying by y above)

$$y^{2^i-1} + b^{2^i-1} + \alpha y^{2^{t-i}-1} + \alpha b^{2^{t-i}-1} = 0,$$

for all $y \in \mathbb{F}_{2^t}^*$. For $y = 1$, we get $b^{2^i-1} + \alpha b^{2^{t-i}-1} = 1 + \alpha$, which renders

$$y^{2^i-1} + \alpha y^{2^{t-i}-1} + 1 + \alpha = 0. \tag{2.4.2}$$

If $\alpha = 0$ then the solution space of Equation (2.4.2) is $\mathbb{F}_{2^e}$. Let $\alpha \neq 0$. We know that for $y \in \mathbb{F}_{2^e}$, $y^{2^i-1} = 1 = y^{2^{t-i}-1}$, since $e = \gcd(i, t)$. Therefore, Equation (2.4.2) is identically zero. Otherwise, substituting $y = c \in \mathbb{F}_{2^t} \backslash \mathbb{F}_{2^e}$ in Equation (2.4.2) $c^{2^i-1} + \alpha c^{2^{t-i}-1} + 1 + \alpha = 0$, so $\alpha = \frac{c+c^{2^i}}{c+c^{2^{t-i}}}$ and then, $\alpha^{2^i} = \frac{(c+c^{2^i})^{2^i}}{(c+c^{2^{t-i}})^{2^i}} = (c + c^{2^i})^{2^i-1}$, that is, $\left(\alpha^{\frac{2^t-1}{2^e-1}}\right)^{2^i} = 1$, since $e \,|\, i$, which implies $\alpha^{\frac{2^t-1}{2^e-1}} = 1$. This is a contradiction, since $\alpha^{\frac{2^t-1}{2^e-1}} \neq 1$ (otherwise, the condition $\alpha \neq \zeta^{s(2^e-1)}$ would be violated). Thus, Equation (2.4.2) does not hold, for all $y \in \mathbb{F}_{2^t}$. Therefore, $D_{(0,b)} f_i$ is not an affine function, and our lemma is shown. ■

Theorem 2.4.2. *The number of distinct* 2*-dimensional subspaces corresponding to constant second-derivatives of f_i is*

$$\frac{(2^t - 1)\,(2^{t+e-1}(2^e + 1) - (2^t + 1))}{3}$$

where f_i is defined as in Equation (2.4.1).

Proof. Let $V = \langle (a, b), (c, d) \rangle$ be any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. The second-order derivative of f_i is

$$\begin{aligned} D_V f_i(x, y) &= f_i(x, y) + f_i(x + a, y + b) + f_i(x + c, y + d) + f_i(x + a + c, y + b + d) \\ &= \mathrm{Tr}_1^t((ad + bc)y^{2^i} + (ad^{2^i} + cb^{2^i})y + \alpha(ad + cb)y^{2^{t-i}} + \alpha(ad^{2^{t-i}} + cb^{2^{t-i}})y \\ &\quad + \gamma x + (ad^{2^i+1} + cb^{2^i+1}) + \alpha(ad^{2^{t-i}+1} + cb^{2^{t-i}+1}) + (a + c)\gamma) \end{aligned}$$

where $\gamma = (bd^{2^i} + b^{2^i} d) + \alpha(bd^{2^{t-i}} + b^{2^{t-i}} d)$.

Case 1: We first assume $b = 0$ and $d = 0$. Then $D_V f_i(x, y) = 0$, for all $(x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. Thus, with respect to any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \{0\}$ the second-order derivative of f_i is 0. Therefore, the number of distinct 2-dimensional subspaces such that $D_V f_i$ is constant, is equal to $\frac{(2^t-1)(2^{t-1}-1)}{3}$.

Case 2: Let $b = 0$ but $d \neq 0$. Then

$$\begin{aligned} D_V f_i(x,y) &= \mathrm{Tr}_1^t \left((ad)y^{2^i} + (ad^{2^i})y + \alpha(ad)y^{2^{t-i}} + \alpha(ad^{2^{t-i}})y + (ad^{2^i+1}) + \alpha(ad^{2^{t-i}+1}) \right) \\ &= \mathrm{Tr}_1^t \left(((ad)^{2^{t-i}} + ad^{2^i} + (\alpha ad)^{2^i} + \alpha ad^{2^{t-i}})y \right) + \mathrm{Tr}_1^t \left(ad^{2^i+1} + \alpha ad^{2^{t-i}+1} \right). \end{aligned}$$

Thus, $D_V f_i(x,y)$ is constant if and only if $(ad)^{2^{t-i}} + ad^{2^i} + (\alpha ad)^{2^i} + \alpha ad^{2^{t-i}} = 0$, and so,

$$\begin{aligned} 0 &= ((ad)^{2^{t-i}} + ad^{2^i} + (\alpha ad)^{2^i} + \alpha ad^{2^{t-i}})^{2^i} \\ &= ad + a^{2^i} d^{2^{2i}} + (\alpha ad)^{2^{2i}} + (\alpha a)^{2^i} d \\ &= (a^{2^i} + (\alpha a)^{2^{2i}}) d^{2^{2i}} + (a + (\alpha a)^{2^i}) d, \end{aligned}$$

which can be written as $h^{2^i} d^{2^{2i}} + hd = 0$ where $h = a + (\alpha a)^{2^i}$. Thus, $h \neq 0$ as $a \neq 0$. Then by Theorem 2.2.1, the above equation has $2^e - 1$ nonzero solutions for d in $\mathbb{F}_{2^t}$. Therefore, for any nonzero $a \in \mathbb{F}_{2^t}$, it is possible to choose d in $2^e - 1$ ways, a can be chosen in $2^t - 1$ ways and c in 2^t ways. Since the subspace generated by $\{(a,0),(c,d)\}$ is equal to the subspace generated by $\{(a,0),(a+c,d)\}$. Therefore the total number of distinct 2-dimensional subspaces such that the second derivative of f_i is constant, is equal to $(2^t - 1)2^{t-1}(2^e - 1)$.

Case 3: Let $b \neq 0$ and $d \neq 0$.

Subcase (*i*): Let $b = d$. Then the subspace generated by $\{(a,b),(c,d)\}$ is equal to the subspace generated by $\{(a+c, b+d),(c,d)\} = \{(a+c,0),(c,d)\}$, which is the same as in the previous case.

Subcase (*ii*): Let $b \neq d$. Then $D_V f_i(x,y)$ is constant if and only if

$$\mathrm{Tr}_1^t \left((ad+bc)y^{2^i} + (ad^{2^i} + cb^{2^i})y + \alpha(ad+cb)y^{2^{t-i}} + \alpha(ad^{2^{t-i}} + cb^{2^{t-i}})y \right) = 0 \qquad (2.4.3)$$

and

$$\gamma = 0. \qquad (2.4.4)$$

From Equation (2.4.4), we have $b^{2^i-1} + \alpha b^{2^{t-i}-1} = d^{2^i-1} + \alpha d^{2^{t-i}-1}$, since $b \neq 0$ and $d \neq 0$.

Again, from Equation (2.4.4),

$$0=\gamma=\gamma^{2^i}=b^{2^i}d^{2^{2i}}+b^{2^{2i}}d^{2^i}+\alpha^{2^i}(b^{2^i}d+bd^{2^i})=(bd^{2^i}+b^{2^i}d)^{2^i}+\alpha^{2^i}(b^{2^i}d+bd^{2^i}).$$

Let $z=bd^{2^i}+b^{2^i}d$. Then the above equation can be written as $z^{2^i}+\alpha^{2^i}z=0$, which has the only solution $z=0$, that is,

$$\begin{aligned}&b^{2^i}d+bd^{2^i}=0\Leftrightarrow\left(\frac{d}{b}\right)^{2^i-1}=1,\quad\text{as}\ \ b\neq 0\ \ \text{and}\ \ d\neq 0,\\&\text{and so, }\frac{d}{b}\in\mathbb{F}_{2^e}^{*},\quad\text{as}\ \ \gcd(t,i)=e.\end{aligned}$$

Since $b\neq d$, for any nonzero b, there exist a nonzero $\lambda\in\mathbb{F}_{2^e}$ with $\lambda\neq 1$ such that $d=\lambda b$. Thus, d can be chosen in 2^e-2 ways and b in 2^t-1 ways.

Further, from Equation (2.4.3), we have

$$\begin{aligned}&\mathrm{Tr}_1^t\left((ad+bc)y^{2^i}+\alpha(ad+cb)y^{2^{t-i}}+y\left((ad^{2^i}+cb^{2^i})+\alpha(ad^{2^{t-i}}+cb^{2^{t-i}})\right)\right)=0,\\\Leftrightarrow\ &\mathrm{Tr}_1^t\left((ad+bc)y^{2^i}+\alpha(ad+cb)y^{2^{t-i}}+y(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})\right)=0,\\\Leftrightarrow\ &\mathrm{Tr}_1^t\left(\left((ad+bc)^{2^{t-i}}+(\alpha(ad+cb))^{2^i}+(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})\right)y\right)=0,\end{aligned}$$

for all $y\in\mathbb{F}_{2^t}$ if and only if the following (equivalent) statements hold

$$\begin{aligned}&(ad+bc)^{2^{t-i}}+(\alpha(ad+cb))^{2^i}+(ad+bc)(b^{2^i-1}+\alpha b^{2^{t-i}-1})=0,\\\Leftrightarrow\ &b^{2^{t-i}}(a\lambda+c)^{2^{t-i}}+b^{2^i}(\alpha(a\lambda+c))^{2^i}+(a\lambda+c)(b^{2^i}+\alpha b^{2^{t-i}})=0,\\\Leftrightarrow\ &b^{2^{t-i}}w^{2^{t-i}}+b^{2^i}(\alpha w)^{2^i}+w(b^{2^i}+\alpha b^{2^{t-i}})=0\ \text{ where }w=a\lambda+c,\\\Leftrightarrow\ &(b^{2^{t-i}}w^{2^{t-i}}+b^{2^i}(\alpha w)^{2^i}+w(b^{2^i}+\alpha b^{2^{t-i}}))^{2^i}=0,\\\Leftrightarrow\ &bw+(\alpha b)^{2^{2i}}w^{2^{2i}}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i}=0,\\\Leftrightarrow\ &w((\alpha b)^{2^{2i}}w^{2^{2i}-1}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i-1}+b)=0.\end{aligned}$$

Therefore, we infer that either $w=0$ or $(\alpha b)^{2^{2i}}w^{2^{2i}-1}+(b^{2^{2i}}+\alpha^{2^i}b)w^{2^i-1}+b=0$, which can be transformed into

$$\begin{aligned}
& (\alpha b)^{2^{2i}} w^{(2^i-1)(2^i+1)} + (b^{2^{2i}} + \alpha^{2^i} b) w^{2^i-1} + b = 0,\\
\Leftrightarrow\ & \alpha^{2^{2i}} b^{2^{2i}} \mu^{2^i+1} + b^{2^{2i}}\mu + \alpha^{2^i} b\mu + b = 0 \ \text{ where } \ w^{2^i-1} = \mu,\\
\Leftrightarrow\ & (\alpha^{2^i}\mu + 1)^{2^i} b^{2^{2i}}\mu + (\alpha^{2^i}\mu + 1)b = 0,\\
\Leftrightarrow\ & b(\alpha^{2^i}\mu + 1)(b^{2^{2i}-1}\mu(\alpha^{2^i}\mu + 1)^{2^i-1} + 1) = 0,\\
& \alpha^{2^i}\mu + 1 \neq 0, \text{ since the only solution of } \alpha^{2^i} w^{2^i} + w = 0 \text{ is } w = 0 \text{ due to } \sigma_6(y),\\
\Leftrightarrow\ & b^{2^{2i}-1}\mu(\alpha^{2^i}\mu + 1)^{2^i-1} + 1 = 0, \ \text{ as } \ b \neq 0 \ \text{ and } \ \alpha^{2^i}\mu + 1 \neq 0,\\
\Leftrightarrow\ & b^{(2^i+1)(2^i-1)} w^{2^i-1}(\alpha^{2^i} w^{2^i-1} + 1)^{2^i-1} + 1 = 0,\\
\Leftrightarrow\ & (b^{2^i+1}(\alpha^{2^i} w^{2^i} + w))^{2^i-1} = 1,\\
\Leftrightarrow\ & b^{2^i+1}(\alpha^{2^i} w^{2^i} + w) \in \mathbb{F}_{2^i}^*,\\
\Leftrightarrow\ & b^{2^i+1}(\alpha^{2^i} w^{2^i} + w) \in \mathbb{F}_{2^e}^*, \ \text{ as } \ \gcd(i,t) = e,
\end{aligned}$$

and thus

$$\alpha^{2^i} w^{2^i} + w = \frac{\lambda'}{b^{2^i+1}}, \ \text{ as } \ b \neq 0 \ \text{ and } \ \lambda' \in \mathbb{F}_{2^e}. \tag{2.4.5}$$

Since the homogeneous part of the above equation is a linear equation which has a unique solution $w = 0$, then Equation (2.4.5) has a unique solution in $\mathbb{F}_{2^t}$ for each $\lambda' \in \mathbb{F}_{2^e}$. Thus, w can be chosen in 2^e ways (including $w = 0$). For fixed a and b, c can be chosen in 2^e ways. Therefore, a can be chosen in 2^t ways, b in $2^t - 1$ ways, d in $2^e - 2$ ways and c in 2^e ways. Each 2-dimensional subspace generated by a pair of vectors (a, b) and (c, d) satisfying the above conditions, contains altogether 6 distinct bases satisfying these conditions. Therefore, the total number of distinct two dimensional subspaces with bases of this type is $\frac{2^{t+e}(2^t-1)(2^e-2)}{6}$. Adding the counts from the above three cases we obtain the total count $\frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3}$, and the theorem is shown. ■

Remark 2.4.3. *If $\alpha = 0$ then the cubic Maiorana–McFarland bent function defined as in Equation* (2.4.1) *is $f_i(x, y) = \mathrm{Tr}_1^t(xy^{2^i+1})$, for all $(x, y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. From Theorem* 2.2.2*, we have the number of constant functions among the second-order derivative of f_i is $\frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3}$.*

In Theorem 2.4.2, we proved that the number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of f_i depends on $e = \gcd(i, t)$. This immediately yields:

Corollary 2.4.4. *If* $\gcd(i,t) \neq \gcd(j,t)$ *then* f_i *and* f_j *are not equivalent where* f_i *and* f_j *are defined as in Equation* (2.4.1)*.*

2.4.2 The subclass associated to $\pi_2(y) = y(\mathrm{Tr}_\ell^t(y) + \alpha y)$

We next consider a class of permutation polynomials constructed by Blokhuis [2] and referred to by Laigle-Chapuy [154].

Theorem 2.4.5 ([2,154])**.** *Let* $t = k\ell$ *where* k *be an odd and* $\ell > 1$ *be any positive integer. Then the following polynomial is a bilinear permutation over* $\mathbb{F}_{2^t}$ *of the form*

$$\pi(x) = x(\mathrm{Tr}_\ell^t(x) + \alpha x)$$

where $\alpha \in \mathbb{F}_{2^\ell} \setminus \mathbb{F}_2$ *and* $\mathrm{Tr}_\ell^t(x) = \sum_{i=0}^{k-1} x^{2^{\ell i}}$*.*

Using this class of permutations we construct a class of cubic Maiorana–McFarland bent functions. Let $t = k\ell$ where k be an odd and $\ell > 1$ be any positive integer. A function $g : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_2$ defined by

$$g(x,y) = \mathrm{Tr}_1^t \left(xy\,\mathrm{Tr}_\ell^t(y) + \alpha xy^2\right), \text{ for all } (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}, \tag{2.4.6}$$

is a cubic Maiorana–McFarland bent. We prove that if $k > 1$ then the functions g belonging to this class do not have any affine derivative.

Theorem 2.4.6. *Let* $t = k\ell$ *where* k *be an odd and* $\ell > 1$ *be any positive integer. If* $k > 1$ *then the cubic Maiorana–McFarland bent function* g *defined as in Equation* (2.4.6) *has no affine derivative.*

Proof. Let (a,b) be an any element of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$.

$$\begin{aligned} D_{(a,b)}g(x,y) &= g(x,y) + g(x+a, y+b) \\ &= \mathrm{Tr}_1^t \left(xy\mathrm{Tr}_\ell^t(y) + (x+a)(y+b)\mathrm{Tr}_\ell^t(y+b) + \alpha xy^2 + \alpha(x+a)(y+b)^2\right) \\ &= \mathrm{Tr}_1^t \left(a\left(y\mathrm{Tr}_\ell^t(y) + \alpha y^2\right) + (x+a)\left(y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) + b\mathrm{Tr}_\ell^t(b) + \alpha b^2\right)\right). \end{aligned}$$

Let $a \neq 0$. Since $y\mathrm{Tr}_\ell^t(y) + \alpha y^2 = 0 \Leftrightarrow y = 0$ or $Tr_\ell^t(y) = \alpha y \Leftrightarrow y = 0$. Thus, if $a \neq 0$, $D_{(a,b)}g$ is a quadratic function. Let us consider $a = 0$, so

$$D_{(0,b)}g(x,y) = \mathrm{Tr}_1^t\left(x\left(y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y)\right) + x\left(b\mathrm{Tr}_\ell^t(b) + \alpha b^2\right)\right),$$

which is an affine function if and only if $p(y) = y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y)$ is constant, for all $y \in \mathbb{F}_{2^t}$. If that is so, since $p(0) = 0$, then $p(y) = y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) = 0$, for all y, in particular, for $y = 1$, we get $b + \mathrm{Tr}_\ell^t(b) = 0$, that is,

$$y\mathrm{Tr}_\ell^t(b) + b\mathrm{Tr}_\ell^t(y) = 0 \Longrightarrow y + \mathrm{Tr}_\ell^t(y) = 0 \Longrightarrow y \in \mathbb{F}_{2^\ell}.$$

Thus, $p(y)$ is not a constant function for all $y \in \mathbb{F}_{2^t}$. Therefore, g does not posses any affine derivative. ■

Remark 2.4.7. *If $k = 1$ then $t = \ell$ and for any $(a,b) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$,*

$$D_{(a,b)}g(x,y) = Tr_1^t((1+\alpha)(xb^2 + a(y+b)^2)),$$

which is an affine function. Therefore, if $k = 1$ then a function g of the form as in Equation (2.4.6) has affine derivatives. Thus, if $k = 1$, f_i and g are affine inequivalent where f_i and g are defined as in Equation (2.4.1) and (2.4.6), respectively.

Theorem 2.4.8. *Let $n = 2t$ and g be defined as in Equation (2.4.6). The number of distinct 2-dimensional subspaces corresponding to constant second derivatives of g is*

$$\frac{2^{-3\ell-1}\left(2^{2(2\ell+t)} + 2^{4\ell+t+1} - 2^{5\ell+t} - 5\cdot 2^{3\ell+2t} + 2^{5\ell+2t} - 2^{2(\ell+t)} + 2^{3\ell+1} + 2^{4t}\right)}{3}.$$

Proof. Let $V = \langle (a,b),(c,d)\rangle$ be any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$.

$$\begin{aligned} D_V g(x,y) &= g(x,y) + g(x+a,y+b) + g(x+c,y+d) + g(x+a+c,y+b+d) \\ &= \mathrm{Tr}_1^t\left((ad+bc)\mathrm{Tr}_\ell^t(y) + \left(a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b)\right)y + \left(ad\mathrm{Tr}_\ell^t(d) + cb\mathrm{Tr}_\ell^t(b)\right)\right. \\ &\quad \left. + \left(b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b)\right)x + (a+c)\left(b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b)\right) + \alpha(ad^2 + cb^2)\right). \end{aligned}$$

Case 1: Let $b = 0$ and $d = 0$. Then $D_V g(x,y) = 0$, for all $(x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$. Thus, with respect to any 2-dimensional subspace of $\mathbb{F}_{2^t} \times \{0\}$, the second-order derivative of g is 0. The number of such distinct 2-dimensional subspaces is $\frac{(2^t-1)(2^{t-1}-1)}{3}$.

Case 2: Let $b = 0$ and $d \neq 0$. Then

$$D_V g(x, y) = \mathrm{Tr}_1^t \left(ad\mathrm{Tr}_\ell^t(y) + a\mathrm{Tr}_\ell^t(d)y + ad\mathrm{Tr}_\ell^t(d) + \alpha ad^2 \right). \tag{2.4.7}$$

Since

$$\begin{aligned} \mathrm{Tr}_1^t \left(ad\mathrm{Tr}_\ell^t(y) \right) &= \mathrm{Tr}_1^t \left(ad \left(y + y^{2^\ell} + y^{2^{2\ell}} + \ldots + y^{2^{(k-1)\ell}} \right) \right) \\ &= \mathrm{Tr}_1^t \left(y \left(ad + (ad)^{2^{(k-1)\ell}} + (ad)^{2^{(k-2)\ell}} + \ldots + (ad)^{2^\ell} \right) \right) \\ &= \mathrm{Tr}_1^t \left(y\, \mathrm{Tr}_\ell^t(ad) \right). \end{aligned}$$

From (2.4.7), we have

$$D_V g(x, y) = \mathrm{Tr}_1^t \left((\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d))y + ad\mathrm{Tr}_\ell^t(d) + \alpha ad^2 \right),$$

which is constant if and only if

$$\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d) = 0. \tag{2.4.8}$$

Subcase (i): Let $a \in \mathbb{F}_{2^\ell}$. Then Equation (2.4.8) is satisfied for all $d \in \mathbb{F}_{2^t}$. Therefore, d can be chosen in $2^t - 1$ ways and a in $2^\ell - 1$ ways. Thus, the number of distinct 2-dimensional subspaces on which the second-derivatives of g are constants is equal to $(2^\ell - 1)2^{t-1}(2^t - 1)$.

Subcase (ii): Let $a \in \mathbb{F}_{2^t} \setminus \mathbb{F}_{2^\ell}$. Then $\mathrm{Tr}_\ell^t(ad) + a\mathrm{Tr}_\ell^t(d) = 0$ if and only if $\mathrm{Tr}_\ell^t(d) = 0$ and $\mathrm{Tr}_\ell^t(ad) = 0$. Since both are $(k-1)$-dimensional $\mathbb{F}_{2^\ell}$-subspaces of $\mathbb{F}_{2^t}$, d can be chosen in $2^{t-2\ell}$ ways and a in $2^t - 2^\ell$ ways. Thus, the number of such distinct 2-dimensional subspaces is $(2^t - 2^\ell)2^{t-1}(2^{t-2\ell} - 1)$.

Case 3: Let $b \neq 0$ and $d \neq 0$ with $b = d$. Then the subspace generated by $\{(a, b), (c, d)\}$ is equal to the subspace generated by $\{(a + c, b + d), (c, d)\} = \{(a + c, 0), (c, d)\}$, which is the same as in the previous case.

Case 4: Let $b \neq 0$ and $d \neq 0$ with $b \neq d$. Then $D_V g(x,y)$ is constant if and only if

$$b\mathrm{Tr}_\ell^t(d) + d\mathrm{Tr}_\ell^t(b) = 0, \text{ for all } x \in \mathbb{F}_{2^t} \tag{2.4.9}$$

and we get the implications

$$\begin{aligned} & \mathrm{Tr}_1^t((ad+bc)\mathrm{Tr}_\ell^t(y) + (a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b))y) = 0, \\ \Leftrightarrow\ & \mathrm{Tr}_1^t((\mathrm{Tr}_\ell^t(ad+bc) + (a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b)))y) = 0, \text{ for all } y \in \mathbb{F}_{2^t}, \\ \Leftrightarrow\ & \mathrm{Tr}_\ell^t(ad+bc) = a\mathrm{Tr}_\ell^t(d) + c\mathrm{Tr}_\ell^t(b). \end{aligned} \tag{2.4.10}$$

Subcase (*i*): Let $\mathrm{Tr}_\ell^t(b) = 0$ and $\mathrm{Tr}_\ell^t(d) = 0$. The dimension of $\ker(\mathrm{Tr}_\ell^t)$ is $t-\ell$ where $\ker(\mathrm{Tr}_\ell^t) = \{x \in \mathbb{F}_{2^t} : \mathrm{Tr}_\ell^t(x) = 0\}$. Thus, d can be chosen in $2^{t-\ell}-1$ ways and b in $2^{t-\ell}-2$ ways. From Equation (2.4.10), we get $\mathrm{Tr}_\ell^t(ad+bc) = 0$, so $\mathrm{Tr}_\ell^t(ad) = \mathrm{Tr}_\ell^t(cb) = \lambda \in \mathbb{F}_{2^\ell}$. For fixed b and d and for each $\lambda \in \mathbb{F}_{2^\ell}$, a and c both can be chosen in $2^{t-\ell}$ ways. Thus, the number of such distinct 2-dimensional subspaces is $\frac{2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3}$.

Subcase (*ii*): Let $\mathrm{Tr}_\ell^t(b) = 0$ but $\mathrm{Tr}_\ell^t(d) \neq 0$ or $\mathrm{Tr}_\ell^t(b) \neq 0$ but $\mathrm{Tr}_\ell^t(d) = 0$. Then from Equation (2.4.9), $b = 0$ or $d = 0$, respectively, which is impossible.

Subcase (*iii*): Let $\mathrm{Tr}_\ell^t(b) \neq 0$ and $\mathrm{Tr}_\ell^t(d) \neq 0$. From Equation (2.4.9), we get

$$d = \frac{\mathrm{Tr}_\ell^t(d)}{\mathrm{Tr}_\ell^t(b)} b, \text{ that is, } d = \beta b \text{ where } \beta = \frac{\mathrm{Tr}_\ell^t(d)}{\mathrm{Tr}_\ell^t(b)} \in \mathbb{F}_{2^\ell}^* \text{ and } \beta \neq 1.$$

For each $b \in \mathbb{F}_{2^t}^*$, d can be chosen in $2^\ell - 2$ ways. From Equation (2.4.10), we get

$$\mathrm{Tr}_\ell^t(b(a\beta + c)) = (a\beta + c)\mathrm{Tr}_\ell^t(b). \tag{2.4.11}$$

Equation (2.4.11) has a solution if and only if $a\beta + c \in \mathbb{F}_{2^\ell}$, so, $c = a\beta + \beta_1$ where $\beta_1 \in \mathbb{F}_{2^\ell}$. Then for any fixed a, c can be chosen in 2^ℓ ways. Therefore, the number of such distinct 2-dimensional distinct subspaces is $\frac{2^{t+\ell}(2^t-1)(2^{\ell-1}-1)}{3}$. Adding all the cases we get our count.

■

In what follows we demonstrate affine inequivalence among the cubic bent functions constructed above. To do this we use Theorem 2.2.2 proved in [111]. However, it is to be remembered that the use of the properties of higher-order derivatives to decide affine inequivalence between bent function was introduced by Dillon [56] way back in the seventies.

Remark 2.4.9. *Let $n = 2t$ be a fixed positive integer. In Theorem 2.4.8, we proved that the number of distinct 2-dimensional subspaces with respect to which the second-order derivatives of g are constants depends on ℓ. Thus, for any fixed n, for different choices of ℓ the number of distinct 2-dimensional subspaces to constant second-derivatives of the corresponding functions are different. Therefore, for any fixed n, for different choices of ℓ the corresponding cubic Maiorana–McFarland bent functions are affine inequivalent.*

Example 2.4.10. *Let $n = 30$. Then $t = 15$ and possible values of ℓ are 3, 5, and 15. If $\ell = 15$ then $k = 1$, and the bent function corresponding to $\ell = 15$ has an affine derivative. Also from Table 2.1, we get the cubic bent functions corresponding to $\ell = 3$, $\ell = 5$ and $\ell = 15$ are mutually affine inequivalent.*

Let $n = 2t$, and $n_1(e)$ and $n_2(\ell)$ be the number of distinct 2-dimensional subspaces of $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ on which the second-derivatives of f_i and g (defined as in Equation (2.4.1) and (2.4.6), respectively) are constants. Then

$$n_1(e) = \frac{(2^t-1)(2^{t+e-1}(2^e+1)-(2^t+1))}{3} \tag{2.4.12}$$

and

$$\begin{aligned} n_2(\ell) =& \frac{(2^t-1)(2^{t+\ell}(2^{\ell-1}-1)+2^{t-1}-1)+2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3} \\ &+ 2^{t-1}((2^\ell-1)(2^t-1)+(2^t-2^\ell)(2^{t-2\ell}-1)). \end{aligned} \tag{2.4.13}$$

Lemma 2.4.11. *If $\ell \geq e$ then $n_2(\ell) > n_1(e)$ where $n_1(e)$ and $n_2(\ell)$ are defined as in Equation (2.4.12) and (2.4.13), respectively.*

Proof. We first compute the difference

$$\begin{aligned} n_2(\ell) - n_1(e) =& (2^\ell-1)2^{t-1}(2^t-1)+(2^t-2^\ell)2^{t-1}(2^{t-2\ell}-1)-(2^t-1)2^{t-1}(2^e-1)+ \\ & \frac{2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3}+\frac{2^{t+\ell}(2^t-1)(2^{\ell-1}-1)}{3}-\frac{2^{t+e}(2^t-1)(2^{e-1}-1)}{3} \\ &= 2^{t-1}(2^t-1)(2^\ell-2^e)+\frac{2^t(2^t-1)(2^\ell(2^{\ell-1}-1)-2^e(2^{e-1}-1))}{3} \\ &+ (2^t-2^\ell)2^{t-1}(2^{t-2\ell}-1)+\frac{2^{2t-\ell}(2^{t-\ell}-1)(2^{t-\ell-1}-1)}{3}. \end{aligned}$$

Case 1: If $\ell = e$ then $t - 2\ell > 0$ and $n_2(\ell) - n_1(e) > 0$.

Case 2: Let $\ell > e$. Then

$$2^{t-1}(2^t - 1)(2^\ell - 2^e) > 0$$

and

$$\frac{2^t(2^t-1)(2^\ell(2^{\ell-1}-1) - 2^e(2^{e-1}-1))}{3} > 0.$$

If $k = 1$ then $2^t - 2^\ell = 0$ and $2^{t-\ell} - 1 = 0$ as $t = l$. Again if $k > 1$ then $2^{t-2\ell} - 1 > 0$ as $t - 2\ell > 0$, and so, $n_2(\ell) - n_1(e) > 0$. ■

Corollary 2.4.12. *If $\ell \geq e$ then f_i and g are affine inequivalent where f_i and g are defined as in Equation* (2.4.1) *and* (2.4.6)*, respectively.*

We compare $n_1(e)$ and $n_2(\ell)$ in Table 2.1, for different values of n.

	$n = 6$	$n = 10$	$n = 12$	$n = 18$		$n = 20$	$n = 30$		
	$e = 1; \ell = 3$	$e = 1; \ell = 5$	$e = 2; \ell = 2$	$e = 1; \ell = 9$	$e = 3; \ell = 3$	$e = 2; \ell = 2$	$e = 1; \ell = 3$	$e = 3; \ell = 5$	$e = 5; \ell = 15$
$n_1(e)$	35	651	12075	174251	3052203	3142315	879630115	12526594731	188614879915
$n_2(\ell)$	651	174251	53675	11453115051	25287339	2831415467	3775311936432811	6052134955691	192153583564270240

Table 2.1: The number of distinct 2-dimensional subspaces on which the second derivative of the cubic Maiorana–McFarland bent functions f_i and g are constants.

Chapter 3

An analysis of the $\mathcal{C}$ class of bent functions

3.1 Introduction

In this chapter, we consider the $\mathcal{C}$ class bent functions, and derive some existence and nonexistence results concerning them. The function $f'(x,y) = x \cdot \pi(y) + \phi_{L^\perp}(x)$ belongs to the class $\mathcal{C}$ provided the bent property (C) is satisfied, see Section 3.3. Certainly, as indicated in Remark 3.3.2, one could construct bent functions in the $\mathcal{C}$ class, but such an approach does not give us an *explicit* construction. The purpose of this chapter is to *fix* a permutation (from some known classes of permutations) and investigate these bent conditions in more detail, and to derive certain (non)existence results concerning the possibility of selecting appropriate subspaces so that the bent functions in the $\mathcal{C}$ class may be constructed. Most notably, for some classes of permutation polynomials there are no suitable linear subspaces of certain dimension for which the modification of $f \in \mathcal{M}$ would give a bent function $f^* \in \mathcal{C}$. On the other hand, some explicit conditions and the existence results could be derived for other classes of permutations. We also extend the original analysis of bent conditions of Carlet in terms of the Walsh–Hadamard spectra and show, for instance, that the modification (addition of the indicator of a linear subspace) of quadratic bent functions in $\mathcal{M}$ only result in bent functions within the completed class $\mathcal{M}$. The main contributions in this chapter can be summarized as follows:

- A classification of linear subspaces that may potentially give rise to bent functions in the $\mathcal{C}$ class is given.

- A theoretical analysis related to the conditions that a permutation π and a linear subspace $L = E \times \mathbb{F}_2^n \subset \mathbb{F}_2^{2n}$ satisfy the bent conditions is presented.

- It is shown that for several classes of permutations π there does not exist 2-dimensional subspace L satisfying the bent conditions. For instance, Theorem 3.3.3 refers to Hou's permutations [152, Theorem B] and Corollary 3.5.10 to certain k-linear split permutations.

- The existence of 2-dimensional linear subspaces satisfying the bent conditions have been confirmed for certain classes of bilinear split permutations, see Theorem 3.5.5, Theorem 3.5.6 and Theorem 3.5.7. Thus, some infinite classes of bent functions in $\mathcal{C}$ have been specified.

3.2 Preliminaries

Two new classes of bent functions were derived by Carlet in [17] which are defined as in Equations (1.2.12) and (1.2.13), respectively. Assuming that f is bent (not necessarily of the form $x \cdot \pi(y)$), two equivalent (and more general) conditions for the function $f^*(x) = f(x) + \phi_L(x)$ to be bent were given in [17, Theorem].

Theorem 3.2.1 ([17, Theorem]). *Let $m = 2n$ and $L = b + L'$ be any flat in $\mathbb{F}_2^m$. Suppose $f \in \mathcal{B}_m$ is a bent function. Then the function $f^*(x) = f(x) + \phi_L(x)$ is bent if and only if one of the following equivalent conditions is satisfied:*

1. *for any $a \in \mathbb{F}_2^m \setminus L'$, $f(x) + f(x+a)$ is balanced on L, that is,*

$$\sum_{x \in L} (-1)^{f(x)+f(x+a)} = 0, \text{ for all } a \in \mathbb{F}_2^m \setminus L'.$$

2. *for any $\lambda \in \mathbb{F}_2^m$, the restriction of the function $\tilde{f}(x) + b \cdot x$ to the flat $\lambda + L'^{\perp}$ is either constant or balanced.*

Also, it was shown in [17, Theorem] that the dimension of L is necessarily larger or equal to n if one of these conditions is satisfied. The following result due to Payne [121] restated by

Berger, Canteaut, Charpin and Laigle-Chapuy [125] provides a complete characterization of such linearized polynomials.

