University of Puerto Rico

Río Piedras Campus

Faculty of Natural Sciences
Department of Mathematics

CONSTRUCTION OF NEW DIFFERENTIALLY δ-UNIFORM FAMILIES

By

Roberto Carlos Reyes Carranza

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY
OF PUERTO RICO, RÍO PIEDRAS CAMPUS

July, 2020

APPROVED BY THE DOCTORAL DISSERTATION

COMMITTEE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN MATHEMATICS

AT THE UNIVERSITY OF PUERTO RICO

ADVISOR:

_____

Heeralal Janwa, Ph.D.

University of Puerto Rico, Río Piedras

READERS:

_____

Puhua Guan, Ph.D.

University of Puerto Rico, Río Piedras

_____

Gary McGuire, Ph.D.

University College Dublin

_____

Luis A. Medina, Ph.D.

University of Puerto Rico, Río Piedras

_____

Pantelimon Stănică, Ph.D.

Naval Postgraduate School

Abstract of Ph. D Thesis Presented to the Graduate School
of the University of Puerto Rico, Río Piedras Campus in Partial Fulfillment of the
Requirements for the Degree of Doctor of Philosophy in Mathematics

CONSTRUCTION OF NEW DIFFERENTIALLY δ-UNIFORM FAMILIES

By

Roberto Carlos Reyes Carranza

June 2020

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY IN MATHEMATICS AT THE UNIVERSITY
OF PUERTO RICO, RÍO PIEDRAS CAMPUS

Our research work is on the construction of new differentially δ-uniform families of vectorial Boolean functions. Almost all of our families have explicit and compact univariate in a polynomial representations with very few terms whose coefficients are either in $\mathbb{F}_2$ or are in a quadratic or cubic extension of it. Therefore they can be efficiently implemented in cryptographic applications. In addition, we have sub-families with high nonlinearity better than most of the differentially δ-uniform families recently discovered. That implies that they offer very good resistance to differential cryptanalysis. Given a differentially δ- uniform vectorial Boolean function $\mathbf{F}$, we give a generalization of a well known theorem of Edel and Pott (based on the APN-switching method of Dillon) for APN functions to differential δ-uniform version. We introduce a new switching method for δ-uniform functions, so that from a vectorial Boolean function $\mathbf{F}$, and another univariate Boolean function f and a vector $\mathbf{u}$, we obtain all the switching neighbors of the form $\mathbf{F} + \mathbf{u} \cdot \mathbf{f}$ (generalizing quadratic switching

APN functions of Budaghyan, Carlet and Leander). Our method gives us necessary and sufficient conditions so that these vectorial Boolean functions are differentially δ-uniform. As applications we obtain explicit families of the form stated.

We also discover a new theorem for a dependent variable version of Edel and Dillon on APN function, which provides a different criterion. We algorithmically apply these new theorems to discover new δ-uniform and new APN functions. Also, another new theorem, with (i, j)-parameter families of functions, generalizes theorems of Budaghyan and Carlet, when we select $j = i$. This way, we also obtain new cubic APN functions. Different parameters generalize other known results and others yield new families with strong nonlinearity and algebraic degrees. Our functions offer strong resistance to both first and second order Fourier transform analysis (better than well known families, e.g. the Gold families).

The remarkable result that the function $x^3 + tr(x^9)$ is an APN function discovered by Budaghyan, Carlet, and Leander has not yet been generalized since 2008. Bracken, Byrne, Markin, and McGuire computed the Walsh spectrum of such a quadratic function. We give a generalization of that result.

We obtain new families of functions generalizing a result of Budaghyan, by replacing a variable v by a polynomial $u(v)$. We give a variation of the idea of switching neighbor of Pott, and Pott-Budaghyan which yields further generalizations, leading to another new δ-uniform family of functions. We also give a second generalization of these results. Also, we formulate a narrow-sense switching technique along an axis. This technique helps us discover two elegant differentially δ-uniform families for each even δ.

We include tables of the values of Walsh Spectrum and other cryptographic properties of the Gold family over finite fields up to degree 15. These include values that have not been computed by others. We thus show that there are cases where Gold families are weak with respect to some cryptographic protocols such as nonlinearity and algebraic multiplicity.

Several authors have shown results on quadratic functions of the type $tr(x^{2^a+1})+tr(x^{2^b+1})$ (Fitgerald, Lahtonen, McGuire and Ward). We open different directions, and give a lower bound for the nonlinearity of the family of functions $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})$. We develop novel techniques to obtain such new families of functions. We apply our methods to study the Walsh spectrum and the nonlinearity profile of our families that are also applicable to families of functions that contain Boolean terms of the form $tr(bx^{2^k+1})$.

We give new differentially 4-uniform permutations in even degree field extension. Thus, we make a significant contribution to an open problem of Bracken and Leander (only a few results in this direction are known).

Para mami

ACKNOWLEDGMENTS

I would like to thank professor Heeralal Janwa.

I would like to thank my committee members {Puhua Guan, Pantelimon Stanica, Gary McGuire, Luis Medina, Heeralal Janwa}.

I would like to thank José Velzáquez and professor Moisés Delgado.

I would like to thank Ivan Castillo from University of Puerto Rico (Physics Department).

I would like to thank Nilo Caituiro.

TABLE OF CONTENTS

LIST OF SYMBOLS

$\mathbb{N}$ set of natural numbers

$\mathbb{Z}$ set of integer numbers

$\mathbb{F}_{p^n}$, $GF(p^n)$ field of order p^n

$\mathbb{F}_{p^n}^*$ multiplicative group (without the zero element)

$(\mathbb{F}_p)^n$, $\mathbb{F}_p^n$ $n-$dimensional vector space

R a ring

$R[x]$ a ring of polynomials in the variable x with coefficients in R

$R[x_1, \cdots, x_n]$ a ring of polynomials in the variables $x_1, \cdots, x_n$ with co-efficients in R

APN almost prefect nonlinear function

$\Delta(f)$ Differential uniformity of a given function f

$\mathrm{tr}(a)$, $\mathrm{tr}_1^n(a)$ trace of a

WLOG without loss of generality

dist d_H Hamming distance

$d^0(f)$ Algebraic degree of a given function f

$\gcd(n, m)$ Greatest common divisor of n and m.

$\mathbb{EG}(n, 2)$ *Euclidean geometry*

CHAPTER 1

INTRODUCTION

Symmetric-key block ciphers are encryption systems in which both parties share the same key or related keys. Some examples of symmetric-key block ciphers are Twofish, Serpent, DES, 3DES, AES, DES-like, etc. Data Encryption Standard (DES) algorithm is a symmetric-key cipher selected in 1977 by the National Bureau of Standards as an official Federal Information Processing Standard for the USA and used worldwide until 2001 when it was substituted by AES. For more information about DES and its properties (see Nyberg [30], Matsui [29]).

Since that time, DES was considered insecure by several applications because of its small key size, and, many attempts to increase the security have failed. DES has been extensively analyzed to capture its weakness. Special attention has been focused on the nonlinear properties of the round function, the S-Boxes. As observed by Nyberg, security of the cipher can be increased by replacing this round function by a function f with high nonlinear properties. Function that provides resistance against differential cryptanalysis are called almost perfect nonlinear (APN) functions, or in more general terms, differentially δ-uniform functions. When $\delta = 2$, f is an APN function. See the precise definition of these functions in Section 1.1.

Since the emergence of the first examples of monomial APN functions (including the well known Gold and Kasami-Welch functions), there exist now some infinite families of non-monomial APN functions and in general differentially δ-uniform functions.

The next two table list some known APN monomials and polynomials functions discovered until now by many mathematicians (see Budaghyan et al. [5]).

$f(x) = x^d$	Exponent d	Constraints
Gold	$2^r + 1$	$(r, n) = 1$
Kasami-Welch	$2^{2r} - 2^r + 1$	$(r, n) = 1$
Welch	$2^r + 3$	$n = 2r + 1$
Niho	$2^r + 2^{r/2} - 1$ $2^r + 2^{(3r+1)/2} - 1$	$n = 2r + 1$, r even $n = 2r + 1$, r odd
Inverse	$2^{2r} - 1$	$n = 2r + 1$
Dobbertin	$2^{4r} + 2^{3r} + 2^{2r} + 2^r - 1$	$n = 5r$

TABLE 1. Monomial APN functions

$f(x)$	Constraints
$x^{2^s+1} + a^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 3t, (t, 3) = (s, 3t) = 1, t \geq 3$ $i \equiv st \mod 3, r = 3 - i$, a is primitive in $\mathbb{F}_{2^n}$
$x^{2^s+1} + a^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 4t, (t, 2) = (s, 2t) = 1, t \geq 3$ $i \equiv st \mod 4, r = 4 - i$, a is primitive in $\mathbb{F}_{2^n}$
$ax^{2^s+1} + a^{2^m}x^{2^{m+s}+2^m} + bx^{2^m+1} +$ $\sum_{j=1}^{m-1} c_j x^{2^{m+i}+2^i}$	$n = 2m$, m odd $c_j \in \mathbb{F}_{2^m}, (s, m) = 1$, s odd a, b are primitive in $\mathbb{F}_{2^n}$
$ax^{2^{n-t}+2^{t+s}} + a^{2^t}x^{2^{s+1}} + bx^{2^{n-t}+1}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en $\mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^t}$
$a^{2^t}x^{2^{n-t}+2^{t+s}} + ax^{2^{s+1}} + bx^{2^{n-t}+1}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en $\mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^t}$
$a^{2^t}x^{2^{n-t}+2^{t+s}} + ax^{2^{s+1}} + bx^{2^{n-t}+1} +$ $ca^{2^t+1}x^{2^{t+s}+2^s}$	$n = 3t, (s, 3t) = 1, (3, t) = 1, 3\|(t + s)$ a es primitive en $\mathbb{F}_{2^n}$, $b, c \in \mathbb{F}_{2^t}, bc \neq 1$
$x^{2^{2k}+2^k} + bx^{q+1} + cx^{q(2^{2k}+2^k)}$	$n = 2m$, m odd, c a power of $(q - s)$ but no a power of $(q - 1)(2^i + 1), cb^q + b \neq 0$
$x^3 + tr_1^n(x^9)$	
$x^{2^k+1} + tr_m^n(x)^{2^k+1}$	$n = 2m = 4t, (n, k) = 1$

TABLE 2. Nonmonomial APN functions

Some examples of differentially 4-uniform functions are shown in the table [8].

In this thesis we highly contribute to the study of differentially δ-uniform functions by providing generalizations of previous methods, new methods, and new families of APN, differentially 4-uniform, differentially 8-uniform functions that extend tables 2 and 3.

We also discover a new theorem for a dependent variable version of Edel and Dillon on APN function, which provides a different criterion. We algorithmically apply these new

$f(x)$	Constraints
x^{2^i+1}	$n = 2k$, k odd, $(n, i) = 2$
$x^{2^{2i}-2^i+1}$	$n = 2k$, k odd, $(n, i) = 2$
x^{-1}	n even
$x^{2^{2i}+2^i+1}$	$n = 4k$, k odd

TABLE 3. Known highly nonlinear differentially 4 uniform permutations

theorems to discover new δ-uniform and new APN functions. Also, another new theorem, with (i, j)-parameter families of functions, generalizes theorems of Budaghyan and Carlet, when we select $j = i$. This way, we also obtain new cubic APN functions. Different parameters generalize other known results and others yield new families with strong nonlinearity and algebraic degrees. Our functions offer strong resistance to both first and second order Fourier transform analysis (better than well known families, e.g. the Gold families).

The remarkable result that the function $x^3 + tr(x^9)$ is an APN function discovered by Budaghyan, Carlet, and Leander has not yet been generalized since 2008. Bracken, Byrne, Markin, and McGuire computed the Walsh spectrum of such a quadratic function. We give a generalization of that result.

We obtain new families of functions generalizing a result of Budaghyan, by replacing a variable v by a polynomial $u(v)$. We give a variation of the idea of switching neighbor of Pott, and Pott-Budaghyan which yields further generalizations, leading to another new δ-uniform family of functions. We also give a second generalization of these results. Also, we formulate a narrow-sense switching technique along an axis. This technique helps us discover two elegant differentially δ-uniform families for each even δ.

We include tables of the values of Walsh Spectrum and other cryptographic properties of the Gold family over finite fields up to degree 15. These include values that have not been computed by others. We thus show that there are cases where Gold families are weak with respect to some cryptographic protocols such as nonlinearity and algebraic multiplicity.

Several authors have shown results on quadratic functions of the type $tr(x^{2^a+1})+tr(x^{2^b+1})$ (Fitgerald, Lahtonen, McGuire and Ward). We open different directions, and give a lower bound for the nonlinearity of the family of functions $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})$. We develop novel techniques to obtain such new families of functions. We apply our methods to study the Walsh spectrum and the nonlinearity profile of our families that are also applicable to families of functions that contain Boolean terms of the form $tr(b^{2^k+1})$.