Theorem 3.2.2 ([125, Theorem 6]). *A polynomial in $\mathbb{F}_{2^n}[X]$ of the form*

$$Q(X) = \sum_{i=1}^{n-1} c_i X^{2^i-1}, c_i \in \mathbb{F}_{2^n}$$

cannot be a permutation polynomial unless $Q(X) = c_k X^{2^k-1}$ with $\gcd(k, n) = 1$ and $c_k \in \mathbb{F}_{2^n}^*$.

Let $Supp(\ell) = \{i : a_i \neq 0\}$ where $\ell \in \mathcal{L}(n)$. Then $P(X) = \frac{\ell(X)}{X}$ is not a permutation if any one of the following conditions are satisfied.

1. The cardinality of $Supp(\ell)$, that is, $|Supp(\ell)| \geq 3$.

2. The coefficient $a_0 = 0$ and $|Supp(\ell)| = 2$.

3. The coefficient $a_0 \neq 0$ and $Supp(\ell) = \{0, k\}$ where $\gcd(k, n) \neq 1$.

Lemma 3.2.3 ([16, Corollary 1]). *Let d, n, s be positive integers satisfying $\gcd(n, s) = 1$ and let*

$$0 \neq g(X) = \sum_{i=0}^{d} r_i X^{2^{si}} \in \mathbb{F}_{2^n}[X].$$

Then the equation $g(X) = 0$ has at most 2^d solutions in $\mathbb{F}_{2^n}$.

3.3 Towards an explicit specification of Carlet's $\mathcal{C}$-class

The $\mathcal{C}$ class of bent function is defined as in Equation (1.2.13). Let L be any linear subspace of $\mathbb{F}_2^n$ and π be any permutation on $\mathbb{F}_2^n$. For construction of bent functions in $\mathcal{C}$ class, it is needed to consider a permutation polynomial π on $\mathbb{F}_2^n$ such that:

$$(C) \quad \phi(a + L) \text{ is a flat (affine subspace), for all } a \in \mathbb{F}_2^n \text{ where } \phi := \pi^{-1}.$$

We will often say that (ϕ, L) *has property* (C).

Certainly, if L has dimension 1 then $\pi^{-1}(a + L) = \phi(a + L)$ is always a one-dimensional flat: if $L = \{0, u\}$ is a one-dimensional subspace then $\phi(a + L) = \{\phi(a), \phi(a + u)\} =$

$\phi(a)+\{0,\phi(a)+\phi(a+u)\}$ where $\phi(a)+\phi(a+u)\neq 0$. So, we will assume from now on that L has dimension ≥ 2. We will identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, and we denote $\phi := \pi^{-1}$. We have the following characterization of a subspace L of dimension ≤ 2.

Lemma 3.3.1. *Suppose $u, v, w, z \in \mathbb{F}_{2^n}$. A set $L = \{u, v, w, z\}$ is a flat of $\mathbb{F}_{2^n}$ of dimension ≤ 2 if and only if $u + v + w + z = 0$.*

Proof. If L is a subspace then without loss of generality, we can assume that $L = \{0, u, v, u+v\}$, which satisfies $0+u+v+u+v = 0$. Reciprocally, we assume that the set $L = \{u, v, w, z\}$ satisfies $u+v+w+z = 0$, and so, $z = u+v+w$. It follows that $u+L = \{0, u+v, u+w, u+(u+v+w) = v+w\}$, which is easily seen to be a subspace of dimension 0, if $u = v = w(= z)$, of dimension 1, if $u \neq v = w$, and of dimension 2, if v and w are independent. ■

Remark 3.3.2. *For a particular value of n, one could take two subspaces L, M in $\mathbb{F}_2^n$ of the same dimension and partition $\mathbb{F}_2^n$ into $\cup_{a\in A}(a+L)$ and $\cup_{b\in B}(b+M)$, with A, B subsets of $\mathbb{F}_2^n$ of the same cardinality $|A| = |B|$, and then take any permutation ϕ that maps the elements of $\{a + L \,|\, a \in A\}$ onto the elements of $\{b + M \,|\, b \in B\}$. The pair (ϕ, L) would satisfy property (C).*

Although the above process works for specific values of n it does not amount to an explicit construction of infinite sets of bent functions within the class $\mathcal{C}$. It is not clear what the explicit representation of these bent functions will be and how they relate to the other known bent functions, like Maiorana–McFarland. For this reason, even after more than two decades we have very little grasp on bent functions in $\mathcal{C}$. We obtain explicit construction of several subclasses of bent functions in $\mathcal{C}$ for the first time. We are also able to identify permutations corresponding to which there are no $\mathcal{C}$ class bent functions.

We start with one specific class of permutations $\{\phi\}$ proposed by Hou [152, Theorem B] and the nonexistence of any 2-dimensional linear subspace L for which the function $x \cdot \pi(y) + \phi_{L^\perp}(x)$ is a bent function in $\mathcal{C}$.

Theorem 3.3.3. *Let $n \geq 1$ and $\phi(x) = ax+bx^{2^n}+x^{2^{n+1}-1}$ be a permutation polynomial over $\mathbb{F}_{2^{2n}}$ (see Hou* [152, Theorem B] *for explicit criteria). Then there exists no 2-dimensional linear subspace, L, of $\mathbb{F}_{2^{2n}}$ such that (ϕ, L) has property (C).*

Proof. Suppose $L = \langle u, v\rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^{2n}}$. Then for any $c \in \mathbb{F}_{2^{2n}}$,

$\phi(c+L)$ is a flat if and only if

$$\begin{aligned}
0 &= \phi(c)+\phi(c+u)+\phi(c+v)+\phi(c+u+v)\\
&= ac+bc^{2^n}+c^{2^{n+1}-1}+a(c+u)+b(c+u)^{2^n}+(c+u)^{2^{n+1}-1}\\
&+a(c+v)+b(c+v)^{2^n}+(c+v)^{2^{n+1}-1}\\
&+a(c+u+v)+b(c+u+v)^{2^n}+(c+u+v)^{2^{n+1}-1}\\
&= c^{2^{n+1}-1}+(c+u)^{2^{n+1}-1}+(c+v)^{2^{n+1}-1}+(c+u+v)^{2^{n+1}-1},
\end{aligned}$$

for all $c \in \mathbb{F}_{2^{2n}}$. Therefore, multiplying the above identity by $c+u+v$ and using the binomial theorem (in characteristic 2) we obtain

$$\begin{aligned}
&(u+v)c^{2^{n+1}-1}+v(c+u)^{2^{n+1}-1}+u(c+v)^{2^{n+1}-1}\\
&=\sum_{j=0}^{2^{n+1}-2}\left(v\,u^{2^{n+1}-1-j}+u\,v^{2^{n+1}-1-j}\right)c^j=0,
\end{aligned}$$

for all $c \in \mathbb{F}_{2^{2n}}$, implying that the polynomial

$$\sum_{j=0}^{2^{n+1}-2}\left(v\,u^{2^{n+1}-1-j}+u\,v^{2^{n+1}-1-j}\right)X^j \in \mathbb{F}_{2^{2n}}[X]$$

has all of its coefficients 0, that is, $v\,u^{2^{n+1}-1-j}+u\,v^{2^{n+1}-1-j}=0$, for all $0\le j\le 2^{n+1}-2$. In particular, for $j=2^{n+1}-3$,

$$u^2v+uv^2=0 \Leftrightarrow u^2v=uv^2 \Leftrightarrow u=v.$$

Thus, there is no 2-dimensional subspace, L, which satisfies the required property. ■

3.4 Some general bent conditions related to $\mathcal{C}$ and $\mathcal{D}$ classes

In this section we investigate the choice of linear subspaces L which may potentially give rise to bent functions in $\mathcal{C}$ for some specific permutations π and later we extend the derived conditions for arbitrary π. The analysis uses more general bent conditions (without requesting that the initial function is in $\mathcal{M}$) given in [17, Theorem].

The class $\mathcal{D}$ was derived using the result that for an n-dimensional subspace L of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ satisfying $f(x,y) = x \cdot \pi(y) = 0$ for any $(x,y) \in L$, the function $x \cdot \pi(y) + \phi_L(x,y)$ is bent (cf. [17, Corollary 1]).

The subclass named $\mathcal{D}_0$ (which is not contained in $\mathcal{M}$ or in $\mathcal{PS}$), deduced by Carlet, corresponds to a special choice of $L = \{0\} \times \mathbb{F}_2^n$. Nevertheless, the fact that $f^*(x,y) = x \cdot \pi(y) + \phi_L(x,y)$ is bent for $L = \{0\} \times \mathbb{F}_2^n$ can also be easily deduced using the condition related to the derivatives of f restricted to L. Indeed, for any $a = (\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus L$ and for $f(x,y) = x \cdot \pi(y)$ we have

$$\sum_{(x,y)\in L} (-1)^{f(x,y)+f(x+\alpha,y+\beta)} = \sum_{x=0,y\in\mathbb{F}_2^n} (-1)^{f(0,y)+f(0+\alpha,y+\beta)} = \sum_{y\in\mathbb{F}_2^n} (-1)^{\alpha\cdot\pi(y+\beta))} = 0$$

where we have used the fact that $\alpha \neq 0$ and thus $\sum_{y\in\mathbb{F}_2^n}(-1)^{\alpha\cdot\pi(y+\beta))} = 0$ since π is a permutation of $\mathbb{F}_2^n$, see [103, Theorem 7.7].

On the other hand, by taking $L = \mathbb{F}_2^n \times \{0\}$, it is obvious that the function

$$\begin{aligned} f^*(x,y) &= x \cdot \pi(y) + \phi_L(x,y) \\ &= x \cdot \pi(y) + \prod_{i=1}^{n}(y_i + 1) = x \cdot \pi(y) + g(y) \end{aligned}$$

is bent, but no new bent functions can be obtained through this selection of L, since $f^* \in \mathcal{M}$. More generally, for the same reason the function $f^*(x,y) = x \cdot \pi(y) + \phi_L(x,y)$ is also in $\mathcal{M}$, for $L = \mathbb{F}_2^n \times E$ where E is k-dimensional linear subspace of $\mathbb{F}_2^n$, $0 \leq k \leq n$. Indeed, since for $L = \mathbb{F}_2^n \times E$ the indicator function $\phi_L(x,y) = g(y)$, for some $g \in \mathcal{B}_n$, again $f^* \in \mathcal{M}$. We formalize the above discussion in the following result.

Proposition 3.4.1. *Let $m = 2n$ and $f \in \mathcal{B}_m$ be a bent function given by $f(x,y) = x \cdot \pi(y)$ where π is a permutation over $\mathbb{F}_2^n$, and $L = \mathbb{F}_2^n \times E$ where $\dim(E) = k$, for $k = 0, \ldots, n$. Then $f^*(x,y) = f(x,y) + \phi_L(x,y)$ is a bent function in class $\mathcal{M}$.*

Thus, the case $L = \mathbb{F}_2^n \times E$ is of no interest to us and it is not treated further.

3.4.1 The analysis for arbitrary π and $L = E \times \mathbb{F}_2^n$

Let us extend our investigation for $f^*(x,y) = x \cdot \pi(y) + \phi_L(x,y)$ to the case when π is any permutation on $\mathbb{F}_2^n$, and $L = E \times \mathbb{F}_2^n$. Notice that this particular choice of L implies that $\phi_L(x,y) = \phi_L(x)$ and therefore we are considering the class $\mathcal{C}$. Assuming $f(x,y) = x \cdot \pi(y)$, we have

$$\begin{aligned} 0 &= \sum_{(x,y)\in L} (-1)^{f(x,y)+f(x+b,y+c)} \\ &= \sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(x+b)\cdot\pi(y+c)} \\ &= \sum_{x\in E}\sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y+c)+x\cdot(\pi(y)+\pi(y+c))} \\ &= \sum_{y\in\mathbb{F}_2^n}\sum_{x\in E} (-1)^{x\cdot(\pi(y)+\pi(y+c))+b\cdot\pi(y+c)}. \end{aligned} \tag{3.4.1}$$

Notice that $(b,c) \neq (0,0)$ and in particular $b \neq 0$, whereas c can be equal to zero. We consider two cases, namely $c = 0$ and $c \neq 0$. If $c = 0$ then the above sum becomes

$$\sum_{x\in E}\sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y)}, \tag{3.4.2}$$

which is zero as $b \neq 0$, again using [103, Theorem 7.7].

If $c \neq 0$ then rewriting Equation (3.4.1) as

$$\sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y+c)} \sum_{x\in E} (-1)^{x\cdot(\pi(y)+\pi(y+c))}, \tag{3.4.3}$$

one easily deduces the following result.

Lemma 3.4.2. *Let $f \in \mathcal{B}_m$ be a bent function given by $f(x,y) = x \cdot \pi(y)$ where π is a permutation over $\mathbb{F}_2^n$, and $L = E \times \mathbb{F}_2^n$ where $\dim(E) = k$, for $k = 1, \ldots, n$. Then a sufficient condition that $f^*(x,y) = f(x,y) + \phi_L(x,y)$ is a bent function in class $\mathcal{C}$ is that,*

$$\sum_{y\in\mathbb{F}_2^n : \pi(y)+\pi(y+c)\in E^\perp} (-1)^{b\cdot\pi(y+c)} = 0,$$

for any $(b,c) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus L$.

Proof. The double sum in Equation (3.4.1) must be equal to zero for any $(b, c) \notin L$. The case $c = 0$ yields (3.4.2) which equals to zero. The case $c \neq 0$ gives (3.4.3) which must be equal to 0 for any $(b, c) \notin L$. We notice that if $\pi(y) + \pi(y + c) \in E^{\perp}$ then $x \cdot (\pi(y) + \pi(y + c)) = 0$ for any $x \in E$, thus the inner sum in (3.4.3) equals to $|E| = 2^k$ for any such $y \in \mathbb{F}_2^n$. Thus, a sufficient condition that Equation (3.4.3) equals to zero is as stated. ■

Remark 3.4.3. *The above condition ensures that even though* $\sum_{x \in E}(-1)^{x\cdot(\pi(y)+\pi(y+c))} \neq 0$ *for some fixed* $y \in \mathbb{F}_2^n$ *(which happens exactly when* $\pi(y) + \pi(y + c) \in E^{\perp}$*) the double sum* (3.4.3) *still equals to zero. The cases dim*$(E) \in \{n-1, n\}$ *are trivial and correspond to the indicator function which is constant (dim*$(E) = n$*) or affine function (dim*$(E) = n-1$*).*

Remark 3.4.4. *Though taking* $f(x, y) = x \cdot \pi(y)$ *is just a special case of considering* f *to be a bent function in* $\mathcal{M}$*, most notably the condition on balancedness of the derivatives on* E *is now related to the balancedness of the derivatives of* π *on* $E^{\perp}$*, as mentioned above.*

Even though the condition of Lemma 3.4.2 appears to be hard one can find permutations π and a suitable subspace E that satisfy the above condition. Nevertheless, to provide a generic method of finding such permutations appears to be difficult.

Example 3.4.5. *Let* $n = 3$ *and* $E = \{000, 010\}$ *thus dim*$(E) = 1$*. Then* $E^{\perp} = \{000, 001, 101, 100\}$*. Let us define a nonlinear permutation* $\pi : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ *and compute the differentials for* $c = (001)$*:*

$y_3y_2y_1$	$\pi(y)$	$\pi(y + 001)$	$\pi(y) + \pi(y + 001)$
000	000	001	001
001	001	000	001
010	011	010	001
011	010	011	001
100	111	110	001
101	110	111	001
110	101	100	001
111	100	101	001

This c *is obviously a linear structure of* π *(thus* $\pi(y) + \pi(y + 001) = 001$*, for all* $y \in \mathbb{F}_2^3$*)*

and since $(001) \in E^{\perp}$ *we have:*

$$\sum_{y\in\mathbb{F}_2^n:\pi(y)+\pi(y+001)\in E^{\perp}} (-1)^{b\cdot\pi(y+001)} = \sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot\pi(y+001)} = 0$$

where the last equality is due to the fact that π *is a permutation and* $b \neq 0$*. For other (nonzero) values of* $c \in \mathbb{F}_2^3$ *it turns out that either* $Im(\pi(y)+\pi(y+c)) \subseteq E^{\perp}$ *or* $Im(\pi(y)+\pi(y+c)) \cap E^{\perp} = \emptyset$*. For instance, one may check that* $Im(\pi(y)+\pi(y+011)) = \{010, 011\}$ *and the intersection with* $E^{\perp}$ *is the empty set.*

In both cases $\sum_{y\in\mathbb{F}_2^n:\pi(y)+\pi(y+c)\in E^{\perp}}(-1)^{b\cdot\pi(y+c)} = 0$*, thus* $f(x,y) = x\cdot\pi(y) + \phi_L(x,y)$ *where* $L = E \times \mathbb{F}_2^3$*, is a bent function on* $\mathbb{F}_2^6$*. For instance, one may check that* $Im(\pi(y)+\pi(y+011)) = \{010, 011\}$*.*

Given the fact that the class $\mathcal{C}$ is constructed by adding the indicator function of a special subspace to a bent function, it may be of interest to investigate the relation between the spectral values of $f(x,y) = x\cdot\pi(y)$ and $f^*(x,y) = f(x,y) + \phi_L(x,y)$. Then requiring that $f^*(x,y)$ is bent implies the following identity

$$\begin{aligned}
W_{f^*}(u,v) &= \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+\phi_L(x,y)+(u,v)\cdot(x,y)} \\
&= W_f(u,v) - 2\sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} \\
&= \pm 2^n - 2\sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)},
\end{aligned}$$

and if f^* is to be bent then we must have

$$W_{f_{|L}}(u,v) = \sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} \in \{0, \pm 2^n\},$$

for any $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. If $L = E \times \mathbb{F}_2^n$, we have

$$W_{f_{|L}}(u,v) = \sum_{x\in E} (-1)^{u\cdot x} \sum_{y\in\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+v\cdot y}$$

and $W_{f_{|L}}(u,0) = 2^n$, for any $u \in \mathbb{F}_2^n$. This is because for any fixed $x \neq 0$ and $v = 0$, the inner sum $\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot\pi(y)} = 0$, unless $x = 0$ and the sum equals then to 2^n.

The next result is now immediate.

Proposition 3.4.6. *Let $f \in \mathcal{B}_m$ be a bent function given by $f(x, y) = x \cdot \pi(y)$ where π is a permutation over $\mathbb{F}_2^n$. Let $L = E \times \mathbb{F}_2^n$. If $f^*(x, y) = f(x, y) + \phi_L(x, y)$ is a bent function then $W_f(u, 0) = 2^n$, for any $u \in \mathbb{F}_2^n$.*

Proof. Assuming $L = E \times \mathbb{F}_2^n$, we only need to prove that $W_f(u, 0) = 2^n$, for any $u \in \mathbb{F}_2^n$, is always satisfied. Indeed,

$$\begin{aligned} W_f(u, 0) &= \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)+(u,v)\cdot(x,y)} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x} \sum_{y\in\mathbb{F}_2^n} (-1)^{x\cdot\pi(y)} = 2^n, \end{aligned}$$

which must be true for all $u \in \mathbb{F}_2^n$. Notice that the inner sum $\sum_{y\in\mathbb{F}_2^n}(-1)^{x\cdot\pi(y)} = 0$ for any fixed x, unless $x = 0$ (since π is a permutation), and therefore $W_f(u, 0) = 2^n$, for all $u \in \mathbb{F}_2^n$. ■

3.4.2 The subcase when π is a linear permutation and $L = E \times \mathbb{F}_2^n$

In this section we consider $f^*(x, y) = x \cdot \pi(y) + \phi_L(x, y)$ where $\pi(y) = yA$ is a linear permutation over $\mathbb{F}_2^n$, $L = E \times \mathbb{F}_2^n$ for some k-dimensional linear subspace E, $0 \le k \le n$, and A is an invertible matrix over $\mathbb{F}_2$ of size $n \times n$ (that is $A \in GL(n, \mathbb{F}_2)$). It will be shown that f^* is always bent regardless the choice of E, but nevertheless f^* is in the completed class $\mathcal{M}^*$.

Theorem 3.4.7. *Let $f^*(x, y) = x \cdot \pi(y) + \phi_L(x, y)$ be a function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and $\pi(y) = yA$, $A \in GL(n, \mathbb{F}_2)$, a linear permutation over $\mathbb{F}_2^n$ so that $f(x, y) = x \cdot \pi(y)$ is bent. Furthermore, let L be of the form $L = E \times \mathbb{F}_2^n$ where E is a k-dimensional linear subspace of $\mathbb{F}_2^n$, for $0 \le k \le n$. Then f^* is a bent function.*

Proof. Since f^* is bent if and only if $f(x, y) + f(x + b, y + c)$ is balanced on $L = E \times \mathbb{F}_2^n$ for any $(b, c) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus L$ we have,

$$\begin{aligned} \sum_{(x,y)\in L} (-1)^{f(x,y)+f(x+b,y+c)} &= \sum_{(x,y)\in L} (-1)^{x\cdot\pi(y)+(x+b)\cdot\pi(y+c)} \\ &= \sum_{x\in E; y\in\mathbb{F}_2^n} (-1)^{x\cdot yA+(x+b)\cdot(yA+cA)} \end{aligned}$$

$$= \sum_{x\in E}(-1)^{(x+b)\cdot cA}\sum_{y\in\mathbb{F}_2^n}(-1)^{b\cdot yA}$$

which must be equal to zero if f^* is bent. Now, since $\pi(y) = yA$ is a permutation over $\mathbb{F}_2^n$ then $\sum_{y\in\mathbb{F}_2^n}(-1)^{bA\cdot y} = 0$, for any $b \neq 0$. Noticing that $b \neq 0$ since $(b, c) \notin L$, we have $\sum_{(x,y)\in L}(-1)^{f(x,y)+f(x+b,y+c)} = 0$, thus f^* is bent. ■

However, it turns out that the functions given by $f^*(x, y) = x \cdot y + \phi_L(x, y)$ (π being a linear permutation) are embedded in $\mathcal{M}$.

Theorem 3.4.8. *Let $f^*(x, y) = x\cdot\pi(y)+\phi_L(x, y)$ be a function on $\mathbb{F}_2^n\times\mathbb{F}_2^n$, and $\pi(y) = yA$ be a linear permutation over $\mathbb{F}_2^n$. Furthermore, let $L = E \times \mathbb{F}_2^n$ where E is a k-dimensional linear subspace of $\mathbb{F}_2^n$, $0 \leq k \leq n$. Then f^* belongs to $\mathcal{M}^*$.*

Proof. It is well-known [56] that $f \in \mathcal{M}^*$ on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ if and only if there exists an n-dimensional subspace, say $U \subset \mathbb{F}_2^{2n}$, such that the second derivatives $D_\alpha D_\beta f(x, y) = 0$, for any $\alpha, \beta \in U$.

Notice that since $L = E \times \mathbb{F}_2^n$, the support of ϕ_L does not depend on the y variables, and so, $\phi_L(x, y) = \phi_L(x)$. Now, for $\alpha = (a, b)$ and $\beta = (c, d)$ where $(a, b), (c, d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ we have,

$$D_\alpha D_\beta(x \cdot yA) = D_\beta(x \cdot bA + a \cdot yA + a \cdot bA),$$

and taking the derivative with respect to $\beta = (c, d)$ gives $D_\alpha D_\beta(x\cdot yA) = c\cdot bA+a\cdot dA$. So it is sufficient to show the existence of U such that both $D_\alpha D_\beta\phi_L(x) = 0$ and $D_\alpha D_\beta(x \cdot yA) = 0$, for any $\alpha, \beta \in U$. Taking $U = \{0\} \times \mathbb{F}_2^n$ so that $a = c = 0$, we clearly have $D_\alpha D_\beta\phi_L(x) = 0$ and $D_\alpha D_\beta(x \cdot y) = b \cdot c + aA \cdot d = 0$, for any $\alpha, \beta \in U$. ■

3.5 k-linear split permutations

In contrast to Theorem 3.3.3 which, for a particular class of permutations introduced by Hou [152] shows the nonexistence of a 2-dimensional linear subspace L, in this section we look for permutations π, and provide both necessary and sufficient conditions on the subspace L, such that (π, L) satisfies the property (C).

It is known that any permutation on a finite field can be written as a polynomial. We consider those permutation polynomials which can be factored (split) into linearized polynomials.

Definition 3.5.1. *A linearized polynomial $\ell \in \mathbb{F}_{2^n}[X]$ is a polynomial of the form*

$$\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i} \text{ with } a_i \in \mathbb{F}_{2^n}.$$

The set of all such polynomials is denoted by $\mathcal{L}(n)$.

The action of a pair of bijective linearized polynomials $(\ell_1, \ell_2) \in \mathcal{L}(n) \times \mathcal{L}(n)$ on $\mathbb{F}_{2^n}[X]$ is defined as $\ell_1 \circ \phi \circ \ell_2$ where $\phi \in \mathbb{F}_{2^n}[X]$. Two polynomials $\phi, \psi \in \mathbb{F}_{2^n}[X]$ are said to be *linearly equivalent* if there exist (bijective) $\ell_1, \ell_2 \in \mathcal{L}(n)$ such that $\ell_1 \circ \phi \circ \ell_2 = \psi$.

Lemma 3.5.2. *Suppose π and ϕ are two linearly equivalent permutations on $\mathbb{F}_{2^n}$ such that $\phi = \ell_1 \circ \pi \circ \ell_2$ where $\ell_1, \ell_2 \in \mathcal{L}(n)$, and L is a linear subspace of $\mathbb{F}_{2^n}$. If $\pi(a + L)$ is a flat for all $a \in \mathbb{F}_{2^n}$, $\phi(a + \ell_2^{-1}(L))$ is a flat for all $a \in \mathbb{F}_{2^n}$.*

Proof. For any $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\phi(a + \ell_2^{-1}(L)) &= \ell_1 \circ \pi \circ \ell_2(a + \ell_2^{-1}(L)) = \ell_1 \circ \pi(\ell_2(a + \ell_2^{-1}(L))) \\ &= \ell_1 \circ \pi(\ell_2(a) + L) = \ell_1(\pi(\ell_2(a) + L)).\end{aligned}$$

Since $\pi(\ell_2(a) + L)$ is a flat and ℓ_1 is a linear permutation, $\ell_1(\pi(\ell_2(a) + L))$ is a flat. ■

Thus it is enough to consider $\mathcal{C}$ type constructions associated to linearly inequivalent permutations. In the spirit of Blokhuis, Coulter, Henderson and O'Keefe [2] and Laigle-Chapuy [154], we extend their construction in the next definition.

We call a polynomial $\phi \in \mathbb{F}_{2^n}[X]$ a *k-linear split* polynomial if it is of the form

$$\phi(X) = \pi_1(X)\pi_2(X)\cdots\pi_k(X) \text{ with } \pi_i \in \mathcal{L}(n), 1 \le i \le k.$$

Blokhuis et al. [2] and Laigle-Chapuy [154] refer to the case $k = 2$ as a bilinear polynomial (some authors prefer Dembowski-Ostrom polynomial), but the “bilinear” notion has a different meaning in too many areas, so we prefer to insert “split” into the definition.

Certainly, if the function associated to the polynomial ϕ is bijective, we will refer to ϕ as a k-linear split permutation.

It is easy to see that using the transformation $Y = \pi_1(X)$, the polynomial ϕ is linearly equivalent to one of the type

$$\phi(Y) = Y\ell_1(Y) \cdots \ell_{k-1}(Y) \text{ where } \ell_i = \pi_i \circ \pi_1^{-1} \in \mathcal{L}(n), \tag{3.5.1}$$

so, we will only consider these forms from here on.

3.5.1 $\mathcal{C}$ type bent functions associated to bilinear split permutations

From our observation (3.5.1) (see also [2, Section 2]), it will be sufficient to investigate the $\mathcal{C}$ type bent functions (in this case) associated to bilinear split permutations of the shape

$$X\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i+1} \text{ with } a_i \in \mathbb{F}_{2^n}.$$

The set of all such polynomials is denoted by $\mathcal{B}(n)$.

Theorem 3.5.3. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation defined by $\phi(x) = x\ell(x) + \ell_0(x)$, for all $x \in \mathbb{F}_{2^n}$ where $\ell, \ell_0 \in \mathcal{L}(n)$. Let $L = \langle u, v \rangle$ be a 2-dimensional subspace. Then (ϕ, L) satisfies the (C) property if and only if $\frac{\ell(u)}{u} = \frac{\ell(v)}{v}$.*

Proof. For L to satisfy the required condition for all $a \in \mathbb{F}_{2^n}$, we must have

$$\begin{aligned}
&\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v) \\
&= a\ell(a) + \ell_0(a) + (a+u)\ell(a+u) + \ell_0(a+u) + (a+v)\ell(a+v) + \ell_0(a+v) \\
&\quad + (a+u+v)\ell(a+u+v) + \ell_0(a+u+v) \\
&= a\ell(a) + a\ell(a) + a\ell(u) + u\ell(a) + u\ell(u) + a\ell(a) + a\ell(v) + v\ell(a) + v\ell(v) \\
&\quad + a\ell(a) + a\ell(u) + a\ell(v) + u\ell(a) + u\ell(u) + u\ell(v) + v\ell(a) + v\ell(u) + v\ell(v) \\
&= u\ell(v) + v\ell(u) = 0.
\end{aligned}$$

Therefore, the necessary and sufficient condition that a 2-dimensional linear subspace $L = \langle u, v \rangle$ has the required property is that $\frac{\ell(u)}{u} = \frac{\ell(v)}{v}$. ■

Corollary 3.5.4. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, defined by $\phi(x) = x\ell(x) + \ell_0(x)$, for all $x \in \mathbb{F}_{2^n}$ where $\ell(X) = \sum_{i=0}^{n-1} a_i X^{2^i} \in \mathcal{L}(n)$. Then there exists a $\mathcal{C}$ type function associated to ϕ if and only if the function $x \mapsto \frac{\ell(x)}{x}$ on $\mathbb{F}_{2^n}^*$ is not a permutation.*

Proof. If there exists a $\mathcal{C}$ type bent function then there exists a subspace L of dimension 2 generated by two vectors u, v such that (ϕ, L) satisfies (C). By Theorem 3.5.3, the map $\lambda : \mathbb{F}_{2^n}^* \to \mathbb{F}_{2^n}^*$ defined by $\lambda(x) = \frac{\ell(x)}{x}$ is not one-to-one, and consequently not a permutation. Conversely, if λ is not a permutation then it is not one-to-one, and consequently, there exist two vectors $u, v \in \mathbb{F}_{2^n}^*$ with $\lambda(u) = \lambda(v)$. Taking $L = \langle u, v \rangle$, again by Theorem 3.5.3, we see that (ϕ, L) satisfies (C). ■

In addition to Remark 3.3.2, it is possible to obtain explicitly $\mathcal{C}$ type bent functions, for a special class of explicit permutations. Thus, for effective construction of the functions in $\mathcal{C}$, there is a need to characterize linear subspaces such as L with respect to permutations over $\mathbb{F}_{2^n}$.

In Theorem 3.5.5 we consider the permutation $\phi(x) = x^{2^{t+1}+1} + x^3 + x$, for all $x \in \mathbb{F}_{2^n}$ where $n = 2t + 1$ (see [48]).

Theorem 3.5.5. *Suppose $\phi(x) = x^{2^{t+1}+1} + x^3 + x$, for all $x \in \mathbb{F}_{2^n}$ where $n = 2t + 1$,* $\gcd(t, n) = 1$. *Then there exists at least one and at most $2(2^n - 2)$ two dimensional linear subspaces L such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{2^n}$.*

Proof. Since, $\frac{\phi(x)-x}{x}$ is not a permutation, by Corollary 3.5.4 there exists at least one function in $\mathcal{C}$ associated to ϕ.

Let $L = \langle u, v \rangle$ be a 2-dimensional subspace of $\mathbb{F}_{2^n}$. The set $\phi(a+L)$ is a flat if and only if

$$\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v) = u^{2^{t+1}}v + uv^{2^{t+1}} + u^2v + uv^2 = 0.$$

Exponentiating both sides of the above equation by 2^{2t}, we obtain

$$\begin{aligned}
&(u^{2^{t+1}}v + uv^{2^{t+1}} + u^2v + uv^2)^{2^{2t}} = 0\\
\text{i.e.,}\quad & u^{2^{3t+1}}v^{2^{2t}} + u^{2^{2t}}v^{2^{3t+1}} + u^{2^{2t+1}}v^{2^{2t}} + u^{2^{2t}}v^{2^{2t}+1} = 0\\
\text{i.e.,}\quad & (u^{2^{2t+1}})^{2^t}v^{2^{2t}} + u^{2^{2t}}(v^{2^{2t+1}})^{2^t} + u^{2^{2t+1}}v^{2^{2t}} + u^{2^{2t}}v^{2^{2t}+1} = 0\\
\text{i.e.,}\quad & u^{2^t}v^{2^{2t}} + u^{2^{2t}}v^{2^t} + uv^{2^{2t}} + u^{2^{2t}}v = 0, \text{ since } u, v \in \mathbb{F}_{2^n} \text{ where } n = 2t+1\\
\text{i.e.,}\quad & (u^{2^t} + u)v^{2^{2t}} + u^{2^{2t}}v^{2^t} + u^{2^{2t}}v = 0.
\end{aligned}$$

Therefore,

$$\sum_{i=0}^{2} c_i v^{2^{it}} = 0 \text{ where } c_2 = u^{2^t} + u, c_1 = c_0 = u^{2^{2t}}. \tag{3.5.2}$$

Since $\gcd(t, n) = 1$ where $n = 2t+1$, the greatest common divisor $\gcd(2^t - 1, 2^{2t+1} - 1) = 1$. Thus $c_2 = u^{2^t} + u = 0$ if and only if $u = 1$. If $u = 1$ then Equation (3.5.2) reduces to $v^{2^t} + v = 0$, which has only one solution $v = 1$. Equation (3.5.2) has at most $2^2 = 4$ solutions if $u \neq 1$, by Lemma 3.2.3 among them one solution is $v = 0$ and another is $v = u$. So, if $u \notin \{0, 1\} \subseteq \mathbb{F}_{2^n}$, we can obtain at most two values of v such that $\{u, v\}$ is linearly independent. Thus, we can obtain at most $2(2^n - 2)$ many subspaces L such that $\phi(a + L)$ is a flat, for all $a \in \mathbb{F}_{2^n}$. If $u = 1$ then the only solution is $v = u = 1$; giving us no subspace L. So the total number of two dimensional subspace L such that $\phi(a + L)$ is flat for all $a \in \mathbb{F}_{2^n}$ is at most $2(2^n - 2)$. ■

We now consider the case of a bilinear split permutation $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $\phi(x) = x^{2^i+1}$, for all $x \in \mathbb{F}_{2^n}$.