We give new differentially 4-uniform permutations in even degree field extension. Thus, we make a significant contribution to an open problem of Bracken and Leander (only a few results in this direction are known).

An Overview of the Thesis: Our research work is on the construction of new differentially δ-uniform families of vectorial Boolean functions. Almost all of our families have explicit and compact univariate in a polynomial representations with very few terms whose coefficients are either in $\mathbb{F}_2$ or are in a quadratic or cubic extension. Therefore they can be efficiently implemented in cryptographic applications. In addition, we have sub-families with high nonlinearity better than most of the differentially δ-uniform families recently discovered. Therefore they offer very good resistance to differential cryptanalysis [30]. Given a differentially δ- uniform vectorial Boolean function $\mathbf{F}$, we give a generalization of a well known theorem of Edel and Pott [21] (based on the APN-switching method of Dillon) for APN functions to differential δ-uniform version. We introduce a new switching method for δ-uniform functions, so that from a vectorial Boolean function $\mathbf{F}$, and another univariate Boolean function f and a vector $\mathbf{u}$, we obtain all the switching neighbors of the form $\mathbf{F}+\mathbf{u}\cdot\mathbf{f}$ in Theorem 2.1.1 (generalizing quadratic switching APN functions of Budaghyan, Carlet and Leander [**?**]. Our method gives us necessary and sufficient conditions so that these vectorial Boolean functions are differentially δ-uniform. As applications we obtain explicit families of the form stated.

We also discover a new theorem for a dependent variable version of Edel and Dillon on APN function, which provides a different criterion. We algorithmically apply these new theorems to discover new δ-uniform and new APN functions. Also, another new theorem, with (i, j)-parameter families of functions, that generalizes theorems of Budaghyan and Carlet (Carlet in [7], [4]), when we select $j = i$ or $i \neq j$ (our Theorem 2.2.3). This way, we also obtain new cubic APN functions. Different parameters generalize other known results and others yield new families with strong nonlinearity and algebraic degrees. Our functions offer strong resistance to both first and second order Fourier transform analysis (better than well known families, e.g. the Gold families).

The remarkable result that the function $x^3 + tr(x^9)$ is an APN function discovered by Budaghyan, Carlet and Leander [6] (see also [21]), has not yet been generalized since 2008. Bracken, Byrne, Markin, and McGuire [1] computed the Walsh spectrum of such a quadratic function. We give a generalization of that result.

We obtain new families of functions generalizing a result of Budaghyan, by replacing a variable v by a polynomial $u(v)$. We give a variation of the idea of switching neighbor of Pott, and Pott-Budaghyan which yields further generalizations, leading to another new δ-uniform family of functions (Corollary 2.2.17). In definition 2.2.1 we give a slight variation of the idea of switching neighbor, which allow us to make a second generalization of that, given in Theorem 2.2.16. Also, using that definition 2.2.1 we discover two beautiful *differentially δ-uniform* families as stated in Theorem 2.2.24.

We include tables of the Walsh spectrum and other cryptographic properties of the Gold family over finite fields up to degree 15. These computations demonstrate that some of the not yet studied Gold functions, especially with $\Delta = 8$ and 16 are unusually interesting. We observe that some have of them have remarkable Walsh spectrum of the forms $\{2^{n-3}, 2^{\frac{n}{2}}, 0\}$, $\{2^{n-4}, 2^{\frac{n}{2}}, 0\}$, $\{2^{\frac{n+3}{2}}, 0\}$ and $\{2^{\frac{n+5}{2}}, 0\}$. We and (we invite others) to investigate such functions with non-traditional Walsh spectrum.

Roy [34] uses some results of Fitzgerald [22] on quadratic functions with two trace terms, $\mathrm{tr}_{K/\mathbb{F}_2}(x(x^{2^a}+x^{2^b}))$ where K is an finite extension of $\mathbb{F}_2$, to generalize some results of Lahtonen, McGuire and Ward [26] on Gold and KasamiWelch functions. Then Roy obtains the Walsh spectrum of these functions under certain conditions introduced by Lahtonen et al. [26].

We study the product case to obtain other families of δ-uniform families. Some of our compact families involve terms of the form $tr(x^{2^k+1})tr(x^{2^j+1})$. The techniques developed by Roy and others are not helpful in our analysis. Among new technique we develop in our thesis is a lower bound for the nonlinearity of the family of functions $f(x) = x^{2^k+1} + (x^{2^k} + x+1)tr(x^{2^k+1})tr(x^{2^j+1})$ given in the Theorems 2.2.16, 4.1.1 and 4,1,4. The method discussed here can also be applied to study the Walsh spectrum and the *nonlinearity profile* of other families of functions that contain boolean terms of the form $tr(bx^{2^k+1})$ (Theorem 2.2.16).

The AES (advanced encryption standard) uses the inverse function, which is known to be a differential 4- uniform function. Finding differential 4- uniform permutation functions with high nonlinearity on even degree fields are a big challenge. In view of these reasons, in [2], Bracken and Leander listed an open problem (it is still open, with few known results):

Open Problem Find more highly nonlinear permutations of even degree fields with differential uniformity of 4.

We give several families of 4-uniform functions for the case when n is even. Thus contributing to a resolution of this open problem. Our 4-functions are of very compact form, unlike those that have been discovered in literature for the even case. Our functions have high nonlinearity. One can find a survey of prior results in Qu, Tan, Tan, and Li [33] of differentially 4-uniform permutations families. Such families of functions are only a few, even without the requirement of high nonlinearity (see also Carlet [10] and Zha [40]). To learn about a class of sporadic binomials permutations with low differential uniformity ($\delta = 4$,

6) see [13]. Yu and Wang built differential 6 and 4- uniform permutations from the inverse function [39].

It is known that if f is a *permutation* on $\mathbb{F}_{2^n}$, then $deg(f) \leq n-1$. If it attains the equality, Zhengbang Zha [40] calls it with *optimal algebraic degree*. In Section 5.1 we give new differentially 4- uniform permutations with optimal algebraic degree (these are given in Theorem 5.1.1). Most of our theorems also cover the case when n is odd. We also obtain not only APN and but also 4 up to 8-uniform functions that have strong nonlinearity and other desirability cryptanalytic profiles suitable for applications (in Chapter 5).

Preliminaries:

Let $\mathbb{F}$ be any field, $\mathbb{F}[x]$ the polynomial ring with coefficients in $\mathbb{F}$, $p(x)$ an irreducible polynomial in $\mathbb{F}[x]$, and $\langle p(x)\rangle$ the ideal of $\mathbb{F}[x]$ generated by $p(x)$. Then the quotient ring $\mathbb{F}[x]/\langle p(x)\rangle$ is a field. In particular, if $\mathbb{F} = \mathbb{F}_p$ (for p a prime number), $p(x)$ irreducible of degree n in $\mathbb{F}_p[x]$, then $\mathbb{F}[x]/\langle p(x)\rangle$ is a finite field of order p^n, the field of polynomials of degree less than n in $\mathbb{F}_p[\alpha]$. Finite fields were discovered by the French mathematician Evariste Galois and then they are usually referred as Galois fields. A finite field of q elements is usually denoted as $\mathbb{F}_q$ or $\mathrm{GF}(q)$ in honor to its discoverer. The number of elements in a finite field must be of the form p^n, where p is a prime integer and n is a positive integer. Finite fields are unique up to isomorphisms.

The order of an element α in $\mathbb{F}_q$ is the smallest positive integer l such that $\alpha^l = 1$. $\mathbb{F}_q$ always contains at least one element of order $q-1$, called a primitive element. For a primitive element α, the $(q-1)$ consecutive powers of α, $\alpha^0 = 1, \alpha, \alpha^2, ..., \alpha^{q-2}$, are all distinct, so they are the $(q-1)$ nonzero elements of $\mathbb{F}_q$. This exponential representation of the nonzero elements of $\mathbb{F}_q$ provides a practical computation of the multiplication of two elements in $\mathbb{F}_q$ by adding their exponents. For the case of the addition of two elements in $\mathbb{F}_q$, exponential representations must be reduced. A primitive element is a root of a primitive polynomial, the irreducible polynomial $p(x)$ in $\mathbb{F}_q[x]$ that is its minimal polynomial. The exponential

representations for the nonzero elements of $\mathbb{F}_q$ are reduced modulo the primitive polynomial to obtain polynomial representations of degree less than n, which are added using the usual polynomial addition. As an example, let us consider the finite field of 8 elements $\mathbb{F}_8$.

Example Let $p(x) = x^3 + x + 1$ be the primitive polynomial. Let α be a root of $p(x)$. This implies that $\alpha^3 + \alpha + 1 = 0$, or equivalently, $\alpha^3 = \alpha + 1$.

Exponential Representation		Polynomial Representation
1	$=$	1
α^1	$=$	α
α^2	$=$	α^2
α^3	$=$	$\alpha + 1$
α^4	$=$	$\alpha^2 + \alpha$
α^5	$=$	$\alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
α^6	$=$	$\alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$
0	$=$	0

Addition is performed using the polynomial representation. To compute $\alpha^4 + \alpha^6$ in GF(8), one begins by substituting the polynomial representations for the exponential representations α^4 and α^6. The polynomial sum of $\alpha^4 + \alpha^6$ may be reexpressed as a power of α.

$$\alpha^4 + \alpha^6 = (\alpha^2 + \alpha) + (\alpha^2 + 1) = \alpha + 1 = \alpha^3.$$

1.1 Differential δ Uniformity

Definition 1.1.1. $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is *almost perfect nonlinear* (APN) if $\forall\ a \neq 0,\ b \in \mathbb{F}_{p^n}$, the equation

$$f(x+a) - f(x) = b,$$

has at most 2 solutions. Equivalently, for $p = 2$:

$$|\{f(x+a) - f(x) : x \in \mathbb{F}_{2^n}\}| \geq 2^{n-1},\ \forall\ a \in \mathbb{F}_{2^n}^*.$$

The best known APN families of functions are the monomials:
Gold: x^{2^i+1}, where $(i,n) = 1$, and
Kasami-Welch: $x^{2^{2i}-2^i+1}$, where $(i,n) = 1$, and n is odd.

Definition 1.1.2. $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is *differentially* $\delta-$ *uniform* if $\forall\ a \neq 0,\ b \in \mathbb{F}_{2^n}$, we have that:

$$|\{x \in \mathbb{F}_{2^n} : f(x+a) - f(x) = b\}| \leq \delta,$$

Definition 1.1.3. $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *linear* if F is a linearized polynomial over $\mathbb{F}_{2^n}$, that is,

$$F(x) = \textstyle\sum_{i=0}^{n-1} c_i x^{2^i},$$

where $c_i \in \mathbb{F}_{2^n}$. Given any $c \in \mathbb{F}_{2^n}$, $F+c$ is called *affine*. We often embed the linear functions into the class of affine ones. If you need to refer to the case $c \neq 0$, you will say strictly affine.

Definition 1.1.4. A polynomial $f \in \mathbb{F}_{2^n}[x]$ is *quadratic* if $\forall k \in \mathbb{F}_{2^n}^*$, the function

$$Q(x) = f(x+k) + f(x) + f(k)$$

is a linearized polynomial in x, or equivalently, if it is $\mathbb{F}_2$- linear.

Definition 1.1.5. Let $G, A_1, A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, and A_1, A_2 are affine permutations, then:

G and $A_1 o G o A_2$ are called *affine equivalent (AE)*.

G and $A_1 o G o A_2 + A$ are called *extended affine equivalent (EAE),* for any affine A.

1.2 Nonlinearity Approach via Reed-Muller Codes

Let $v = (v_1, v_2, \cdots, v_m)$ denote a vector which ranges over $\mathbb{F}_2^m$, and $\boldsymbol{f}$ a vector of length 2^m obtained from a Boolean function $f(v_1, v_2, \cdots, v_m)$ over $\mathbb{F}_2^m$.

Definition 1.2.1. (Reed-Muller Codes) ([28], [14])

The r^{th} *order binary Reed-Muller* code $\mathcal{R}(r, m)$ of length $n = 2^m$, for $0 \leq r \leq m$, is the set of all vectors $\boldsymbol{f}$, where $f(v_1, v_2, \cdots, v_m)$ is the corresponding Boolean function which is a polynomial of degree at most r. The degree of a Boolean function f is called its algebraic degree.

The first-order Reed-Muller code $\mathcal{R}(1, m)$ consists of all vectors $u_0 1 + \sum_{i=1}^{m} u_i v_i$, $u_i \in \{0, 1\}$, corresponding to linear Boolean functions.

For any vector $\mathbf{u} = (u_1, u_2, \cdots, u_m)$ in $\mathbb{F}_2^m$, $f(\mathbf{u})$ will denote the value of f at $\mathbf{u}$, or equally the component of $\boldsymbol{f}$ in the place corresponding to $\mathbf{u}$.

It will be convenient to have a name for the real vector obtained from a binary vector $\boldsymbol{f}$ by replacing $1's$ by $-1's$ and $0's$ by $+1's$-call it F. Thus the component of F in the place corresponding to u is

$$F(u) = (-1)^{f(u)}.$$

Hadamard transforms and Cosets of $\mathcal{R}(1, m)$

The Hadamard transform of a real vector F is given by

$$\begin{aligned} \hat{F}(u) &= \textstyle\sum_{v \in \mathbb{F}_2^m} (-1)^{u.v} F(v),\ u \in \mathbb{F}_2^m, \\ &= \textstyle\sum_{v \in \mathbb{F}_2^m} (-1)^{u.v + f(v)}. \qquad (1) \end{aligned}$$

$\hat{F}$ is a real vector of length 2^m. Alternatively,

$$\hat{F} = FH,$$

where H is the $2^m \times 2^m$ symmetric Hadamard matrix given by

$$H = (H_{u,v}), \;\; H_{u,v} = (-1)^{u.v}, \;\; u, v \in \mathbb{F}_2^m.$$

Consequently,

$$F = \tfrac{1}{2^m}\hat{F}H,$$

or

$$F(v) = \tfrac{1}{2^m}\sum_{v\in\mathbb{F}_2^m}(-1)^{u.v}\hat{F}(u).$$

Observe from (1) that $\hat{F}(u)$ is equal to the number of 0's minus the number of 1's in the binary vector

$$\boldsymbol{f} + \sum_{i=1}^{m} u_i v_i$$

Thus

$$\hat{F}(u) = 2^m - 2\text{dist}\{\boldsymbol{f},\ \textstyle\sum_{i=1}^{m} u_i v_i\},$$

or

$$\text{dist}\{\boldsymbol{f},\ \textstyle\sum_{i=1}^{m} u_i v_i\} = \tfrac{1}{2}\{2^m - \hat{F}(u)\}.$$

Also

$$\text{dist}\{\boldsymbol{f},\ 1 + \textstyle\sum_{i=1}^{m} u_i v_i\} = \tfrac{1}{2}\{2^m + \hat{F}(u)\},\ u \in \mathbb{F}_2^m.$$

Now the weight distribution of that coset (of a code $\mathcal{C}$) which contains f gives the distances of f to the linear codewords of $\mathcal{C}$. Therefore we have proved:

Theorem 1.2.1 ([28]). The weight distribution of the coset of $\mathcal{R}(1, m)$ which contains f is

$$\tfrac{1}{2}\{2^m \pm \hat{F}(u)\} \quad \text{for } u \in \mathbb{F}_2^m.$$

The weight distribution of the coset containing f is thus determined by the Hadamard transform of F.

Definition 1.2.2. (Nonlinearity) The nonlinearity of a Boolean function f, is defined to be $NL(f) = d(f, RM(1,m))$ (i.e. the distance of f from $RM(1,m)$). Therefore it is also the weight of the coset $f + RM(1,m)$. And it also equal to the value attained in Theorem 1.2.1.

Corollary 1.2.2. The covering radius of the Reed-Muller code $R(1,m)$, $\rho(RM(1,m)) = max_f NL(f)$, where f varies over all Boolean function of order $\leq m$.

Proposition 1.2.3. (Covering Radius Bound) $\rho(R(r,n)) \leq 2^{n-1} - 2^{(n/2)-r}$.

Bent Functions

Definition 1.2.3. [28]

A Boolean function $f(v_1, v_2, \cdots, v_m)$ is called *bent* if the Hadamard transform coefficients $\hat{F}(u)$ given by Equation (1) are all $\pm 2^{\frac{m}{2}}$, when m is even.

Theorem 1.2.4. A bent function $f(v_1, v_2, \cdots, v_m)$ is further away from any linear function

$$a_0 1 + \sum_{i=1}^{m} a_i v_i$$

then any other Boolean function. More precisely, $f(v_1, v_2, \cdots, v_m)$ is bent iff the corresponding vector $\boldsymbol{f}$ has distance $2^{m-1} \pm 2^{\frac{m}{2}-1}$ from every codeword of $\mathcal{R}(1,m)$. If f is not bent, $\boldsymbol{f}$ has distance less than $2^{m-1} - 2^{\frac{m}{2}-1}$ from some codeword of $\mathcal{R}(1,m)$.

Theorem 1.2.5. If $f(v_1, v_2, \cdots, v_m)$ is bent and $m > 2$, then $\deg f \leq \frac{1}{2}m$.

A continuation some families of bent functions.

Theorem 1.2.6.

$$h(u_1, \cdots, u_m, v_1, \cdots, v_n) = f(u_1, \cdots, u_m) + g(v_1, \cdots, v_n)$$

is a bent function (of $m+n$ arguments) iff f and g are bent functions.

Corollary 1.2.7.

$$v_1v_2 + v_3v_4 + \cdots + v_{m-1}v_m$$

is a bent function, for any even $m \geq 2$.

Theorem 1.2.8. For any function $g(v_1, \cdots, v_m)$, the function

$$f(u_1, \cdots, u_m, v_1, \cdots, v_m) = \sum_{i=1}^{m} u_i v_i + g(v_1, \cdots, v_m)$$

is bent.

Vectorial Boolean Functions

Definition 1.2.4. Let n and m be two positive integers. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n, m)-functions, vectorial Boolean functions or S-Boxes. The term S-Box is the most often used in cryptography, but is dedicated to the vectorial functions whose role is to provide confusion into the system.

Definition 1.2.5. We shall call Walsh transform W_F of an (n, m)- function F as the function which maps any ordered pair $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\sum_{x \in \mathbb{F}_2^n} (-1)^{v.F(x) \oplus u.x}$.

From now on in the rest of this chapter and the thesis, wherever suitable, as vector spaces, we will identify the extension field $\mathbb{F}_{2^n}$ with its isomorphic vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. When $n = m$, then the Walsh transform of any (n, n)-vectorial Boolean function can be represented in the special form as

$$W_F(u, v) = \sum_{x \in F_{2^n}} (-1)^{tr(vF(x)+ux)},$$

where $tr(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the *trace function* from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$, and where F is now represented uniquely as function over the field $\mathbb{F}_{2^n}$ (see [11]). The set $\mathcal{W}_F = \{W_F(u, v) : u, v \in \mathbb{F}_{2^n}, v \neq 0\}$ is called the *Walsh Spectrum* of the function F (to read about *Classical Walsh Spectrum* see [21]). The set $\{|W_F(u, v)| : u, v \in \mathbb{F}_{2^n}, v \neq 0\}$ is called the *extended Walsh spectrum* of F, and *Walsh support* of F the set of those (u, v) such that $W_F(u, v) \neq 0$.

A generalization to (n, m)- functions of the notion of the nonlinearity of Boolean functions have been studied by Nyberg [31], Chabaud and Vaudenay [12]:

Definition 1.2.6. Given a (n, m)-vectorial Boolean function F, for any non-zero $v \in \mathbb{F}_2^m$, the component function along v is defined to be the from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, as the function that maps x to $v.F(x)$. The nonlinearity of this component function is the nonlinearity of this Boolean function.

Definition 1.2.7. [11] The nonlinearity $NL(F)$ of an (n, m)- function F is the minimum nonlinearity of all the component functions $x \in \mathbb{F}_2^n \to v.F(x)$, $v \in \mathbb{F}_2^m$, $v \neq 0$.

In other words, $NL(F)$ equals the minimum Hamming distance between all the component functions of F and all affine functions on n variables. This quantifies the level of resistance of the S-box to the linear attack.

The nonlinearity and the maximal magnitude of its Walsh transform have the following relation:

$$NL(F) = 2^{n-1} - \tfrac{1}{2} max_{u \in \mathbb{F}_2^n,\ v \in \mathbb{F}_2^{m*}} |W_F(u, v)|.$$

The covering radius of the first-order Reed-Muller code of length 2^n is upper bounded by

$$2^{n-1} - 2^{\frac{n}{2}-1}.$$

Therefore, from the upper bound on the $\rho(RM(1, n))$ (from Proposition 1.2.3 , we have the upper bound, for any (n, m)-vectorial Boolean function F:

$$NL(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \qquad (2)$$

Therefore, $n = m$, the upper bound is obtained only when n is even (see [11]). That is, for n even, the Boolean function gives the coset of highest weight; that is the weight of this coset is equal to the covering radius. In the odd n case, there are some conjectures. For further reference on the covering radius go to by Cohen, Karpovsky, and Schatz in [15], [14].

Definition 1.2.8. A (n, m)- function is called bent if it achieves the covering radius bound (2) with equality.

The notion of bent vectorial function is invariant under composition on the left and on the right by affine automorphisms and by the addition of affine functions. Clearly, an (n, m)-function is bent if and only if all the component functions $v.F$, $v \neq 0$ of F are bent (i.e. each achieves the same bound). Hence, the algebraic degree of any bent (n, m)- function is at most $n/2$.

Definition 1.2.9. The (n, n)- functions F which achieve the bound of Theorem 1 with equality - that is, $NL(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$ (n odd)- are called *almost bent (AB) or maximum nonlinear*.

Since bent n-variable Boolean functions exist only if n is even, bent (n, m)- functions exist only under this same hypothesis. According to the following Nyberg's result, (n, n)- bent functions do not exist:

Proposition 1.2.9. Bent (n, m)- functions exist only if n is even and $m \leq n/2$.

The almost bent (AB) functions are those (n, n)- functions whose Walsh Spectrum $\mathcal{W}_F$ equals $\{0, \pm 2^{\frac{n+1}{2}}\}$ as it is proven in [13] (indeed, the maximum of a sequence of nonnegative integers equals the ratio of the sum of their squares over the sum of their values if and only if these integers take at most one nonzero value). Note that this condition does not depend on the choice of the inner product.

For n even, the maximum nonlinearity of function F is not yet known, which is conjectured to be $2^{n-1} - 2^{\frac{n}{2}}$.

Function	d	Conditions	Nonlinearity	Reference
Gold	$2^i + 1$	$\gcd(i, n) = 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd $2^{n-1} - 2^{\frac{n}{2}}$, n even	[30], [21]
Kassami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd $2^{n-1} - 2^{\frac{n}{2}}$, n even	[25], [26], [21]
Welch	$2^t + 3$	$n = 2t + 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$	

TABLE 4. Nonlinearities of known APN monomials, x^d, over $\mathbb{F}_2^n$

There exists a bound on the algebraic degree of AB functions, similar to the bound for bent functions:

Proposition 1.2.10. [11] Let F be any (n, n)- function ($n \geq 3$). If F is AB, then the algebraic degree of F is less than or equal to $(n + 1)/2$.

Proposition 1.2.11. [11] Every AB function is APN.

1.3 Dillon Switching Construction

We introduce group ring (a free module) notation useful to describe the technique of *switching* an APN function [21], [20], [19], i.e., obtain functions with low differential uniformity by changing a component function of a known such function, that was first observed by John Dillon. Let $\mathbb{F}$ be an arbitrary field (the elements of this ring are the scalars) and $(G, +)$ an abelian group (its elements are the basis). Let the set $\mathbb{F}[G]$, which consists of all elements of the form $\sum_{g \in G} a_g g$, where $a_g \in \mathbb{F}$ and each g of G is considered, together with the addition in a component-wise fashion, multiplication and the scalar multiplication, which are defined respectively as

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G}(a_g + b_g)g,$$

$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g := \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})g, \text{ and}$$

$$\alpha . \sum_{g\in G} a_g g := \sum_{g\in G}(\alpha a_g)g,$$

$(\mathbb{F}[G], +, \ ., .)$ becomes an algebra, the so called **group algebra**.

Given a (n, n) function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, consider the *group algebra* $\mathbb{F}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$, where the formal sums $\sum_{v\in F_2^n} c(v)(v, F(v))$, $c(v) \in \mathbb{F}$, denote it's elements. We focus on the case $c(v) \in \mathbb{F}_2 \subseteq \mathbb{F}$. We associate a *group algebra element corresponding to the graph of the function* F, $G_F := \sum_{v\in F_2^n} 1(v, F(v))$, which consists of all pairs $(v, F(v))$, $v \in \mathbb{F}_2^n$.