Theorem 3.5.6. *Suppose $\phi(x) = x^{2^r+1}$, for all $x \in \mathbb{F}_{2^n}$ where $\gcd(r, n) = e$, n/e is odd and $\gcd(2^n - 1, 2^r + 1) = 1$.*

(i) Then (ϕ, L) (where L is a subspace of $\dim(L) = 2$) satisfies the (C) property if and only if $L = \langle u, cu \rangle$ where $u \in \mathbb{F}_{2^n}^*$ and $1 \neq c \in \mathbb{F}_{2^e}^*$.

(ii) We assume that $e = \gcd(n, r) > 1$ and $L = \langle u_1, c_1u_1, \ldots, c_{s-1}u_1 \rangle$, $\dim(L) = s$, $c_i \in \mathbb{F}_{2^e}^*$, $1 \leq i \leq s - 1$, $s \geq 2$, and $u_1 \in \mathbb{F}_{2^n}^*$. Then (ϕ, L) satisfies the (C) property.

Proof. We first show (i). Suppose that $L = \langle u, v \rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^n}$. For any $a \in \mathbb{F}_{2^n}$, we have

$$a + L = \{a, a + u, a + v, a + u + v\}.$$

The set $\phi(a + L)$ is a flat if and only if

$$\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v) = 0.$$

Therefore, we have

$$\begin{aligned}
&\phi(a)+\phi(a+u)+\phi(a+v)+\phi(a+u+v)\\
&=a^{2^r+1}+(a+u)^{2^r+1}+(a+v)^{2^r+1}+(a+u+v)^{2^r+1}\\
&=a^{2^r+1}+a^{2^r+1}+au^{2^r}+a^{2^r}u+u^{2^r+1}+a^{2^r+1}+av^{2^r}+a^{2^r}v+v^{2^r+1}\\
&\quad+a^{2^r+1}+a(u+v)^{2^r}+a^{2^r}(u+v)+(u+v)^{2^r+1}\\
&=uv^{2^r}+u^{2^r}v\\
&=uv^{2^r}+u^{2^r}v=0.
\end{aligned}$$

It follows that $(uv^{-1})^{2^r-1}=1$. Combining with this the fact that $(uv^{-1})^{2^n-1}=1$, for $u,v\in\mathbb{F}_{2^n}^*$, and $\gcd(2^n-1,2^r-1)=2^e-1$ we obtain $(uv^{-1})^{2^e-1}=1$. Therefore, $L=\langle u,cu\rangle$ where $u\in\mathbb{F}_{2^n}^*$ and $c\in\mathbb{F}_{2^e}^*$.

We next show (ii). Assume that $L=\langle u_1,c_1u_1,\ldots,c_{s-1}u_1\rangle$ is of dimension $s\geq 2$ where $u_1\in\mathbb{F}_{2^n}^*, c_i\in\mathbb{F}_{2^e}^*$, $\gcd(2^r-1,2^n-1)=2^e-1$. Then (ϕ,L) satisfies the (C) property, which is equivalent to the fact that for any $u,v\in L$ there exists $w\in L$ such that $\phi(a+u)+\phi(a+v)+\phi(a)+\phi(a+w)=0$. To show this, we take $u=\alpha u_1, v=\beta u_1$, $\alpha,\beta\in\mathbb{F}_{2^e}^*$, and define $w:=u+v=(\alpha+\beta)u_1\in L$. Then

$$\begin{aligned}
&\phi(a+u)+\phi(a+v)+\phi(a)+\phi(a+w)\\
&=(a+u)^{1+2^r}+(a+v)^{1+2^r}+a^{1+2^r}+(a+u+v)^{1+2^r}\\
&=au^{2^r}+ua^{2^r}+av^{2^r}+va^{2^r}+a(u+v)^{2^r}+(u+v)a^{2^r}+uv^{2^r}+vu^{2^r}\\
&=uv^{2^r}+vu^{2^r}=\alpha u_1(\beta u_1)^{2^r}+\beta u_1(\alpha u_1)^{2^r}\\
&=\alpha\beta u_1^{1+2^r}+\alpha\beta u_1^{1+2^r}=0
\end{aligned}$$

where we used that $\alpha^{2^r}=\alpha,\beta^{2^r}=\beta$, since both $\alpha,\beta\in\mathbb{F}_{2^e}^*$. The claim is shown. ■

From the above theorem we note that if $e=1$ then there is no linear subspace of dimension 2 such that function in $\mathcal{C}$ can be constructed with respect to the class of permutations under consideration.

The following bilinear split permutations (all are linearly equivalent to each other) are constructed by Blokhuis et al. [2] on $\mathbb{F}_{2^n}$ where $0<i<n$ and $e=\gcd(i,n)$ (see also Laigle-Chapuy [154]):

1. X^{2^i+1} where n/e is odd.

2. $X^{2^i+1} + aX^{2^{n-i}+1}$ where n/e is odd and $a^{(2^n-1)/(2^e-1)} \neq 1$.

3. $X^{2^{2i}+1} + (aX)^{2^i+1} + aX^2$ where $n = 3i$ and $a^{(2^n-1)/(2^e-1)} \neq 1$.

By Theorem 3.5.6 and Lemma 3.5.2 we can derive explicit choices of L which yield $\mathcal{C}$ class bent functions associated to the above permutations.

We consider bilinear split permutations of the form

$$\phi(x) = x(\mathrm{Tr}_l^n(x) + ax) \tag{3.5.3}$$

where $l > 1$, $a \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ and $\mathrm{Tr}_l^n(x) = \sum_{i=0}^{k-1} x^{2^{li}}$. For details we refer to [2, 154]. We show here that bent functions in the $\mathcal{C}$ class, corresponding to ϕ, can be constructed by adding indicator functions of subspaces of codimension 2. The number of such subspaces is also obtained.

Theorem 3.5.7. *Let $n = kl$ where k be odd and l be any positive integer. Consider ϕ as given in Equation (3.5.3). Then the total number of 2-dimensional linear subspaces of $\mathbb{F}_{2^n}$ which satisfy the condition (C) required for the construction of $\mathcal{C}$ type bent functions is $(2^n - 1)(2^l - 2) + (2^{n-l} - 1)(2^{n-l} - 2)$.*

Proof. Let $L = \langle u, v\rangle$ be any two dimensional subspace of $\mathbb{F}_{2^n}$. We know that for any $c \in \mathbb{F}_{2^n}$, $\phi(c+L)$ is flat if and only if $\phi(c) + \phi(c+u) + \phi(c+v) + \phi(c+u+v) = 0$, that is,

$$\begin{aligned} &c(\mathrm{Tr}_l^n(c) + ac) + (c+u)(\mathrm{Tr}_l^n(c+u) + a(c+u)) + (c+v)(\mathrm{Tr}_l^n(c+v) \\ &+a(c+v)) + (c+u+v)(\mathrm{Tr}_l^n(c+u+v) + a(c+u+v)) = 0. \end{aligned} \tag{3.5.4}$$

Since $a(c^2 + (c+u)^2 + (c+v)^2 + (c+u+v)^2) = 0$ and Equation (3.5.4) can be rewritten as

$$\begin{aligned} 0 &= c\mathrm{Tr}_l^n(c) + c\mathrm{Tr}_l^n(c) + c\mathrm{Tr}_l^n(u) + u\mathrm{Tr}_l^n(c) + u\mathrm{Tr}_l^n(u) + c\mathrm{Tr}_l^n(c) + c\mathrm{Tr}_l^n(v) + v\mathrm{Tr}_l^n(c) + \\ &\quad v\mathrm{Tr}_l^n(v) + c\mathrm{Tr}_l^n(c) + c(\mathrm{Tr}_l^n(u) + \mathrm{Tr}_l^n(v)) + (u+v)\mathrm{Tr}_l^n(c) + (u+v)(\mathrm{Tr}_l^n(u) + \mathrm{Tr}_l^n(v)) \\ &= u\mathrm{Tr}_l^n(u) + v\mathrm{Tr}_l^n(v) + u\mathrm{Tr}_l^n(u) + u\mathrm{Tr}_l^n(v) + v\mathrm{Tr}_l^n(u) + v\mathrm{Tr}_l^n(v) = u\mathrm{Tr}_l^n(v) + v\mathrm{Tr}_l^n(u), \end{aligned}$$

then $\phi(c+L)$ is flat if and only if $u\mathrm{Tr}_l^n(v) + v\mathrm{Tr}_l^n(u) = 0$, that is, $\frac{\mathrm{Tr}_l^n(u)}{u} = \frac{\mathrm{Tr}_l^n(v)}{v}$.

Therefore, $\mathcal{C}$ type functions associated to ϕ exist if and only if the function $x \mapsto \frac{\mathrm{Tr}_l^n(x)}{x}$ is not a permutation on $\mathbb{F}_{2^n}$. We know that a polynomial in $\mathbb{F}_{2^n}[x]$ of the form $Q(x) = \sum_{i=0}^{n-1} c_i x^{2^i-1}$, $c_i \in \mathbb{F}_{2^n}$ can not be a permutation polynomial unless $Q(x) = c_k x^{2^k-1}$ with $\gcd(k, n) = 1$ and $c_k \in \mathbb{F}_{2^n}^*$.

Let $k = 1$ then $\mathrm{Tr}_l^n(x) = x$. It is obvious that $x \mapsto \frac{\mathrm{Tr}_l^n(x)}{x} = 1$ is not a permutation. If $k \geq 3$ then it is not a permutation polynomial where k is odd. Thus, for the permutation ϕ we can find at least one 2-dimensional subspace of $\mathbb{F}_{2^n}$ which satisfies the condition (C). Let $\alpha = \mathrm{Tr}_l^n(u)$ and $\beta = \mathrm{Tr}_l^n(v)$.

Case 1: Let $\alpha \neq 0$ and $\beta \neq 0$. Then $\phi(c + L)$ is flat if and only if $\alpha v + \beta u = 0 \Rightarrow v = \frac{\beta}{\alpha} u$, that is, $v = \lambda u$ where $\lambda = \frac{\beta}{\alpha} \in \mathbb{F}_{2^l}^*$ and $\lambda \neq 1$ as $u \neq v$. Therefore, for any $u \in \mathbb{F}_{2^n}^*$, we can choose v in $2^l - 2$ ways. Thus, the total number of 2-dimensional subspaces is $(2^n - 1)(2^l - 2)$.

Case 2: Let $\alpha = 0$ and $\beta \neq 0$. Then $\alpha v + \beta u = 0$ implies $\beta u = 0$, and thus $u = 0$ (since $\beta \neq 0$), which is not possible. The case $\alpha \neq 0$ and $\beta = 0$ implies that $v = 0$, which is also not possible.

Case 3: Let $\alpha = 0$ and $\beta = 0$. Then $\phi(c + L)$ is flat if and only if $u, v \in \ker(\mathrm{Tr}_l^n) \setminus \{0\}$ with $u \neq v$ where $\ker(\mathrm{Tr}_l^n) = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_l^n(x) = 0\}$. Therefore, the dimension of $\ker(\mathrm{Tr}_l^n)$ is $kl - l$. Thus, u can be chosen in $2^{kl-l} - 1$ ways and v in $2^{kl-l} - 2$ ways. Hence the total number of 2-dimensional subspaces is $(2^{kl-l} - 1)(2^{kl-l} - 2)$.

To summarize, for any value of $l > 1$, the total number of 2-dimensional subspaces of $\mathbb{F}_{2^n}$ which satisfies the condition (C) required for the construction of $\mathcal{C}$ type bent functions is $(2^n - 1)(2^l - 2) + (2^{n-l} - 1)(2^{n-l} - 2)$. ■

Example 3.5.8. *Let $n = 2p$ where p is any odd prime, $r = 2$ and $e = \gcd(n, r) = 2$. Since n/e is odd, it is known that* $\gcd(2^r + 1, 2^n - 1) = 1$. *Therefore, $\phi(x) = x^{2^r+1}$ is a permutation on $\mathbb{F}_{2^n}$. Let ζ be a primitive element of $\mathbb{F}_{2^n}$. Therefore, $\lambda = \zeta^{\frac{2^n-1}{2^e-1}} = \zeta^{\frac{2^n-1}{3}}$ is a generator of $\mathbb{F}_{2^e}$. Suppose that the permutation $\pi(x) = \phi^{-1}(x) = x^{\gamma}$ where $\gamma(2^r + 1) \equiv 1 \pmod{2^n - 1}$. Given r and n, γ can be computed easily by the Euclidean algorithm. Consider the Maiorana–McFarland bent $f(x, y) = x \cdot \pi(y)$. According to Theorem* 3.5.6 *if we choose $L = \langle 1, \lambda \rangle$ then the function $f^*(x, y) = x \cdot \pi(y) + \phi_{L^\perp}(x)$ is in $\mathcal{C}$. The bent function f^* can* *be explicitly written as*

$$\begin{aligned} f^*(x,y) &= \mathrm{Tr}_1^n(xy^\gamma) + (\mathrm{Tr}_1^n(x)+1)(\mathrm{Tr}_1^n(\lambda x)+1) \\ &= \mathrm{Tr}_1^n(xy^\gamma) + \mathrm{Tr}_1^n(x)\mathrm{Tr}_1^n(\lambda x) + \mathrm{Tr}_1^n((1+\lambda)x) + 1. \end{aligned}$$

Thus we have obtained an infinite class of bent functions in $\mathcal{C}$ other than $\mathcal{D}_0$. Whether the bent functions obtained in this way are affine inequivalent to Maiorana–McFarland bent functions seems to be a difficult problem, which we leave for future research.

3.5.2 $\mathcal{C}$ type bent functions associated to k-linear split permutations

We next look at $\mathcal{C}$ type bent functions associated to trilinear split permutations.

Theorem 3.5.9. *Suppose $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation of the form $\phi(x) = x\ell_1(x)\ell_2(x)$, for all $x \in \mathbb{F}_{2^n}$ where $\ell_1(X) = \sum_{i=0}^{n-1} a_i X^{2^i}, \ell_2(X) = \sum_{i=0}^{n-1} b_i X^{2^i} \in \mathcal{L}(n)$ $(a_i, b_i \in \mathbb{F}_{2^n})$, and $L = \langle u, v\rangle$ is a 2-dimensional subspace of $\mathbb{F}_{2^n}$. Then $\phi(a+L)$ is a flat for all $a \in \mathbb{F}_{2^n}$ if and only if*

$$\begin{aligned} &\sum_{1\le i,j\le n-1} a_i b_j \left(u^{2^i}v^{2^j} + v^{2^i}u^{2^j}\right) + \sum_{j=0}^{n-1} (a_0 b_j + a_j b_0)\left(uv^{2^j} + u^{2^j}v\right) = 0, \\ &\sum_{j=0}^{n-1} (a_i b_j + a_j b_i)\left(uv^{2^j} + u^{2^j}v\right) = 0, \quad \textit{for all } i = 1,\dots,n-1, \\ &\sum_{0\le i,j\le n-1} a_i b_j \left((u+v)\left(u^{2^i}v^{2^j} + v^{2^i}u^{2^j}\right) + uv^{2^i+2^j} + vu^{2^i+2^j}\right) = 0. \end{aligned} \tag{3.5.5}$$

Proof. Using Lemma 3.3.1, we see that $\phi(a+L)$ is a flat for all $a \in \mathbb{F}_{2^n}$ if and only if

$$\begin{aligned} &\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v) \\ &= a[\ell_1(u)\ell_2(v) + \ell_1(v)\ell_2(u)] + \ell_1(a)[u\ell_2(v) + v\ell_2(u)] \\ &+ \ell_2(a)[u\ell_1(v) + v\ell_1(u)] + u\ell_1(u)\ell_2(v) + u\ell_1(v)\ell_2(u) \\ &+ u\ell_1(v)\ell_2(v) + v\ell_1(u)\ell_2(u) + v\ell_1(u)\ell_2(v) + v\ell_1(v)\ell_2(u) = 0, \end{aligned} \tag{3.5.6}$$

for all $a \in \mathbb{F}_{2^n}$. Substituting ℓ_1, ℓ_2 in Equation (3.5.6) we obtain

$$\begin{aligned}\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}(a_ib_j + a_jb_i)u^{2^i}v^{2^j}\right) a + \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j}v)b_j\right) a^{2^i} \\ + \sum_{i=0}^{n-1} b_i \left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j}v)a_j\right) a^{2^i}\end{aligned}$$

$$+ u\ell_1(u)\ell_2(v) + u\ell_1(v)\ell_2(u) + u\ell_1(v)\ell_2(v) + v\ell_1(u)\ell_2(u) + v\ell_1(u)\ell_2(v) + v\ell_1(v)\ell_2(u)$$

$$\begin{aligned}&= \left(\sum_{0\leq i,j\leq n-1}(a_ib_j + a_jb_i)u^{2^i}v^{2^j}\right) a + \sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j}v)\right)(a_ib_j + a_jb_i)\, a^{2^i} \\ &\quad + (u+v)\sum_{0\leq i,j\leq n-1} a_ib_ju^{2^i}v^{2^j} + (u+v)\sum_{0\leq i,j\leq n-1} a_ib_ju^{2^i}v^{2^j} \\ &\quad + u\sum_{0\leq i,j\leq n-1} a_ib_jv^{2^i+2^j} + v\sum_{1\leq i,j\leq n-1} a_ib_ju^{2^i+2^j} \\ &= \left(\sum_{1\leq i,j\leq n-1}(a_ib_j + a_jb_i)u^{2^i}v^{2^j} + \left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j}v)\right)(a_0b_j + a_jb_0)\right) a \\ &\quad + \sum_{i=1}^{n-1}\left(\sum_{j=0}^{n-1}(uv^{2^j} + u^{2^j}v)\right)(a_ib_j + a_jb_i)\, a^{2^i} \\ &\quad + (u+v)\sum_{0\leq i,j\leq n-1} a_ib_j(u^{2^i}v^{2^j} + v^{2^i}u^{2^j}) + \sum_{0\leq i,j\leq n-1} a_ib_j(uv^{2^i+2^j} + vu^{2^i+2^j}) = 0,\end{aligned}$$

for all $a \in \mathbb{F}_{2^n}$. Thus, in order to construct $\mathcal{C}$ type bents associated to the permutation ϕ with $L = \langle u, v\rangle$, we must obtain linearly independent vectors in $u, v \in \mathbb{F}_{2^n}$ satisfying the system of Equations (3.5.5). ■

Corollary 3.5.10. *Let us consider the case when $\phi(x) = x^{1+2^r+2^s}$, for all $x \in \mathbb{F}_{2^n}$ where $1 < r < s$. Then there is no 2-dimensional subspace $L = \langle u, v\rangle$ satisfying the (C) property.*

Proof. By the previous theorem, the system of Equations (3.5.5) reduces to

$$\begin{aligned}&a_rb_s(u^{2^r}v^{2^s} + u^{2^s}v^{2^r}) = 0 \\ &(uv^{2^s} + u^{2^s}v)a_rb_s = 0 \\ &(uv^{2^r} + u^{2^r}v)a_rb_s = 0 \\ &u^{1+2^r}v^{2^s} + u^{1+2^s}v^{2^r} + uv^{2^s+2^r} + u^{2^s+2^r}v + u^{2^r}v^{1+2^s} + u^{2^s}v^{1+2^r} = 0.\end{aligned}$$

Since $a_r \neq 0$ and $b_s \neq 0$ we obtain the system

$$\begin{aligned}
&u^{2^r}v^{2^s} + u^{2^s}v^{2^r} = 0\\
&uv^{2^s} + u^{2^s}v = 0\\
&uv^{2^r} + u^{2^r}v = 0\\
&u^{1+2^r}v^{2^s} + u^{1+2^s}v^{2^r} + uv^{2^s+2^r} + u^{2^s+2^r}v + u^{2^r}v^{1+2^s} + u^{2^s}v^{1+2^r} = 0,
\end{aligned} \tag{3.5.7}$$

that is, $(uv^{-1})^{2^{n+s-r}-1} = 1$, $(uv^{-1})^{2^s-1} = 1$ and $(uv^{-1})^{2^r-1} = 1$. Let

$$\gcd\left(2^n - 1, 2^{n+s-r} - 1, 2^r - 1, 2^s - 1\right) = 2^e - 1$$

(it is immediate that if L exists then we must have $e > 1$). Then $uv^{-1} \in \mathbb{F}_{2^e}$. Since $e > 1$, there exists $1 \neq c \in \mathbb{F}_{2^e}^*$ such that $v = cv$. Substituting $v = cu$ in the last equation of (3.5.7) we obtain

$$cu^{1+2^r+2^s} + cu^{1+2^r+2^s} + c^2u^{1+2^s+2^r} + cu^{1+2^s+2^r} + c^2u^{1+2^r+2^s} + c^2u^{1+2^r+2^s} = 0,$$

that is, $(c+c^2)u^{1+2^r+2^s} = 0$, implying $c \in \{0, 1\}$, which is a contradiction. Therefore, there is no trilinear split permutation of the above form for which we can construct a 2-dimensional subspace $L = \langle u, v\rangle$ with the required conditions. ■

We can extend the previous theorem to the general case of k-linear split permutations, showing in our next theorem a nonexistence result.

Theorem 3.5.11. *If $\phi(x) = x^{\sum_{i=0}^{k} 2^{r_i}}$ $(k \geq 2)$, for all $x \in \mathbb{F}_{2^n}$ where $r_0 = 0 < r_1 < \ldots < r_k < n$ then there is no 2-dimensional subspace L such that (ϕ, L) satisfies the (C) property.*

Proof. We assume that L exists, and so, there exists $u, v \in \mathbb{F}_{2^n}$ that are $\mathbb{F}_2$–linearly independent such that (ϕ, L) satisfies the (C) property. For a subset $A \subseteq \{0, 1, \ldots, k\}$ (for convenience, we write the set $\{0, 1, \ldots, k\}$ as $[0, k]$), we denote by $R_A := \sum_{i\in A} 2^{r_i}$ and $\bar{A} = [0, k] \setminus A$, with the convention that if $A = \emptyset$ then $R_A = 0$.

Since, $\phi(a + L)$ is a flat, then $\phi(a) + \phi(a + u) + \phi(a + v) + \phi(a + u + v) = 0$, and so,

$$0 \;=\; a^{R_{[0,k]}} + (a + u)^{R_{[0,k]}} + (a + v)^{R_{[0,k]}} + (a + u + v)^{R_{[0,k]}}$$

$$\begin{aligned}
&= a^{R_{[0,k]}} + \prod_{i=0}^{k}(a+u)^{2^{r_i}} + \prod_{i=0}^{k}(a+v)^{2^{r_i}} + \prod_{i=0}^{k}(a+u+v)^{2^{r_i}} \\
&= a^{R_{[0,k]}} + \prod_{i=0}^{k}\left(a^{2^{r_i}} + u^{2^{r_i}}\right) + \prod_{i=0}^{k}\left(a^{2^{r_i}} + v^{2^{r_i}}\right) + \prod_{i=0}^{k}\left(a^{2^{r_i}} + (u+v)^{2^{r_i}}\right) \\
&= a^{R_{[0,k]}} + \sum_{A\subseteq[0,k]} a^{R_A}u^{R_{\bar{A}}} + \sum_{A\subseteq[0,k]} a^{R_A}v^{R_{\bar{A}}} + \sum_{A\subseteq[0,k]} a^{R_A}(u+v)^{R_{\bar{A}}} \\
&= \sum_{A\subsetneqq[0,k]} \left(u^{R_{\bar{A}}} + v^{R_{\bar{A}}} + (u+v)^{R_{\bar{A}}}\right) a^{R_A},
\end{aligned}$$

for all $a \in \mathbb{F}_{2^n}$. That is, the polynomial

$$\sum_{A\subsetneqq[0,k]} \left(u^{R_{\bar{A}}} + v^{R_{\bar{A}}} + (u+v)^{R_{\bar{A}}}\right) X^{R_A}$$

has 2^n roots, but its degree is $R_{[0,k]} = \sum_{i=0}^{k} 2^{r_i} < 2^n$, and therefore all its coefficients must be 0. Hence (replacing $\bar{A}$ by A, under the condition $A \neq \emptyset$), we have

$$u^{R_A} + v^{R_A} + (u+v)^{R_A} = 0, \text{ for all } A \subseteq [0,k], A \neq \emptyset. \tag{3.5.8}$$

Now, taking $A = \{0, i\}, 1 \le i \le k$, and simplifying, we get

$$vu^{2^{r_i}} + uv^{2^{r_i}} = 0, \text{ for all } 1 \le i \le k,$$

and so, $vu^{-1} \in \mathbb{F}^*_{2^{r_i}}, 1 \le i \le k$. Thus, if $2^e - 1 = \gcd(2^n - 1, 2^{r_1} - 1, \ldots, 2^{r_k} - 1)$ (certainly, if L of dimension 2 exists, it is necessary that $e > 1$) then $v = cu$, for some $c \in \mathbb{F}^*_{2^e} \setminus \{1\}$. Substituting $v = cu$ in Equation (3.5.8) with $A = \{0, 1, 2\}$, we obtain

$$cu^{1+2^{r_1}+2^{r_2}} + cu^{1+2^{r_1}+2^{r_2}} + c^2u^{1+2^{r_2}+2^{r_1}} + cu^{1+2^{r_2}+2^{r_1}} + c^2u^{1+2^{r_1}+2^{r_2}} + c^2u^{1+2^{r_1}+2^{r_2}} = 0,$$

that is,

$$(c + c^2)u^{1+2^{r_1}+2^{r_2}} = 0,$$

implying $c \in \{0, 1\}$, which is a contradiction. Therefore, there are no 2-dimensional subspaces L for which we can construct $\mathcal{C}$ type bent functions corresponding to k-linear split monomial permutations. ■

For permutations on $\mathbb{F}_{2^n}$ of the form $\phi(x) = x^{\sum_{i=1}^{k} 2^{r_i}}$ ($k \geq 2$), we can inquire whether there are subspaces of dimension > 2 associated to $\mathcal{C}$ type bent functions. While in general we cannot answer that question, we can certainly derive some necessary conditions.

Theorem 3.5.12. *Let ϕ be a monomial permutation of degree k, that is, $\phi(x) = x^{\sum_{i=1}^{k} 2^{r_i}}$, $0 = r_1 < \ldots < r_k < n$, $k \geq 2$. A necessary condition for (ϕ, L) (with L of dimension $s \geq 2$) to satisfy the (C) property is*

$$\sum_{u \in L} u^{R_A} = 0, \text{ for all } \emptyset \neq A \subseteq [0, k]. \tag{3.5.9}$$

Moreover, if (ϕ, L) with L of dimension $s \geq 2$ satisfies the property (C) then both $2^s - 1, 2^n - 2^s$ must be in $\mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$ where $2^n - 1 = \prod_{i=1}^{\ell} p_i^{e_i}$ is the prime power factorization (we adopt the convention that $0 \in \mathbb{N}$).

Proof. Since for subspaces or flats of dimension $s \geq 2$ the sum of all elements must be zero, we can infer (as we have done in the proof of our previous theorem) that for all $a \in \mathbb{F}_{2^n}$,

$$\begin{aligned} 0 &= \sum_{u \in L} \phi(a+u) = \sum_{u \in L} \prod_{i=1}^{k} (a+u)^{2^{r_i}} \\ &= \sum_{u \in L} \sum_{A \subseteq [0,k]} u^{R_A} a^{R_{\bar{A}}} \\ &= \sum_{\emptyset \neq A \subseteq [0,k]} \left(\sum_{u \in L} u^{R_A} \right) a^{R_{\bar{A}}}. \end{aligned}$$

As before, the polynomial $\sum_{\emptyset \neq A \subseteq [0,k]} \left(\sum_{u \in L} u^{R_A} \right) X^{R_{\bar{A}}}$ with degree $< 2^n$ and has 2^n roots, and so, all coefficients must be zero (the terms $X^{R_{\bar{A}}}$ are all distinct for different $\bar{A}$ by the uniqueness of binary representations), from which we infer the first claim.

It is well-known (see Lam and Leung [136, 137] and Sivek [47]) that a sum of k distinct m-th roots of unity is zero (we say that m is k-balancing) if and only if both k and $m - k$ are in $\mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$ where $m = \prod_{i=1}^{\ell} p_i^{e_i}$ is the prime power factorization. Since the elements $u \in L \subseteq \mathbb{F}_{2^n}$ are $(2^n - 1)$-th roots of unity, condition (3.5.9) shows that $(2^n - 1)$ is $(2^s - 1)$-balancing (since the cardinality of L^* is $2^s - 1$). Expressing $2^n - 1 = \prod_{i=1}^{\ell} p_i^{e_i}$, then the previous result forces both $2^s - 1$ and $2^n - 2^s$ to be in $\mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$. ■

Using some elementary number theory arguments, we can easily get several results regarding the nonexistence of subspaces as in property (C). Let $\mathbf{p}(N)$ denote the smallest prime factor of N.

Corollary 3.5.13. *With the notations of Theorem* 3.5.12*, the following statements are true:*

(i) If $1 < s < \log_2(\mathbf{p}(2^n - 1))$*, or* $\log_2(2^n - \mathbf{p}(2^n - 1)) < s < n$ *then there are no pairs* (ϕ, L) *satisfying the* (C) *property where* $\dim(L) = s$ *and* ϕ *is a monomial permutation.*

(ii) Let $n = P$ *be a prime number. If* $2^n - 1 = p$ *is a Mersenne prime, or* $2^n - 1 = p\,q$*, a product of two primes then there are no subspaces of dimension* $1 < s < n$ *satisfying the* $\mathcal{C}$ *type bent condition* (C) *for a monomial permutation* ϕ *of degree* $k \geq 3$*.*

Proof. The first claim follows easily observing that, by Theorem 3.5.12, if $s < \log_2(\mathbf{p}(2^n - 1))$ then $2 \leq 2^s - 1 < \mathbf{p}(2^n - 1) \in \{p_1, \ldots, p_\ell\}$, and so, $2^s - 1 \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$; if $s > \log_2(2^n - \mathbf{p}(2^n - 1))$ then $2^n - 2^s < \mathbf{p}(2^n - 1)$, and so, $2^n - 2^s \notin \mathbb{N}p_1 + \cdots + \mathbb{N}p_\ell$.

Regarding claim (ii), if $2^n - 1 = p$ is a Mersenne prime then, by Theorem 3.5.12, $2^n - 1$ is $(2^s - 1)$-balancing, and so, one needs $2^s - 1 = ap$ and $2^n - 2^s = Ap$, for some nonnegative integers a, A. Thus, $2^n - 1 = (A + a)p = p$, which implies that $(a, A) \in \{(0, 1), (1, 0)\}$, therefore, either $s = 0$, or $s = n$, which contradicts our assumption that $2 \leq s < n$.

To show the second part of claim (ii), observe that by Theorem 3.5.12, there exist nonnegative integers a, b, A, B such that

$$\begin{aligned} 2^n - 1 &= p\,q, \\ 2^s - 1 &= ap + bq, \\ 2^n - 2^s &= Ap + Bq, \end{aligned}$$

from which we derive that $(A + a)p + (B + b)q = p\,q$, and so, $A + a \equiv 0 \pmod{q}, B + b \equiv 0 \pmod{p}$. If $ab \neq 0$, since A, B, a, b are nonnegative and $A < q, a < q, B < p, b < p$ then $A = q - a, B = p - b$. But then, $2^n - 2^s = Ap + Bq = 2pq - (ap + bq) = pq + (pq - 2^s + 1) > 2^n$, which is a contradiction. Thus, $ab = 0$, and without loss of generality, we assume that $b = 0$, but then $B = 0$, as well. Thus, $2^s - 1 = ap, 2^n - 2^s = (q - a)p$. It is well-known that $\gcd(2^n - 1, 2^s - 1) = 2^{\gcd(n,s)} - 1$. Since $p | 2^n - 1, p | 2^s - 1$ and n is prime (thus, for $2 \leq s < n$, $\gcd(n, s) = 1$), then $p | 2^{\gcd(n,s)} - 1 = 1$, which is a contradiction. ■

Permutation $\phi = \pi^{-1}$ where $f(x, y) = x \cdot \pi(y)$	Condition for (ϕ, L) to satisfy (C). # of 2-dimensional subspaces $L = \tau$
$\phi(x) = x^{2^{t+1}+1} + x^3 + x$, $n = 2t + 1$, $\gcd(t, n) = 1$.	$1 \leq \tau \leq 2(2^n - 2)$
$\phi(x) = x^{2^r+1}$, $\gcd(r, n) = e$, n/e odd, $\gcd(2^n - 1, 2^r + 1) = 1$	If and only if $L = \langle u, cu \rangle$, $u \in \mathbb{F}_{2^n}^*$, $1 \neq c \in \mathbb{F}_{2^e}^*$
$\phi(x) = x^{1+2^r+2^s}$, $1 < r < s$	No 2-dimensional subspace satisfying (C)
$\phi(x) = x^{\sum_{i=0}^{k} 2^{r_i}}$, $k \geq 2$, $r_0 = 0 < r_1 < \ldots < r_k < n$	No 2-dimensional subspace satisfying (C)
$\phi(x) = x(\mathrm{Tr}_l^n(x) + ax)$, $l > 1$, $a \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$	$\tau = (2^n - 1)(2^l - 2)$ $+(2^{n-l} - 1)(2^{n-l} - 2)$

Table 3.1: List of $\phi = \pi^{-1}$ where $f(x, y) = x \cdot \pi(y)$, along with the conditions for satisfying property (C)

Chapter 4

Subspace sum of generalized Boolean function and their properties

4.1 Introduction

In 1985, Kumar et al. [98] introduced the concept of *generalized bent functions* $f : \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q$ where $q > 1$ is a positive integer and gave constructions for every possible q and n, except for n is odd and $q \equiv 2 \pmod 4$. Later, *generalized bent functions* over a finite field $\mathbb{F}_{p^n}$ was studied by Ambrosimov [4]. There has been a flourish of new research in this area, with new constructions being displayed, characterizations, and even connecting them to certain combinatorial objects such as partial difference sets, strongly regular graphs and association schemes (see [10, 155, 157]). For efficient wireless communication, *generalized bent functions* are used for large signal sets with low maximum crosscorrelation [53, 112, 116, 127, 158]. Helleseth et al. [128] identified some monomial and quadratic bent functions over the finite fields of odd characteristic. Budaghyan et al. [66] identified some non-quadratic *generalized bent functions* which does not belong to complete Maiorana–McFarland class and proved that the complete generalized Maiorana–McFarland class does not cover all quadratic bent functions, which is not case for binary. In this chapter, we consider the *generalized Boolean functions* from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ where p is prime and their set is denoted by $\mathcal{B}_n^p$. We characterize the subspace sum of $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$ (denoted by $\mathcal{S}_V f$). Also we show that if $f, h \in \mathcal{B}_n^p$ are affine equivalent then so are $\mathcal{S}_V f$ and $\mathcal{S}_V h$ where V is a subspace of $\mathbb{F}_p^n$. Further, we extend to characteristic $p > 2$ a binary result of Dillon, concerning the vanishing subspace sum of any Maiorana–McFarland bent functions.

4.2 Preliminaries

In what follows, p denotes an (arbitrary, but fixed) odd prime number. Let $\mathcal{A}$ be a group algebra of $\mathbb{F}_p^n$ over $\mathbb{F}_p$, defined as in Section 1.3. Suppose $\mathcal{P}$ is a maximal ideal of $\mathcal{A}$, defined as in Equation (1.3.1). We now state a generalization (due to Charpin [87,88]) of Berman's Theorem.

Theorem 4.2.1 ([39, Theorem 5.19])**.** *For any $0 \leq r \leq n(p-1)$, $\mathcal{R}_p(r,n) = \mathcal{P}^{n(p-1)-r}$ where $\mathcal{R}_p(r,n)$ is a generalized Reed–Muller codes.*

Let $t = k(p-1)$ where k be a positive integer. From [39, Corollary 4.12], we know that $\mathcal{P}^t$ is a subspace generated by the codewords whose support are k-dimensional subspaces of $\mathbb{F}_p^n$. The basis of $\mathcal{A}$ was exploited by Jennings [107], and is now called a Jennings basis of $\mathcal{A}$.

Theorem 4.2.2 ([39, Theorem 4.10])**.** *Let $g_1, g_2, \ldots, g_n$ be a basis of $\mathbb{F}_p^n$. Then the set*

$$\left\{\prod_{i=1}^{n}(x^{g_i}-1)^{k_i} : (k_1, k_2, \ldots, k_n) \in \mathbb{F}_p^n\right\}$$

is a basis of $\mathcal{A}$. Moreover,

$$\left\{\prod_{i=1}^{n}(x^{g_i}-1)^{k_i} : \sum_{i=1}^{n} k_i \geq t, (k_1, k_2, \ldots, k_n) \in \mathbb{F}_p^n\right\}$$

form a basis of $\mathcal{P}^t$.

Theorem 4.2.3 ([98, Theorem 1])**.** *Let $m = 2n$ and $f : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ be a generalized Boolean function of the form*

$$f(x,y) = x \cdot \pi(y) + g(y)$$

where π be an arbitrary permutation polynomial over $\mathbb{F}_p^n$ and $g \in \mathcal{B}_n^p$. Then f is a regular bent and the dual function of f is $\tilde{f}(x,y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$. Also, we refer to [55].

The class of bent functions defined as in Theorem 4.2.3 is called generalized Maiorana–McFarland bent functions and their set is denoted by $\mathcal{M}^p$. In the binary case, the completed Maiorana–McFarland class contains all quadratic bent functions which are the simplest and best understood. However, this does not hold in the generalized case.

Fact 4.2.4 ([128, Fact 1]). *Let α be a primitive element of $\mathbb{F}_{3^6}$. Any ternary function f from $\mathbb{F}_{3^6}$ to $\mathbb{F}_3$ of the form*

$$f(x) = \mathrm{Tr}_1^6(\alpha^7 x^{98})$$

is bent and not weakly regular bent.

4.3 Subspace sum of a function

Let $f \in \mathcal{B}_n^p$ and V be any k-dimensional subspace of $\mathbb{F}_p^n$. Then there exists k linearly independent elements $a_1, a_2, \ldots, a_k \in \mathbb{F}_p^n$ such that

$$V = \langle a_1, a_2, \ldots, a_k \rangle = \{a \in \mathbb{F}_p^n : a = \sum_{i=1}^{k} c_i a_i \text{ where } c_i \in \mathbb{F}_p, 1 \leq i \leq k\}.$$

Definition 4.3.1. *The subspace sum of $f \in \mathcal{B}_n^p$ with respect to a subspace V of $\mathbb{F}_p^n$ is a generalized Boolean function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, $\mathcal{S}_V f$, defined by*

$$\mathcal{S}_V f(x) = \sum_{v \in V} f(x+v), \textit{ for all } x \in \mathbb{F}_p^n.$$

More precisely, $\mathcal{S}_V f(x)$ is the sum of the values of f on the coset $x + V$, which depends on V only, not on the dimension of V.

Remark 4.3.2. *Let $j \in \mathbb{F}_p$ and $V = \langle a \rangle$ be an one dimensional subspace of $\mathbb{F}_p^n$. Then $\mathcal{S}_V f(x) = \mathcal{S}_V f(x + ja)$, for all $x \in \mathbb{F}_p^n$.*

4.3.1 Derivative and subspace sum of a function

If $p = 2$, the subspace sum of a Boolean function with respect to a k-dimensional subspace is same as the kth order derivative, and therefore our following results naturally extends the binary case.

Lemma 4.3.3. *Let $f \in \mathcal{B}_n^p$ and k be a positive integer less than or equal to p. Then for any $a \in \mathbb{F}_p^n$,*

$$\underbrace{D_aD_a\dots D_a}_{k-times} f(x) = \sum_{i=0}^{k}(-1)^i\binom{k}{i}f(x+(k-i)a), \text{ for all } x \in \mathbb{F}_p^n. \tag{4.3.1}$$

More precisely, if $k = p$ then both sides are equal to 0.

Proof. Certainly, the result is true for $k = 1$, so we now let $k = 2$. Then for $a \in \mathbb{F}_p^n$,

$$D_aD_af(x) = f(x+2a) - 2f(x+a) + f(x) = \sum_{i=0}^{2}(-1)^i\binom{2}{i}f(x+(2-i)a), \text{ for all } x \in \mathbb{F}_p^n.$$

We assume the claim happens for an arbitrary positive integer $r < p$, that is,

$$\underbrace{D_aD_a\dots D_a}_{r-\text{times}} f(x) = \sum_{i=0}^{r}(-1)^i\binom{r}{i}f(x+(r-i)a), \tag{4.3.2}$$

for all $x \in \mathbb{F}_p^n$. Taking the derivative of both sides of Equation (4.3.2) with respect to a, we get

$$\begin{aligned}
&\underbrace{D_aD_a\dots D_a}_{(r+1)-\text{times}} f(x) = D_a\{\underbrace{D_aD_a\dots D_a}_{r-\text{times}} f\}(x)\\
&= \sum_{i=0}^{r}(-1)^i\binom{r}{i}f(x+(r-i+1)a) - \sum_{i=0}^{r}(-1)^i\binom{r}{i}f(x+(r-i)a)\\
&= f(x+(r+1)a) + \sum_{i=1}^{r}(-1)^i\binom{r}{i}f(x+(r-i+1)a)\\
&+ \sum_{i=0}^{r-1}(-1)^{i+1}\binom{r}{i}f(x+(r-i)a) + (-1)^{r+1}f(x)\\
&= f(x+(r+1)a) + \sum_{j=0}^{r-1}(-1)^{j+1}\binom{r}{j+1}f(x+(r-j)a)\\
&+ \sum_{i=0}^{r-1}(-1)^{i+1}\binom{r}{i}f(x+(r-i)a) + (-1)^{r+1}f(x), \quad j = i-1\\
&= f(x+(r+1)a) + \sum_{i=0}^{r-1}(-1)^{i+1}\left\{\binom{r}{i+1} + \binom{r}{i}\right\}f(x+(r-i)a) + (-1)^{r+1}f(x)
\end{aligned}$$

$$= f(x+(r+1)a) + \sum_{i=0}^{r-1}(-1)^{i+1}\binom{r+1}{i+1}f(x+(r-i)a) + (-1)^{r+1}f(x)$$
$$= f(x+(r+1)a) + \sum_{j=1}^{r}(-1)^{j}\binom{r+1}{j}f(x+(r+1-j)a) + (-1)^{r+1}f(x), \;\; j=i+1$$
$$= \sum_{i=0}^{r+1}(-1)^{i}\binom{r+1}{i}f(x+(r+1-i)a).$$

From elementary number theory we know that for a prime p

$$\binom{p}{i} \equiv 0 \pmod{p}, \;\; i \in \{1,2,\dots,p-1\}.$$

Thus, if $k=p$ then the right hand side of Equation (4.3.1) consists only $f(x)$ and $-f(x)$, and the lemma is shown. ■

Theorem 4.3.4. *Suppose $V=\langle a\rangle$ is an arbitrary 1-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$. Then*

$$\mathcal{S}_V f(x) = \underbrace{D_a D_a \dots D_a}_{(p-1)-times} f(x), \;\; \textit{for all } x \in \mathbb{F}_p^n.$$

Furthermore, for any $r \in \{0,1,2,\dots,p-1\}$

$$r\mathcal{S}_V f(x) = D_{ra} \underbrace{D_a \dots D_a}_{(p-2)-times} f(x), \;\; \textit{for all } x \in \mathbb{F}_p^n.$$

Proof. Using the previous lemma and the known elementary number theory congruence

$$\binom{p-1}{j} \equiv (-1)^j \pmod{p}$$

where p is an odd prime and $0 \le j \le p-1$, we get the first claim.

Let $r \in \{0,1,2,\dots,p-1\}$ and $V=\langle a\rangle$ be an one dimensional subspace of $\mathbb{F}_p^n$. Suppose

$g(x) = \underbrace{D_aD_a \dots D_a}_{(p-2)-\text{times}} f(x)$, for all $x \in \mathbb{F}_p^n$. Then

$$\begin{aligned} D_{ra} \underbrace{D_a \dots D_a}_{(p-2)-\text{times}} f(x) &= D_{ra}g(x) = g(x+ra) - g(x) \\ &= g(x+ra) - g(x+(r-1)a) + \dots + g(x+a) - g(x) \\ &= D_a g(x+(r-1)a) + D_a g(x+(r-2)a) + \dots + D_a g(x) \\ &= \mathcal{S}_V f(x+(r-1)a) + \mathcal{S}_V f(x+(r-2)a) + \dots + \mathcal{S}_V f(x) \\ &= \mathcal{S}_V f(x) + \mathcal{S}_V f(x) + \dots + \mathcal{S}_V f(x), \text{ using Remark 4.3.2} \\ &= r\mathcal{S}_V f(x), \end{aligned}$$

thus showing our second claim. ■

As an example, let $p = 3$ and V be an one dimensional subspace generated by $a \in \mathbb{F}_3^n$. Then

$$\begin{aligned} \mathcal{S}_V f(x) &= f(x+2a) + f(x+a) + f(x) = D_aD_af(x) \\ 2\mathcal{S}_V f(x) &= 2D_aD_af(x) = D_{2a}D_af(x) = D_aD_{2a}f(x). \end{aligned}$$

Theorem 4.3.5. *Let $V = \langle a_1, a_2, \dots, a_k \rangle$ be a k-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$. Then*

$$\mathcal{S}_V f(x) = \underbrace{D_{a_1} \dots D_{a_1}}_{(p-1)-\textit{times}} \dots \underbrace{D_{a_k} \dots D_{a_k}}_{(p-1)-\textit{times}} f(x), \text{ for all } x \in \mathbb{F}_p^n.$$

Proof. Without loss of generality, let $V_j = \langle a_1, a_2, \dots, a_j \rangle$, $1 \le j \le k$, be a j-dimensional subspace of $\mathbb{F}_p^n$ and for $j = k$, $V_k = V$. The result is true for $k = 1$, so we now let $k = 2$. Let

$$g(x) = \underbrace{D_{a_2} \dots D_{a_2}}_{(p-1)-\text{times}} f(x) = \sum_{i_2=0}^{p-1} f(x + i_2a_2), \text{ for all } x \in \mathbb{F}_p^n.$$

Then

$$\begin{aligned} \underbrace{D_{a_1} \dots D_{a_1}}_{(p-1)-\text{times}} \underbrace{D_{a_2} \dots D_{a_2}}_{(p-1)-\text{times}} f(x) &= \underbrace{D_{a_1} \dots D_{a_1}}_{(p-1)-\text{times}} g(x) = \sum_{i_1=0}^{p-1} g(x + i_1a_1) \\ &= \sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} f(x + i_2a_2 + i_1a_1) = \mathcal{S}_{V_2} f(x). \end{aligned}$$

We now assume that the result is true for $k = r$, that is,

$$\begin{aligned}\mathcal{S}_{V_r} f(x) &= \underbrace{D_{a_1} \dots D_{a_1}}_{(p-1)-\text{times}} \dots \underbrace{D_{a_r} \dots D_{a_r}}_{(p-1)-\text{times}} f(x) \\ &= \sum_{i_1=0}^{p-1} \dots \sum_{i_r=0}^{p-1} f(x + i_r a_r + \dots + i_1 a_1),\end{aligned}$$

for all $x \in \mathbb{F}_p^n$. Therefore,

$$\begin{aligned}\underbrace{D_{a_{r+1}} \dots D_{a_{r+1}}}_{(p-1)-\text{times}} \underbrace{D_{a_1} \dots D_{a_1}}_{(p-1)-\text{times}} \dots \underbrace{D_{a_r} \dots D_{a_r}}_{(p-1)-\text{times}} f(x) &= \sum_{i_{r+1}=0}^{p-1} \mathcal{S}_{V_r} f(x + i_{r+1} a_{r+1}) \\ &= \sum_{i_{r+1}=0}^{p-1} \sum_{i_1=0}^{p-1} \dots \sum_{i_r=0}^{p-1} f(x + i_{r+1} a_{r+1} + i_r a_r + \dots + i_1 a_1) = \mathcal{S}_{V_{r+1}} f(x),\end{aligned}$$

and the theorem is shown. ■

4.3.2 Codes and subspace sum of a function

Proposition 4.3.6. *Let $V = \langle a_1, a_2, \dots, a_k \rangle$ be a k-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$ of degree r. Suppose $h(x) = \mathcal{S}_V f(x)$, for all $x \in \mathbb{F}_p^n$. Then $\left(\sum_{v \in V} X^v\right) \Omega_f$ is the associated codeword of $\mathcal{S}_V f$, that is,*

$$\Omega_h = \left(\sum_{v \in V} X^v\right) \Omega_f.$$

Proof. Let $f \in \mathcal{B}_n^p$ and $a \in \mathbb{F}_p^n$. Then

$$X^a \Omega_f = X^a \sum_{g \in \mathbb{F}_p^n} f(g) X^g = \sum_{g \in \mathbb{F}_p^n} f(g) X^{g+a} = \sum_{g \in \mathbb{F}_p^n} f(g-a) X^g.$$

Since any $v \in V$ can be written as $v = \sum_{i=1}^k c_i a_i$ where $c_i \in \mathbb{F}_p$, $i \in \{1, 2 \dots, k\}$ and so,

$$\begin{aligned}\left(\sum_{v \in V} X^v\right) \Omega_f &= \sum_{g \in \mathbb{F}_p^n} \left(\sum_{v \in V} f(g-v)\right) X^g = \sum_{g \in \mathbb{F}_p^n} \left(\sum_{v \in V} f(g+v)\right) X^g \\ &= \sum_{g \in \mathbb{F}_p^n} \mathcal{S}_V f(g) X^g = \Omega_{\mathcal{S}_V f} = \Omega_h.\end{aligned}$$

■

Proposition 4.3.7. *Let V be a k-dimensional subspace of $\mathbb{F}_p^n$ and $f \in \mathcal{B}_n^p$ of degree r. Then* *the degree of $\mathcal{S}_V f$ is less than or equal to $r - k(p-1)$. In particular, the subspace sum of f with respect to any one dimensional subspace of $\mathbb{F}_p^n$ have degree at most $r - p + 1$.*

Proof. Let $V = \langle a_1, a_2, \ldots, a_k \rangle$ be a k-dimensional subspace of $\mathbb{F}_p^n$ and $y = \sum_{v \in V} X^v$ be the codeword of support V. Then

$$y\Omega_f = \left(\sum_{v \in V} X^v \right) \Omega_f = \sum_{g \in \mathbb{F}_p^n} \mathcal{S}_V f(g) X^g.$$

Since the degree of $f \in \mathcal{B}_n^p$ is r, and so, Ω_f is in $\mathcal{P}^{n(p-1)-r}$, which does not depend on y. Moreover, $\dim V = k$ and y is a minimum codeword of $\mathcal{P}^{k(p-1)}$. Thus, the codeword $y\Omega_f$ is in $\mathcal{P}^{k(p-1)}\mathcal{P}^{n(p-1)-r} = \mathcal{P}^{n(p-1)-r+k(p-1)}$, which is $\{0\}$ for $r \leq k(p-1) - 1$. When $r = k(p-1) + d$, $d \geq 0$, the degree of $\mathcal{S}_V f$ is at most $d = r - k(p-1)$. ■

Proposition 4.3.8. *Let V be a k-dimensional subspace of $\mathbb{F}_p^n$. Suppose that $y = \sum_{v \in V} X^v$ and $V_1 = V, V_2, \ldots, V_t$ are distinct cosets of V where $t = p^{n-k}$. Let $x = \sum_{g \in \mathbb{F}_p^n} x_g X^g \in \mathcal{A}$, and for each i, denote by x_i the restriction of x to V_i and $N_i = \sum_{g \in V_i} x_g$. Then*

$$xy = \sum_{i=1}^{t} (N_i \pmod{p}) \sum_{g \in V_i} X^g.$$

Furthermore,

1. *$xy = 0$ if and only if $N_i \equiv 0 \pmod{p}$, for all i, $1 \leq i \leq t$ and $xy \neq 0$ if and only if there exists at least one $1 \leq i \leq t$ such that $N_i \not\equiv 0 \pmod{p}$.*

2. *$wt(xy) = \lambda_0 p^k$ where λ_0 is the number of x_i for which $N_i \not\equiv 0 \pmod{p}$.*

Proof. Since $\mathbb{F}_p^n = \bigcup_{i=1}^t V_i$ and let $V_i = a_i + V$, for all $i = 1, 2, \ldots, t$ with $a_1 = 0$. Then

$$x = \sum_{g \in \mathbb{F}_p^n} x_g X^g = \sum_{i=1}^{t} \sum_{g \in V_i} x_g X^g = \sum_{i=1}^{t} X^{a_i} \sum_{u \in V} x_{a_i + u} X^u.$$

Now

$$\begin{aligned} xy &= \left(\sum_{i=1}^{t} X^{a_i} \sum_{u\in V} x_{a_i+u} X^{u}\right)\left(\sum_{v\in V} X^{v}\right) = \sum_{i=1}^{t} X^{a_i} \sum_{u\in V} x_{a_i+u}\left(\sum_{v\in V} X^{u+v}\right) \\ &= \sum_{i=1}^{t} X^{a_i}\left(\sum_{u\in V} x_{a_i+u}\right)\left(\sum_{v\in V} X^{v}\right), \quad \text{as } \ X^{u}y = y \ \text{ for any } \ u\in V \\ &= \sum_{i=1}^{t}\left(\sum_{v\in V} X^{a_i+v}\right)\left(\sum_{u\in V} x_{a_i+u}\right) = \sum_{i=1}^{t}(N_i \pmod p)\sum_{g\in V_i} X^{g}. \end{aligned}$$

If $N_i \equiv 0 \pmod p$ for all i, $1 \le i \le t$, then $xy = 0$ and conversely. Since $\sum_{g\in V_i} X^g$ is the all one-vector of length p^k and support V_i. Then $wt(xy) = \lambda_0 p^k$ where λ_0 is the number of x_i for which $N_i \not\equiv 0 \pmod p$. ■

4.3.3 Affine equivalence of subspace sums

In this section, we generalize a result of Dillon [56].

Theorem 4.3.9. *Let $f \in \mathcal{B}_n^p$ and $\mathcal{S}_k[f]$ denotes the multiset of all subspace sum of f with respect to k-dimensional subspaces of $\mathbb{F}_p^n$. If $f, h \in \mathcal{B}_n^p$ are affine equivalent, so are $\mathcal{S}_k[f]$ and $\mathcal{S}_k[h]$. Precisely, if the nonsingular affine transformation A (operating on $\mathbb{F}_p^n$) map f onto h, it also maps $\mathcal{S}_k[f]$ onto $\mathcal{S}_k[h]$.*

Proof. Suppose that $h(x) = f(xA + b)$, for all $x \in \mathbb{F}_p^n$ where $A \in GL(n, \mathbb{F}_p)$ and $b \in \mathbb{F}_p^n$. Let E be an arbitrary k-dimensional subspace of $\mathbb{F}_p^n$. For all $x \in \mathbb{F}_p^n$,

$$\begin{aligned} \mathcal{S}_E h(x) &= \sum_{a\in E} g(x+a) = \sum_{a\in E} f(xA + aA + b) \\ &= \sum_{a\in E} f(xA + b + aA) = \sum_{c\in E_1} f(xA + b + c) \text{ where } E_1 = \{c : c = aA, a \in E\} \\ &= \mathcal{S}_{E_1} f(xA + b), \end{aligned}$$

since the maps $a \longrightarrow aA$ is a permutation of the k-dimensional subspace E of $\mathbb{F}_p^n$. The theorem is shown. ■

Corollary 4.3.10. *If $\mathcal{P}$ is any affine invariant for $\mathcal{B}_n^p$ then*

$$f \longrightarrow \mathcal{P}\{\mathcal{S}_k[f]\}$$

is also an affine invariant for $\mathcal{B}_p^n$.

4.3.4 Maiorana–McFarland bent functions and subspace sums

In [66, Proposition 1], Budaghyan et al. proved that if $f \in \mathcal{B}_n^p$ belongs to the complete Maiorana–McFarland class then there exists an $\frac{n}{2}$-dimensional subspace of $\mathbb{F}_p^n$ such that all second-order derivatives is 0 where n is even. We derive a necessary condition for Maiorana–McFarland class bent functions.

Theorem 4.3.11. *Let $m = 2n$ and f be a generalized Maiorana–McFarland bent function defined as in Theorem 4.2.3. Then there exists an n-dimensional subspace E of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ such that*

1. *the subspace sum of f with respect to any one dimensional subspaces of E is 0 if p is odd.*
2. *the subspace sum of f with respect to any two dimensional subspaces of E is 0 if $p = 2$.*

Proof. Let V be a subspace of $\mathbb{F}_p^n \times \mathbb{F}_p^n$. The subspace sum of f with respect to V is

$$\begin{aligned}\mathcal{S}_V f(x,y) &= \sum_{(u,v)\in V} f(x+u, y+v)\\ &= \sum_{(u,v)\in V} \left((x+u)\cdot\pi(y+v) + g(y+v)\right).\end{aligned} \tag{4.3.3}$$

Let $v = 0$. Then V is a subspace of $E = \mathbb{F}_p^n \times \{0\}$. From Equation (4.3.3), we get

$$\mathcal{S}_V f(x,y) = \sum_{(u,0)\in V} (x+u)\cdot\pi(y) + |V|g(y) = \sum_{(u,0)\in V} (x+u)\cdot\pi(y).$$

Let p be an odd prime and $V = \langle (a,0)\rangle$ be an one dimensional subspace of E. Then

$$\mathcal{S}_V f(x,y) = p\left(x + \frac{p-1}{2}a\right)\cdot\pi(y) = 0, \text{ for all } (x,y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n.$$

Let $p = 2$ and $V = \langle (a,0), (c,0)\rangle$ be a two dimensional subspace of E, then

$$\mathcal{S}_V f(x,y) = 0, \text{ for all } (x,y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n.$$

■

Helleseth and Kholosha [128] verified the Fact 4.2.4 by computer calculations, however, proving this result theoretically and probably finding the whole class of similar functions remains an open problem. Using Theorem 4.3.11, it is shown that the function defined as in Fact 4.2.4 does not belong to complete $\mathcal{M}^p$ class.

Theorem 4.3.12. *The function f defined as in Fact 4.2.4 does not belong to the complete $\mathcal{M}^p$ class.*

Proof. Let f be equivalent to a function from class $\mathcal{M}^p$. From Theorem 4.3.11, we have there exists a 3-dimensional subspace E of $\mathbb{F}_{3^6}$ such that the subspace sum of f with respect to any one dimensional subspace of E is 0. Let $V = \langle a \rangle$ where $a \in \mathbb{F}_{3^6}^*$. Then

$$\mathcal{S}_V f(x) = f(x) + f(x+a) + f(x+2a) = \mathrm{Tr}_1^6(\alpha^7(x^{98} + (x+a)^{98} + (x+2a)^{98})). \quad (4.3.4)$$

Since the 3-ary representation of 98 is $(0,1,0,1,2,2)$ as $98 = 3^4 + 3^2 + 2 \cdot 3 + 2$. Thus, all the monomials in $(x+a)^{98}$ are of the form x^d with

$$d = (0, d_4, 0, d_2, d_1, d_0) \quad (4.3.5)$$

where $d_4, d_2 \in \{0,1\}$ and $d_1, d_0 \in \{0,1,2\}$. The coefficient of the monomial $x^{2 \cdot 3+2}$ in $(x+a)^{98}$ is $a^{3^4+3^2}$. Thus, the coefficient of the monomial $x^{2 \cdot 3+2}$ in Equation (4.3.4) is

$$\alpha^7(a^{3^4+3^2} + (2a)^{3^4+3^2}) = (1 + 2^{3^4+3^2})\alpha^7 a^{3^4+3^2} = 2\alpha^7 a^{3^4+3^2}$$

as $2^{3^4+3^2} \equiv 1 \pmod 3$. Since $3^i(2 \cdot 3 + 2) \not\equiv 2 \cdot 3 + 2 \pmod{728}$, for all $1 \leq i \leq 5$. It is also obvious that, $3^i d \not\equiv (0,0,0,0,2,2) \pmod{728}$, for all $1 \leq i \leq 5$ where d is defined as in Equation (4.3.5) with $d \neq (0,0,0,0,2,2)$. If $\mathcal{S}_V f(x) = 0$ for all $x \in \mathbb{F}_{3^6}$ then all the coefficient of the monomial in Equation (4.3.4) must equal 0, and therefore $2\alpha^7 a^{3^4+3^2} = 0$, which is a contradiction. Thus, we can not find a subspace E of $\mathbb{F}_{3^6}$ with dimension 3 such that the subspace sum of f with respect to any one dimensional subspace of E is 0. ■

Chapter 5

Construction of $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ classes of bent functions

5.1 Introduction

In this chapter, we consider the *generalized Boolean functions* from $\mathbb{F}_p^{2n}$ to $\mathbb{F}_p$ where p is an odd prime integer. In binary case, Carlet [17] constructed two new classes (so-called $\mathcal{C}$, $\mathcal{D}$) of bent functions by modifying the Maiorana–McFarland bent functions. In chapter 3, we derived some existence and nonexistence results concerning the bent functions in the $\mathcal{C}$ class for many of the known classes of permutations over $\mathbb{F}_{2^n}$. We construct two new classes of *generalized bent functions*, denoted by $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$. Here $\mathcal{D}_0^p$ is a subclass of $\mathcal{D}^p$ and we observe that if $f \in \mathcal{D}_0^p$ is an m variables function then $m \equiv 0 \pmod 4$. Further, we prove that $\mathcal{M}^p$ and $\mathcal{D}_0^p \subseteq \mathcal{D}^p$ are overlapping classes, but in general not included in one another. We further derive some existence and nonexistence results concerning the bent functions in $\mathcal{C}^p$ class for many classes of permutations and suitable linear subspaces of the dimension less than and equal to 2 for $p = 3$.

5.2 Preliminaries

In what follows, p denotes an (arbitrary, but fixed) odd prime number.

Lemma 5.2.1 ([17, Generalization of Lemma 1])**.** *Let E be any linear subspace of $\mathbb{F}_p^n$ and*

$f \in \mathcal{B}_n^p$ be a regular bent, and the dual of f be $\tilde{f}$. Then for any elements $a, b \in \mathbb{F}_p^n$, we have

$$\sum_{x \in -a+E} \zeta^{f(x)-b\cdot x} = p^{\dim E - \frac{n}{2}} \zeta^{a\cdot b} \sum_{x \in b+E^{\perp}} \zeta^{\tilde{f}(x)-a\cdot x}$$

where $\zeta = e^{\frac{2\pi\imath}{p}}$ is the p^{th} complex root of unity, $\imath^2 = -1$.

If $a = b = 0$ and $\dim E = \frac{n}{2}$ ($\dim E$ denotes the dimension of a vector space E) then from Lemma 5.2.1, we get

$$\sum_{x \in E} \zeta^{f(x)} = \sum_{x \in E^{\perp}} \zeta^{\tilde{f}(x)}.$$

Therefore, if the restriction $f_{/E}$ of f to E is i then also the restriction $\tilde{f}_{/E^{\perp}}$ of $\tilde{f}$ to $E^{\perp}$ is i where $i \in \{0, 1, \ldots, p-1\}$. In [17, page 85], Carlet constructed a *generalized bent function* in the following way. Let q be any even positive integer and $\mathbb{Z}_q$ be the ring of integers modulo q. Let E be any subgroup of order q^n of $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$ and π any permutation on $\mathbb{Z}_q^n$ such that $x \cdot \pi(y) = 0$, for any $(x, y) \in E$. Then the function $f : \mathbb{Z}_q^n \times \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q$, defined as

$$f(x, y) = x \cdot \pi(y) + \frac{q}{2}\phi_E(x, y), \tag{5.2.1}$$

is bent.

5.3 Construction of $\mathcal{D}^p$ and $\mathcal{D}_0^p$ classes of bent functions

We modify the Carlet's construction defined as in Equation (5.2.1) (for the environment in consideration) in our next theorem where we further show that the functions are also regular.

Theorem 5.3.1. *Let $E = E_1 \times E_2$ where $E_1, E_2 \subseteq \mathbb{F}_p^n$ with $\dim E_1 + \dim E_2 = n$ and $\epsilon \in \mathbb{F}_p$. The generalized Boolean function f on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form*

$$f(x, y) = x \cdot \pi(y) + \epsilon\phi_E(x, y)$$

is a regular generalized bent function where π is an arbitrary permutation polynomial over $\mathbb{F}_p^n$ such that $\pi(E_2) = E_1^{\perp}$.

Proof. Let $(a,b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ and $\zeta = e^{\frac{2\pi\imath}{p}}$ be the p^{th} complex root of unity, $\imath^2 = -1$. From Theorem 4.2.3, we have

$$\sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} = p^n\zeta^{-b\cdot\pi^{-1}(a)},$$

so

$$\begin{aligned}
\mathcal{H}_f(a,b) &= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)+\epsilon\phi_E(x,y)-a\cdot x-b\cdot y}\\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n\setminus E} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + \zeta^{\epsilon}\sum_{(x,y)\in E}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y}\\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + (\zeta^{\epsilon}-1)\sum_{(x,y)\in E}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \qquad (5.3.1)\\
&= p^n\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^{\epsilon}-1)\sum_{(x,y)\in E}\zeta^{-a\cdot x-b\cdot y}\\
&= p^n(\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^{\epsilon}-1)\phi_{E^{\perp}}(a,b)).
\end{aligned}$$

Let $(a,b) \notin E^{\perp}$. Then $\phi_{E^{\perp}}(a,b) = 0$, and so,

$$\sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{f(x,y)-a\cdot x-b\cdot y} = p^n\zeta^{-b\cdot\pi^{-1}(a)} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E^{\perp}}(a,b)}. \qquad (5.3.2)$$

Let $(a,b) \in E^{\perp}$. Then $b\cdot\pi^{-1}(a) = 0$ (by Lemma 5.2.1) and $\phi_{E^{\perp}}(a,b) = 1$, and so,

$$\sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{f(x,y)-a\cdot x-b\cdot y} = p^n\zeta^{\epsilon} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E^{\perp}}(a,b)}. \qquad (5.3.3)$$

From (5.3.1), (5.3.2) and (5.3.3), we infer

$$\mathcal{H}_f(a,b) = p^n\zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E^{\perp}}(a,b)}, \text{ for all } (a,b)\in\mathbb{F}_p^n\times\mathbb{F}_p^n.$$

Thus, f is a regular *generalized bent Boolean function.* ■

Remark 5.3.2. *The dual of a function f as in Theorem* 5.3.1 *is*

$$\tilde{f}(x,y) = y\cdot\pi^{-1}(x) + \epsilon\phi_{E^{\perp}}(x,y),$$

for all $(x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$, *and the set of all such functions* f *is denoted by* $\mathcal{D}^p$.

Lemma 5.3.3. *Let* $n = 2t$ *be an even integer and* p *be an odd prime. Then for all* $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_p^n$,

$$\phi_{E_0}(x, y) = \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j)$$

where $E_0 = \{0\} \times \mathbb{F}_p^n$.

Proof. We know that

$$\phi_{E_0}(x, y) = \begin{cases} 1, & \text{if } \ x = 0; \\ 0, & \textit{otherwise.} \end{cases}$$

If $x \neq 0$, there exists at least one $j \in \{1, 2, \ldots, n\}$ such that $x_j \neq 0$, so $\prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j) = 0$. Assume now that $x = 0$. Then

$$\prod_{i=1}^{n} \prod_{j=1}^{p-1} (0 - j) = \prod_{i=1}^{n} (p-1)! = 1 = ((p-1)!)^n = ((p-1)!)^{2t},$$

using Wilson's Theorem, $(p - 1)! \equiv -1 \pmod{p}$, which renders

$$\prod_{i=1}^{n} \prod_{j=1}^{q-1} (x_i - j) = 1,$$

and the lemma is shown. ■

For the special case of Theorem 5.3.1, we let $E_1 = \{0\}$, $E_2 = \mathbb{F}_p^n$ and $E_0 = \{0\} \times \mathbb{F}_p^n$ where n is even. Then the *generalized Boolean functions* on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form

$$f(x, y) = x \cdot \pi(y) + \epsilon \phi_{E_0}(x, y) = x \cdot \pi(y) + \epsilon \prod_{i=1}^{n} \prod_{j=1}^{p-1} (x_i - j)$$

is a regular *generalized bent function.* This class of bent functions will be denoted by $\mathcal{D}_0^p$ and it is a subclass of $\mathcal{D}^p$. Observe that if $f \in \mathcal{D}_0^p$ is an m variables Boolean function then $m \equiv 0 \pmod{4}$.

The next theorem surprisingly shows that $\mathcal{M}^p$ and $\mathcal{D}_0^p \subseteq \mathcal{D}^p$ are overlapping classes, but in general not included in one another.

Theorem 5.3.4. *In general, $\mathcal{D}_0^p$ and $\mathcal{D}^p$ are not included in the class $\mathcal{M}^p$. Further, the class $\mathcal{M}^p$ is in general not included in $\mathcal{D}_0^p$ and $\mathcal{D}^p$ classes.*

Proof. Let $f \in \mathcal{D}^p$ written as

$$f(x, y) = x \cdot \pi(y) + \epsilon\phi_E(x, y) \tag{5.3.4}$$

with $\epsilon \in \mathbb{F}_p$, $E = E_1 \times E_2$ where $E_1, E_2 \subseteq \mathbb{F}_p^n$ of $\dim E_1 + \dim E_2 = n$ and π be a permutation over $\mathbb{F}_p^n$ such that $\pi(E_2) = E_1^\perp$.