Let U a subgroup of G, consider the following canonical group homomorphism:

$$\begin{array}{rll} \varphi_U : G \to & \frac{G}{U} \\ g & g + U. \end{array}$$

φ_U can be extended by linearity to a homomorphism from $\mathbb{F}[G]$ to $\mathbb{F}[\frac{G}{U}]$:

$$\begin{array}{rccc} \varphi_U : & \mathbb{F}[G] & \to & \mathbb{F}[\frac{G}{U}] \\ & D = \sum_{g\in G} a_g g & & \varphi_U(D) := \sum_{g\in G} a_g(g + U) \end{array}$$

$\varphi_U(D) = \sum_{g\in G} a_g(g + U) = \sum_{g+U\in \frac{G}{U}}(\sum_{h\in g+U} a_h)(g + U)$, the last sum is in terms of the cosets $g+U$, where we take the sum of all coefficients a_h, such that $h+U = g+U$. If D has only coefficients (a_g) 1 or 0, so that $D = \sum_{g\in G,\ a_g=1} 1g$ corresponds to a set $D = \{g : a_g = 1\} \subseteq G$, then the coefficient of $g + U$ in $\varphi_U(D)$ is the following sum in $\mathbb{F}$:

$$\sum_{h\in g+U} a_h (\in \{0, 1\}) = \sum_{h\in g+U,\ a_h=1} 1 = \big|D \cap (g + U)\big|.$$

In particular, if each coset of U meets D in at most one element, i.e. $\big|(g+U)\cap D\big| \in \{0,1\}$, $\forall g \in G$, then:

$$\varphi_U(D) = \sum_{g+U\in\frac{G}{U}} \big|(g+U)\cap D\big|(g+U) = \sum_{g+U\in\frac{G}{U},\ \big|(g+U)\cap D\big|=1} g+U$$

and it has only coefficients 0 and 1. This is the case if U is a subgroup of $(\leq)$ $\{0\}\times\mathbb{F}_2^n$.

Definition 1.3.1. [21] Let U be a subgroup of $\mathbb{F}_2^n \times \mathbb{F}_2^n$. We say that the functions F and $H : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are **switching neighbours** with respect to U if $\varphi_U(G_F) = \varphi_U(G_H)$. We say that F and H are switching neighbours in the narrow sense if $U \leq \{0\}\times\mathbb{F}_2^n$ and $\dim(U) = 1$.

If F and H are switching neighbors with respect to U, we may obtain H from F by first projecting G_F onto $\varphi_U(G_F)$, and then lifting this element to G_H, which give us the images of H.

$U \leq \{0\}\times\mathbb{F}_2^n$ has the advantage that the coefficients of $\varphi_U(G_F)$ are 0 and 1 only, since the cosets of $\{0\}\times\mathbb{F}_2^n$ (and therefore also the cosets of U) meet G_F no more than once, at $(0, F(0))$. G_F can be seen as our D above. In this case, $\varphi_U(G_F)$ corresponds to a mapping $F_U : \mathbb{F}_2^n \to \frac{\mathbb{F}_2^n}{U'}$ with $F_U(v) := F(v) + U'$ and $U' = \{u : (0,u) \in U\}$, where U' is basically the same as U.

Now we study the equation $\varphi_U(G_F) = \varphi_U(G_H)$ in more detail. First consider $\varphi_U(G_F)$:

$$\varphi_U(G_F) = \sum_{x\in\mathbb{F}_2^n} 1((x,F(x))+U) = \sum_{(x,F(x))+U\ \in\ \frac{\mathbb{F}_2^n\times\mathbb{F}_2^n}{U}} \Big(\sum_{h\ \in\ (x,F(x))+U} 1_h\Big)((x,F(x))+U)$$

as a formal sum in $\mathbb{F}[\frac{\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}}{U}]$. Then $\varphi_U(G_F) = \varphi_U(G_H)$ as group ring elements if and only if $\varphi_U(G_F) - \varphi_U(G_H) = \sum_{x\in\mathbb{F}_2^n} 0((x,F(x))+U) = \sum_{x\in\mathbb{F}_2^n} 0\{(x,F(x)+u) : u \in U'\}$. Then

$\{(x, F(x)+u) : u \in U'\} = \{(x, H(x)+u) : u \in U'\}$, $\forall x \in \mathbb{F}_2^n$, i.e. $\{F(x)+u : u \in U'\} = \{H(x)+u : u \in U'\}$, $\forall x \in \mathbb{F}_2^n \Leftrightarrow H(x) \in F(x)+U'$, $\forall x \in \mathbb{F}_2^n$.

Proposition 1.3.1. Let F, $H : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and let $U \leq \{0\} \times \mathbb{F}_2^n$. Then

$$F_U = H_U \text{ iff } (0, F(v) - H(v)) \in U, \forall\ v \in \mathbb{F}_2^n.$$

If $U = \{(0,0), (0,u)\}$, then $F_U = H_U$ iff there is a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $H(v) = F(v) + f(v).u$.

Proof: The first part of the proposition is given by definition, for the second part the function f is defined via

$$f(v) := \begin{cases} 0, & \text{if } F(v) = H(v), \\ 1, & \text{else.} \end{cases}$$

The functions $F(x) = x^3$ and $H(x) = x^3 + tr(x^9)$ are switching neighbours in the narrow sense: Take the 1-dimensional subspace U generated by $(0,1) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. Then $\varphi_U(G_F) = \varphi_U(G_H)$. We note that this does not prove that $x^3 + tr(x^9)$ is an APN function.

The aforementioned proposition shows that one may obtain all switching neighbors of F in the narrow sense (with respect to a one-dimensional subspace) by adding a Boolean function f times a vector $u \neq 0$. Let F be an APN function, the following theorem of Edel and Pott [21] gives a necessary and sufficient condition for f to produce another (not necessarily equivalent) APN function by the application of the switching method:

Theorem 1.3.2. [21] Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Let $u \in \mathbb{F}_2^n$, $u \neq 0$, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, and $H(v) := F(v) + f(v).u$. Then:

$$H \text{ is an APN function} \iff$$

$$\text{For all } x,\ y,\ a \in \mathbb{F}_2^n,\ [F(x) + F(x+a) + F(y) + F(y+a) = u \qquad (2)$$

$$\text{implies } f(x)+f(x+a)+f(y)+f(y+a)=0\big]$$

Proof:

We will prove the contrapositive of both statements, dividing each into separate cases:

Case 1: H is not APN $\Longrightarrow [\exists\, x, y, a \in \mathbb{F}_2^n$ such that $[F(x)+F(x+a)+F(y)+F(y+a)=u$ and $f(x)+f(x+a)+f(y)+f(y+a)=1(\neq 0)\ ]]$

Proof:

H is not APN, then $\exists\ a \neq 0,\ b \in \mathbb{F}_2^n$ such that the equation $H(x+a)+H(x)=b$ has exactly 4 solutions x, $x+a$, y, $y+a$. That is two values that satisfy equation (1):

$$F(x+a)+uf(x+a)+F(x)+uf(x)=b$$

$$F(x+a)+F(x)+u(f(x+a)+f(x))=b \qquad (1)$$

and two values that satisfy equation (2):

$$F(y+a)+uf(y+a)+F(y)+uf(y)=b$$

$$F(y+a)+F(y)+u(f(y+a)+f(y))=b. \qquad (2)$$

Subcase 1.1: Suppose that $f(x+a)+f(x)=0$. Given this case, Equation (1) is reducted to:

$$F(x+a)+F(x)=b \qquad (3)$$

$f(y+a)+f(y)$ can not be 0, because otherwise Equation (2) becomes:

$$F(y+a)+F(y)=b. \qquad (4)$$

From (3) and (4) $\Delta_a F(x)=b$ has 4 solutions x, $x+a$, y, $y+a$, which contradicts the fact that F is APN. Thus $f(y+a)+f(y)=1$.

In summary, if $f(x+a)+f(x)=0$, then $f(y+a)+f(y)=1$. On the other hand, using the same procedure, $f(x+a)+f(x)=1$ then $f(y+a)+f(y)=0$.

Without loss of generality, we consider the sub case $f(x+a)+f(x) = 0$ and $f(y+a)+f(y) = 1$. From Equation (1) we have:

$$F(x+a) + F(x) + u(0) = b$$

$$F(x+a) + F(x) = b \text{ and } f(x+a) + f(x) = 0. \tag{5}$$

From Equation (2) we have:

$$F(y+a) + F(y) + u(1) = b \text{ and } f(y+a) + f(y) = 1 \tag{6}$$

Adding equations (5) and (6), we have:

$$F(x+a) + F(x) + F(y+a) + F(y) = u \text{ and}$$

$$f(x+a) + f(x) + f(y+a) + f(y) = 1.$$

Subcase 1.2: If we assume $f(x+a) + f(x) = 1$ (this makes $f(y+a) + f(y) = 0$), then we reach the same conclusion.

Case 2: [There exists 4 elements x, $x+a$, y, $y+a$ in $\mathbb{F}_2^n$, where $a \neq 0$, such that $[F(x) + F(x+a) + F(y) + F(y+a) = u$ and $f(x) + f(x+a) + f(y) + f(y+a) = 1]] \Longrightarrow H$ is not APN.

Proof:

Let $F(x+a) + F(x) = b$, for some b in $\mathbb{F}_2^n$. Substituting this into the equation $F(x) + F(x+a) + F(y) + F(y+a) = u$, we have:

$$F(y+a) + F(y) = b + u.$$

Subcase 2.1: If $f(x+a) + f(x) = 0$ (recall this makes $f(y+a) + f(y) = 1$), then:

$$H(x) + H(x+a) = F(x) + F(x+a) + (f(x+a) + f(x))u = b \text{ and}$$

$$H(y) + H(y+a) = F(y) + F(y+a) + (f(y+a) + f(y))u = b + u + (1)u = b.$$

Thus the equation $\Delta_a H(x) = b$ has 4 solutions, x, $x+a$, y, $y+a$, and H as such cannot be APN.

Subcase 2.2: If $f(x+a)+f(x) = 1$ (recall this makes $f(y+a)+f(y) = 0$), then:

$$H(x) + H(x+a) = F(x) + F(x+a) + (f(x+a) + f(x))u = b + u \text{ and}$$

$$H(y) + H(y+a) = F(y) + F(y+a) + (f(y+a) + f(y))u = b + u.$$

Thus the equation $\Delta_a H(x) = b+u$ has 4 solutions, x, $x+a$, y, $y+a$, and H cannot be APN.

Budaghyan and Carlet discovered the beautiful general example ([6], [21], [20], [19]) that the switching neighbour of x^3 in the narrow sense with respect to $U = \{(0,0),(0,1)\}$, given by $x^3 + tr(x^9)$, is APN. They prove a theorem that is based on quadratic APN functions, linear Boolean functions, and quadratic Boolean functions. As a consequence they prove that $x^3 + tr(x^9)$. We directly prove it using Theorem 1.3.2 and using elementary means to shows that $x^3 + tr(x^9)$ is APN.

Theorem 1.3.3. The function $x^3 + tr(x^9)$ is APN over $\mathbb{F}_2^n$.

Proof:

We will show the result using Theorem 1.3.2, where $F(x) = x^3$ is the APN function F on $\mathbb{F}_2^n$, the nonzero vector $u = 1$, and the Boolean function $f(x) = tr(x^9)$. Let any $x, y, a \in \mathbb{F}_2^n$ such that $F(x) + F(x+a) + F(y) + F(y+a) = u$, that is $x^2a + a^2x + y^2a + a^2y = 1$. By the hypothesis $F(x) + F(x+a) + F(y) + F(y+a) = u$ and $u \neq 0$, then a can't be zero. Then:

$$(x+y)^2 a = a^2(x+y) + 1$$

$$\Rightarrow (x+y)^2 = a(x+y) + \tfrac{1}{a}$$

$$\Rightarrow (x+y)^4 = a^2(x+y)^2 + \tfrac{1}{a^2}$$

$$\Rightarrow (x+y)^4 = a^2(a(x+y) + \tfrac{1}{a}) + \tfrac{1}{a^2}$$

$$\Rightarrow (x+y)^4 = a^3(x+y) + a + \tfrac{1}{a^2}$$

$$\Rightarrow (x+y)^8 = a^6(x+y)^2 + a^2 + \tfrac{1}{a^4}$$

$$\Rightarrow (x+y)^8 = a^7(x+y) + a^5 + a^2 + \tfrac{1}{a^4}$$

So, multiplying by a (we get the conjugates a^6, a^3) and applying the trace:

$$tr((x+y)^8 a + a^8(x+y)) = tr(a^6 + a^3) + tr(\tfrac{1}{a^3}) = tr(\tfrac{1}{a^3})$$

The equation $x^2a + a^2x = 1$ implies that a (or x) belong to a set of small cardinality. Since $F(x) + F(x+a) = x^2a + a^2x + F(a) = 1 + a^3$, $F(x) + F(x+a) = 1 + a^3$, could have 2 or no solution (because F is APN). In the following, for the set of all $a's$ we will verify that $tr(\frac{1}{a^3})$ is a constant. Dividing by a^3, the equation $(x+y)^2 a = a^2(x+y) + 1$ becomes:

$$(\tfrac{x+y}{a})^2 + \tfrac{x+y}{a} = \tfrac{1}{a^3},$$

then $tr(\frac{1}{a^3}) = 0$.

Then for those x, y, a such that $F(x) + F(x+a) + F(y) + F(y+a) = u$, we obtain:

$$f(x) + f(x+a) + f(y) + f(y+a) = tr((x+y)^8 a + a^8(x+y)) = 0.$$

Remark Also by application of Theorem 1.3.2 we found that, for n even, the function $x^3 + tr(x^3)$ is APN over $\mathbb{F}_2^n$.

CHAPTER 2

CONSTRUCTION OF NEW DIFFERENTIALLY δ-UNIFORM FAMILIES

One of our main contributions in this chapter is Theorem 2.1.1. In this theorem, we give a general framework for constructing new δ- uniform functions from given ones. As applications of our new Theorem 2.1.1, we derive other theorems. Theorem 1, given in [6] by Budaghyan et al., establishes a general approach for constructing new quadratic APN functions from known ones there are families of functions of this class that also are obtained from Theorem 2.1.1. The well known function of Budaghyan et al., $B(x) = x^3 + tr(x^9)$, belongs to this class of functions. We also show that our new Theorem 2.1.3 is a generalization of the previously mentioned result. Theorem 2.1.1 implies Theorem 2.1.3.

We generalize a Theorem of Edel and Pott on obtaining new APN functions from existing APN functions. Our generalization gives new δ- uniform functions from existing δ- uniform functions. In particular our Theorem 2.1.1 implies Theorem 1.3.2 of Edel [21], [20], [19] (which is one important result on APN functions and their resistance to differential cryptanalysis).

We also discover a new theorem (Theorem 2.1.2) that is an independent variable version of the Edel- Dillon Theorem on APN function, but it provides different criteria. Next in this research, we algorithmically apply these new theorems to discover new δ-uniform and new APN functions.

Moreover, we provide concrete examples of differentially δ-uniform switching neighbors where Theorems 2.1.1 and 2.1.3 apply but not the results of Theorem 1.3.2 [21] of Edel and Pott nor the results of Theorem 1 of Budaghyan et al. [6].

2.1 Differentially δ-Uniform Switching Neighbours in the Narrow Sense

Given a differentially δ-uniform function F, our following theorem generalize Theorem 1.3.2 of Edel and Pott [21] which is given only for APN functions, to the differential uniform case, giving a necessary, and sufficient condition for f to get all the differentially δ- uniform switching neighbors of F, in the narrow sense, with respect to a one-dimensional subspace:

Theorem 2.1.1. [Differentially uniform version]

Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a *differentially δ-uniform* function. Let $u \in \mathbb{F}_2^n$, $u \neq 0$, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, $A = \{x \in \mathbb{F}_2^n; f(x+a)+f(x) = 0\}$, $B = \{x \in \mathbb{F}_2^n; f(x+a)+f(x) = 1\}$, and $H(v) := F(v) + f(v).u$. Then:

$$H \text{ is a } \textit{differentially } \delta\textit{-uniform} \text{ function} \iff$$

$$[\text{For all } a \neq 0, \text{ and } \delta + 2 \text{ values } x_i \in A \neq \emptyset \text{ and } x'_j \in B \neq \emptyset,$$

$$[F(x_i) + F(x_i + a) + F(x'_j) + F(x'_j + a) = u \qquad (2)$$

$$\text{implies } f(x_i) + f(x_i + a) + f(x'_j) + f(x'_j + a) = 0\ ]].$$

Proof:

We will prove the contrapositive of both statements, dividing each into separate cases:

Case 1: H is not *differentially δ-uniform* $\implies$ [$\exists$ $\delta + 2$ values $x_i \in A \neq \emptyset$ and $x'_j \in B \neq \emptyset$, where $a \neq 0$, such that $[F(x_i) + F(x_i + a) + F(x'_j) + F(x'_j + a) = u$ and $f(x_i) + f(x_i + a) + f(x'_j) + f(x'_j + a) = 1\ ]]$.

Proof:

H is not *differentially δ-uniform*, then $\exists$ $a \neq 0$, $b \in \mathbb{F}_2^n$ such that the equation $H(x + a) + H(x) = b$ has at least $\delta + 2$ solutions. If we assume all solutions are in only one of the two sets A or B. That is the solution set S is a subset of one, A or B. Then, for any $x \in S$, $\Delta_a H(x) = F(x + a) + uf(x + a) + F(x) + uf(x) = F(x + a) + F(x) + u(f(x + a) + f(x)) = F(x + a) + F(x) + u(\varepsilon) = b$, for some $\varepsilon \in \mathbb{F}_2$. Then:

$$\text{For any } x \in S,\ F(x + a) + F(x) = b + \varepsilon u, \text{ where } b + \varepsilon u \text{ is constant.} \qquad (1)$$

From (1) we would have that the equation for the uniform differentiability of function F, $\Delta_a F(x) = b + \varepsilon u$, has $|S| \geq \delta + 2$ solutions, which contradicts the fact that F is *differentially δ-uniform*. Thus, $S \cap A \neq \emptyset$ and $S \cap B \neq \emptyset$.

Then, $\forall x_i \in S \cap A$, $\forall x'_j \in S \cap B$:

$$F(x_i + a) + F(x_i) = b + u(0) \text{ and } f(x_i + a) + f(x_i) = 0, \text{ and} \tag{2}$$

$$F(x'_j + a) + F(x'_j) = b + u(1) \text{ and } f(x'_j + a) + f(x'_j) = 1. \tag{3}$$

Adding the systems of equations (2) and (3), there are $\delta + 2$ values $x_i \in A \neq \emptyset$ and $x'_j \in B \neq \emptyset$, where $a \neq 0$, such that:

$$F(x_i + a) + F(x_i) + F(x'_j + a) + F(x'_j) = u \text{ and}$$

$$f(x_i + a) + f(x_i) + f(x'_j + a) + f(x'_j) = 1.$$

Case 2: Conversely, [There exists $\delta + 2$ elements x_i in $A \neq \emptyset$ and x'_j in $B \neq \emptyset$, where $a \neq 0$, such that $[F(x_i)+F(x_i+a)+F(x'_j)+F(x'_j+a) = u$ and $f(x_i)+f(x_i+a)+f(x'_j)+f(x'_j+a) = 1]]$ $\Longrightarrow H$ is not *differentially δ-uniform*.

Proof:

Let $F(x_{i_0} + a) + F(x_{i_0}) = b$, for some $(x_{i_0}, b) \in A \times \mathbb{F}_2^n$. Substituting this into the equation $F(x_i) + F(x_i + a) + F(x'_j) + F(x'_j + a) = u$, we have:

$$F(x'_j + a) + F(x'_j) = b + u, \forall x'_j \in B.$$

Thus, $F(x_i) + F(x_i + a) + F(x'_j) + F(x'_j + a) = F(x_i) + F(x_i + a) + b + u = u, \forall x_i \in A$. Then:

$$F(x_i + a) + F(x_i) = b, \forall x_i \in A.$$

Then:

$$H(x_i) + H(x_i + a) = F(x_i) + F(x_i + a) + (f(x_i + a) + f(x_i))u = b \text{ and}$$

$$H(x'_j) + H(x'_j + a) = F(x'_j) + F(x'_j + a) + (f(x'_j + a) + f(x'_j))u = b.$$

Thus the equation $\Delta_a H(x) = b$ has $\delta + 2$ solutions, $x_i \in A$, $x'_j \in B$, and H as such can not be *differentially δ-uniform*.

The following theorem can simplify the calculations to verify if a function of the form $F(v + f(v).u)$ is APN, we give this without demonstration.

Theorem 2.1.2. Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Let $\mathbf{u} \in \mathbb{F}_2^n$, $\mathbf{u} \neq 0$, and $f : \mathbb{F}_2^n \to \mathbb{F}_2$ a Boolean function. Then $F(v + f(v).\mathbf{u})$ is an APN function if and only if

$$\forall\ a \neq 0,\ x\ \neq y \in \mathbb{F}_2^n,$$

$$F(x)+F(x+a)+F(y)+F(y+a+u) = 0 \implies (f(x) = 1 \vee f(x+a) = 1 \vee f(y) = 1 \vee f(y+a) = 0),$$

$$F(x)+F(x+a)+F(y+u)+F(y+a) = 0 \implies (f(x) = 1 \vee f(x+a) = 1 \vee f(y) = 0 \vee f(y+a) = 1),$$

$$F(x)+F(x+a)+F(y+u)+F(y+a+u) = 0 \implies (f(x) = 1 \vee f(x+a) = 1 \vee f(y) = 0 \vee f(y+a) = 0),$$

$$F(x)+F(x+a+u)+F(y+u)+F(y+a) = 0 \implies (f(x) = 1 \vee f(x+a) = 0 \vee f(y) = 0 \vee f(y+a) = 1),$$

$$F(x) + F(x + a + u) + F(y + u) + F(y + a + u) = 0 \implies (f(x) = 1\ \vee\ f(x + a) = 0\ \vee\ f(y) = 0\ \vee\ f(y + a) = 0),$$

$$F(x + u) + F(x + a) + F(y + u) + F(y + a + u) = 0 \implies (f(x) = 0\ \vee\ f(x + a) = 1\ \vee\ f(y) = 0\ \vee\ f(y + a) = 0).$$

The famous result that the function $B(x) = x^3 + tr(x^9)$ (equivalently $x^3 + a^{-1}tr(a^3x^9)$, where $a \neq 0$) is *differentially* 2*-uniform*, found by Budaghyan, Carlet, and Leander in [6], [21], $B(x)$ has not been generalized since 2008. In a different way, Irene Villa [37] (2019) has studied functions of the form $L_1(x^3) + L_2(x^9)$, where L_1, L_2 are linear functions. On the other hand, Bracken, Byrne, Markin, and McGuire [1] computed the Walsh spectrum of such quadratic function. Next, we give the new theorem (with a plain proof) which is a generalization of the B of Budaghyan et al.

Theorem 2.1.3. Let $F(x) = x^3 + \mu tr(G(x))$ be a *differentially* δ*-uniform* function over $\mathbb{F}_2^n$, where G is any polynomial, δ is 2 (or 4), and $\bar{\mu} \neq 0$ and $\mu \in \mathbb{F}_2^n$. Then, the following switching neighbours of F in the narrow sense are *differentially* δ*-uniform* over $\mathbb{F}_2^n$:

a) $\Gamma_1(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(x^9)$, where μ, $\bar{\mu}$ are cubic roots of the unit ($\mu^3 = \bar{\mu}^3 = 1$).

b) $\Gamma_2(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(x^9)$, where $\bar{\mu}^3 = 1$, and $\mu = 0$.

c) $\Gamma_3(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(x^3)$, where $tr(\mu) = tr(\bar{\mu}) = 0$.