Assume that $f \in \mathcal{M}^p$, and so, f can be expressed as

$$f(x, y) = x \cdot \pi_1(y) + g(y) \tag{5.3.5}$$

where π_1 is a permutation over $\mathbb{F}_p^n$ and $g \in \mathcal{B}_n^p$. Putting $x = 0$ in both Equations (5.3.4) and (5.3.5), we get $g(y) = \epsilon\phi_E(0, y)$, and so,

$$x \cdot (\pi(y) - \pi_1(y)) = \epsilon(\phi_E(0, y) - \phi_E(x, y)). \tag{5.3.6}$$

Observe now that the left hand part of Equation (5.3.6) is linear with respect to the variable x, as opposed to the right hand part of Equation (5.3.6) which may not be linear with respect to the variable x (by choosing a suitable nonlinear function $\phi_E(x, y)$ and $\epsilon \neq 0$). Thus, in general, the classes $\mathcal{D}_0^p$ and $\mathcal{D}^p$ are not included in class $\mathcal{M}^p$.

For example, if $p = 3$ and $n = 4$, we let $f : \mathbb{F}_3^4 \times \mathbb{F}_3^4 \to \mathbb{F}_3$,

$$f(x, y) = x \cdot \pi(y) + \epsilon(x_1 - 1)(x_1 - 2)(x_2 - 1)(x_2 - 2)(x_3 - 1)(x_3 - 2)(x_4 - 1)(x_4 - 2)$$

where $x = (x_1, x_2, x_3, x_4), y = (y_1, y_2, y_3, y_4) \in \mathbb{F}_3^4$ and $\epsilon \in \mathbb{F}_3^*$. The previous nonlinearity condition on $\phi_E(0, y) - \phi_E(x, y)$ is obviously satisfied, and so $f \in \mathcal{D}_0^p$ does not belong to $\mathcal{M}^p$.

Conversely, let $f \in \mathcal{M}^p$, and assume that it also belongs to $\mathcal{D}^p$. Thus, for all $(x, y) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$

$$f(x, y) = x \cdot \psi(y) + g(y) = x \cdot \psi_1(y) + \epsilon\phi_E(x, y)$$

where ψ and ψ_1 are permutations over $\mathbb{F}_p^n$ and $E = E_1 \times E_2$ where $E_1, E_2 \subseteq \mathbb{F}_p^n$ of $\dim E_1 +$

$\dim E_2 = n$ and $\psi_1(E_2) = E_1^\perp$. Then $g(y) = \epsilon\phi_E(0, y) \in \{0, \epsilon\}$, for all $y \in \mathbb{F}_p^n$, that is, the range set of g contain at most two distinct elements. Therefore, if the range set of g contain at least three distinct elements, the corresponding $\mathcal{M}^p$ functions f does not belong to $\mathcal{D}^p$, and our theorem is shown. ■

5.4 Construction of $\mathcal{C}^p$ class of bent functions

The $\mathcal{C}$ class of bent functions was constructed by Carlet [17], which is defined as in Equation (1.2.13). We now generalize Carlet's result.

Theorem 5.4.1. *Let L be any linear subspace of $\mathbb{F}_p^n$ and π be any permutation on $\mathbb{F}_p^n$ such that for any element λ of $\mathbb{F}_p^n$, the set $\pi^{-1}(\lambda + L)$ is a flat. Then the function f on $\mathbb{F}_p^n \times \mathbb{F}_p^n$ of the form*

$$x \cdot \pi(y) + \epsilon\phi_{L^\perp}(x)$$

is a generalized bent function where $\epsilon \in \mathbb{F}_p$.

Proof. Let $E = L^\perp \times \mathbb{F}_p^n$ and $\zeta = e^{\frac{2\pi\imath}{p}}$ be the p^{th} complex root of unity, $\imath^2 = -1$. For any $(a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$, we have

$$\begin{aligned}
\mathcal{H}_f(a,b) &= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n} \zeta^{x\cdot\pi(y)+\epsilon\phi_{L^\perp}(x)-a\cdot x-b\cdot y} \\
&= \sum_{y\in\mathbb{F}_p^n}\left(\sum_{x\in\mathbb{F}_p^n\setminus L^\perp}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + \zeta^\epsilon\sum_{x\in L^\perp}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y}\right) \\
&= \sum_{(x,y)\in\mathbb{F}_p^n\times\mathbb{F}_p^n}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} + (\zeta^\epsilon - 1)\sum_{(x,y)\in L^\perp\times\mathbb{F}_p^n}\zeta^{x\cdot\pi(y)-a\cdot x-b\cdot y} \qquad (5.4.1) \\
&= p^n\zeta^{-b\cdot\pi^{-1}(a)} + (\zeta^\epsilon - 1)|L^\perp|\sum_{x\in a+L}\zeta^{-b\cdot\pi^{-1}(x)}, \quad \text{using Lemma 5.2.1} \\
&= p^n\left(\zeta^{-b\cdot\pi^{-1}(a)} + \frac{(\zeta^\epsilon - 1)}{|L|}\sum_{x\in\pi^{-1}(a+L)}\zeta^{-b\cdot x}\right).
\end{aligned}$$

Let $E_a = \{\pi^{-1}(a + u) : u \in L\}$. If $b \notin E_a^\perp$ then $\sum_{x\in\pi^{-1}(a+L)}\zeta^{-b\cdot x} = 0$, and from Equation (5.4.1) we get

$$\mathcal{H}_f(a,b) = p^n(-1)^{-b\cdot\pi^{-1}(a)} = p^n\zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E_a^\perp}(b)}. \qquad (5.4.2)$$

If $b \in E_a^{\perp}$ then $b \cdot \pi^{-1}(a) = 0$ and $\sum\limits_{x \in \pi^{-1}(a+L)} \zeta^{-b\cdot x} = |L|$. From Equation (5.4.1) we get

$$\mathcal{H}_f(a,b) = p^n \zeta^{\epsilon} = p^n \zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E_a^{\perp}}(b)}. \qquad (5.4.3)$$

Therefore, from Equations (5.4.1), (5.4.2) and (5.4.3) we get

$$\mathcal{H}_f(a,b) = p^n \zeta^{-b\cdot\pi^{-1}(a)+\epsilon\phi_{E_a^{\perp}}(b)}, \text{ for all } (a,b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n,$$

and the theorem is shown. ■

The class of bent functions defined as in Theorem 5.4.1 will be denoted by $\mathcal{C}^p$.

Corollary 5.4.2. *In general, the class $\mathcal{C}^p$ is not included in the class $\mathcal{M}^p$.*

Proof. Let $f \in \mathcal{C}^p$. If $L = \mathbb{F}_p^n$, the class $\mathcal{C}^p$ contains the class $\mathcal{D}_0^p$, and so, also $\mathcal{C}^p$ is not included in the $\mathcal{M}^p$ class. ■

5.5 Existence and nonexistence of $\mathcal{C}^p$ classes of bent functions

For construction of *generalized bent functions* defined as in Theorem 5.4.1, it is needed to consider a permutation polynomial π on $\mathbb{F}_p^n$ such that $\pi^{-1}(a+L)$ is a flat for any $a \in \mathbb{F}_p^n$. In chapter 3, we derived some existence and nonexistence results concerning the bent functions in the $\mathcal{C}$ class for many of the known classes of permutations over $\mathbb{F}_{2^n}$. We investigate below these conditions for many classes of permutations and suitable linear subspaces of the dimension less than and equal to 2 for $p = 3$.

Lemma 5.5.1. *Let $u_1, u_2, u_3 \in \mathbb{F}_3^n$. A set $L = \{u_1, u_2, u_3\}$ is flat of $\mathbb{F}_3^n$ of dimension ≤ 1 if and only if $u_1 + u_2 + u_3 = 0$.*

Proof. If L is a subspace, without loss of generality, we may assume that $L = \{0, u_1, 2u_1\}$, which satisfies $0 + u_1 + 2u_1 = 0$. Conversely let $L = \{u_1, u_2, u_3\}$ with $u_1 + u_2 + u_3 = 0$, i.e., $u_3 = 2u_1 + 2u_2$. It follows that $2u_1 + L = \{0, u_2 + 2u_1, u_1 + 2u_2\} = \langle u_1 + 2u_2 \rangle$. The lemma is proved. ■

Theorem 5.5.2. *Consider the permutation polynomial over $\mathbb{F}_{3^4}$, $\phi(x) = x + x^{17}$* [72]*. Then there is no* 1*-dimensional subspace L of $\mathbb{F}_{3^4}$ such that $\phi(a+L)$ is flat for all $a \in \mathbb{F}_{3^4}$.*

Proof. Let $L = \{0, u, 2u\}$, $u \in \mathbb{F}_{3^4}^*$. Then for any $a \in \mathbb{F}_{3^4}$, $\phi(a+L)$ is flat if and only if

$$\begin{aligned} &\phi(a) + \phi(a+u) + \phi(a+2u) = 0 \Leftrightarrow a^{17} + (a+u)^{17} + (a+2u)^{17} = 0 \\ \Leftrightarrow &2a^{15}u^2 + 2a^{13}u^4 + 2a^{11}u^6 + 2a^9u^8 + a^7u^{10} + a^5u^{12} + a^3u^{14} + au^{16} = 0. \end{aligned} \tag{5.5.1}$$

Equation (5.5.1) holds for all $a \in \mathbb{F}_{3^4}$ if and only if $u = 0$, which contradicts $\dim L = 1$. ■

Remark 5.5.3. *We can certainly construct functions in $\mathcal{C}^3$. For example, consider the permutation polynomial $\phi(x) = 1 + x$ over $\mathbb{F}_{3^4}$* [104, Theorem 1.1]*. Then for any* 1*-dimensional subspace L of $\mathbb{F}_{3^4}$, $\phi(a+L)$ is flat for all $a \in \mathbb{F}_{3^4}$, since, for $L = \{0, u, 2u\}$, $u \in \mathbb{F}_{3^4}^*$, then $\phi(a) + \phi(a+u) + \phi(a+2u) = 0$, for all $a \in \mathbb{F}_{3^4}$. If $L = \langle u, v\rangle$ is a* 2*-dimensional subspace of $\mathbb{F}_{3^4} \times \mathbb{F}_{3^4}$ and $a \in \mathbb{F}_{3^4}$ then*

$$\begin{aligned} \phi(a+L) = \{&\phi(a), \phi(a+u), \phi(a+v), \phi(a+u+v), \phi(2u), \phi(2v), \phi(a+2u), \phi(a+2v), \\ &\phi(a+2u+v), \phi(a+u+2v), \phi(a+2u+2v)\} = 1 + a + L. \end{aligned}$$

Theorem 5.5.4. *Let ϕ be a permutation polynomial defined as in* [72] *on $\mathbb{F}_{3^4}$ of the form*

$$\phi(x) = x(x^{16} + 1) = x^{17} + x.$$

Then there is no 2*-dimensional subspace $L = \langle u, v\rangle$ such that $\phi(a+L)$ is flat for all $a \in \mathbb{F}_{3^4}$.*

Proof. Let $a \in \mathbb{F}_{3^4}$. If $\phi(a+L)$ is a flat,

$$\begin{aligned} &\phi(a) + \phi(a+u) + \phi(a+v) + \phi(a+u+v) + \phi(a+2u) + \phi(a+2v) + \\ &\phi(a+2u+v) + \phi(a+u+2v) + \phi(a+2u+2v) = 0. \end{aligned} \tag{5.5.2}$$

The linear part of Equation (5.5.2) certainly sums to 0. Furthermore,

$$\begin{aligned} (a+u)^{17} &= a^{17} + 2a^{16}u + a^{15}u^2 + 2a^{14}u^3 + a^{13}u^4 + 2a^{12}u^5 + a^{11}u^6 + 2a^{10}u^7 + a^9u^8 \\ &\quad + a^8u^9 + 2a^7u^{10} + a^6u^{11} + 2a^5u^{12} + a^4u^{13} + 2a^3u^{14} + a^2u^{15} + 2au^{16} + u^{17}, \\ (a+v)^{17} &= a^{17} + 2a^{16}v + a^{15}v^2 + 2a^{14}v^3 + a^{13}v^4 + 2a^{12}v^5 + a^{11}v^6 + 2a^{10}v^7 + a^9v^8 \\ &\quad + a^8v^9 + 2a^7v^{10} + a^6v^{11} + 2a^5v^{12} + a^4v^{13} + 2a^3v^{14} + a^2v^{15} + 2av^{16} + v^{17}, \end{aligned}$$

$$\begin{aligned}
(a{+}u+v)^{17} &= a^{17}+2a^{16}(u+v)+a^{15}(u+v)^2+2a^{14}(u+v)^3+a^{13}(u+v)^4\\
&\quad+2a^{12}(u+v)^5+a^{11}(u+v)^6+2a^{10}(u+v)^7+a^9(u+v)^8+a^8(u+v)^9+2a^7(u\\
&\quad+v)^{10}+a^6(u+v)^{11}+2a^5(u+v)^{12}+a^4(u+v)^{13}+2a^3(u+v)^{14}+a^2(u+v)^{15}\\
&\quad+2a(u+v)^{16}+(u+v)^{17},\\
(a{+}2u)^{17} &= a^{17}+2a^{16}(2u)+a^{15}(2u)^2+2a^{14}(2u)^3+a^{13}(2u)^4+2a^{12}(2u)^5\\
&\quad+a^{11}(2u)^6+2a^{10}(2u)^7+a^9(2u)^8+a^8(2u)^9+2a^7(2u)^{10}+a^6(2u)^{11}\\
&\quad+2a^5(2u)^{12}+2a^3(2u)^{14}+a^2(2u)^{15}+2a(2u)^{16}+(2u)^{17},\\
(a{+}2v)^{17} &= a^{17}+2a^{16}(2v)+a^{15}(2v)^2+2a^{14}(2v)^3+a^{13}(2v)^4+2a^{12}(2v)^5\\
&\quad+a^{11}(2v)^6+2a^{10}(2v)^7+a^9(2v)^8+a^8(2v)^9+2a^7(2v)^{10}+a^6(2v)^{11}\\
&\quad+2a^5(2v)^{12}+a^4(2v)^{13}+2a^3(2v)^{14}+a^2(2v)^{15}+2a(2v)^{16}+(2v)^{17},\\
(a{+}2u+v)^{17} &= a^{17}+2a^{16}(2u+v)+a^{15}(2u+v)^2+2a^{14}(2u+v)^3+a^{13}(2u+v)^4\\
&\quad+2a^{12}(2u+v)^5+a^{11}(2u+v)^6+2a^{10}(2u+v)^7+a^9(2u+v)^8+a^8(2u+v)^9\\
&\quad+2a^7(2u+v)^{10}+a^6(2u+v)^{11}+2a^5(2u+v)^{12}+a^4(2u+v)^{13}+2a^3(2u+v)^{14}\\
&\quad+a^2(2u+v)^{15}+2a(2u+v)^{16}+(2u+v)^{17},\\
(a{+}u+2v)^{17} &= a^{17}+2a^{16}(u+2v)+a^{15}(u+2v)^2+2a^{14}(u+2v)^3\\
&\quad+a^{13}(u+2v)^4+2a^{12}(u+2v)^5+a^{11}(u+2v)^6+2a^{10}(u+2v)^7+a^9(u+2v)^8\\
&\quad+a^8(u+2v)^9+2a^7(u+2v)^{10}+a^6(u+2v)^{11}+2a^5(u+2v)^{12}+a^4(u+2v)^{13}\\
&\quad+2a^3(u+2v)^{14}+a^2(u+2v)^{15}+2a(u+2v)^{16}+(u+2v)^{17},\\
(a+2u+2v)^{17} &= a^{17}+2a^{16}(2u+2v)+a^{15}(2u+2v)^2+2a^{14}(2u+2v)^3\\
&\quad+a^{13}(2u+2v)^4+2a^{12}(2u+2v)^5+a^{11}(2u+2v)^6+2a^{10}(2u+2v)^7+a^9(2u+2v)^8\\
&\quad+a^8(2u+2v)^9+2a^7(2u+2v)^{10}+a^6(2u+2v)^{11}+2a^5(2u+2v)^{12}+a^4(2u+2v)^{13}\\
&\quad+2a^3(2u+2v)^{14}+a^2(2u+2v)^{15}+2a(2u+2v)^{16}+(2u+2v)^{17}.
\end{aligned}$$

Adding all these equations, and collecting powers of a, we obtain

$$\begin{aligned}
&9a^{17}=0,\\
&2a^{16}\left(u+v+(u+v)+2u+2v+(2u+v)+(u+2v)+(2u+2v)\right)=0,\\
&a^{15}\left(u^2+v^2+(u+v)^2+(2u)^2+(2v)^2+(2u+v)^2+(u+2v)^2+(2u+2v)^2\right)=0,
\end{aligned}$$

$$\begin{aligned}
&2a^{14}\left(u^3+v^3+(u+v)^3+(2u)^3+(2v)^3+(2u+v)^3+(u+2v)^3+(2u+2v)^3\right)=0,\\
&a^{13}\left(u^4+v^4+(u+v)^4+(2u)^4+(2v)^4+(2u+v)^4+(u+2v)^4+(2u+2v)^4\right)=0,\\
&2a^{12}\left(u^5+v^5+(u+v)^5+(2u)^5+(2v)^5+(2u+v)^5+(u+2v)^5+(2u+2v)^5\right)=0,\\
&a^{11}\left(u^6+v^6+(u+v)^6+(2u)^6+(2v)^6+(2u+v)^6+(u+2v)^6+(2u+2v)^6\right)=0,\\
&2a^{10}\left(u^7+v^7+(u+v)^7+(2u)^7+(2v)^7+(2u+v)^7+(u+2v)^7+(2u+2v)^7\right)=0,\\
&a^{9}\left(u^8+v^8+(u+v)^8+(2u)^8+(2v)^8+(2u+v)^8+(u+2v)^8+(2u+2v)^8\right)\\
&\quad=a^9(u^6v^2+u^4v^4+u^2v^6),\\
&a^{8}\left(u^9+v^9+(u+v)^9+(2u)^9+(2v)^9+(2u+v)^9+(u+2v)^9+(2u+2v)^9\right)=0,\\
&2a^{7}\left(u^{10}+v^{10}+(u+v)^{10}+(2u)^{10}+(2v)^{10}+(2u+v)^{10}+(u+2v)^{10}+(2u+2v)^{10}\right)=0,\\
&a^{6}\left(u^{11}+v^{11}+(u+v)^{11}+(2u)^{11}+(2v)^{11}+(2u+v)^{11}+(u+2v)^{11}+(2u+2v)^{11}\right)=0,\\
&2a^{5}\left(u^{12}+v^{12}+(u+v)^{12}+(2u)^{12}+(2v)^{12}+(2u+v)^{12}+(u+2v)^{12}+(2u+2v)^{12}\right)=0,\\
&a^{4}\left(u^{13}+v^{13}+(u+v)^{13}+(2u)^{13}+(2v)^{13}+(2u+v)^{13}+(u+2v)^{13}+(2u+2v)^{13}\right)=0,\\
&2a^{3}\left(u^{14}+v^{14}+(u+v)^{14}+(2u)^{14}+(2v)^{14}+(2u+v)^{14}+(u+2v)^{14}+(2u+2v)^{14}\right)\\
&\quad=2a^3(u^{12}v^2+2u^{10}v^4+2u^4v^{10}+u^2v^{12}),\\
&a^{2}\left(u^{15}+v^{15}+(u+v)^{15}+(2u)^{15}+(2v)^{15}+(2u+v)^{15}+(u+2v)^{15}+(2u+2v)^{15}\right)=0,\\
&2a\left(u^{16}+v^{16}+(u+v)^{16}+(2u)^{16}+(2v)^{16}+(2u+v)^{16}+(u+2v)^{16}+(2u+2v)^{16}\right)\\
&\quad=2a(2u^{12}v^4+u^{10}v^6+u^6v^{10}+2u^4v^{12}),\\
&u^{17}+v^{17}+(u+v)^{17}+(2u)^{17}+(2v)^{17}+(2u+v)^{17}+(u+2v)^{17}+(2u+2v)^{17}=0.
\end{aligned}$$

From (5.5.2), we get that if $\phi(a+L)$ is flat then

$$\begin{aligned}
&a(u^{12}v^4+2u^{10}v^6+2u^6v^{10}+u^4v^{12})+a^3(2u^{12}v^2+u^{10}v^4+u^4v^{10}+2u^2v^{12})+\\
&\qquad a^9(u^6v^2+u^4v^4+u^2v^6)=0,
\end{aligned}$$

which is satisfied for all $a\in\mathbb{F}_{3^4}$ only when

$$\begin{aligned}
&u^{12}v^4+2u^{10}v^6+2u^6v^{10}+u^4v^{12}=0,\\
&2u^{12}v^2+u^{10}v^4+u^4v^{10}+2u^2v^{12}=0,\\
&u^6v^2+u^4v^4+u^2v^6=0.
\end{aligned}$$

Since

$$\begin{aligned}
& u^6v^2 + u^4v^4 + u^2v^6 = 0 \\
\Leftrightarrow\ & u^4 + u^2v^2 + v^4 = 0, \ \text{ as } \ u, v \neq 0 \\
\Leftrightarrow\ & (2u^2 + v^2)^2 = 0 \ \text{ or } \ (u^2 + 2v^2)^2 = 0 \\
\Leftrightarrow\ & u = v \ \text{ or } \ u = 2v,
\end{aligned}$$

which is not possible as u and v are linearly independent. ■

Chapter 6

Second-order Nonlinearity Bounds of cubic MMF bent-negabent functions constructed by using Feistel functions

6.1 Introduction

The nega–Hadamard transform of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$ is the complex valued function

$$\mathcal{N}_f(a) = 2^{-\frac{n}{2}} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ax)} \imath^{wt(x)}$$

where $\imath^2 = -1$. The multiset $[\mathcal{N}_f(a) : a \in \mathbb{F}_{2^n}]$ is said to be the nega spectrum of f.

Definition 6.1.1. *A function $f \in \mathcal{B}_n$ is said to be negabent if and only if $|\mathcal{N}_f(a)| = 1$, for all $a \in \mathbb{F}_{2^n}$.*

Note that all affine functions (both with an even and an odd numbers of variables) are negabent. For an even number of variables, a negabent function is called bent-negabent if it is also a bent function. The bent-negabent functions was introduced by Riera and Parker [33]. Construction of bent-negabent functions was proposed by Parker and Pott [73], and negabent functions in Maiorana–McFarland class was considered by Schmidt, Parker and Pott [64].

A permutation $\phi : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is said to be complete mapping polynomial if $x \mapsto \phi(x)+x$ is also a permutation. A Feistel function $\pi : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \longrightarrow \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ is defined as $\pi(x, y) =$

$(y, x+h(y))$, for all $x, y \in \mathbb{F}_{2^t}$ where h is any function on $\mathbb{F}_{2^t}$. It is proved by Markovski and Mileva [118] that if h is a permutation then the Feistel function π is a complete mapping permutation. Using the permutation π it possible to construct a Maiorana–McFarland type bent functions

$$f : (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \longrightarrow \mathbb{F}_2$$

defined by $f((x_1, x_2), (y_1, y_2)) = (x_1, x_2) \cdot \pi(y_1, y_2)$, for all $x_j, y_j \in \mathbb{F}_{2^t}$, $j = 1, 2$. If h is permutation then π is a complete mapping polynomial, which implies that the function f is affine equivalent to a bent-negabent function (cf. [97]). The maximum algebraic degree of π is $t-1$ and therefore it is possible to obtain bent-negabent functions of algebraic degree t by using this technique. For further details we refer to [9, 64, 73, 146]

In the next section we concentrate our effort on a particular class of cubic Maiorana–McFarland bent-negabent functions and determine the weights of their second derivative along with a lower bound of their second-order nonlinearities. Also we identify subclasses bent-negabent functions within this class.

6.2 Main results

In this section we take $m = 4t$ and $t \geq 3$. Let $h(y) = y^{2^i+1}$, for all $y \in \mathbb{F}_{2^t}$ where $\gcd(t, i) = e$ and $i \in \mathbb{Z}$ such that $1 \leq i < t$, $\gcd(2^i + 1, 2^t - 1) = 1$. Since h is a permutation we obtain cubic Maiorana–McFarland bent-negabent functions of the form

$$f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t(x_1 y_2 + x_2 y_1 + x_2 y_2^{2^i+1}), \tag{6.2.1}$$

for all $x_j, y_j \in \mathbb{F}_{2^t}$, $j = 1, 2$.

Lemma 6.2.1. *The cubic Maiorana–McFarland bent-negabent function f_i defined as in Equation (6.2.1) has affine derivatives at $((a_1, 0), (b_1, 0))$ where $a_1, b_1 \in \mathbb{F}_{2^t}$.*

Proof. Let $((a_1, a_2), (b_1, b_2)) \in (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t})$. Then

$$\begin{aligned} D_{((a_1,a_2),(b_1,b_2))} f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t(&a_2 y_2^{2^i+1} + (x_2 + a_2)(y_2^{2^i} b_2 + y_2 b_2^{2^i}) + x_2 b_2^{2^i+1} + \\ &x_1 b_2 + a_1 y_2 + x_2 b_1 + a_2 y_1) + f_i((a_1, a_2), (b_1, b_2)). \end{aligned} \tag{6.2.2}$$

If $a_2 \neq 0$ then Equation (6.2.2) is quadratic. Suppose that $a_2 = 0$. Then Equation (6.2.2) is affine if and only if $p(y_2) = y_2^{2^i} b_2 + y_2 b_2^{2^i}$ is constant for all $y_2 \in \mathbb{F}_{2^t}$. Since $p(0)$ is equal to 0, that is, Equation (6.2.2) is affine if and only if for all $y_2 \in \mathbb{F}_{2^t}$,

$$y_2^{2^i} b_2 + y_2 b_2^{2^i} = 0. \tag{6.2.3}$$

If $b_2 = 0$ then Equation (6.2.3) is identically zero. If $b_2 \neq 0$ then Equation (6.2.3) holds only when $y_2 = \alpha b_2$ where $\alpha \in \mathbb{F}_{2^e}$, and the lemma is shown. ■

6.2.1 Affine inequivalence subclasses

Theorem 6.2.2. *Let V be any 2-dimensional subspace of $(\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t})$. Then the number of such distinct subspaces on which $D_V f_i$ is constant is given by*

$$\frac{(2^t - 1)(2^{5t+e-1}(2^e + 1) + (2^t + 1)(2^{4t-1} - 2^{2t} - 1))}{3}$$

where f_i is defined as in Equation (6.2.1).

Proof. Let, $V = \langle ((a_1, a_2), (b_1, b_2)), ((c_1, c_2), (d_1, d_2)) \rangle$ be any 2-dimensional subspace of $(\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t})$. The second derivative of f_i with respect to V is

$$\begin{aligned} D_V f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t((a_1 d_2 + b_2 c_1) + (a_2 d_1 + b_1 c_2) + ((a_2 d_2 + b_2 c_2) + (a_2 d_2^{2^i} + \\ b_2^{2^i} c_2)^{2^i}) y_2^{2^i} + (a_2 + c_2)(b_2^{2^i} d_2 + b_2 d_2^{2^i}) + (b_2^{2^i} d_2 + b_2 d_2^{2^i}) x_2 + (a_2 d_2^{2^i+1} + b_2^{2^i+1} c_2)). \end{aligned} \tag{6.2.4}$$

Case 1*:* Let (b_1, b_2)=(d_1, d_2)=$(0, 0)$. Then $V = \langle ((a_1, a_2), (0, 0)), ((c_1, c_2), (0, 0)) \rangle$ and $D_V f_i((x_1, x_2), (y_1, y_2)) = 0$, for all $x_j, y_j \in \mathbb{F}_{2^t}$, $j = 1, 2$. Thus, with respect to any 2-dimensional subspace of $(\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\{0\} \times \{0\})$ the second derivative of f_i is 0. The number of such distinct 2-dimensional subspace is $\frac{(2^{2t}-1)(2^{2t-1}-1)}{3}$.
Case 2*:* Let $b_2 = 0$ and $d_2 \neq 0$. Then from Equation (6.2.4), we get

$$D_V f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t((a_1 d_2 + (a_2 d_1 + b_1 c_2) + (a_2 d_2^{2^i+1}) + (a_2 d_2 + (a_2 d_2^{2^i})^{2^i}) y_2^{2^i}),$$

which is constant if and only if $a_2 d_2 + (a_2 d_2^{2^i})^{2^i} = 0$.

Subcase (i): Let $a_2 \neq 0$. Then $a_2 d_2 \neq 0$, and so,

$$\begin{aligned} & a_2 d_2 + (a_2 d_2^{2^i})^{2^i} = 0 \Leftrightarrow a_2^{2^i} d_2^{2^{2i}} = a_2 d_2 \\ \Leftrightarrow\ & a_2^{2^i-1} d_2^{2^{2i}-1} = 1, \text{ since } a_2 \neq 0, d_2 \neq 0 \\ \Leftrightarrow\ & (a_2 d_2^{2^i+1})^{2^i-1} = 1 \Leftrightarrow a_2 d_2^{2^i+1} \in \mathbb{F}_{2^i}^* \\ \Leftrightarrow\ & a_2 d_2^{2^i+1} \in \mathbb{F}_{2^e}^* \text{ as } \gcd(i,t) = e. \end{aligned}$$

For any $a_2 \in \mathbb{F}_{2^t}^*$, it is possible to chose d_2 in $2^e - 1$ ways. a_1, b_1, c_1, c_2, d_1 can be chosen in 2^t ways and a_2 in $2^t - 1$ ways. Again the subspace generated by $\{((a_1, a_2), (b_1, 0)), ((c_1, c_2), (d_1, d_2))\}$ is same as the subspace generated by $\{((a_1, a_2), (b_1, 0)), ((a_1 + c_1, a_2 + c_2), (b_1 + d_1, d_2))\}$. Therefore, the total number of distinct 2-dimensional subspace such that the second derivative of f_i is constant is equal to $\frac{2^t(2^t-1)2^t 2^{2t} 2^t (2^e-1)}{2} = \frac{2^{5t}(2^t-1)(2^e-1)}{2}$.

Subcase (ii): Let $a_2 = 0$. Then $D_V f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t(a_1 d_2 + b_1 c_2)$, which is constant. In this subcase, a_1, b_1, c_1, c_2, d_1 can be chosen in 2^t ways and d_2 in $2^t - 1$ ways except a_1, b_1 both are equal to 0. Therefore, the number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of f_i is $\frac{(2^{2t}-1)2^{3t}(2^t-1)}{2}$.

Case 3: Let b_2=0 and d_2=0. From Equation (6.2.4), we get $D_V f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t(a_2 d_1 + b_1 c_2)$, which is constant.

Subcase (i): Let b_1=0 and $d_1 \neq 0$. Since the subspace generated by $\{((a_1, a_2), (0, 0)), ((c_1, c_2), (d_1, 0))\}$ is same as the subspace generated by $\{((a_1, a_2), (0, 0)), ((a_1 + c_1, a_2 + c_2), (d_1, 0))\}$. Therefore, the number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of f_i is $\frac{(2^{2t}-1)2^{2t}(2^t-1)}{2}$.

Subcase (ii): Let $b_1 \neq 0$ and $d_1 \neq 0$ with $b_1 \neq d_1$. If $b_1 = d_1$ then the subspace generated by $\{((a_1, a_2), (b_1, 0)), ((c_1, c_2), (d_1, 0))\}$ is same as the subspace generated by $\{((a_1 + c_1, a_2 + c_2), (b_1 + d_1, 0)), ((c_1, c_2), (d_1, 0))\}$, i.e., $\{((a_1 + c_1, a_2 + c_2), (0, 0)), ((c_1, c_2), (d_1, 0))\}$. Here a_1, a_2, c_1, c_2, can be chosen in 2^t ways, b_1 in $2^t - 1$ ways and d_1 in $2^t - 2$ ways. Therefore, the number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of f_i is $\frac{2^{2t}(2^t-1)2^{2t}(2^t-2)}{6} = \frac{2^{4t}(2^t-1)(2^t-2)}{6}$.

Case 4: Let $b_2 \neq 0$ and $d_2 \neq 0$ with $b_2 \neq d_2$. If $b_2 = d_2$ then the subspace generated by $\{((a_1, a_2), (b_1, b_2)), ((c_1, c_2), (d_1, d_2))\}$ is same as the subspace generated by $\{((a_1 + c_1, a_2 + c_2), (b_1 + d_1, b_2 + d_2)), ((c_1, c_2), (d_1, d_2))\}$, i.e., $\{((a_1 + c_1, a_2 + c_2), (b_1 +$

$d_1, 0)), ((c_1, c_2), (d_1, d_2))\}$. From Equation (6.2.4), we get $D_V f_i$ is constant if and only if

$$(a_2d_2 + b_2c_2) + (a_2d_2^{2^i} + b_2^{2^i}c_2)^{2^i} = 0 \text{ and } (b_2^{2^i}d_2 + b_2d_2^{2^i}) = 0.$$

Since

$$\begin{aligned} b_2^{2^i}d_2 + b_2d_2^{2^i} = 0 \Leftrightarrow \left(\frac{d_2}{b_2}\right)^{2^i-1} &= 1 \text{ as } b_2 \neq 0, d_2 \neq 0 \\ \Leftrightarrow \frac{d_2}{b_2} \in \mathbb{F}_{2^e}^* \text{ as } \gcd(i,t) = e. \end{aligned}$$

Let $d_2 = b_2\lambda$ where $\lambda \in \mathbb{F}_{2^e}^*$ and $\lambda \neq 1$ as $d_2 \neq b_2$. Thus, for each nonzero $b_2 \in \mathbb{F}_{2^t}$, it is possible to choose d_2 in $2^e - 2$ ways. From the first condition we obtain:

$$\begin{aligned} & a_2d_2 + c_2b_2 + (a_2d_2^{2^i} + c_2b_2^{2^i})^{2^i} = 0 \\ \Leftrightarrow\ & b_2(a_2\lambda + c_2) + (b_2^{2^i}(a_2\lambda + c_2))^{2^i} = 0 \\ \Leftrightarrow\ & (b_2^{2^i+1}(a_2\lambda + c_2))^{2^i-1} = 1, \text{ if } a_2\lambda + c_2 \neq 0 \\ \Leftrightarrow\ & b_2^{2^i+1}(a_2\lambda + c_2) \in \mathbb{F}_{2^i}^* \\ \Leftrightarrow\ & b_2^{2^i+1}(a_2\lambda + c_2) \in \mathbb{F}_{2^e}^*, \text{ as } \gcd(i,t) = e \\ \Leftrightarrow\ & b_2^{2^i+1}(a_2\lambda + c_2) = \lambda' \in \mathbb{F}_{2^e}^* \\ \Leftrightarrow\ & c_2 = a_2\lambda + \frac{\lambda'}{b_2^{2^i+1}}. \end{aligned}$$

Thus, a_1, a_2, b_1, c_1, d_1 can be chosen in 2^t ways, b_2 in $2^t - 1$ ways, c_2 in 2^e ways and d_2 in $2^e - 2$ ways (including the case for which $a_2\lambda + c_2 = 0$). Each 2-dimensional subspace generated by a pair of vectors $((a_1, a_2), (b_1, b_2)), ((c_1, c_2), (d_1, d_2))$, satisfying the above conditions, contains altogether 6 distinct bases satisfying these conditions. Therefore, the number of distinct 2-dimensional subspaces corresponding to constant second-derivatives of f_i is $\frac{2^{5t+e}(2^t-1)(2^e-2)}{6}$.