Proof:

a) and b) We will prove the result by Theorem 2.1.1, where $F(x) = x^3 + \mu tr(G(x))$ is *differentially δ-uniform* on $\mathbb{F}_2^n$, the nonzero vector $u = \bar{\mu}$, and the Boolean function $f(x) = tr(x^9)$. Let $a \neq 0$, and any $\delta + 2$ values x_i, $x_i + a$, x_j, $x_j + a \in \mathbb{F}_2^n$ such that $F(x_i) + F(x_i + a) + F(x_j) + F(x_j + a) = u$, that is, $x_i^2 a + a^2 x_i + x_j^2 a + a^2 x_j = t$, where $t = \bar{\mu} - \mu tr(G(x_i) + G(x_i + a) + G(x_j) + G(x_j + a))$, then:

$$(x_i + x_j)^2 a = a^2(x_i + x_j) + t$$

$$\Rightarrow (x_i + x_j)^2 = a(x_i + x_j) + \tfrac{t}{a}$$

$$\Rightarrow (x_i + x_j)^4 = a^2(x_i + x_j)^2 + \tfrac{t^2}{a^2}$$

$$\Rightarrow (x_i + x_j)^4 = a^2(a(x_i + x_j) + \tfrac{t}{a}) + \tfrac{t^2}{a^2}$$

$$\Rightarrow (x_i + x_j)^4 = a^3(x_i + x_j) + at + \tfrac{t^2}{a^2}$$

$$\Rightarrow (x_i + x_j)^8 = a^6(x_i + x_j)^2 + a^2 t^2 + \tfrac{t^4}{a^4}$$

$$\Rightarrow (x_i + x_j)^8 = a^7(x_i + x_j) + a^5 t + a^2 t^2 + \tfrac{t^4}{a^4}.$$

So, multiplying by a (we get the conjugates $a^6 t$ and $a^3 t^2$, subject to $t^4 = t$) and applying the trace:

$$tr((x_i + x_j)^8 a + a^8(x_i + x_j)) = tr(a^6 t + a^3 t^2) + tr(\tfrac{t^4}{a^3}) = tr(\tfrac{t}{a^3}).$$

Dividing by a^3, the equation $(x_i + x_j)^2 a = a^2(x_i + x_j) + t$, and taking the trace:

$$0 = tr((\tfrac{x_i + x_j}{a})^2 + \tfrac{x_i + x_j}{a}) = tr(\tfrac{t}{a^3}).$$

Then for those whose $a \neq 0$ and $\delta + 2$ values x_i, $x_i + a$, x_j, $x_j + a$ such that $F(x_i) + F(x_i + a) + F(x_j) + F(x_j + a) = u$, we obtain:

$$f(x_i) + f(x_i + a) + f(x_j) + f(x_j + a) = tr((x_i + x_j)^8 a + a^8(x_i + x_j)) = 0.$$

The condition $t^4 = t$, where $t = \bar{\mu} - \mu tr(G(x_i) + G(x_i + a) + G(x_j) + G(x_j + a))$, $\mu \neq 0$, $\bar{\mu} \neq 0$:

$$t^4 = t \text{ iff } \bar{\mu}^4 = \bar{\mu} \text{ and } (\bar{\mu} + \mu)^4 = \bar{\mu} + \mu$$

$\bar{\mu}^4 = \bar{\mu}$, $\bar{\mu} \neq 0 \Rightarrow \bar{\mu}^3 = 1$.

$(\bar{\mu} + \mu)^4 = \bar{\mu} + \mu$, then:

If $\bar{\mu} = \mu \Rightarrow \mu^3 = 1$ also.

If $\bar{\mu} \neq \mu \Rightarrow (\bar{\mu} + \mu)^3 = 1$, $\bar{\mu}^2\mu + \bar{\mu}\mu^2 + \mu^3 = 0$. Then:

$\bar{\mu} \neq \mu$ and $\mu = 0$. Or

If $\bar{\mu} \neq \mu$ and $\mu \neq 0$, then $\frac{\bar{\mu}}{\mu}(\bar{\mu}^2\mu + \bar{\mu}\mu^2 + \mu^3) = 0$, $\bar{\mu}^2\mu + \bar{\mu}\mu^2 = 1$. Then $\mu^3 = 1$.

The functions Γ_1 and Γ_2 are *differentially δ-uniform* over $\mathbb{F}_2^n$.

c) We will show the result by applying Theorem 2.1.1 for the case where $f(x) = tr(x^3)$. By taking the trace on the equation $(x_i + x_j)^2 a = a^2(x_i + x_j) + t$ and the fact that $tr(G(x_i) + G(x_i + a) + G(x_j) + G(x_j + a))$ is Boolean implies:

$$f(x_i) + f(x_i + a) + f(x_j) + f(x_j + a) = tr((x_i + x_j)^2 a + a^2(x_i + x_j)) = 0 \text{ iff } tr(\bar{\mu}) = 0 \text{ and}$$
$$tr(\bar{\mu} + \mu) = 0$$

we found that the function Γ_3 is *differentially δ-uniform* over $\mathbb{F}_2^n$.

Remark For $G(x) = 0$, $\mu = \bar{\mu} = 1$, and x^3 APN over $\mathbb{F}_2^n$, Theorem 2.1.3 implies that $\Gamma_1(x) = x^3 + tr(x^9)$ is APN. This can also be done by choosing $\bar{\mu} = 1$ in $\Gamma_2(x)$. Furthermore, the function G could be chosen as *non-quadratic*. As another application of our Theorem 2.1.3, the following results can be verified:

Corollary 2.1.4. $\varphi(x) = x^3 + tr(x^5) + tr(x^9)$ is the only switching neighbor in the narrow sense, of $F(x) = x^3 + tr(x^5)$, of the form $x^3 + tr(x^5) + 1.tr(x^k)$, where $tr(x^k)$ is nonlinear, such that φ preserves the same *differential 2-uniformity* of F over $\mathbb{F}_2^5$.

By application of Corollary 2.1.5 we get new differential 4, 6, and 8 uniform functions; see the following tables of examples. We leave this as an exercise of this section the following result:

Corollary 2.1.5. Let $F(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x))$ a *differentially δ-uniform* function over $\mathbb{F}_2^n$, where G, H are any polynomials, $\delta \leq 8$, and μ, $\bar{\mu}, \bar{\bar{\mu}}$ are cubic roots of the unity. Then the following switching neighbour of F in the narrow sense also is *differentially δ-uniform* over $\mathbb{F}_2^n$:

$$\Gamma_1(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x)) + \bar{\bar{\mu}} tr(x^9).$$

Remark. Given G, H any polynomials over $\mathbb{F}_2^n$, $\delta \leq 8$, and μ, $\bar{\mu}, \bar{\bar{\mu}}$ cubic roots of the unity. Then:

a) $\Delta(x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x)) + \bar{\bar{\mu}} tr(x^9)) = \delta$ does not imply that $\Delta(x^3 + \mu tr(G(x))) = \delta$,

b) $\Delta(x^3 + \mu tr(G(x))) = \delta$ does not imply that $\Delta(x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x)) + \bar{\bar{\mu}} tr(x^9)) = \delta$. But

c) $\Delta(x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x)) + \bar{\bar{\mu}} tr(x^9)) = \delta$ implies $\Delta(x^3 + \mu tr(G(x)) + \bar{\mu} tr(H(x))) = \delta$.

Examples The following tables show cases where Theorems 2.1.1 and 2.1.3 apply, but not the results of Edel and Pott (Theorem 1.3.2 [21]), nor Theorem 1 of Budaghyan et al. [6]. For example, the switching neighbous of $F(x) = x^3 + tr(\alpha x^9)$ in the narrow sense, $x^3 + tr(\alpha x^9) + u.tr(x^9)$, where $f(x) = tr(x^9)$, and u such that $u^3 = 1$, Theorem 2.1.3. give us new *differentially δ-uniform* functions, Γ_1, from another *differentially δ-uniform* functions, for $\delta = 2, 4$. Where $\Delta(.)$ is the uniform differentiability of the given function (for computer programs see Appendix I):

$\mathbb{F}_{2^n}$	$\Delta(F(x))$	$\Delta(\Gamma_1(x) = x^3 + tr(x^5) + 1.tr(x^9))$
$\mathbb{F}_{2^4}$	2	2
$\mathbb{F}_{2^5}$	2	2
$\mathbb{F}_{2^6}$	4	4
$\mathbb{F}_{2^7}$	4	4
$\mathbb{F}_{2^8}$	4	4
$\mathbb{F}_{2^9}$	4	4
$\mathbb{F}_{2^{10}}$	4	4

TABLE 5. Switching neighbour of $F(x) = x^3 + tr(x^5)$

$\mathbb{F}_{2^n}$	$\Delta(x^3 + 1.tr(x^7))$	$\Delta(x^3 + 1.tr(x^7) + \bar{\mu}tr(x^{11}))$	$\Delta(x^3 + 1.tr(x^7) + \bar{\mu}tr(x^{11}) + \bar{\bar{\mu}}tr(x^9))$
$\mathbb{F}_{2^4}$	2	4, if $\bar{\mu} = \alpha^2 + \alpha$	4, if $\bar{\mu} = \alpha^2 + \alpha$, $\bar{\bar{\mu}} = \bar{\mu} + 1$
$\mathbb{F}_{2^5}$	4	only one cubic root of the unit	only one cubic root of the unit
$\mathbb{F}_{2^6}$	4	6, if $\bar{\mu} = \alpha^3 + \alpha^2 + \alpha$	6, if $\bar{\mu} = \alpha^3 + \alpha^2 + \alpha$, $\bar{\bar{\mu}} = \bar{\mu} + 1$
$\mathbb{F}_{2^7}$	4	only one cubic root of the unit	only one cubic root of the unit
$\mathbb{F}_{2^8}$	4	8, if $\bar{\mu} = \alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha$	8, if $\bar{\mu} = \alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha$, $\bar{\bar{\mu}} = \bar{\mu} + 1$
$\mathbb{F}_{2^9}$	4	only one cubic root of the unit	only one cubic root of the unit
$\mathbb{F}_{2^{10}}$	4	8, if $\bar{\mu} = \alpha^5 + \alpha^3 + \alpha$	8, if $\bar{\mu} = \alpha^5 + \alpha^3 + \alpha$, $\bar{\bar{\mu}} = \bar{\mu} + 1$

TABLE 6. Corollary 2.1.5 applies, where $G(x) = x^7$, $H(x) = x^{11}$ are *cubic* functions, $\bar{\mu}^3 = \bar{\bar{\mu}}^3 = 1$, and α *a primitive element*

$\mathbb{F}_{2^n}$	$\Delta(F(x))$	$\Delta(\Gamma_1(x) = x^3 + tr(x^3) + 1.tr(x^9))$
$\mathbb{F}_{2^4}$	2	2
$\mathbb{F}_{2^5}$	4	4
$\mathbb{F}_{2^6}$	2	2
$\mathbb{F}_{2^7}$	4	4
$\mathbb{F}_{2^8}$	2	2
$\mathbb{F}_{2^9}$	4	4
$\mathbb{F}_{2^{10}}$	2	2

TABLE 7. Switching neighbour of $F(x) = x^3 + tr(x^3)$

$\mathbb{F}_{2^n}$	$\Delta(F(x))$	$\Delta(x^3 + tr(\alpha x^9) + u.tr(x^9))$	$\Delta(x^3 + tr(\alpha x^9) + 1.tr(x^3))$
$\mathbb{F}_{2^4}$	2	2, if $u \in 1^{\frac{1}{3}} = \{\alpha^2 + \alpha,\ \alpha^2 + \alpha + 1,\ 1\}$ 2, if $u = \alpha$	2
$\mathbb{F}_{2^5}$	4	8, if $u = \alpha$ 4, if $u = 1$	4
$\mathbb{F}_{2^6}$	4	4, if $u \in 1^{\frac{1}{3}} = \{\alpha^3 + \alpha^2 + \alpha,\ \alpha^3 + \alpha^2 + \alpha + 1,\ 1\}$ 4, if $u = \alpha$	4
$\mathbb{F}_{2^7}$	4	8, if $u = \alpha$ 4, if $u = 1$	4
$\mathbb{F}_{2^8}$	4	4, if $u \in 1^{\frac{1}{3}} = \{\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha,$ $\alpha^7 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha + 1,\ 1\}$. 8, if $u = \alpha$	4
$\mathbb{F}_{2^9}$	4	8, if $u = \alpha$ 4, if $u = 1$	4
$\mathbb{F}_{2^{10}}$	4	4, if $u \in 1^{\frac{1}{3}} = \{\alpha^5 + \alpha^3 + \alpha,\ \alpha^5 + \alpha^3 + \alpha + 1,\ 1\}$ 8, if $u = \alpha$	4

TABLE 8. Switching neighbours of $F(x) = x^3 + tr(\alpha x^9)$, α *a primitive element*

2.2 Construction of Differentially δ-Uniform Families

Our new Theorem 2.2.3 in this section generalizes Theorem 2 in [7], [4], of Budaghyan, Carlet, and Pott, for equal parameters ($j = i$). Our Theorem 2.2.3 considers the case for $i \neq j$. Our Corollary 2.2.17 generalizes Theorem 2.2.3. And, our new Theorems 2.2.16 and 2.2.19 generalize Corollary 2.2.17.

In Section 2.1 we have dealt with the *differentially δ-uniform* functions, $\bar{F}(v) := F(v) + f(v).u$, where f is a Boolean function, and u is a non-zero constant in $\mathbb{F}_2^n$. In this section we obtain families of these functions $\bar{F}$ but for u being the *affine function* $u = u(v) = v^{2^j} + v + 1$, found in our new Theorem 2.2.3 and its generalization, the Corollary 2.2.17. In the main theorem of Section 5.1, Theorem 5.1.1, u is the function defined by $u = v^{2^{2i}-2^i} + v^{2^{2i}-(2)2^i+1} + v^{2^{2i}-(2)2^i} + v^{2^{2i}-(3)2^i+1} + v^{2^{2i}-(3)2^i} + \cdots + v^{2^i+1} + v^{2^i} + v + 1$, which for example, if $i = 3$, it can be verified that u becomes a *cubic function*. Moreover, in the main theorem of Section 5.1, Theorem 5.1.1, $d^0(u(v)) = i < d^0(F(v)) = i + 1$, but $d^0(\mathcal{K}(v)) = n - 1$. We obtain families of functions for $u = u(v)$ being non constant, up to its generalization to a polynomial version instead, given by corollaries 2.2.7 and 2.2.9, and Theorem 2.2.8. In general, we are looking for functions of the form $F(v + f(v).u)$, see Definition 2.2.1 on switching neighbous in the narrow sense along the x- axis. Definition 2.2.1 allows us to make a second generalization of that to the polynomial version instead, both being as general as possible ($u(v)$ and $f(v)$, so $\bar{F}$), described in Theorem 2.2.16 and Theorem 2.2.19, Corollary 2.2.17, 2.2.18, and Theorem 2.2.21. Finally, based on the idea established in Definition 2.2.1, we discover two new and beautiful *differentially δ-uniform* families, on Theorem 2.2.24.

A large part of our machinery follows from to the next new Lemma 2.2.1.

Lemma 2.2.1. [existence and uniqueness of solution] Let $c \in \mathbb{F}_{2^n}$, $i \in \mathbb{N}$, n even. The equation $x + tr(x^{2^i+1}) = c$ has a unique solution. This solution is given by $x = c + tr(c^{2^i+1})$.

Proof:

The term $tr(x^{2^i+1})$ is Boolean, then there are two defined cases. In the equation for x, $x + tr(x^{2^i+1}) = c$, there are only two possible solutions, c and $c+1$. If x_0 is a solution for that equation,

then x_0+1 is not a solution because: $x_0+1+tr(x_0+1)^{2^i+1} = x_0+1+tr(x_0^{2^i+1})+tr(x_0^{2^i}+x_0)+tr(1) = 1+(x_0+tr(x_0^{2^i+1}))+(tr(x_0^{2^i})+tr(x_0))+tr(1) = 1+c+0+0 = c+1 \neq c$. Thus, the solution for this equation is unique.

If $tr(c^{2^i+1}) = 0$, then $x = c$ is the solution of the equation. But if $tr(c^{2^i+1}) = 1$, then $x = c+1$ is the solution of the given equation: $c+1+tr(c+1)^{2^i+1} = c+1+tr(c^{2^i+1})+tr(c^{2^i}+c)+tr(1) = c$. But in each case we can write as follows, $x = c+0 = c+tr(c^{2^i+1})$, and the other case $x = c+1 = c+tr(c^{2^i+1})$.

Lemma 2.2.2. Let $c \in \mathbb{F}_{2^n}$, $i \in \mathbb{N}$, n odd. Then the equation $x + tr(x^{2^i+1}) = c$ has no solution, if $tr(c^{2^i+1}) = 1$, and has the two solutions c, $c+1$, if $tr(c^{2^i+1}) = 0$.

Proof:

The term $tr(x^{2^i+1})$ is Boolean, then are defined two cases. In the equation for x, $x+tr(x^{2^i+1}) = c$, there are only two possible solutions, c and $c+1$. We define $\varphi(x) = x + tr(x^{2^i+1})$, then $\varphi(x_0+1) = x_0+1+tr(x_0+1)^{2^i+1} = x_0+1+tr(x_0^{2^i+1})+tr(x_0^{2^i}+x_0)+tr(1) = x_0+tr(x_0^{2^i+1}) = \varphi(x_0)$, which means $\varphi(x_0+1) = x_0+tr(x_0^{2^i+1}) = \varphi(x_0)$. Then, x_0 is a solution for that equation, if and only if x_0+1 is a solution.

If $tr(c^{2^i+1}) = 0$, then $x = c$, $c+1$ are the solutions of the equation. But if $tr(c^{2^i+1}) = 1$, the equation has no solutions.

Theorem 2.2.3. The family of functions $f(x) = x^{2^j+1}+(x^{2^j}+x+1)tr(x^{2^i+1})$, such that $\gcd(j, n) = 1$, n even, and $i \in \mathbb{N}$, is at least *differentially* 4-*uniform* over $\mathbb{F}_{2^n}$ (i.e. f could be *differentially* 2-*uniform* over $\mathbb{F}_{2^n}$).

Proof:

The function f can be written in the compact form $f(x) = (x + tr(x^{2^i+1}))^{2^j+1}$. We establish its corresponding differential equation to be studied:

$$D_a f(x) = (x + tr(x^{2^i+1}) + tr(x^{2^i}a + a^{2^i}x) + tr(a^{2^i+1}) + a)^{2^j+1} - (x + tr(x^{2^i+1}))^{2^j+1} = b$$

The term $tr(x^{2^i}a+a^{2^i}x)+tr(a^{2^i+1})+a$ is susceptible to being zero, then its corresponding equation for $b=0$, $D_af(x)=0$, is satisfied for all elements of $\mathbb{F}_{2^n}$, but it could be happen only for $a=1$.

Case $a\neq 1$. **Subcase** $tr(x^{2^i}a+a^{2^i}x)=0$: The equation $D_af(x)=b$ becomes:

$$(x+tr(x^{2^i+1})+tr(a^{2^i+1})+a)^{2^j+1}-(x+tr(x^{2^i+1}))^{2^j+1}=b$$

Because of $gcd(j,\,n)=1$, this equation has at most two solutions for the variable $y=x+tr(x^{2^i+1})$, which will be denoted by $y=x_1$ and $y=x_1+tr(a^{2^i+1})+a$. The term $tr(x^{2^i+1})$ is Boolean, then there are defined two cases. In the equation for x, $x+tr(x^{2^i+1})=y$, there are only two possible solutions, y and $y+1$. Besides, the value of $tr(y^{2^i+1})$ divides in two disjoint cases. Afterward, we try to solve the equations $x+tr(x^{2^i+1})=y$, for each value of y.

The equation $x+tr(x^{2^i+1})=x_1,$ by Lemma 2.2.1, has the solution $x=x_1+tr(x_1^{2^i+1})$.
The equation $x+tr(x^{2^i+1})=x_1+tr(a^{2^i+1})+a,$ by Lemma 2.2.1, has the solution $x=x_1+tr(a^{2^i+1})+a+tr(x_1+tr(a^{2^i+1})+a)^{2^i+1}$.
Then there are at most two solutions.

Subcase $tr(x^{2^i}a+a^{2^i}x)=1$: The equation $D_af(x)=b$ becomes:

$$(x+tr(x^{2^i+1})+tr(a^{2^i+1})+a+1)^{2^j+1}-(x+tr(x^{2^i+1}))^{2^j+1}=b.$$

Because of $gcd(j,\,n)=1$, this equation has at most two solutions for the variable $y=x+tr(x^{2^i+1})$, denoted by $y=x_2$ and $y=x_2+tr(a^{2^i+1})+a+1$. Afterward, we solve the equations $x+tr(x^{2^i+1})=y$, for each value of y.

The equation $x+tr(x^{2^i+1})=x_2$, by Lemma 2.2.1, has the solution $x=x_2+tr(x_2^{2^i+1})$.
The equation $x+tr(x^{2^i+1})=x_2+tr(a^{2^i+1})+a+1,$ by Lemma 2.2.1, has the solution $x=x_2+tr(a^{2^i+1})+a+1+tr(x_2+tr(a^{2^i+1})+a+1)^{2^i+1}$.
Then there are at most two solutions.

Case $a=1$. Let $D_1f(x)=(x+tr(x^{2^i+1})+1)^{2^j+1}-(x+tr(x^{2^i+1}))^{2^j+1}=b$. This equation can be treated as the equations that appear in the case for $a\neq 1$. So, the equation $D_1f(x)=b$ has at most two solutions.

In conclusion, for n even, the equation $D_af(x)=b$ has at most four solutions.

Examples Theorem 2.2.3 set up a variety of examples with low differentiability, which can be verified using the software SAGE 8.0 in a PC of 16 RAM memory:

The entire family of functions $\{x^{2^1+1}+(x^{2^1}+x+1)tr(x^{2^1+1}),\ x^{2^1+1}+(x^{2^1}+x+1)tr(x^{2^2+1}),\ x^{2^1+1}+(x^{2^1}+x+1)tr(x^{2^3+1}),\ x^{2^3+1}+(x^{2^3}+x+1)tr(x^{2^1+1}),\ x^{2^3+1}+(x^{2^3}+x+1)tr(x^{2^2+1}),\ x^{2^3+1}+(x^{2^3}+x+1)tr(x^{2^3+1})\}$ is an APN family over $\mathbb{F}_{2^4}$.

The family of functions $\{x^{2^j+1}+(x^{2^j}+x+1)tr(x^{2^i+1})$; for $i \in \{2,4\},\ j \in \{1,5\}\}$ is *differentially* 4-*uniform* over $\mathbb{F}_{2^6}$, whereas the family of functions $\{x^{2^j+1}+(x^{2^j}+x+1)tr(x^{2^i+1})$; for $i \in \{1,3,5\},\ j \in \{1,5\}\}$ is APN over $\mathbb{F}_{2^6}$.

Over $\mathbb{F}_{2^8}$, the family of functions $\{x^{2^1+1}+(x^{2^1}+x+1)tr(x^{2^i+1})$; for $i \in \{2,3,5,6\}\}$ is *differentially* 4-*uniform*, whereas the family of functions $\{x^{2^1+1}+(x^{2^1}+x+1)tr(x^{2^i+1})$; for $i \in \{1,4,7\}\}$ is APN.

Over $\mathbb{F}_{2^8}$, the family of functions $\{x^{2^3+1}+(x^{2^3}+x+1)tr(x^{2^i+1})$; for $i \in \{1,2,6,7\}\}$ is *differentially* 4-*uniform*, whereas the family of functions $\{x^{2^3+1}+(x^{2^3}+x+1)tr(x^{2^i+1})$; for $i \in \{3,4,5\}\}$ is APN.

Remark These examples show cases of APN functions as in Theorem 2 in [7], [4]. Note that there are also for $i \neq j$ new APN functions, in each one of these finite fields. Our Theorem 2.2.3 generalizes the theorem of Budaghyan et al., where $j = i$. We obtain new APN and diff. 4-uniform functions not obtainable by the results of Budaghyan et al. By putting a condition on i in relation to the field degree, n, one subfamily of this form is given by our next result.

Corollary 2.2.4. The family of functions $f(x) = x^{2^j+1} + (x^{2^j} + x + 1)tr(x^{2^{\frac{n}{2}}+1})$, such that $gcd(j, n) = 1$, and n even, is APN over $\mathbb{F}_{2^n}$.

Proof:

For any a, x in $\mathbb{F}_{2^n}$, $(x^{2^{\frac{n}{2}}}a)^{2^{\frac{n}{2}}} = xa^{2^{\frac{n}{2}}}$, i.e. $x^{2^{\frac{n}{2}}}a$ and $a^{2^{\frac{n}{2}}}x$ are conjugates. So for $i = \frac{n}{2}$ in the demonstration of Theorem 2.2.3, we have the identity, $tr(x^{2^i}a + a^{2^i}x) = 0$ on $\mathbb{F}_{2^n}$. Then for any $a \neq 0$, and b in $\mathbb{F}_{2^n}$, the equation $D_a f(x) = b$ has at most two solutions.

Conjecture 1. The family of functions $f(x) = x^{2^j+1} + (x^{2^j} + x + tr(1) + 1)tr(x^{2^i+1} + xtr(1))$ is at least *differentially* 4-*uniform* over $\mathbb{F}_{2^n}$, for n even, $gcd(j, n) = 1$, $n \geqslant 4$.

Note that in the proof of Theorem 2.2.3 there is no a restriction to consider an APN function in general instead of the Gold function $F(x) = x^{2^j+1}$, and we make it more precise in the following theorem.

Theorem 2.2.5. The family of functions $f(x) = F(x+tr(x^{2^i+1}))$ is at least *differentially* 4-*uniform*, where F is an APN function, over $\mathbb{F}_{2^n}$, where n is even.

Theorem 2.2.6. [differentially uniform version] The family of functions $f(x) = F(x+tr(x^{2^i+1}))$ is *differentially* γ-*uniform*, where $\delta \leq \gamma \leq 2\delta$, F is *differentially* δ-*uniform*, and n even, over $\mathbb{F}_{2^n}$.

Proof:

Use F *differentially* δ-*uniform* instead of F Gold type in the proof of Theorem 2.2.3.

Corollary 2.2.7. The functions $f(x) = x^{2^{2j}+2^j+1} + (x^{2^{2j}+2^j} + x^{2^{2j}+1} + x^{2^{2j}} + x^{2^j+1} + x^{2^j} + x + 1)tr(x^{2^i+1})$ are at least *differentially* 8-*uniform* over $\mathbb{F}_{2^{4j}}$, where i, $j \in \mathbb{N}$.