Adding the all cases we get the result.

■

We obtain the following corollary form Theorem 1.2.39 and Theorem 6.2.2.

Corollary 6.2.3. *If* $\gcd(i,t) \neq \gcd(j,t)$ *then* f_i *and* f_j *are not equivalent where* f_i *and* f_j *are defined as in Equation* (6.2.1).

6.2.2 Second-order nonlinearities

Theorem 6.2.4. *Let $m = 4t$, $t \geq 3$ and i, $1 \leq i < t$ such that* $\gcd(i, t) = e$ *and* $\gcd(2^i + 1, 2^t - 1) = 1$. *Let $f_i \in \mathcal{B}_m$ be a function of the form given by Equation* (6.2.1). *Then*

$$nl_2(f_i) \geq 2^{m-1} - \frac{1}{2}\sqrt{2^{7t+e} - 2^{\frac{11t+e}{2}} + 2^{6t}(2^{\frac{t+e}{2}} - 2^e + 1)}.$$

Proof. Let $a = (a_1, b_1)$ and $b = (b_1, b_2)$ where $a_j, b_j \in \mathbb{F}_{2^t}$, $j = 1,\ 2$. To find $nl_2(f_i)$ it is need to find nonlinearity of $D_{(a,b)}f_i$, for all $(a, b) \in (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t})$. Let $k(a, b)$ be the dimension of the kernel of the bilinear form associated to $D_{(a,b)}f_i$, i.e., the dimension of $\mathcal{E}_{D_{(a,b)}f_i}$. Since

$$\mathcal{E}_{D_{(a,b)}f_i} = \{((c_1, c_2), (d_1, d_2)) \in (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) \times (\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}) : D_{(c,d)}D_{(a,b)}f_i = constant\}$$

where $c = (c_1, c_2)$, $d = (d_1, d_2)$ and $c_j, d_j \in \mathbb{F}_{2^t}$, $j = 1,\ 2$.

$$\begin{aligned} D_{(c,d)}D_{(a,b)}f_i((x_1,x_2),(y_1,y_2)) = \mathrm{Tr}_1^t(&(a_1d_2 + b_2c_1) + (a_2d_1 + b_1c_2) + ((a_2d_2 + b_2c_2)+ \\ &(a_2d_2^{2^i} + b_2^{2^i}c_2)^{2^i})y_2^{2^i} + (a_2 + c_2)(b_2^{2^i}d_2 + b_2d_2^{2^i}) + (b_2^{2^i}d_2 + b_2d_2^{2^i})x_2+ \\ &(a_2d_2^{2^i+1} + b_2^{2^i+1}c_2)). \end{aligned} \tag{6.2.5}$$

Case 1*:* Let $b_2 = 0$. From Equation (6.2.5), we get

$$D_{(c,d)}D_{(a,b)}f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t((a_1d_2 + (a_2d_1 + b_1c_2) + (a_2d_2 + (a_2d_2^{2^i})^{2^i})y_2^{2^i} + a_2d_2^{2^i+1}),$$

which is constant if and only if $a_2d_2 + (a_2d_2^{2^i})^{2^i} = 0$.

Subcase (i): Let $b_2 = 0$ but $a_2 \neq 0$. If $d_2 = 0$ then $D_{(c,d)}D_{(a,b)}f_i((x_1, x_2), (y_1, y_2))$ is constant, for all $x_j, y_j \in \mathbb{F}_{2^t}$, $j = 1, 2$. It is possible to choose c_1, c_2 and d_1 in 2^t ways. Thus, the total number of ways in which $((c_1, c_2), (d_1, 0))$ can be chosen so that $D_{(c,d)}D_{(a,b)}f_i$ is constant is 2^{3t}.

Again if $d_2 \neq 0$ then $D_{(c,d)}D_{(a,b)}f_i$ is constant if and only if

$$\begin{aligned} & a_2d_2 + (a_2d_2^{2^i})^{2^i} = 0 \Leftrightarrow a_2^{2^i}d_2^{2^{2i}} = a_2d_2 \\ \Leftrightarrow\ & (a_2d_2^{2^i+1})^{2^i-1} = 1 \Leftrightarrow a_2d_2^{2^i+1} \in \mathbb{F}_{2^i}^* \\ \Leftrightarrow\ & a_2d_2^{2^i+1} \in \mathbb{F}_{2^e}^* \text{ as } \gcd(i,t) = e. \end{aligned}$$

For each nonzero choice of a_2, it is possible to choose d_2 in $2^e - 1$ ways. c_1,c_2 and d_1 can be chosen in 2^t ways. Thus, the total number of ways in which $((c_1, c_2), (d_1, d_2))$ can be chosen so that $D_{(c,d)}D_{(a,b)}f_i$ is constant is $2^{3t}(2^e - 1)$ ways. If $b_2 = 0$ and $a_2 \neq 0$ then the total number of ways in which $((c_1, c_2), (d_1, d_2))$ can be chosen such that $D_{(c,d)}D_{(a,b)}f_i$ is constant is $2^{3t}(2^e - 1) + 2^{3t}$ $=2^{3t+e}$.

Subcase (ii): Let $b_2 = 0$ and $a_2 = 0$. Then $D_{(c,d)}D_{(a,b)}f_i((x_1, x_2), (y_1, y_2)) = \mathrm{Tr}_1^t(a_1d_2+b_1c_2)$, which is constant. It is possible to choose c_1, c_2, d_1, d_2 in 2^t ways. Thus, the total number of ways in which $((c_1, c_2), (d_1, d_2))$ can be chosen such that $D_{(c,d)}D_{(a,b)}f_i$ is constant is 2^{4t}.

Case 2: Let $b_2 \neq 0$. Then $D_{(c,d)}D_{(a,b)}f_i((x_1, x_2), (y_1, y_2))$ is constant if and only if

$$b_2^{2^i}d_2 + b_2d_2^{2^i} = 0 \text{ and } (a_2d_2 + b_2c_2) + (a_2d_2^{2^i} + b_2^{2^i}c_2)^{2^i} = 0.$$

Subcase (i): Let $b_2 \neq 0$ but $d_2 = 0$. Then $D_{(c,d)}D_{(a,b)}f_i$ is constant if and only if

$$\begin{aligned} & b_2c_2 + (b_2^{2^i}c_2)^{2^i} = 0 \Leftrightarrow c_2^{2^i}b_2^{2^{2i}} = c_2b_2 \\ \Leftrightarrow\ & (c_2b_2^{2^i+1})^{2^i-1} = 1, \text{ let } c_2 \neq 0 \\ \Leftrightarrow\ & c_2b_2^{2^i+1} \in \mathbb{F}_{2^i}^* \Leftrightarrow c_2b_2^{2^i+1} \in \mathbb{F}_{2^e}^* \text{ as } \gcd(i,t) = e. \end{aligned}$$

For each choice of b_2, it is possible to choose c_2 in 2^e ways (including $c_2 = 0$). c_1 and d_1 can be chosen in 2^t ways. Thus, the total number of ways in which $((c_1, c_2), (d_1, 0))$ can be chosen so that $D_{(c,d)}D_{(a,b)}f_i$ is constant is 2^{2t+e} ways.

Subcase (ii): Let $b_2 \neq 0$ and $d_2 \neq 0$. Then $D_{(c,d)}D_{(a,b)}f_i$ is constant if and only if

$$b_2^{2^i}d_2 + b_2d_2^{2^i} = 0 \text{ and } (a_2d_2 + b_2c_2) + (a_2d_2^{2^i} + b_2^{2^i}c_2)^{2^i} = 0.$$

From the first part of the above equation, we get

$$\begin{aligned} & b_2^{2^i} d_2 + b_2 d_2^{2^i} = 0 \Leftrightarrow b_2^{2^i} d_2 = b_2 d_2^{2^i} \\ \Leftrightarrow\ & \left(\frac{d_2}{b_2}\right)^{2^i-1} = 1 \Leftrightarrow \frac{d_2}{b_2} \in \mathbb{F}_{2^i}^* \\ \Leftrightarrow\ & \frac{d_2}{b_2} \in \mathbb{F}_{2^e}^* \ \text{ as } \ \gcd(i,t) = e \\ \Leftrightarrow\ & d_2 = \lambda b_2 \ \text{ where } \ \lambda \in \mathbb{F}_{2^e}^*. \end{aligned}$$

For each non zero $b_2 \in \mathbb{F}_{2^t}$, it is possible to choose d_2 in $2^e - 1$ ways .

$$\begin{aligned} & (a_2 d_2 + b_2 c_2) + (a_2 d_2^{2^i} + b_2^{2^i} c_2)^{2^i} = 0 \\ \Leftrightarrow\ & b_2(a_2\lambda + c_2) + b_2^{2^{2i}} (a_2\lambda + c_2)^{2^i} = 0 \\ \Leftrightarrow\ & (b_2^{2^i+1}(a_2\lambda + c_2))^{2^i-1} = 1, \text{ let } \ a_2\lambda + c_2 \neq 0 \\ \Leftrightarrow\ & b_2^{2^i+1}(a_2\lambda + c_2) \in \mathbb{F}_{2^e}^* \ \text{ as } \ \gcd(i,t) = e. \end{aligned}$$

So, $c_2 = a_2\lambda + \frac{\lambda'}{b_2^{2^i+1}}$ where $\lambda' \in \mathbb{F}_{2^e}^*$. Therefore, c_1 and d_1 can be chosen in 2^t ways and c_2 in 2^e ways (including $a_2\lambda + c_2 = 0$). Thus, the total number of ways in which $((c_1, c_2), (d_1, d_2))$ can be chosen so that $D_{(c,d)}D_{(a,b)}f_i$ is constant is $2^{2t+e}(2^e - 1)$ ways.

If $b_2 \neq 0$ then the total number of ways in which $((c_1, c_2), (d_1, d_2))$ can be chosen such that $D_{(c,d)}D_{(a,b)}f_i$ is constant is $2^{2t+e}(2^e - 1) + 2^{2t+e}$ $=2^{2t+2e}$.

So, the dimension of $\mathcal{E}_{D_{(a,b)}f_i}$ is

$$k(a,b) = k((a_1, a_2), (b_1, b_2)) = \begin{cases} 4t, & \text{if } a_2 = 0, b_2 = 0; \\ 3t + e, & \text{if } a_2 \neq 0, b_2 = 0; \\ 2t + 2e, & \text{if } a_2 = 0, b_2 \neq 0; \\ 2t + 2e, & \text{if } a_2 \neq 0, b_2 \neq 0. \end{cases}$$

Let $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t} = \mathbb{F}_{2^t}^2$. The nonlinearity of $D_{(a,b)}f_i$ is

$$\begin{aligned} nl(D_{(a,b)}f_i) &= 2^{m-1} - \frac{1}{2} \max_{(u,v) \in \mathbb{F}_{2^t}^2 \times \mathbb{F}_{2^t}^2} \mid W_{D_{(a,b)}f_i}(u,v) \mid \\ &= 2^{m-1} - \frac{1}{2} 2^{\frac{m+k(a,b)}{2}}. \end{aligned}$$

By Proposition 1.2.20, we get

$$nl_2(f_i) \geq \frac{1}{2} \max_{(a,b)\in\mathbb{F}_{2^t}^2\times\mathbb{F}_{2^t}^2} nl(D_{(a,b)}f_i) = \frac{1}{2}(2^{m-1} - \frac{1}{2}2^{\frac{m+2t+2e}{2}}). \tag{6.2.6}$$

By Proposition 1.2.21, we get

$$nl_2(f_i) \geq 2^{m-1} - \frac{1}{2}\sqrt{2^{2m} - 2\sum_{(a,b)\in\mathbb{F}_{2^t}^2\times\mathbb{F}_{2^t}^2} nl(D_{(a,b)}f_i)}.$$

$$\begin{aligned}
\sum_{(a,b)\in\mathbb{F}_{2^t}^2\times\mathbb{F}_{2^t}^2} nl(D_{(a,b)}f_i) &= \sum_{((a_1,0),(b_1,0))} nl(D_{(a,b)}f_i) + \sum_{((a_1,a_2),(b_1,0)),a_2\neq 0} nl(D_{(a,b)}f_i) + \\
&\quad \sum_{((a_1,0),(b_1,b_2)),b_2\neq 0} nl(D_{(a,b)}f_i) + \sum_{((a_1,a_2),(b_1,b_2)),a_2\neq 0,b_2\neq 0} nl(D_{(a,b)}f_i) \\
&= 2^{2t}(2^{m-1} - \frac{1}{2}2^{\frac{m+4t}{2}}) + 2^{2t}(2^t-1)(2^{m-1} - \frac{1}{2}2^{\frac{m+3t+e}{2}}) \\
&\quad + 2^{3t}(2^t-1)(2^{m-1} - \frac{1}{2}2^{\frac{m+2t+2e}{2}}) \\
&= 2^{8t-1} - 2^{6t-1} + \frac{1}{2}(2^{6t+e} + 2^{\frac{11t+e}{2}} - 2^{7t+e} - 2^{\frac{13t+e}{2}}).
\end{aligned}$$

Thus,

$$nl_2(f_i) \geq 2^{m-1} - \frac{1}{2}\sqrt{2^{7t+e} - 2^{\frac{11t+e}{2}} + 2^{6t}(2^{\frac{t+e}{2}} - 2^e + 1)}. \tag{6.2.7}$$

Subtracting the lower bound obtained in Equation (6.2.6) from the lower bound obtained in Equation (6.2.7), we get

$$\begin{aligned}
2^{m-1} - &\frac{1}{2}\sqrt{2^{7t+e} - 2^{\frac{11t+e}{2}} + 2^{6t}(2^{\frac{t+e}{2}} - 2^e + 1)} - \frac{1}{2}(2^{m-1} - \frac{1}{2}2^{\frac{m+2t+2e}{2}}) \\
&= \frac{1}{4}(2^m + 2^{\frac{3m}{4}+e}) - \frac{1}{2}\sqrt{2^{\frac{7m}{4}+e} - 2^{\frac{11m}{8}+\frac{e}{2}} + 2^{\frac{3m}{2}}(2^{\frac{m}{8}+\frac{e}{2}} - 2^e + 1)} \geq 0
\end{aligned}$$

for sufficiently large m. Therefore, the lower bound obtained in Equation (6.2.7) is the better lower bound than Equation (6.2.6), and the theorem is shown. ■

Let $m = 4t$, $t \geq 3$ and

$$\begin{aligned} n_{t,i}(e) &= \frac{(2^t-1)(2^{5t+e-1}(2^e+1)+(2^t+1)(2^{4t-1}-2^{2t}-1))}{3}, \\ m^1_{t,i}(e) &= \frac{1}{2}(2^{m-1} - \frac{1}{2}2^{\frac{m+2t+2e}{2}}), \\ m^2_{t,i}(e) &= 2^{m-1} - \frac{1}{2}\sqrt{2^{7t+e} - 2^{\frac{11t+e}{2}} + 2^{6t}(2^{\frac{t+e}{2}} - 2^e + 1)} \end{aligned}$$

where $1 \leq i < t$ such that $\gcd(i,t) = e$ and $\gcd(2^i+1, 2^t-1) = 1$. Since for any fixed m, $n_{t,i}(e)$, $m^1_{t,i}(e)$ and $m^2_{t,i}(e)$ depends on e only. We compute $n_{t,i}(e)$, $m^1_{t,i}(e)$ and $m^2_{t,i}(e)$ in Table 6.1, for different values of m and e.

	$m = 12$	$m = 20$	$m = 24$		$m = 28$
	$t = 3; e = 1$	$t = 5; e = 1$	$t = 6; e = 1$	$t = 6; e = 2$	$t = 7; e = 1$
$n_{t,i}(e)$	271019	1218620075	79090592427	236930640555	5096560306859
$m^1_{t,i}(e)$	768	245760	4063232	3932160	66060288
$m^2_{t,i}(e)$	947	386478	6848097	6239867	116951970

	$m = 36$	
	$t = 9; e = 1$	$t = 9; e = 3$
$n_{t,i}(e)$	20981579529235115	218752935040559787
$m^1_{t,i}(e)$	17112760320	16911433728
$m^2_{t,i}(e)$	32180055793	30035054993

Table 6.1: The number of distinct 2-dimensional subspaces on which the second-derivative is constant and the second-order nonlinearity bounds of the cubic MMF bent-negabent functions f_i.

Chapter 7

Gowers U_3 norm of some classes of bent Boolean functions

7.1 Introduction

The problem of constructing Boolean functions in n variables with highest possible second-order nonlinearity is connected to the covering radius problem of second-order Reed–Muller codes. Both these problems are difficult to solve. The Gowers U_3 norm of a Boolean function is a measure of its resistance to quadratic approximations. In this chapter, we compute Gowers U_3 norms for some classes of Maiorana–McFarland bent functions. In particular, we explicitly determine the value of the Gowers U_3 norm of Maiorana–McFarland bent functions obtained by using APN permutations. We further prove that this value is always smaller than the Gowers U_3 norms of Maiorana–McFarland bent functions obtained by using differentially δ-uniform permutations for all $\delta \geq 4$. We also compute the Gowers U_3 norms for a class of cubic monomial functions, not necessarily bent, and show that for $n = 6$, these norm values are less than that of Maiorana–McFarland bent functions. Further, we computationally show that there exist 6-variable functions in this class which are not bent but achieve the maximum second-order nonlinearity for 6 variables.

7.2 Preliminaries

In this chapter, we introduce a slightly different notations for convenience. Let $[n]$ denotes the set $\{1, 2, \ldots, n\}$. Any function F from $\mathbb{F}_2^n$ (or, from $\mathbb{F}_{2^n}$) to $\mathbb{F}_2$ is said to be a Boolean function in n variables and their set is denoted by $\mathcal{B}_n$. The character form associated to $F \in \mathcal{B}_n$, denoted by the corresponding lower case letter f, is defined by $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$. For any $a \in \mathbb{F}_2^n$, $\varphi_a \in \mathcal{B}_n$ is defined as $\varphi_a(x) = a \cdot x$, for all $x \in \mathbb{F}_2^n$. The Walsh–Hadamard transform of $F \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$ is defined as

$$\mathcal{F}(F + \varphi_a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{F(x)+\varphi_a(x)} = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\varphi_a(x)}.$$

The Fourier transform of f at $a \in \mathbb{F}_2^n$, denoted by $\widehat{f}$, is defined as

$$\widehat{f}(a) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{\varphi_a(x)} = \frac{1}{2^n} \mathcal{F}(F + \varphi_a).$$

The Walsh–Hadamard spectrum of F is the multiset $[\mathcal{F}(F + \varphi_a) : a \in \mathbb{F}_2^n]$ and the Fourier spectrum of f (or, of F) is $[\widehat{f}(a) : a \in \mathbb{F}_2^n]$. The derivative of $F \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_2^n$ is defined by $D_a F(x) = F(x + a) + F(x)$, for all $x \in \mathbb{F}_2^n$. If $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$ then

$$D_a f(x) = (-1)^{D_a F(x)} = (-1)^{F(x+a)+F(x)} = f(x)f(x + a).$$

Definition 7.2.1. *A Boolean function $F \in \mathcal{B}_n$ (n even) is said to be bent if and only if there exists another Boolean function $\widetilde{F} \in \mathcal{B}_n$ such that $\mathcal{F}(F + \varphi_a) = 2^{\frac{n}{2}}(-1)^{\widetilde{F}(a)}$, for all $a \in \mathbb{F}_2^n$. The Boolean function $\widetilde{F}$ is said to be the dual of F and is also a bent function.*

The first generic technique for constructing bent functions was proposed by Rothaus [86]. The functions so obtained are referred to as Maiorana–McFarland bent functions.

Definition 7.2.2. *Suppose $m = 2n$ where $n \in \mathbb{Z}^+$, π is a permutation on $\mathbb{F}_{2^n}$ and $g \in \mathcal{B}_n$. A function of the form $F(x, y) = \pi(x) \cdot y + g(x)$, for all $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, is said to be a Maiorana–McFarland bent function.*

The Walsh–Hadamard transform of a bent function F is related to the Walsh–Hadamard transform of its dual $\widetilde{F}$ as we see next.

Proposition 7.2.3 ([19, Lemma 2])**.** *Let F be a bent function in n variables and $\widetilde{F}$ be its dual. Then for any $a, b \in \mathbb{F}_2^n$, we have*

$$\mathcal{F}(D_a\widetilde{F} + \varphi_b) = \mathcal{F}(D_bF + \varphi_a). \tag{7.2.1}$$

7.3 Gowers uniformity norms

Let $f : V \to \mathbb{R}$ be any function on a finite set V and $B \subseteq V$. Then $\mathbb{E}_{x\in B}[f(x)] := \frac{1}{|B|}\sum_{x\in B} f(x)$ is the average of f over B. The connection between the expected values of $F : \mathbb{F}_2^n \to \mathbb{F}_2$ and its character form f is given in the lemma below.

Lemma 7.3.1. *We have $\mathbb{E}_{x\in B}[f(x)] = 1 - 2\,\mathbb{E}_{x\in B}[F(x)]$.*

Proof. Using the fact that $(-1)^b = 1 - 2b$, for $b \in \{0, 1\}$, we write

$$\begin{aligned}\mathbb{E}_{x\in B}[f(x)] &= \frac{1}{|B|}\sum_{x\in B} f(x) = \frac{1}{|B|}\sum_{x\in B}(-1)^{F(x)}\\ &= \frac{1}{|B|}\sum_{x\in B}(1 - 2F(x)) = 1 - 2\,\mathbb{E}_{x\in B}[F(x)].\end{aligned}$$

■

Definition 7.3.2 ([143, Definition 2.2.1])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. For every $k \in \mathbb{Z}^+$, we define the kth-dimension Gowers uniformity norm (the U_k norm) of f to be*

$$\|f\|_{U_k} = \left(\mathbb{E}_{x,x_1,\ldots,x_k\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f\left(x + \sum_{i\in S} x_i\right)\right]\right)^{\frac{1}{2^k}}.$$

Gowers norms for $k = 1, 2, 3$ are explicitly presented below (cf. [132, 143]).

$$\begin{aligned}\|f\|_{U_1} &= |\ \mathbb{E}_{x,h\in\mathbb{F}_2^n}[f(x)f(x+h)]\ |^{1/2}\\ &= |\ \mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)]\ |\ .\\ \|f\|_{U_2} &= |\ \mathbb{E}_{x,h_1,h_2\in\mathbb{F}_2^n}[f(x)f(x+h_1)f(x+h_2)f(x+h_1+h_2)]\ |^{1/4}\\ &= |\ \mathbb{E}_{h_1\in\mathbb{F}_2^n}\ |\ \mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)f(x+h_1)]\ |^2|^{1/4},\\ \|f\|_{U_3} &= |\ \mathbb{E}_{x,h_1,h_2,h_3\in\mathbb{F}_2^n}[f(x)f(x+h_1)f(x+h_2)f(x+h_1+h_2)\\ &\qquad \times f(x+h_3)f(x+h_1+h_3)f(x+h_2+h_3)f(x+h_1+h_2+h_3)]\ |^{1/8}\ .\end{aligned}$$

It is not difficult (and we will see some instances of this claim later) to see that one can recursively define the Gowers norms by

$$\begin{aligned}\|f\|_{U_1} &= |\mathbb{E}_{x\in\mathbb{F}_2^n}[f(x)]|,\\ \|f\|_{U_{k+1}} &= \left(\mathbb{E}_{h\in\mathbb{F}_2^n}[\|D_h f\|_{U_k}^{2^k}]\right)^{1/2^{k+1}}.\end{aligned}$$

The connection between the Gowers uniformity norms and correlation of a function with polynomials with a certain degree bound is described by results obtained by Gowers, Green and Tao [11, 126]. For a survey we refer to Chen [143].

Theorem 7.3.3 ([143, Fact 2.2.1])**.** *Let $k \in \mathbb{Z}^+$, $\epsilon > 0$. Let $P : \mathbb{F}_2^n \to \mathbb{F}_2$ be a polynomial of degree at most k, and $f : \mathbb{F}_2^n \to \mathbb{R}$. Suppose $\left|\mathbb{E}_x[f(x)(-1)^{P(x)}]\right| \geq \epsilon$. Then $\|f\|_{U_{k+1}} \geq \epsilon$.*

Theorem 7.3.3 implies that if a Boolean function has low Gowers U_{k+1} norm then it has low correlation with all the polynomials functions on $\mathbb{F}_2^n$ of degrees at most k. In other words it has high kth-order nonlinearity.

It is known that the U_k, for $k > 1$, is a norm, that is, it is homogeneous, nonnegative, nondegenerate and respects the triangle inequality. It is also known that the sequence of norms $\{U_k\}_k$ is monotonically increasing, that is, $\|f\|_{U_k} \leq \|f\|_{U_{k+1}}$, $k \geq 0$.

It is known that the Gowers U_2 norm of a function is the ℓ_4 norm of its Fourier transform, more precisely:

Theorem 7.3.4 ([126, 143])**.** *Let $f : \mathbb{F}_2^n \to \mathbb{R}$. Then*

$$\|f\|_{U_2}^4 = \sum_{x\in\mathbb{F}_2^n} \widehat{f}(x)^4. \tag{7.3.1}$$

The following is an extension of Theorem 7.3.4.

Theorem 7.3.5. *Let $k \in \mathbb{Z}^+$, $k \geq 2$. Let $F \in \mathcal{B}_n$ and $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$. Then*

$$\|f\|_{U_k}^{2^k} = \frac{1}{2^{(k-2)n}} \sum_{h_1,\ldots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{D_{h_1,\ldots,h_{k-2}} f}(x)^4.$$

Proof. Let $g = D_{h_1,\ldots,h_{k-2}} f$ where $h_1, \ldots, h_{k-2} \in \mathbb{F}_2^n$. For any $k \in \mathbb{Z}^+$, the kth dimensional

Gowers uniformity norm of f is

$$\begin{aligned}
\|f\|_{U_k}^{2^k} &= \mathbb{E}_{x,h_1,\dots,h_k\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f(x+\sum_{i\in S} h_i)\right]\\
&= \frac{1}{2^{(k+1)n}} \sum_{x,h_1,\dots,h_k\in\mathbb{F}_2^n} g(x)g(x+h_{k-1})g(x+h_k)g(x+h_{k-1}+h_k)\\
&= \frac{1}{2^{(k+1)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} g(x)g(x+h_{k-1}) \sum_{h_k\in\mathbb{F}_2^n} g(x+h_k)g(x+h_{k-1}+h_k)\\
&= \frac{1}{2^{(k+1)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} g(x)g(x+h_{k-1}) \sum_{y\in\mathbb{F}_2^n} g(y)g(y+h_{k-1})\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{g}(x)^2(-1)^{h_{k-1}\cdot x} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(y)^2(-1)^{h_{k-1}\cdot y}\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{h_{k-1}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(x)^2\widehat{g}(y)^2(-1)^{h_{k-1}\cdot(x+y)}\\
&= \frac{1}{2^{(k-1)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n} \widehat{g}(x)^2\widehat{g}(y)^2 \sum_{h_{k-1}\in\mathbb{F}_2^n} (-1)^{h_{k-1}\cdot(x+y)}\\
&= \frac{1}{2^{(k-2)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{g}(x)^4\\
&= \frac{1}{2^{(k-2)n}} \sum_{h_1,\dots,h_{k-2}\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} \widehat{D_{h_1,\dots,h_{k-2}} f}(x)^4
\end{aligned}$$

where we used the fact (see [135]) that the autocorrelation

$$C_g(u) = \sum_{x\in\mathbb{F}_2^n} g(x)g(x+u) = 2^n \sum_x \hat{g}(x)^2(-1)^{u\cdot x},\ u\in\mathbb{F}_2^n,$$

as well as [135, Lemma 2.6] giving $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot w} = 2^n$ if $w=0$, and 0, if $w\neq 0$. ■

Theorem 7.3.6. *Let $F, G\in\mathcal{B}_n$ be affine equivalent and $k\in\mathbb{Z}^+$. Suppose $f(x)=(-1)^{F(x)}$ and $g(x)=(-1)^{G(x)}$ for all $x\in\mathbb{F}_2^n$ are the character form associated to F and G, respectively. Then the kth-dimension Gowers uniformity norm of f and g are equal, that is,*

$$\|f\|_{U_k} = \|g\|_{U_k}.$$

Proof. Let $G(x) = F(xA + b)$, for all $x \in \mathbb{F}_2^n$ where $A \in GL(n, \mathbb{F}_2)$ and $b \in \mathbb{F}_2^n$.

$$\begin{aligned}
\|g\|_{U_k} &= \left(\mathbb{E}_{x,h_1,\dots,h_k \in \mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} g(x + \sum_{i\in S} h_i)\right]\right)^{\frac{1}{2^k}} \\
&= \left(\frac{1}{2^{(k+1)n}} \sum_{h_1,\dots,h_k\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} g(x+\sum_{i\in S} h_i)\right]\right)^{\frac{1}{2^k}} \\
&= \left(\frac{1}{2^{(k+1)n}} \sum_{h_1,\dots,h_k\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f(xA+\sum_{i\in S}(h_iA)+b)\right]\right)^{\frac{1}{2^k}} \\
&= \left(\frac{1}{2^{(k+1)n}} \sum_{a_1,\dots,a_k\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f(xA+b+\sum_{i\in S} a_i)\right]\right)^{\frac{1}{2^k}}, \text{ let } a_i = h_iA, i \in S \\
&= \left(\frac{1}{2^{(k+1)n}} \sum_{a_1,\dots,a_k\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^n}\left[\prod_{S\subseteq[k]} f(y+\sum_{i\in S} a_i)\right]\right)^{\frac{1}{2^k}}, \text{ let } y = xA + b \\
&= \|f\|_{U_k}.
\end{aligned}$$

■

The proof of the next corollary follows directly from Theorem 7.3.6.

Corollary 7.3.7. *Let $F, G \in \mathcal{B}_n$ and there exists a $k \in \mathbb{Z}^+$ such that $\|f\|_{U_k} \neq \|g\|_{U_k}$ where f and g are the associated character form of F and G, respectively. Then F and G are affine inequivalent.*

It is more convenient to calculate the Gowers norms of a bent function for $k = 1$ and 2. Let $F \in \mathcal{B}_n$ be a bent function and $f(x) = (-1)^{F(x)}$, for all $x \in \mathbb{F}_2^n$. Then

1. $\|f\|_{U_1} = 2^{-\frac{n}{2}}$.
2. $\|f\|_{U_2} = 2^{-\frac{n}{4}}$, i.e., $\|f\|_{U_1} = (\|f\|_{U_2})^2$.

7.3.1 Gowers U_3 norm of the dual of a bent function

It is known that the dual of a bent function is bent. However, it is not known whether a bent function and its dual have the same second-order nonlinearity. We prove that the Gowers U_3 norms of a bent and its dual are equal and therefore they provide equal "resistance" to quadratic approximations.

Proposition 7.3.8. *Let the character forms associated to a bent function $F \in \mathcal{B}_n$ and its dual $\widetilde{F}$ be f and $\widetilde{f}$, respectively. Then*

$$\|f\|_{U_3} = \|\widetilde{f}\|_{U_3}.$$

Proof. The Gowers U_3 norm of f is

$$\begin{aligned}
\|f\|_{U_3}^8 &= \left| \frac{1}{2^{4n}} \sum_{h\in\mathbb{F}_2^n} \sum_{h_1\in\mathbb{F}_2^n} \sum_{h_2\in\mathbb{F}_2^n} \sum_{x\in\mathbb{F}_2^n} (-1)^{D_hF(x)+D_hF(x+h_1)+D_hF(x+h_2)+D_hF(x+h_1+h_2)} \right| \\
&= \frac{1}{2^n} \sum_{h\in\mathbb{F}_2^n} \frac{1}{2^n} \sum_{h_1\in\mathbb{F}_2^n} \left(\frac{1}{2^n} \sum_{x\in\mathbb{F}_2^n} (-1)^{D_hF(x)+D_hF(x+h_1)} \right)^2 \\
&= \frac{1}{2^n} \sum_{h\in\mathbb{F}_2^n} \mathbb{E}_{h_1\in\mathbb{F}_2^n} \left[\mathbb{E}_{x\in\mathbb{F}_2^n} \left[(-1)^{D_hF(x)+D_hF(x+h_1)} \right]^2 \right] \\
&= \frac{1}{2^n} \sum_{h\in\mathbb{F}_2^n} \|D_hf\|_{U_2}^4 = \frac{1}{2^n} \sum_{h\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} \widehat{D_hf}(a)^4, \quad \text{by (7.3.1)} \\
&= \frac{1}{2^{5n}} \sum_{h\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} \mathcal{F}(D_hF + \varphi_a)^4 = \frac{1}{2^{5n}} \sum_{a\in\mathbb{F}_2^n} \sum_{h\in\mathbb{F}_2^n} \mathcal{F}(D_a\widetilde{F} + \varphi_h)^4, \text{by (7.2.1)} \\
&= \|\widetilde{f}\|_{U_3}^8.
\end{aligned}$$

■

7.3.2 Gowers U_3 norm of Maiorana–McFarland bents of the form $\mathrm{Tr}_1^n(yx^{2^i+1})$

Gangopadhyay et al. [110] employed the recursive framework developed by Carlet to identify cubic Maiorana–McFarland bent functions having high second-order nonlinearities. Below we describe the subclass of Maiorana–McFarland bent functions considered in [110] which was originally constructed by Canteaut and Charpin [5]. It is shown in [110] that bent functions on 10 variables having maximum known second-order nonlinearity exist within this class.

Let $m = 2n$. We identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^m$ with $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. In the next theorem we consider cubic Maiorana–McFarland bent functions of the form

$$F_i(x,y) = \mathrm{Tr}_1^n(yx^{2^i+1}) \tag{7.3.2}$$

where $x, y \in \mathbb{F}_{2^n}$, $m \geq 6$, i is an integer such that $1 \leq i < n$, $\gcd(2^n-1, 2^i+1) = 1$ and $\gcd(i,n) = e$.

Theorem 7.3.9. *If $F_i \in \mathcal{B}_m$ is a function of the form given by Equation (7.3.2) and f_i is the associated character form then*

$$\|f_i\|_{U_3}^8 = \frac{2^m + 2^{n+e}(2^e+1)(2^n-1)}{2^{2m}}. \tag{7.3.3}$$

Thus, the Gowers U_3 norm is minimum if and only if $e = 1$.

Proof. For any function $F \in \mathcal{B}_m$ with f as the associated character form, the Gowers U_3 norm can be written as

$$\begin{aligned}
\|f\|_{U_3}^8 &= \left| \frac{1}{2^{4m}} \sum_{h,h_1,h_2,x \in \mathbb{F}_2^m} (-1)^{D_{h,h_1,h_2}F(x)} \right| \\
&= \left| \frac{1}{2^{4m}} \sum_{h_1,h_2 \in \mathbb{F}_2^m} \sum_{h,x \in \mathbb{F}_2^m} (-1)^{D_h(D_{h_1,h_2}F)(x)} \right| \\
&= \frac{1}{2^{4m}} \left| \sum_{h_1,h_2 \in \mathbb{F}_2^m} \left(\sum_{x \in \mathbb{F}_2^m} (-1)^{D_{h_1,h_2}F(x)} \right)^2 \right|.
\end{aligned}$$

Let $S(h_1,h_2;F) := \sum_{x \in \mathbb{F}_2^m} (-1)^{D_{h_1,h_2}F(x)}$. We note that $S(h_1,h_2;F) = 2^m$ if either $h_1 = h_2$ or exactly one of h_1, h_2 is 0, so

$$\begin{aligned}
\|f\|_{U_3}^8 &= \frac{1}{2^{4m}} \left| \sum_{h_1,h_2 \in \mathbb{F}_2^m} S(h_1,h_2;F)^2 \right| \\
&= \frac{1}{2^{4m}} \left| 2^{2m} \left(\sum_{h_1 \in \mathbb{F}_2^m} 1 + \sum_{\substack{h_2 \in \mathbb{F}_2^m \setminus \{0\} \\ h_1 = 0}} 1 + \sum_{\substack{h_1 \in \mathbb{F}_2^m \setminus \{0\} \\ h_2 = 0}} 1 \right) + \sum_{\substack{h_1,h_2 \in \mathbb{F}_2^m \setminus \{0\} \\ h_1 \neq h_2}} S(h_1,h_2;F)^2 \right| \\
&= \frac{1}{2^{4m}} \left| 2^{2m}(3 \cdot 2^m - 2) + \sum_{\substack{h_1,h_2 \in \mathbb{F}_2^m \setminus \{0\} \\ h_1 \neq h_2}} S(h_1,h_2;F)^2 \right|.
\end{aligned}$$

Replacing F by F_i we note that, since F_i is a cubic function, $S(h_1, h_2; F_i)$ is either 0 or $\pm 2^m$. Therefore, we have to count the pairs (h_1, h_2) for which $S(h_1, h_2; F_i) = \pm 2^m$. Similar counting is performed in [110] and [111, Theorem 4]. However, for completeness we recall the basic steps.

Let $h_1 = (b, a)$ and $h_2 = (d, c)$ where $a, b, c, d \in \mathbb{F}_{2^n}$.

$$\begin{aligned} D_{(b,a),(d,c)}F_i(x,y) = {} & \mathrm{Tr}_1^n(((ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i})x^{2^i}) + \mathrm{Tr}_1^n((bd^{2^i}+b^{2^i}d)y) \\ & + \mathrm{Tr}_1^n(ad^{2^i+1}+cb^{2^i+1}) + \mathrm{Tr}_1^n((a+c)(bd^{2^i}+b^{2^i}d)). \end{aligned}$$

Case 1*:* If $b = d = 0$ then $D_{(b,a),(d,c)}F_i(x,y) = 0$, for all $(x,y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$. The number of such points is $(2^n-1)(2^n-2)$.

Case 2*:* If $b = 0$ and $d \neq 0$ then

$$D_{(d,c),(0,a)}F_i(x,y) = \mathrm{Tr}_1^n((ad+(ad^{2^i})^{2^i})x^{2^i}) + \mathrm{Tr}_1^n(ad^{2^i+1}),$$

which is constant if and only if

$$\begin{aligned} & ad+(ad^{2^i})^{2^i} = ad + a^{2^i}d^{2^{2i}} = 0, & \\ \text{i.e.,}\quad & a^{2^i-1}d^{2^{2i}-1} = (ad^{2^i+1})^{2^i-1} = 1, & \text{since } d \neq 0 \text{ and } a \neq 0, \\ \text{i.e.,}\quad & ad^{2^i+1} \in \mathbb{F}_{2^e}^*, & \text{as } \gcd(i,t) = e. \end{aligned}$$

Thus, given any $a \in \mathbb{F}_{2^n} \setminus \{0\}$, c and d can be chosen in 2^n and $2^e - 1$ ways, respectively, such that the second-derivative under consideration is constant. Therefore, among all the derivatives of the form $D_{(d,c),(0,a)}F_i$, exactly $2^n(2^n-1)(2^e-1)$ are constants.

Similarly, if $b \neq 0$ and $d = 0$ among all the derivatives of the form $D_{(0,c),(b,a)}F_i$ then exactly $2^n(2^n-1)(2^e-1)$ are constants.

Case 3*:* Suppose $b \neq 0$ and $d \neq 0$.

Subcase (*i*)*:* Let $b = d$. Then $D_{(d,c),(b,a)}F_i = D_{(0,c+a),(b,a)}F_i = D_{(d,c),(0,a+c)}F_i$. In this case $a \neq c$, since otherwise $(b,a) = (d,c)$ which is already dealt with. Thus, among all the derivatives of the form $D_{(d,c),(b,a)}F_i$, exactly $2^n(2^n-1)(2^e-1)$ are constants.

Subcase (*ii*)*:* Let $b \neq d$. The second-derivative $D_{(d,c),(b,a)}F_i$ is constant if and only if

$$(ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i} = 0 \quad \text{and} \quad bd^{2^i}+b^{2^i}d = 0.$$

From the second condition we obtain $(b^{-1}d)^{2^i-1} = 1$. Since $b, d \in \mathbb{F}_{2^n}$, $(b^{-1}d)^{2^t-1} = 1$.

Combining these two we obtain $(b^{-1}d)^{2^e-1} = 1$, which implies that $b^{-1}d \in \mathbb{F}_{2^e}^*$. Thus, $d = \gamma b$ where $\gamma \in \mathbb{F}_{2^e}^*$. Since $b \neq d$, $\gamma \neq 1$. Therefore, for each choice of b it is possible to choose d in $2^e - 2$ different ways. From the first condition we obtain:

$$\begin{aligned} & ad + cb + (ad^{2^i} + cb^{2^i})^{2^i} = b(a\gamma + c) + (b^{2^i}(a\gamma + c))^{2^i} = 0, \\ \text{i.e.,}\quad & (b^{2^i+1}(a\gamma + c))^{2^i-1} = 1, \text{ if } a\gamma + c \neq 0. \\ \text{i.e.,}\quad & b^{2^i+1}(a\gamma + c) = \gamma' \in \mathbb{F}_{2^e}^*, \text{ so, } c = a\gamma + \tfrac{\gamma'}{b^{2^i+1}}. \end{aligned}$$

Note that a can be chosen in 2^n ways, b in $2^n - 1$ ways, d in $2^e - 2$ ways and c in 2^e ways (including the case for which $a\gamma + c = 0$). So the total number of ways in which $(b, a), (d, c)$ can be chosen is

$$2^{n+e}(2^n - 1)(2^e - 2).$$

Combining all the above counts we obtain

$$\|f_i\|_{U_3}^8 = \frac{2^m + 2^{n+e}(2^e + 1)(2^n - 1)}{2^{2m}}.$$

■

It is observed from Equation (7.3.3) that for $e = 1$, the Gowers U_3 norm of F_i

$$\|f_i\|^8 = \frac{7 \cdot 2^n - 6}{2^{3n}}$$

is minimum. It has been experimentally checked in [110, Section 3] that for $m = 2n = 10$, $1 \leq i \leq 4$ (therefore, $e = 1$), the functions F_i's have the largest known second-order nonlinearity.

7.3.3 Gowers U_3 norms of Maiorana–McFarland bent functions constructed by using APN and differentially 4-uniform permutations

A vectorial Boolean function $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, also referred to as an (n, n)-function, is said to be differentially δ-uniform if

$$\delta(a, b) = |\{x \in \mathbb{F}_2^n : \phi(x) + \phi(x + a) = b\}| \leq \delta,$$

for all $a, b \in \mathbb{F}_2^n$ with $a \neq 0$. We denote the set $\{x \in \mathbb{F}_2^n : \phi(x)+\phi(x+a) = b\}$ by $\Delta(a, b)$, for all $a, b \in \mathbb{F}_2^n$ with $a \neq 0$. If ϕ is differentially 2-uniform then it is said to be an almost perfect nonlinear (APN) function. If ϕ is an APN function and a permutation then we refer to it as an APN permutation on $\mathbb{F}_2^n$. There are several applications of APN functions, but perhaps the most significant is that if the S-box (vectorial Boolean function) is based upon an APN function, the probability of success for the differential attack is minimized [30]. Certainly, in block cipher design, invertibility is essential, so the S-boxes must be permutations. There are very few classes of APN functions, like monomials APN, which are completely described, and there are many APN questions still open (like the existence of APN permutations in *all* even dimensions; in fact, we barely know of a single example in dimension 6). The connection with linear codes is well-known via a result of Carlet, Charpin and Zinoviev [26], stating that $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $f(0) = 0$ is APN if and only if the binary linear code with parity check matrix of columns $(\alpha^i, f(\alpha^i))^T$, $1 \leq i \leq 2^n - 1$, has minimum distance 5 (α is a primitive element of $\mathbb{F}_{2^n}$). We refer the reader to the huge body of literature on differential uniform and APN functions [30, 31, 61, 70, 134, 156] and their references. Let

$$E_i = \{(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0 \text{ and } \delta(a, b) = i\},$$

for all nonnegative integers i. It is easy to see that $E_i = \emptyset$, if $i \equiv 1 \pmod 2$.

Lemma 7.3.10. *Suppose that $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Then the cardinality of $E_2 = \{(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0$ and $\delta(a, b) = 2\}$ is $|E_2| = 2^{n-1}(2^n - 1)$.*

Proof. Let $a \in \mathbb{F}_2^n \setminus \{0\}$. We know that $D_a\phi(x) = D_a\phi(x + a) = b \in \mathbb{F}_2^n$, for all $x \in \mathbb{F}_2^n$. Therefore, the cardinality of the range of the function $D_a\phi$ is at most 2^{n-1}. Suppose that $\{x_i : i = 1, 2, \ldots, 2^{n-1}\} \subseteq \mathbb{F}_2^n$ such that $x_j \neq x_i$ and $x_j \neq x_i + a$, for all $i \neq j$ and $D_a\phi(x_i) = D_a\phi(x_i + a) = b_i$, for all $i = 1, 2, \ldots, 2^{n-1}$. Then

$$\begin{aligned} b_i = b_j \;&\Leftrightarrow\; D_a\phi(x_i) = D_a\phi(x_j) \\ &\Leftrightarrow\; D_a(\phi(x_i) + \phi(x_j)) = 0 \\ &\Leftrightarrow\; D_a(\phi(x_i) + \phi(x_i + b)) = 0 \text{ where } b = x_i + x_j, \\ &\Leftrightarrow\; D_aD_b\phi(x_i) = 0, \end{aligned}$$

which is not possible, since ϕ is APN (cf. [30, page 417]). Therefore, for each choice of

$a \in \mathbb{F}_2^n \setminus \{0\}$ we obtain exactly 2^{n-1} distinct b's in $\mathbb{F}_2^n \setminus \{0\}$ such that $\delta(a,b) = 2$. Since a's can be chosen in $2^n - 1$ many ways, $|E_2| = 2^{n-1}(2^n - 1)$. ■

Lemma 7.3.11. *Let ϕ be a differentially δ-uniform (n,n)-function where $\delta = 2k$, and*

$$E_{2i} = \{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : a \neq 0 \text{ and } \delta(a,b) = 2i\},$$

for all $i \in \{0,1,\ldots,k\}$. Then $\sum_{i=1}^{k} i\,|E_{2i}| = 2^{n-1}(2^n - 1)$.

Proof. For each $a \in \mathbb{F}_2^n \setminus \{0\}$, it is possible to find a set $\{x_1, \ldots, x_{2^{n-1}}\}$ such that $x_i + a \neq x_j$, whenever $i \neq j$, so that $\mathbb{F}_2^n = \{x_1, \ldots, x_{2^{n-1}}\} \cup \{(x_1 + a), \ldots, (x_{2^{n-1}} + a)\}$. We construct a list of differences as in Table 7.1.

No.	Output differences		
1	$\phi(x_1) + \phi(x_1 + a)$	$=$	b_1
2	$\phi(x_2) + \phi(x_2 + a)$	$=$	b_2
$\vdots$	$\ldots$		
j	$\phi(x_j) + \phi(x_j + a)$	$=$	b_j
$\vdots$	$\ldots$		
2^{n-1}	$\phi(x_{2^{n-1}}) + \phi(x_{2^{n-1}} + a)$	$=$	$b_{2^{n-1}}$

Table 7.1: List of (not necessarily distinct) output differences when the input difference is a.

If $\delta(a,b) \neq 0$ then $(a,b) \in E_{2i}$ for a unique $i \in \{1,\ldots,k\}$, and we have a subset $S_{(a,b)}^{(i)} \subseteq \{1,\ldots,2^{n-1}\}$, with $|S_{(a,b)}^{(i)}| = i$, such that $\phi(x_j) + \phi(x_j + a) = b_j = b$, for all $j \in S_{(a,b)}^{(i)}$. We say that i rows of $S_{(a,b)}^{(i)}$ are covered by (a,b). If we consider the collection of all tables like Table 7.1, one for each $a \in \mathbb{F}_2^n \setminus \{0\}$ then for each $(a,b) \in E_{2i}$, i rows of $S_{(a,b)}^{(i)}$ are covered. It can be checked that $S_{(a,b)}^{(i)} = S_{(a,b')}^{(i')}$ if and only if $i = i'$ and $b = b'$, otherwise, $S_{(a,b)}^{(i)} \cap S_{(a,b')}^{(i')} = \emptyset$.

The total number of rows covered (considering all the distinct $2^n - 1$ tables, one corresponding to each $a \in \mathbb{F}_2^n \setminus \{0\}$) if we vary (a,b) over the whole of E_{2i} is $i\,|E_{2i}|$. If we repeat this process for each $i \in \{1,\ldots,k\}$, eventually all the rows of all the 2^{n-1} tables will be exhausted and the claimed identity is shown. ■

Theorem 7.3.12. *Let $F \in \mathcal{B}_m$ be a Maiorana–McFarland bent function of the form*

$$F(x,y) = \phi(x) \cdot y + h(x),$$

for all $x, y \in \mathbb{F}_2^n$ where $h \in \mathcal{B}_n$ and ϕ is an APN permutation on $\mathbb{F}_2^n$. Then the Gowers U_3 norm of the character form $f = (-1)^F$ is

$$\|f\|_{U_3}^8 = \frac{7 \cdot 2^n - 6}{2^{3n}}. \tag{7.3.4}$$

Proof. Using Theorem 7.3.5,

$$\begin{aligned}
\|f\|_{U_3}^8 &= \frac{1}{2^m} \sum_{(\alpha,\beta)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \widehat{D_{(\alpha,\beta)} f}(a,b)^4 \\
&= \frac{1}{2^{5m}} \sum_{(\alpha,\beta)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}F(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= \frac{1}{2^{5m}} (A + B + C)
\end{aligned}$$

where

$$\begin{aligned}
A &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,0)}F(x,y)+a\cdot x+b\cdot y} \right)^4, \\
&= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{a\cdot x+b\cdot y} \right)^4 = 2^{4m}, \\
B &= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,\beta)}F(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x+b\cdot y} \right)^4 \\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x} \sum_{y\in\mathbb{F}_2^n} (-1)^{b\cdot y} \right)^4 \\
&= \sum_{\beta\in\mathbb{F}_2^n\setminus\{0\}} \sum_{a\in\mathbb{F}_2^n} \left(2^n \sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x} \right)^4 \\
&= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi(x)+a\cdot x} \right)^4 - 2^{2m} \sum_{a\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x} \right)^4 \\
&= 2^{2m}(3 \cdot 2^{4n} - 2 \cdot 2^{3n} - 2^{4n}), \text{ (cf. [30, page 418])} \\
&= 2^{3m+n+1}(2^n - 1),
\end{aligned}$$

$$
\begin{aligned}
C &= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}F(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)+(\phi(x)+\phi(x+\alpha)+b)\cdot y} \right)^4 \\
&= \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)} \sum_{y\in\mathbb{F}_2^n} (-1)^{(\phi(x)+\phi(x+\alpha)+b)\cdot y} \right)^4 \\
&= 2^{2m} \sum_{\alpha\in\mathbb{F}_2^n\setminus\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi(x+\alpha)+h(x)+h(x+\alpha)} \right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi(x)+b\cdot\beta+h(x)+h(x+\alpha)} \right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \left(\sum_{x\in\Delta(\alpha,b)=\{x_{\alpha b},x_{\alpha b}+\alpha\}} (-1)^{a\cdot x+\beta\cdot\phi(x)+h(x)+h(x+\alpha)} \right)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \big((-1)^{a\cdot x_{\alpha b}+\beta\cdot\phi(x_{\alpha b})+h(x_{\alpha b})+h(x_{\alpha b}+\alpha)} \\
&\qquad\qquad + (-1)^{a\cdot(x_{\alpha b}+\alpha)+\beta\cdot\phi(x_{\alpha b}+\alpha)+h(x_{\alpha b}+\alpha)+h(x_{\alpha b})} \big)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} \big((1+(-1)^{a\cdot\alpha+b\cdot\beta})(-1)^{a\cdot x_{\alpha b}+\beta\cdot\phi(x_{\alpha b})+h(x_{\alpha b})+h(x_{\alpha b}+\alpha)} \big)^4 \\
&= 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_2} (8+8(-1)^{a\cdot\alpha+b\cdot\beta}) \\
&= 2^{2m} \sum_{(\alpha,b)\in E_2} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} 8 + 2^{2m+3} \sum_{(\alpha,b)\in E_2} \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} (-1)^{b\cdot\beta+\alpha\cdot a} \\
&= 2^{3m+3}\left|E_2\right|, \text{ since } (\alpha,b)\neq(0,0), \text{ the sum } \sum_{\beta\in\mathbb{F}_2^n} \sum_{a\in\mathbb{F}_2^n} (-1)^{b\cdot\beta+\alpha\cdot a} = 0.
\end{aligned}
$$

From Lemma 7.3.10, we have $|E_2| = 2^{n-1}(2^n-1)$. So

$$
\|f\|_{U_3}^8 = \frac{1}{2^{2m}}(2^m + 2^{n+1}(2^n-1) + 8\left|E_2\right|) = \frac{7\cdot 2^n - 6}{2^{3n}},
$$

and the claim is shown. ■

Corollary 7.3.13. *Let* $\|f_i\|_{U_3}^8$ *and* $\|f\|_{U_3}^8$ *be defined as in Equation* (7.3.3) *and* (7.3.4), *respectively. Then*

$$
\|f_i\|_{U_3}^8 - \|f\|_{U_3}^8 = \frac{(2^n-1)(2^e+3)(2^e-2)}{2^{3n}}.
$$

Therefore, $\|f_i\|_{U_3}^8 \geq \|f\|_{U_3}^8$*, with equality holding only when* $e = 1$*, that is,* $\gcd(n, i) = 1$.

Theorem 7.3.14. *Let* $G \in \mathcal{B}_m$ *be a Maiorana–McFarland bent function of the form*

$$G(x, y) = \psi(x) \cdot y + h(x),$$

for all $x, y \in \mathbb{F}_2^n$ *where* $h \in \mathcal{B}_n$ *and* ψ *is a differentially* 4*-uniform permutation and not an APN permutation on* $\mathbb{F}_2^n$*. Then the Gowers* U_3 *norm of the character form* $g = (-1)^G$ *is*

$$\|g\|_{U_3}^8 > \frac{7 \cdot 2^n - 6}{2^{3n}}.$$

Proof. Using similar arguments as in the proof of Theorem 7.3.12,

$$\|g\|_{U_3}^8 = \frac{1}{2^{5m}}(A_1 + B_1 + C_1)$$

where

$$\begin{aligned}
A_1 &= \sum_{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} \left(\sum_{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{D_{(0,0)}G(x,y) + a \cdot x + b \cdot y} \right)^4 = 2^{4m}, \\
B_1 &= \sum_{\beta \in \mathbb{F}_2^n \setminus \{0\}} \sum_{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} \left(\sum_{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{D_{(0,\beta)}G(x,y) + a \cdot x + b \cdot y} \right)^4 \\
&= \sum_{\beta \in \mathbb{F}_2^n \setminus \{0\}} \sum_{a \in \mathbb{F}_2^n} \left(2^n \sum_{x \in \mathbb{F}_2^n} (-1)^{\beta \cdot \psi(x) + a \cdot x} \right)^4 \\
&\geq 2^{3m+n+1}(2^n - 1), \quad \text{(cf. [30, page 415])}, \\
C_1 &= \sum_{\alpha \in \mathbb{F}_2^n \setminus \{0\}} \sum_{\beta \in \mathbb{F}_2^n} \sum_{(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} \left(\sum_{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}G(x,y) + a \cdot x + b \cdot y} \right)^4 \\
&= 2^{2m} \sum_{a \in \mathbb{F}_2^n} \sum_{\beta \in \mathbb{F}_2^n} \sum_{i=1}^{2} \sum_{(\alpha,b) \in E_{2i}} \left(\sum_{x \in \Delta(\alpha,b)} (-1)^{a \cdot x + \beta \cdot \psi(x) + h(x) + h(x+\alpha)} \right)^4 \\
&= C_{11} + C_{12}, \\
C_{11} &= 2^{2m} \sum_{a \in \mathbb{F}_2^n} \sum_{\beta \in \mathbb{F}_2^n} \sum_{(\alpha,b) \in E_2} \left(\sum_{x \in \Delta(\alpha,b)} (-1)^{a \cdot x + \beta \cdot \psi(x) + h(x) + h(x+\alpha)} \right)^4 = 2^{3m+3}|E_2|,
\end{aligned}$$

$$C_{12} = 2^{2m} \sum_{a\in\mathbb{F}_2^n} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\psi(x)+h(x)+h(x+\alpha)} \right)^4 .$$

For each $(\alpha, b) \in E_4$, there exist four distinct elements $x_1, x_1+\alpha, x_2, x_2+\alpha \in \mathbb{F}_2^n$ such that $D_\alpha\psi(x_j) = D_\alpha\psi(x_j+\alpha) = b$ where $j = 1$ and 2. For $j = 1$ and 2,

$$\begin{aligned} S_j &= (-1)^{a\cdot x_j+\beta\cdot\psi(x_j)+h(x_j)+h(x_j+\alpha)} + (-1)^{a\cdot(x_j+\alpha)+\beta\cdot\psi(x_j+\alpha)+h(x_j+\alpha)+h(x_j)} \\ &= (1+(-1)^{a\cdot\alpha+\beta\cdot b})(-1)^{\epsilon_j}, \end{aligned}$$

where $\epsilon_j = a\cdot x_j + \beta\cdot\psi(x_j) + h(x_j) + h(x_j+\alpha)$. Further,

$$\begin{aligned} C_{12} &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (S_1+S_2)^4 \\ &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b})^4((-1)^{\epsilon_1}+(-1)^{\epsilon_2})^4 \\ &= 2^{2m} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (8+8(-1)^{a\cdot\alpha+\beta\cdot b})(1+(-1)^{\epsilon_1+\epsilon_2})^4 \\ &= 2^{2m+6} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b})(1+(-1)^{\epsilon_1+\epsilon_2}) \\ &= 2^{2m+6} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_4} \sum_{a\in\mathbb{F}_2^n} (1+(-1)^{a\cdot\alpha+\beta\cdot b}+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{a\cdot\alpha+\beta\cdot b+\epsilon_1+\epsilon_2}) \\ &= 2^{3m+6}|E_4|. \end{aligned}$$

We note that, $\sum_{a\in\mathbb{F}_2^n}((-1)^{a\cdot\alpha+\beta\cdot b}+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{a\cdot\alpha+\beta\cdot b+\epsilon_1+\epsilon_2}) = 0$, since $\alpha \neq 0, x_1+x_2 \neq 0$ and $x_1+x_2+\alpha \neq 0$.

$$\begin{aligned} C_1 = C_{11} + C_{12} &= 2^{3m+3}(|E_2| + 8|E_4|) \\ &= 2^{3m+n+2}(2^n-1) + 3\cdot 2^{3m+4}|E_4| > 2^{3m+n+2}(2^n-1), \end{aligned}$$

and the claimed inequality follows. ■

Corollary 7.3.15. *The Gowers U_3 norm of a Maiorana–McFarland bent function constructed by using a differentially 4-uniform permutation is always larger than the Gower norm of any Maiorana–McFarland bent function obtained by using an APN permutation.*

Proof. The proof is immediate from the results of Theorems 7.3.12 and 7.3.14. ■

Theorem 7.3.16. *Let K be a bent function on $\mathbb{F}_2^m \cong \mathbb{F}_2^n \times \mathbb{F}_2^n$, $m = 2n$, defined by*

$$K(x,y) = \phi_\delta(x) \cdot y$$

where ϕ_δ is a differentially δ-uniform permutation on $\mathbb{F}_2^n$, $\delta = 2t$. The Gowers U_3 norm of $k(x,y) = (-1)^{K(x,y)}$, $(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, is

$$\|k\|_{U_3}^8 \geq \frac{7 \cdot 2^n - 6}{2^{3n}}.$$

Proof. Using similar arguments as in Theorem 7.3.12,

$$\|k\|_{U_3}^8 = \frac{1}{2^{5m}}(A_1^{'} + B_1^{'} + C_1^{'})$$

where

$$\begin{aligned}
A_1^{'} &= \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,0)}K(x,y)+a\cdot x+b\cdot y} \right)^4 = 2^{4m}, \\
B_1^{'} &= \sum_{\beta\in\mathbb{F}_2^n\backslash\{0\}} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(0,\beta)}K(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= \sum_{\beta\in\mathbb{F}_2^n\backslash\{0\}} \sum_{a\in\mathbb{F}_2^n} \left(2^n \sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot\phi_\delta(x)+a\cdot x} \right)^4 \\
&\geq 2^{3m+n+1}(2^n - 1), \quad \text{(cf. [30, page 415])}, \\
C_1^{'} &= \sum_{\alpha\in\mathbb{F}_2^n\backslash\{0\}} \sum_{\beta\in\mathbb{F}_2^n} \sum_{(a,b)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} \left(\sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} (-1)^{D_{(\alpha,\beta)}K(x,y)+a\cdot x+b\cdot y} \right)^4 \\
&= 2^{2m} \sum_{a,\beta\in\mathbb{F}_2^n} \sum_{i=1}^{t} \sum_{(\alpha,b)\in E_{2i}} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi_\delta(x)} \right)^4 \\
&= C_{11}^{'} + C_{12}^{'} + \ldots + C_{1t}^{'}
\end{aligned}$$

where

$$C_{1j}^{'} = 2^{2m} \sum_{a,\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_{2j}} \left(\sum_{x\in\Delta(\alpha,b)} (-1)^{a\cdot x+\beta\cdot\phi_\delta(x)} \right)^4, 1 \leq j \leq t.$$

Now we claim that, $C_{1j}^{'} \geq 2^{3m+3}(j|E_{2j}|)$, for all $j \in \{1, 2, \ldots, t\}$. Since $C_{11}^{'} = 2^{3m+3}|E_2|$ and $C_{12}^{'} \geq 2^{3m+3}(2|E_4|)$, for each $(\alpha, b) \in E_{2j}$, there exist $2j$ distinct elements $x_1, x_1+\alpha, x_2, x_2+\alpha, \ldots, x_j, x_j+\alpha \in \mathbb{F}_2^n$ such that $D_\alpha\phi_\delta(x_s) = D_\alpha\phi_\delta(x_s+\alpha)$=b, $s \in \{1, 2, \ldots, j\}$. Let

$$S_s = (-1)^{a\cdot x_s+\beta\cdot\phi_\delta(x_s)} + (-1)^{a\cdot(x_s+\alpha)+\beta\cdot\phi_\delta(x_s+\alpha)} = \left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)(-1)^{\epsilon_s}$$

where $\epsilon_s = a \cdot x_s + \beta \cdot \phi_\delta(x_s)$, for all $s \in \{1, 2, \ldots, j\}$. Thus,

$$\begin{aligned} C_{1j}^{'} &= 2^{2m} \sum_{a,\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_{2j}} (S_1+S_2+\ldots+S_j)^4 \\ &= 2^{2m} \sum_{a,\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_{2j}} \left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)^4 ((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\ldots+(-1)^{\epsilon_j})^4 \\ &= 2^{2m+3} \sum_{a,\beta\in\mathbb{F}_2^n} \sum_{(\alpha,b)\in E_{2j}} \left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right) ((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\ldots+(-1)^{\epsilon_j})^4 . \end{aligned}$$

Since,

$$\begin{aligned} &((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\ldots+(-1)^{\epsilon_j})^4 \\ =&\left(1+(-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right)^4 \\ =&1+4\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right) \\ &+6\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right)^2 \\ &+4\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right)^3 \\ &+\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right)^4 . \end{aligned}$$

Again,

$$\begin{aligned} &\left((-1)^{\epsilon_1+\epsilon_2}+(-1)^{\epsilon_1+\epsilon_3}+\ldots+(-1)^{\epsilon_1+\epsilon_j}\right)^4 \\ =&\left(1+(-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\ldots+(-1)^{\epsilon_2+\epsilon_j}\right)^4 \\ =&1+4\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\ldots+(-1)^{\epsilon_2+\epsilon_j}\right) \\ &+6\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\ldots+(-1)^{\epsilon_2+\epsilon_j}\right)^2 \\ &+4\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\ldots+(-1)^{\epsilon_2+\epsilon_j}\right)^3 \\ &+\left((-1)^{\epsilon_2+\epsilon_3}+(-1)^{\epsilon_2+\epsilon_4}+\ldots+(-1)^{\epsilon_2+\epsilon_j}\right)^4 . \end{aligned}$$

After $(j-2)$ similar steps, we get,

$$\left((-1)^{\epsilon_{j-2}+\epsilon_{j-1}}+(-1)^{\epsilon_{j-2}+\epsilon_j}\right)^4=\left(1+(-1)^{\epsilon_{j-1}+\epsilon_j}\right)^4=8+8(-1)^{\epsilon_{j-1}+\epsilon_j}.$$

Therefore, $((-1)^{\epsilon_1}+(-1)^{\epsilon_2}+\ldots+(-1)^{\epsilon_j})^4=(j-2)+8+P_1=j+P$ where $P=P_1+6$ is the sum of some positive integer and terms of the form $(-1)^{\sum_{l\in E}\epsilon_l}$, $E\subseteq[j]$ with some multiplicity. Since for any $E\subseteq[j]$, $\sum_{a\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}x_l)\cdot a}$, $\sum_{a\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}x_l+\alpha)\cdot a}$, $\sum_{\beta\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}\phi_\delta(x_l))\cdot\beta}$ and $\sum_{\beta\in\mathbb{F}_2^n}(-1)^{(\sum_{l\in E}\phi_\delta(x_l)+b)\cdot\beta}$ are nonnegative integers,

$$\begin{aligned}
C_{1j}^{'}&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(1+(-1)^{a\cdot\alpha+b\cdot\beta}\right)(j+P)\\
&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(j+P+j(-1)^{a\cdot\alpha+b\cdot\beta}+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\\
&=2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}j+2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}\left(P+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\\
&\geq 2^{2m+3}\sum_{a,\beta\in\mathbb{F}_2^n}\sum_{(\alpha,b)\in E_{2j}}j=2^{3m+3}(j|E_{2j}|),
\end{aligned}$$

as $\sum_{a\in\mathbb{F}_2^n}\sum_{\beta\in\mathbb{F}_2^n}\left(P+P(-1)^{a\cdot\alpha+b\cdot\beta}\right)\geq 0$. Thus,

$$\begin{aligned}
C_1^{'}&=C_{11}^{'}+C_{12}^{'}+\ldots+C_{1t}^{'}\\
&\geq 2^{3m+3}(|E_2|+2|E_4|+\ldots+t|E_{2t}|)\\
&=2^{3m+n+2}(2^n-1),
\end{aligned}$$

and the theorem follows. ■

The proof of the next corollary follows directly from Theorem 7.3.12 and 7.3.16.

Corollary 7.3.17. *The Gowers U_3 norm of a Maiorana–McFarland bent function defined as in Theorem 7.3.16 is always larger than the norm of a Maiorana–McFarland bent function obtained by using an APN permutation.*

7.3.4 Gowers U_3 norm for a class of cubic monomial function

This section is aimed at demonstrating how we envision the use of Gowers U_3 norm to identify the classes of functions with potentially high second-order nonlinearity. This section also shows that the largest second-order nonlinearity may not be observed within the class of bent functions. We consider a class of cubic monomial function similar to those considered by Canteaut, Charpin and Kyureghyan [7].

Theorem 7.3.18. *Let $m = 3r$, $r > 1$ be a positive integer. Let $F_r \in \mathcal{B}_m$ be a cubic Boolean function defined by*

$$F_r(x) = \mathrm{Tr}_1^n(\lambda x^{2^{2r}+2^r+1}),$$

for all $x \in \mathbb{F}_{2^m}$ where $\lambda \in \mathbb{F}_{2^r}^*$ and $f_r(x) = (-1)^{F_r(x)}$, for all $x \in \mathbb{F}_{2^m}$. Then the Gowers U_3 norm of f_r is

$$\|f_r\|_{U_3} = \frac{2^m + 2^r(2^m-1)}{2^{2m}}. \tag{7.3.5}$$

Proof. The Gowers U_3 norm of f_r can be written as

$$\begin{aligned}
\|f_r\|_{U_3}^8 &= \frac{1}{2^{4m}}\left|\sum_{a,b,h,x\in\mathbb{F}_{2^m}} (-1)^{D_{a,b,h}F_r(x)}\right| \\
&= \frac{1}{2^{4m}}\left|\sum_{a,b\in\mathbb{F}_{2^m}}\sum_{h,x\in\mathbb{F}_{2^m}} (-1)^{D_{a,b}F_r(x)+D_{a,b}F_r(x+h)}\right| \\
&= \frac{1}{2^{4m}}\left|\sum_{a,b\in\mathbb{F}_{2^m}}\left(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{D_{a,b}F_r(x)}\right)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}\left(\sum_{a\in\mathbb{F}_{2^m}} 1 + \sum_{\substack{b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a=0}} 1 + \sum_{\substack{a\in\mathbb{F}_{2^m}\setminus\{0\}\\ b=0}} 1\right) + \sum_{\substack{a,b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a\neq b}}\left(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{D_{a,b}F_r(x)}\right)^2\right| \\
&= \frac{1}{2^{4m}}\left|2^{2m}(3\cdot 2^m - 2) + \sum_{\substack{a,b\in\mathbb{F}_{2^m}\setminus\{0\}\\ a\neq b}}\left(\sum_{x\in\mathbb{F}_{2^m}} (-1)^{D_{a,b}F_r(x)}\right)^2\right|.
\end{aligned}$$

Since $\deg(D_{a,b}F_r)$ is at most 1, $D_{a,b}F_r$ is either balanced or constant. We find those nonzero $a, b \in \mathbb{F}_{2^m}$ with $a \neq b$ such that $D_{a,b}F_r(x)$ is constant for all $x \in \mathbb{F}_{2^m}$.

$$D_{a,b}F_r(x) = \mathrm{Tr}_1^m(\lambda(a^{2^r}b+ab^{2^r})x)+\mathrm{Tr}_1^m\left(\lambda\left((a^{2^{2r}}b^{2^r+1}+a^{2^r+1}b^{2^{2r}})+(a^{2^{2r}}+b^{2^{2r}})(a^{2^r}b+ab^{2^r})\right)\right)$$

$D_{a,b}F_r(x)$ is constant for all $x \in \mathbb{F}_{2^m}$ if and only if

$$\lambda\left(a^{2^r}b+ab^{2^r}\right)=0 \;\Leftrightarrow\; a^{2^r}b+ab^{2^r}=0 \;\Leftrightarrow\; \left(\frac{b}{a}\right)^{2^r-1}=1 \;\Leftrightarrow\; \frac{b}{a}\in\mathbb{F}_{2^r}\setminus\mathbb{F}_2 \;\Leftrightarrow\; b=\beta a$$

where $\beta \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Thus, given any $a \in \mathbb{F}_{2^m}^*$, b can be chosen in $2^r - 2$ ways. Therefore, the total number of ways in which a, b can be chosen is $(2^m - 1)(2^r - 2)$. Thus,

$$\|f_r\|_{U_3} = \frac{2^m + 2^r(2^m - 1)}{2^{2m}},$$

which shows the theorem. ■

We compare Gowers U_3 norms of a cubic Maiorana–McFarland bent function, f say, constructed by using APN permutations as in Theorem 7.3.12, and cubic monomial Boolean functions considered above. Let $m = 2n = 3r$, i.e., $n = \frac{3r}{2}$.

$$\begin{aligned} \|f_r\|_{U_3}^8 - \|f\|_{U_3}^8 &= \frac{2^m + 2^r(2^m - 1)}{2^{2m}} - \frac{7 \cdot 2^n - 6}{2^{3n}} \\ &= \frac{2^m + 2^{m+r} - 2^r - 7 \cdot 2^m + 6 \cdot 2^n}{2^{2m}} \\ &= \frac{6 \cdot 2^n + 2^m(2^r - 6) - 2^r}{2^{2m}}. \end{aligned}$$

It can be directly checked that if $r = 2$ then $\|f_r\|_{U_3}^8 < \|f\|_{U_3}^8$ and if $r \geq 3$ then $\|f_r\|_{U_3}^8 > \|f\|_{U_3}^8$. This suggests that the second-order nonlinearity of f_r is greater than the one of f if $m = 6$ and for $m \geq 10$ such is not the case.

There are three known affine inequivalent classes of cubic bent functions in 6 variables [86]. It is also known that all the cubic bents are affine equivalent to Maiorana–McFarland bent functions. By direct computation we have found that their second-order nonlinearities are 8, 12 and 16. Motivated by the low Gowers U_3 norm of F_2, obtained by substituting $r = 2$ in Equation (7.3.5), we have computed the second-order nonlinearity of F_2. We find that while it is not bent, having nonlinearity 22, its second-order nonlinearity has the maximum possible value in $\mathcal{B}_6$, namely 18. However, the reversal of the inequality sign for $r \geq 3$ indicates that this trend will not extend to 12 variables, i.e., for $r = 4$.

Chapter 8

Conclusion and Future scope

8.1 Conclusion

In this thesis, we analyze some classes of bent functions and derive results related to their explicit constructions and affine equivalence. We further identify some Boolean functions which have high second-order nonlinearity using the Gowers U_3 norm and for the particular case $n = 6$, we get a class of cubic Boolean functions possessing maximum second-order nonlinearity.

We prove that cubic Maiorana–McFarland bent functions which are constructed by using some known types of permutation polynomials (see [2,154]) have no affine derivative. We have obtained many affine inequivalent classes of bent functions within the considered functions.

The problem of specifying suitable linear subspaces of low dimension for some generic classes of permutations related to the derivations of new bent functions in $\mathcal{C}$ has been partially addressed. The results clearly indicate the hardness of this problem due to the fact that whereas some "suitable" permutations may finally yield bent functions within class $\mathcal{C}$, for other permutations such functions simply cannot exist.

For the generalized case, that is, Boolean functions defined over any finite field, we introduce the subspace sum concept (depending upon the derivatives) and prove many of its properties. In particular, it is shown that the subspace sum is an affine invariant and, consequently, a necessary condition is derived for the Maiorana–McFarland bent functions. We construct two new classes of generalized bent functions (namely, $\mathcal{D}^p$, $\mathcal{D}_0^p$ and $\mathcal{C}^p$ where

$\mathcal{D}_0^p$ is a subclass of $\mathcal{D}^p$). We derive some existence and nonexistence results concerning the bent functions in $\mathcal{C}^p$ class for some known classes of permutations over $\mathbb{F}_p^n$.

We construct a class of cubic Maiorana–McFarland bent-negabent functions by using Feistel functions, and prove that it has affine derivatives over a subspace. Then we calculate weight distributions of second-derivatives and obtain the lower bound of their second-order nonlinearities.

We locate some functions with low Gowers U_3 norms. We explicitly compute the Gowers U_3 norm of cubic Maiorana–McFarland bent functions and demonstrate that the norm depends on the differential property of the associated permutation rather than its algebraic degree. Since the Gowers U_3 norms are related to the second-order nonlinearity of the Boolean functions, their dependence of differential properties rather than degree is noteworthy. We also compute the Gowers U_3 norms for a class of cubic monomial functions, not necessarily bent, and show that for $n = 6$, these norm values are less than that of Maiorana-McFarland bent functions. Further, we computationally show that there exist 6-variable functions in this class which are not bent but achieve the maximum second-order nonlinearity for 6 variables.

8.2 Future scope

There are many open questions on Boolean functions and generalized Boolean functions apart from the results given in this thesis. We summarize below some open problems which immediately arise from our study.

- The challenge in this direction of research is to explicitly characterize all bent functions for all dimensions. We mention here that the total number of bent functions is only known for $n \leq 8$ (see [120,135]). The problem is intractable since most of the methods for counting bent functions rely on an incomplete set of invariants and search space is doubly-exponential in n.

- Given any two Boolean functions, deciding whether they are equivalent or not is an important open question. Direct verification requires computational complexity of $O(2^{n^2})$. Finding out an appropriate set of invariants to distinguish bent functions with better resolution is extremely important.

- It appears that additional efforts are needed for getting a better understanding and for deriving more explicit subclasses within the $\mathcal{C}$ and $\mathcal{D}$ class. Also, the question whether the classes of permutations specified and related subspaces indeed give rise to bent functions outside $\mathcal{M}$ (and possibly outside $\mathcal{PS}$ as well) remains open.

- Using the subspace sum concept one can consider the *generalized Boolean functions* and may be able to construct or identify new classes of *generalized bent functions*.

- The covering radius of rth order Reed–Muller codes and finding a Boolean function having highest possible rth order nonlinearity are equivalent problems. Both are difficult to solve. Applicability of the Gowers uniformity norms point to an interesting direction of research.

Bibliography

[1] A. A. Bovdi, *Group Algebra*, In Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer, 2001.

[2] A. Blokhuis, R. S. Coulter, M. Henderson and C. M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, In: Jungnickel D., Niederreiter H. (eds), Finite Fields and Applications, Springer, Berlin, Heidelberg, pp. 37–42, 2001.

[3] A. Biryukov, S. Mukhopadhyay and P. Sarkar, *Improved Time-Memory Trade-Offs with Multiple Data*, SAC 2005. LNCS, Springer, vol. 3897, pp. 110–127, 2006.

[4] A. C. Ambrosimov, *Properties of the Bent Functions of q-Ary Logic over Finite Fields*, Discrete Mathematics, vol. 6 (3), pp. 50–60, 1994.

[5] A. Canteaut and P. Charpin, *Decomposing bent functions*, IEEE Transactions on Information Theory, vol. 49 (8), pp. 2004–2019, 2003.

[6] A. Canteaut and M. Trabbia, *Improved fast correlation attacks using parity-check equations of weight* 4 *and* 5, In Advanced in Cryptology EUROCRYPT'00, LNCS, Springer, vol. 1807, pp. 573–588, 2000.

[7] A. Canteaut, P. Charpin and G. M. Kyureghyan, *A new class of monomial bent functions*, Finite Fields and their Applications, vol. 14 (1), pp. 221–241, 2008.

[8] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001, http://www.cacr.math.uwaterloo.ca/hac.

[9] A. Muratović-Ribić and E. Pasalic, *A note on complete polynomials over finite fields and their applications in cryptography*, Finite Fields and Their Applications, vol. 25, pp. 306–315, 2014.

[10] A. Pott, Y. Tan, T. Feng and S. Ling, *Association schemes arising from bent functions*, Designs, Codes and Cryptography, vol. 59 (1), pp. 319–331, 2011.

[11] B. Green and T. Tao, *An inverse theorem for the Gowers $U^3(G)$ norm*, arXiv:0503014v3 [math.NT], 5 Aug 2006.

[12] B. Green, T. Tao and T. Ziegle, *An inverse theorem for the Gowers' $U^{s+1}[N]$-norm*, Annals of Mathematics, vol. 176 (2), pp. 1231–1372, 2012.

[13] B. K. Roy, *A Brief Outline of Research on Correlation Immune Functions*, ACISP 2002, LNCS, Springer-Verlag, vol. 2384, pp. 379–394, 2002.

[14] B. Wu, *$\mathcal{PS}$ bent functions constructed from finite pre-quasifield spreads*, In ArXiv e-print, 2013.

[15] C. Carlet and A. Klapper, *Upper bounds on the numbers of resilient functions and of bent functions*, In 23rd Sysmposium on Information Theory in the Bexelux, Louvain-La-Neuve, Belgique, 2002.

[16] C. Bracken, E. Byrne, N. Markin and G. McGuire, *Determining the nonlinearity of a new family of APN functions*, AAECC 2007, LNCS, Springer, vol. 4851, pp. 72–79, 2007.

[17] C. Carlet, *Two new classes of bent functions*, in: Proc. EUROCRYPT'93, LNCS, Springer, vol. 765, pp. 77–101, 1994.

[18] C. Carlet, *A construction of bent functions*, In Finite Fields and Applications, vol. 233, London Mathematical Society, pp. 47–58, 1996.

[19] C. Carlet, *On Cryptographic Propagation Criteria for Boolean Functions*, Information and Computation, vol. 151 (1-2), pp. 32–56, 1999.

[20] C. Carlet, *The complexity of Boolean functions from cryptographic viewpoint*, In: Dagstuhl Seminar Proceedings, 06111, Complexity of Boolean Functions, 2006.

[21] C. Carlet, *On bent and highly nonlinear balanced/resilient functions and their algebraic immunities*, In proceeding of the AAECC 2006, LNCS, Springe-Verlag, vol. 3857, pp. 1–28, 2006.

[22] C. Carlet, *On the higher order nonlinearities of algebraic immune functions*, In CRYPTO'06, LNCS, Springe-Verlag, vol. 4117, pp. 584–601, 2006.

[23] C. Carlet, *More $\mathcal{PS}$ and $\mathcal{H}$-like bent functions*, In Cryptology ePrint Archive, Report 2015/168, 2015.

[24] C. Carlet and C. Ding, *Highly nonlinear mappings*, Journal of Complexity, vol. 20 (23), pp. 205–244, 2004.

[25] C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra, *Algebraic immunity for cryptographically significant Boolean functions: Analysis and Construction*, IEEE Transactions on Information Theory, vol. 52 (7), pp. 1259–1269, 2006.

[26] C. Carlet, P. Charpin and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Designs, Codes and Cryptography, vol. 15 (2), pp. 125–156, 1998.

[27] C. Carlet and S. Mesnager, *Improving the upper bounds on the covering radii of binary Reed-Muller codes*, IEEE Transactions on Information Theory, vol. 53 (1), pp. 162–173, 2007.

[28] C. Carlet, *Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications*, IEEE Transactions on Information Theory, vol. 54 (3), pp. 1262–1272, 2008.

[29] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes, in Boolean Methods and Models*, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press [Online]. Available: http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html l, to be published.

[30] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge Univ. Press, Yves Crama and Peter L. Hammer (eds.), pp. 257–397, 2010.

[31] C. Carlet, *Vectorial (Multi-Output) Boolean Functions for Cryptography, in Boolean Methods and Models*, Y. Crama and P. Hammer, Eds. Cam-

bridge, U.K.: Cambridge Univ. Press [Online]. Available: http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.htm, to be published.

[32] C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, LNCS, Springer, vol. 561, 1991.

[33] C. Riera and M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Transactions on Information Theory, vol. 52 (9), pp. 4142–4159, 2006.

[34] C. E. Shannon, *Communication theory of secrecy sysytem*, In Bell sysytem tecnical journal, vol. 28, pp. 776–779, 1949.

[35] D. K. Dalai, S. Maitra and S. Sarkar, *Basic theory in construction of Boolean functions with maximum possible annihilator immunity*, Designs, Codes and Cryptography, vol. 40 (1), pp. 41–58, 2005.

[36] D. R. Stinson, *Cryptography Theory and Practic*, CRC Press, Second Edition, 2002.

[37] D. Tang, C. Carlet and X. Tang, *On the second-order nonlinearities of some bent functions*, Information Sciences, vol. 223, pp. 322–330, 2013.

[38] E. F. Assums, Jr and J. D. Key, *Polynomial codes and finite Geometries*, 1996.

[39] E. F. Assmus and J. Key, *Polynomial Codes and Finite Geometries*, in Handbook of Coding Theory–Part 2: Connections (V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds.), Amsterdam The Netherlands: Elsevier, 1998, Ch. 16, pp. 1269–1343.

[40] E. R. Berlekamp and L. R. Welch, *Weight distributions of the cosets of the* $(32, 6)$ *Reed–Muller code*, IEEE Transactions on Information Theory, vol. 18 (1), pp. 203–207, 1972.

[41] F. J. MacWilliams and N. J. A. Sloane, *The theory of error–correcting codes*, North-Holland, Amsterdam, 1977.

[42] F. Xiutao and G. Gong, *On Algebraic Immunity of Trace Inverse Functions on Finite Fields of Characteristic Two*, Journal of Systems Science and Complexity, vol. 29 (1), pp. 272–288, 2016.

[43] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Elsevier, 1997.

[44] G. Kabatiansky and C. Tavernier, *List decoding of second order Reed-Muller codes*, In: Proceedings of the eighth International Symposium of Communication Theory and Applications, Ambleside, UK, July 2005.

[45] G. Sun and C. Wu, *The lower bounds on the second order nonlinearity of a class of Boolean functions with high nonlinearity*, Applicable Algebra in Engineering, Communication and Computing, vol. 22 (1), pp. 37–45, 2011.

[46] G. Sun and C. Wu, *The lower bounds on the second order nonlinearity of three classes of Boolean functions with high nonlinearity*, Information Sciences, vol. 179 (3), pp. 267–278, 2009.

[47] G. Sivek, *On vanishing sums of distinct roots of unity*, Integers, vol. 10 (3), pp. 365–368, 2009.

[48] H. Dobbertin, *Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case*, IEEE Transactions on Information Theory, vol. 45 (4), pp. 1271–1275, 1999.

[49] H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, Fast Software Encryption, Leuven 1994, LNCS, vol. 1008, pp. 61–74, 2005.

[50] I. Dumer, G. Kabatiansky and C. Tavernier, *List decoding of second order Reed-Muller codes up to the Johnson bound with almost linear complexity*, In: Proceedings of the IEEE International Symposium on Information Theory, Seattle, WA, July 2006, pp. 138–142.

[51] J. Arndt, *Matters Computational: Ideas, Algorithms, Source Code*, Springer, 2010.

[52] J. D. Golić and M. J. Mihaljević, *A Generalized Correlation Attack on a Class of Stream Ciphers Based on the Levenshtein Distance*, Journal of Cryptology, vol. 3 (3), pp. 201–212, 1991.

[53] J. D. Olsen, R. A. Scholtz and L. R. Welch, *Bent-function sequences*, IEEE Transactions on Information Theory, vol. 28 (6), pp. 858–864, 1982.

[54] J. F. Dillon, *A survey of bent functions*, NSA Tecnical Journal, Special issue, pp. 191–215, 1974.

[55] J. F. Dillon, *Elementary Hadamard Difference Sets*, PhD Thesis, University of Maryland, 1974.

[56] J. F. Dillon, *Elementary Hadamard difference sets*, in: Proceedings of 6th S. E. Conference on Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249, 1975.

[57] J. Golic, *Fast low order approximation of cryptographic functions*, In: Proceedings of the EUROCRYPT'96, LNCS, Springer, vol. 1996, pp. 268–282, 1996.

[58] J. J. Mykkeltveit, *The covering radius of the* $(128, 8)$ *Reed-Muller code is 56*, IEEE Transactions on Information Theory, vol. 26 (3), pp. 359–362, 1980.

[59] J. L. Massey, *Shift-register synthesis and BCH decoing*, IEEE Transactions on Information Theory, Vol. 15 (1), pp. 122–127, 1969.

[60] K. G. Paterson, *On Codes with Low Peak-to-Average Power Ratio for Multicode CDMA*, IEEE Transactions on Information Theory, vol. 50 (3), pp. 550–558, 2004.

[61] K. Nyberg, *Differentially uniform mapping for cryptography*, Proceeding of EUROCRYPT'93, LNCS, Springer, vol. 765, pp. 55–64, 1994.

[62] K. Nyberg and R. L. Knudsen, *Provable security against a differential attacks*, Journal of Cryptology, vol. 14 (1), pp. 27–38, 1995.

[63] K.-U. Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*, In IEEE International Symposium on Information TheoryISIT-2007, France, Proceedings (2007), pp. 2781-2785 (http://arxiv.org/abs/cs.IT/0611162).

[64] K.-U. Schmidt, M. G. Parker and A. Pott, *Negabent functions in the Maiorana–McFarland class*, In Proc. International Conference on Sequences and Their Applications 2008, LNCS, Springer, vol. 5203, pp. 390–402, 2008.

[65] L. Budaghyan, C. Carlet and A. Pott, *New classes of almost bent and almost perfact nonlinear functions*, IEEE Transactions on Information Theory, vol. 52 (3), pp. 1141–1152, 2006.

[66] L. Budaghyan, C. Carlet, T. Helleseth and A. Kholosha, *Generalized Bent Functions and their Relation to Maiorana–McFarland Class*, IEEE International Symposium on Information Theory, pp. 1212–1215, 2012.

[67] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer, 2015.

[68] L. Poinsot, *Multidimensional Bent Functions*, GESTS Intern. Transactions on Comput. Sci. Eng., vol. 18 (1), pp. 185–195, 2005.

[69] L. Poinsot and S. Harari, *Generalized Boolean Bent Functions*, In Progress in Cryptology INDOCRYPT 2004, India, LNCS, vol. 3348, pp. 107–119, 2005.

[70] L. Qu, Y. Tan, C. Li and G. Gong, *More constructions of differentially* 4*-uniform permutations on* $\mathbb{F}_{2^{2k}}$, Designs, Codes and Cryptography, vol. 78 (2), pp. 391–408, 2016.

[71] L. R. Knudsen and M. J. B. Robshaw, *Non-linear approximations in linear cryptanalysis*, In: Proceedings of the EUROCRYPT'96, LNCS, Springer, vol. 1070 pp. 224–236, 1996.

[72] L. Wang, *On Permutation Polynomials*, Finite Fields and Their Applications, vol. 8 (3), pp. 311–322, 2002.

[73] M. G. Parker and A. Pott, *On Boolean functions which are bent and negabent*, In: Proc. Int. Conf. Sequences, Subsequences, Consequences 2007, LNCS, Springer, vol. 4893, pp. 9–23, 2007.

[74] M. J. Mihaljević, M. P. C. Fossorier and H. Imai, *A Low-Complexity and High-Performance Algorithm for the Fast Correlation Attack*, FSE 2000, LNCS, Springer, vol. 1978, pp. 196–212, 2001.

[75] M. Kontak and J. Szmidt, *Nonlinearity of Round Function*, Control and Cybernatics, vol. 36 (4), pp. 1037–1044, 2007.

[76] M. Matsui, *Linear cryptanalysis method for DES cipher*, In: Proceedings of the EUROCRYPT'93, LNCS, Springer, vol. 765, pp. 386–397, 1994.

[77] M. P. C. Fossorier, M. J. Mihaljević and H. Imai, *Modeling Block Decoding Approaches for the Fast Correlation Attack*, IEEE Transactions on Information Theory, vol. 53 (12), pp. 4728–4737, 2007.

[78] N. Courtois, *Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt*, In Proceedings of the ICISC'02, LNCS, Springer, vol. 2587, pp. 182–199, 2002.

[79] N. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, Advances in Cryptology CRYPTO'03, LNCS, Springer-Verlag, vol. 2729, pp. 176–194, 2003.

[80] N. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, Advance in Cryptology EUROCRYPT'03, LNCS, Springer-Verlag, vol. 2656, pp. 346–359, 2003.

[81] N. J. Patterson and D. H. Wiedemann, *The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least 16276*, IEEE Transactions on Information Theory, vol. 29 (3), pp. 354–356, 1983.

[82] N. N. Tokareva, *The Bent Functions: Results and Applications. An Overview*, Prikl. Diskret. Mat., vol. 2 (1), pp. 15–37, 2009.

[83] N. N. Tokareva, *Generalizations of Bent functions. A survey*, Journal of Applied and Industrial Mathematics, vol. 5 (1), pp. 110–129, 2011.

[84] O. A. Logachev, A. A. Salnikov, and V. V. Yashchenko, *Bent Functions Over a Finite Abelian Group*, Diskret.Mat., vol. 9 (4), pp. 3–20, 1997.

[85] O. A. Logachev, A. A. Salnikov and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptography, Translations of Mathematical Monographs*, American Mathematical society, vol. 241, 2012.

[86] O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A, vol. 20 (3), pp. 300–305, 1976.

[87] P. Charpin, *Codes cycliques étendus invariants sous le groupe affine*, Thèse de Doctorat d'État Université Paris VII, 1987.

[88] P. Charpin, *Une generalisation de la construction de Berman des codes de Reed et Muler p-aires*, Communication in Algebra, vol. 16 (11), pp. 2231–2246, 1988.

[89] P. Charpin, *Normal Boolean functions*, Journal of Complexity, vol. 20 (2-3), pp. 245–265, 2004.

[90] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, *On Correlation-Immune Functions*, In Proc. CRYPTO'91, LNCS 576, Springer-Verlag, pp. 86–100, 1992.

[91] P. Charpin and S. Sarkar, *Polynomials with Linear Structure and Maiorana–McFarland Construction*, IEEE Transactions on Information Theory, vo. 57(6), pp. 3796–3804, 2011.

[92] P. Delsarte, J. M. Goethals and F. J. MacWilliams, *On Generalized Reed-Muller Codes and Their Relatives*, Information and Control, vol. 16 (5), pp. 403–442, 1970.

[93] P. Langevin, G. Leander, P. Rabizzoni and J. P. Zanotti, *Counting all bent functions in dimension eight* 99270589265934370305785861242880, Designs, Codes and Cryptography, vol. 59 (1), pp. 193–205, 2011.

[94] P. Lisoněk and H. Y. Lu, *Bent functions on parcial spreads*, Designs, Codes and Cryptography, vol. 73 (1), pp. 209–216, 2014.

[95] P. Sarkar and S. Maitra, *Construction of nonlinear Boolean functions with important cyrptographic properties*, In: Proceedings of the EUROCRYPT'00, LNCS, Springer, vol. 1870, pp. 485–506, 2000.

[96] P. Sarkar and S. Maitra, *Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes*, Theory of Computing Systems, vol. 35 (1), pp. 39–57, 2002.

[97] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay and S. Maitra, *Investigations on bent and negabent functions via the nega–Hadamard transform*, IEEE Transactions on Information Theory, vol. 58 (6), pp. 4064–4072, 2012.

[98] P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalized bent functions and their properties*, Journal of Combinatorial Theory, Series A, vol. 40 (1), pp. 90–107, 1985.

[99] R. Fourquet and C. Tavernier, *An improved list decoding algorithm for the second order Reed-Muller codes and its applications*, Designs Codes and Cryptography, vol. 49 (1), pp. 323–340, 2008.

[100] R. J. Lecner, *Harmonic analysis of switching functions*, In: Mukhopadhyay A., editor. Recent developments in switching theory, New York: Academic Press, 1971.

[101] R. L. Knudsen and M. J. B. Robshaw, *Nonlinear approximations in linear cryptanalysis*, In proceeding of EUROCRYPT'96, LNCS, Springer-Verlag, vol. 1070, pp. 224–236, 1996.

[102] R. L. McFarland, *A family of noncyclic difference sets*, J. Combinatorial Theory, Series A, vol. 15 (1), pp. 1–10, 1973.

[103] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983.

[104] R. Matthews, *Permutation Properties of polynomials* $1 + x + \cdots + x^k$ *over a finite field*, Proceedings of the American Mathematical Society, vol. 120 (1), pp. 47–51, 1994.

[105] R. S. Coulter, *On the evaluation of a class of Weil sums in characteristic* 2, New Zealand Journal of Mathematics, vol. 28, pp. 171–184, 1999.

[106] S. Agievich, *On the representation of bent functions by bent rectangles*, In probabilistic Methods in Discrete Mathematics, Proceeding of the Fifty International Petrozavodsk Conference (Petrozavodsk, 2000), Utrecht Boston: VSP, pp. 121–124, 2002.

[107] S. A. Jenning, *The structure of the group ring of a p-group over a modular field*, Transactions of the American Mathematical Society, vol. 50, pp. 175–185, 1941.

[108] S. Chakraborty, S. Das, D. K. Das and B. B. Bhattacharya, *Synthesis of Symmetric Functions for Path-Delay Fault Testability*, IEEE Transactions on CAD Integrated Circuits and Systems, vol. 19 (9), pp. 1076–1081, 2000.

[109] S. Gangopadhyay, B. Singh and V. Vetrivel, *Investigations on cubic rotation symmetric bent functions*, Electronic Notes in Discrete Mathematics, vol. 56, pp. 15–19, 2016.

[110] S. Gangopadhyay, S. Sarkar and R. Telang, *On the lower bounds of the second order nonlinearities of some Boolean functions*, Information Sciences, vol. 180 (2), pp. 266–273, 2010.

[111] S. Gangopadhyay, *Affine inequivalence of cubic Maiorana–McFarland type bent functions*, Discrete Applied Mathematics, vol. 161 (7–8), pp. 1141–1146, 2013.

[112] S. H. Kim and J. S. No, *New families of binary sequences with low correlation*, IEEE Transactions on Information Theory, vol. 49 (11), pp. 3059–3065, 2003.

[113] S. Kavut, S. Maitra, S. Sarkar and M. D. Yücel, *Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity* > 240, In: Proceedings of the INDOCRYPT'06, LNCS, Springer, vol. 4329, pp. 266–279, 2006.

[114] S. Kavut and M. D. Yücel, *Generalized rotation symmetric and dihedral symmetric Boolean functions - 9 variable Boolean functions with nonlinearity 242*, In: Proceedings of the AAECC'07, LNCS, Springer, vol. 4851, pp. 266–279, 2007.

[115] S. Maitra and P. Sarkar, *Highly nonlinear resilient functions optimizing Siegnethalers Inequality*, CRYPTO99, LNCS, Springer, vol. 1666, pp. 198–215, 1999.

[116] S. M. Golomb and G. Gong, *Signal Design for Good Correlationfor Wireless Communication, Cryptography and Radar*, Cambridge University Press, Cambridge, 2005.

[117] S. Mukhopadhyay and P. Sarkar, *Application of LFSRs in Time/Memory Trade-Off Cryptanalysis*, WISA 2005, LNCS, Springer Berlin Heidelberg, vol. 3786, pp. 25–37, 2006.

[118] S. Markovski and A. Mileva, *Generating huge quasigroups from small non-linear bijections via extended Feistel function*, Quasigroups and related systems, vol. 17, pp. 91–106, 2009.

[119] S. Mesnager, *On p-ary bent functions from (maximal) partial spreads*, In International conference Finite field and their applications Fq12, New york, 2015.

[120] S. Mesnager, *Bent Functions, Fundamentals and Results*, Springer, 2016.

[121] S. Payne, *Complete determination of translation ovoids in finite Desarguian planes*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. vol. 51, pp. 328–331, 1971.

[122] S. Palit and B. K. Roy, *Cryptanalysis of LFSR-Encrypted Codes with Unknown Combining Function*, ASIACRYPT'99, LNCS, Springer-Verlag, vol. 1716, pp. 306–320, 1999.

[123] S. Palit, B. K. Roy and A. De, *A Fast Correlation Attack for LFSR-Based Stream Ciphers*, ACNS 2003, LNCS, Springer-Verlag, vol. 2846, pp. 331–342, 2003.

[124] S. Rønjom and T. Hellseeth, *A new attack on filter generator*, IEEE Transactions on Information Theory, Vol. 53 (5), pp. 1752–1758, 2007.

[125] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, *Almost perfect nonlinear functions over* $\mathbb{F}_{2^n}$, IEEE Transactions on Information Theory, vol. 52 (9), pp. 4160–4170, 2006.

[126] T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. vol. 11(3), pp. 465–588, 2001.

[127] T. Helleseth and P. V. Kumar, *Sequences with low correlation*, In Handbook of Coding Theory II, North-Holland, Amsterdam, pp. 1765–1853, 1998.

[128] T. Helleseth and A. Kholosha, *Monomial and quadratic bent functions over the finite fields of odd characteristic*, IEEE Transactions on Information Theory, vol. 52 (5), pp. 2018–2032, 2006.

[129] T. Iwata and K. Kurosawa, *Probabilistic higher order differential attack and higher order bent functions*, In: Proceedings of the ASIACRYPT'99, LNCS, Springer, vol. 1716, pp. 62–74, 1999.

[130] T. Jakobsen and L. R. Knudsen, *Attacks on block ciphers of low algebraic degree*, Journal of Cryptology, vol. 14 (3), pp. 197–210, 2001.

[131] T. Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Transactions on Information Theory, vol. 30 (5), pp. 776–780, 1984.

[132] T. Tao, *Structure and randomness in combinatorics*, arXiv:0707.4269v2 [math.CO], 3 Aug 2007.

[133] T. Wada, *Characteristic of Bit Sequences Applicable to Constant Amplitude Orthogonal Multicode systems*, IEICE Trans. Fundamentals, E83-A (11), pp. 2160–2164, 2000.

[134] T. Wu and G. Gong, *Two new message authentication codes based on APN functions and stream ciphers*, Security and Communication Networks, vol. 9 (12), pp. 1864–1871, 2016.

[135] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press, San Diego, CA, 2009.

[136] T. Y. Lam and K. H. Leung, *On vanishing sums of mth roots of unity in finite fields*, Finite Fields and Their Applications, vol. 2 (4), pp. 422–438, 1996.

[137] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, Journal of Algebra, vol. 224 (1), pp. 91–109, 2000.

[138] U. M. Maurer, *New approaches to the design of self-synchronizing stream ciphers*, In: Proceedings of the EUROCRYPT'91, LNCS, Springer, vol. 547, pp. 458–471, 1991.

[139] V. Bergelson, T. Tao and T. Ziegle, *An inverse theorem for the uniformity seminorms associated with the action of $\mathbb{F}_p^\infty$*, Geom. Funct. Anal, vol. 19 (6), pp. 1539–1596, 2001.

[140] V. I. Solodovnikov, *Bent Functions from a Finite Abelian Group to a Finite Abelian Group*, Diskret. Mat., vol. 14 (1), pp. 99–113, 2002.

[141] V. V. Chepyzhov and B. Smeets, *On a fast correlation attacks on stream ciphers*, In proceeding of EUROCRYPT'91, LNCS, Springer, vol. 547, pp. 176–185, 1992.

[142] V. V. Chepyzhov, T. Johansson and B. Smeets, *A simple algorithm for fast correlation attacks on stream ciphers*, In B. Schneier editor, FSE 2000, LNCS, Springer-Verlag, vol. 1978, pp. 181–195, 2001.

[143] V. Y-W. Chen, *The Gowers' norm in the testing of Boolean functions*, Ph.D. thesis. Massachusetts Institute of Technology, June 2009.

[144] W. Millan, *Low order approximation of cipher functions*, In: Cryptographic policy and algorithms, LNCS, Springer, vol. 1029, pp. 144–155, 1996.

[145] W. Meier, E. Pasalic and C. Carlet, *Algebraic attacks and decomposition of Boolean functions*, In EUROCRYPT'04, LNCS, Springer-Verlag, vol. 3027, pp. 474–491, 2004.

[146] W. Su, A. Pott and X. Tang, *Characterization of negabent functions and construction of bent–negabent functions with maximum algebraic degree*, IEEE Transactions on Information Theory, vol. 59 (6), pp. 3387–3395, 2013.

[147] X.-D. Hou, *Some results on the covering radii of Reed-Muller codes*, IEEE Transactions on Information Theory, vol. 39 (2), pp. 366–378, 1993.

[148] X.-D. Hou, *Further results on the covering radii of Reed–Muller codes*, Designs, Codes and Cryptography, vol. 3 (2), pp. 167–177, 1993.

[149] X.-D. Hou, *Cubic bent functions*, Discrete Mathematics, vol. 189 (1–3), pp. 149–161, 1998.

[150] X.-D. Hou, *q-ary bent functions constructed from chain rings*, Finite Fields and Their Applications, vol. 4 (1), pp. 55–61, 2004.

[151] X.-D. Hou, *p-ary and q-ary versions of certain result about bent functions and resilient functions*, Finite Fields and Their Applications, vol. 10 (4), pp. 555–582, 2004.

[152] X.-D. Hou, *Determination of a type of permutation trinomial over finite fields I, II*, manuscripts, 2013, 2014: available at `http://arxiv.org/abs/1309.3530` and `http://arxiv.org/abs/1404.1822`.

[153] X. Guo-Zhen and J. L. Massey, *A Spectral Characterization of Correlation-Immune Combining Functions*, IEEE Transactions on Information Theory, vol. 34 (3), pp. 569–571, 1988.

[154] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields and Their Applications, vol. 13 (1), pp. 58–70, 2007.

[155] Y. M. Chee, Y. Tan and X. D. Zhang, *Strongly regular graphs constructed from p-ary bent functions*, Journal of Algebraic Combinatorics, vol. 34 (2), pp. 251–266, 2011.

[156] Y. Tan, G. Gong and B. Zhu, *Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions*, Cryptography and Communications, vol. 8 (2), pp. 291-311, 2016.

[157] Y. Tan, A. Pott and T. Feng, *Strongly regular graphs associated with ternary bent functions*, Journal of Combinatorial Theory, Series A, vol. 117 (6), pp. 668–682, 2010.

[158] Z. Zhoua and X. Tang, *New nonbinary sequence families with low correlation, large size, and large linear span*, Applied Mathematics Letters, vol. 24 (7), pp. 1105–1110, 2011.