Proof:

Applying Theorem 2.2.6 for the *differentially* 4-*uniform* function $F(x) = x^{2^{2j}+2^j+1}$ (permutation iff j is odd) over $\mathbb{F}_{2^{4j}}$ [2].

Examples

The family of functions $\{x^7 + (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)tr(x^{2^i+1})$; for $i \in \{1, 2, 3\}\}$ are *differentially* 4-*uniform* over $\mathbb{F}_{2^4}$.

The family of functions $\{x^{21}+(x^{20}+x^{17}+x^{16}+x^5+x^4+x+1)tr(x^{2^i+1})$; for $i \in \{1, 2, 3, 5, 6, 7\}\}$ are *differentially* 8-*uniform* over $\mathbb{F}_{2^8}$, except for one!, $f(x) = x^{21}+(x^{20}+x^{17}+x^{16}+x^5+x^4+x+1)tr(x^{17})$ are *differentially* 4-*uniform* over $\mathbb{F}_{2^8}$.

Theorem 2.2.8. The family of functions $f(x) = F(x+tr(x^{2^{\frac{n}{2}}+1}))$ is *differentially* δ-*uniform*, where F are *differentially* δ-*uniform*, over $\mathbb{F}_{2^n}$, where n is even.

Proof:

For any a, x in $\mathbb{F}_{2^n}$, $(x^{2^{\frac{n}{2}}}a)^{2^{\frac{n}{2}}} = xa^{2^{\frac{n}{2}}}$. So for $i = \frac{n}{2}$ in the demonstration of Theorem 2.2.6, which is the generalization of Theorem 2.2.3 for F *differentially* δ-*uniform* instead of the Gold family, x^{2^j+1}, the next identity is satisfied, $tr(x^{2^i}a + a^{2^i}x) = 0$ on $\mathbb{F}_{2^n}$. Then for any $a \neq 0$, and b in $\mathbb{F}_{2^n}$, the equation $D_a f(x) = b$ attains at most δ solutions.

Corollary 2.2.9. The functions $f(x) = x^{2^{2j}+2^j+1} + (x^{2^{2j}+2^j} + x^{2^{2j}+1} + x^{2^{2j}} + x^{2^j+1} + x^{2^j} + x + 1)tr(x^{2^{2j}+1})$ is *differentially* 4-*uniform* over $\mathbb{F}_{2^{4j}}$, where $j \in \mathbb{N}$.

Proof:

We apply Theorem 2.2.8 for the *differentially* 4-*uniform* function $F(x) = x^{2^{2j}+2^j+1}$ (permutation iff j is odd) over $\mathbb{F}_{2^{4j}}$ [2].

Remark In the aforementioned examples the only member of that family over $\mathbb{F}_{2^8}$, which is a *differentially* 4-*uniform*, is the function $f(x) = x^{21} + (x^{20} + x^{17} + x^{16} + x^5 + x^4 + x + 1)tr(x^{17})$, found by our Corollary 2.2.9.

Conjecture 2. The family of functions $f(x) = F(x+tr(x^{2^i+3}))$ are *differentially* γ-*uniform*, where $\delta \leq \gamma \leq 4\delta$, F is *differentially* δ-*uniform*, over $\mathbb{F}_{2^n}$, where n is even.

Lemma 2.2.10. Let $c \in \mathbb{F}_{2^n}$, $j \geq 1$, each $i_k \in \mathbb{N}$, n even. The equation $x + tr(x^{2^i+1} + x^{2^j+1}) = c$ has only one solution, $x = c + tr(c^{2^i+1} + c^{2^j+1})$.

Proof:

Solution Uniqueness: Let $\varphi(x) := x + tr(x^{2^i+1} + x^{2^j+1})$. The term $tr(x^{2^i+1} + x^{2^j+1})$ is Boolean, then the equation for x, $\varphi(x) = c$, has only two possible solutions, c and $c+1$. If x_0 is a solution for that equation, then $x_0 + 1$ is not a solution: $\varphi(x_0 + 1) = x_0 + 1 + tr(x_0^{2^i+1} + 1 + x_0^{2^j+1} + 1) = x_0 + tr(x_0^{2^i+1} + x_0^{2^j+1}) + 1 = \varphi(x_0) + 1 \neq \varphi(x_0) = c$, because of the identity $tr(x+1)^{2^k+1} = tr(x^{2^k+1} + 1)$ on F_{2^n}, $\forall k \in \mathbb{N}$. Then the solution for this equation is unique.

Form of the Solution: From our experience with Lemma 2.2.1, we are motivated to consider the following form of the solution, $x = c + tr(c^{2^i+1} + c^{2^j+1})$. If $tr(c^{2^i+1} + c^{2^j+1}) = 0$, then $\varphi(c + tr(c^{2^i+1} + c^{2^j+1})) = \varphi(c) = c + tr(c^{2^i+1} + c^{2^j+1}) = c + 0 = c$. On the other hand, if $tr(c^{2^i+1} + c^{2^j+1}) = 1$, then $\varphi(c + tr(c^{2^i+1} + c^{2^j+1})) = \varphi(c+1) = \varphi(c) + 1 = c + tr(c^{2^i+1} + c^{2^j+1}) + 1 = c + 1 + 1 = c$, as in a previous calculation, where $\varphi(x_0 + 1) = \varphi(x_0) + 1$. So in both cases $x = c + tr(c^{2^i+1} + c^{2^j+1})$ is the solution for the given equation, $\varphi(x) = c$.

Theorem 2.2.11. [for Addition] The family of functions $f(x) = F(x + tr(x^{2^{i_1}+1}) + tr(x^{2^{i_2}+1}) + \cdots + tr(x^{2^{i_j}+1}))$ are *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $j \geq 1$, each $i_k \in \mathbb{N}$, F is *differentially δ-uniform*, over $\mathbb{F}_{2^n}$, where n is even.

Proof:

WLOG, we give the demonstration for two terms. Given $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, considering the corresponding differential equation for f to be studied:

$$D_a f(x) = F(x + tr(x^{2^i+1}) + tr(x^{2^j+1}) + tr(x^{2^i}a + a^{2^i}x + x^{2^j}a + a^{2^j}x) + tr(a^{2^i+1} + a^{2^j+1}) + a) - F(x + tr(x^{2^i+1}) + tr(x^{2^j+1})) = b.$$

Case $a \neq 1$. **Subcase** $tr(x^{2^i}a + a^{2^i}x + x^{2^j}a + a^{2^j}x) = 0$: The equation $D_a f(x) = b$ becomes:

$$F(x + tr(x^{2^i+1}) + tr(x^{2^j+1}) + tr(a^{2^i+1} + a^{2^j+1}) + a) - F(x + tr(x^{2^i+1}) + tr(x^{2^j+1})) = b$$

Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + tr(x^{2^i+1} + x^{2^j+1})$, which will be denoted by $y = y_t$ and $y = y_t + tr(a^{2^i+1} + a^{2^j+1}) + a$, for $1 \leq t \leq \frac{\delta}{2}$. In the following, we solve the equations $x + tr(x^{2^i+1} + x^{2^j+1}) = y$, for each value of y.

The equation $x + tr(x^{2^i+1} + x^{2^j+1}) = y_t$, by Lemma 2.2.10, has the unique solution $x = y_t + tr(y_t^{2^i+1} + y_t^{2^j+1})$, for $1 \leq t \leq \frac{\delta}{2}$.

The equation $x + tr(x^{2^i+1} + x^{2^j+1}) = y_t + tr(a^{2^i+1} + a^{2^j+1}) + a$, by Lemma 2.2.10, has the unique solution $x = y_t + tr(a^{2^i+1} + a^{2^j+1}) + a + tr((y_t + tr(a^{2^i+1} + a^{2^j+1}) + a)^{2^i+1} + (y_t + tr(a^{2^i+1} + a^{2^j+1}) + a)^{2^j+1}) = y_t + tr(a^{2^i+1} + a^{2^j+1}) + a + tr((y_t + a)^{2^i+1} + (y_t + a)^{2^j+1}) = y_t + a + tr(y_t^{2^i+1} + y_t^{2^j+1} + (y_t^{2^i} + y_t^{2^j})a + (a^{2^i} + a^{2^j})y_t)$, because of $tr(a^{2^i+1} + a^{2^j+1})$ is Boolean and $tr(1) = 0$, for $1 \leq t \leq \frac{\delta}{2}$.

Then there are at most δ solutions.

Subcase $tr(x^{2^i}a + a^{2^i}x + x^{2^j}a + a^{2^j}x) = 1$: The equation $D_a f(x) = b$ becomes:

$$F(x + tr(x^{2^i+1}) + tr(x^{2^j+1}) + tr(a^{2^i+1} + a^{2^j+1}) + a + 1) - F(x + tr(x^{2^i+1}) + tr(x^{2^j+1})) = b$$

Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + tr(x^{2^i+1} + x^{2^j+1})$, which will be denoted by $y = z_t$ and $y = z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1$, for $1 \leq t \leq \frac{\delta}{2}$. In the following, we solve the equations $x + tr(x^{2^i+1} + x^{2^j+1}) = y$, for each value of y.

The equation $x + tr(x^{2^i+1} + x^{2^j+1}) = z_t$, by Lemma 2.2.10, has the unique solution $x = z_t + tr(z_t^{2^i+1} + z_t^{2^j+1})$, for $1 \leq t \leq \frac{\delta}{2}$.

The equation $x + tr(x^{2^i+1} + x^{2^j+1}) = z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1$, by Lemma 2.2.10, has the unique solution $x = z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1 + tr((z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1)^{2^i+1} + (z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1)^{2^j+1}) = z_t + tr(a^{2^i+1} + a^{2^j+1}) + a + 1 + tr((z_t + a)^{2^i+1} + (z_t + a)^{2^j+1}) = z_t + a + 1 + tr(z_t^{2^i+1} + z_t^{2^j+1} + (z_t^{2^i} + z_t^{2^j})a + (a^{2^i} + a^{2^j})z_t)$, because of $tr(a^{2^i+1} + a^{2^j+1})$ is Boolean and $tr(1) = 0$, for $1 \leq t \leq \frac{\delta}{2}$.

Then there are at most δ solutions.

Case $a = 1$. $D_1 f(x) = F(x + tr(x^{2^i+1} + x^{2^j+1}) + 1) - F(x + tr(x^{2^i+1} + x^{2^j+1})) = b$, this equation can be treated as the equations that appear in the case for $a \neq 1$. So the equation $D_1 f(x) = b$ has at most δ solutions.

In conclusion, for n even, for any $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, the equation $D_a f(x) = b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$.

Remark For $i_1, i_2, \cdots, i_j$, such that, $tr(x^{2^{i_1}} a + a^{2^{i_1}} x) = \cdots = tr(x^{2^{i_j}} a + a^{2^{i_j}} x) = 0$ on $\mathbb{F}_{2^n}$, the functions in Theorem 2.2.11, $f(x) = F(x + tr(x^{2^{i_1}+1}) + tr(x^{2^{i_2}+1}) + \cdots + tr(x^{2^{i_j}+1}))$, become *differentially δ-uniform*.

Then Theorem 2.2.3 becomes a particular case of the following corollary.

Corollary 2.2.12. The family of functions $\varphi(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1} + x^{2^{i_2}+1} + \cdots + x^{2^{i_j}+1})$, such that $gcd(k, n) = 1$, and n even, are at least *differentially 4-uniform* over $\mathbb{F}_{2^n}$.

Examples The entire family of functions $\{x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1} + x^{2^{i_2}+1})$; for any $k \in \{1, 3\}$, i_1 and $i_2 \in \{1, 2, 3\}\}$ are APN over $\mathbb{F}_{2^4}$.

Over $\mathbb{F}_{2^6}$, the family of functions $\{x^{2^1+1} + (x^{2^1} + x + 1)tr(x^{2^i+1} + x^{2^j+1})$; for $1 \leq i < j \leq 5\}$ are *differentially 4-uniform*, except for $\{x^{2^1+1} + (x^{2^1} + x + 1)tr(x^{2^1+1} + x^{2^3+1})$, $x^{2^1+1} + (x^{2^1} + x + 1)tr(x^{2^1+1} + x^{2^5+1})$, $x^{2^1+1} + (x^{2^1} + x + 1)tr(x^{2^2+1} + x^{2^4+1})$, $x^{2^1+1} + (x^{2^1} + x + 1)tr(x^{2^3+1} + x^{2^5+1})\}$ which is APN.

Lemma 2.2.13. Let $c \in \mathbb{F}_{2^n}$, i, $j \in \mathbb{N}$, n even. The equation $x + tr(x^{2^i+1})tr(x^{2^j+1}) = c$ has only one solution, $x = c + tr(c^{2^i+1})tr(c^{2^j+1})$.

Proof:

Solution Uniqueness: Let $\varphi(x) := x + tr(x^{2^i+1})tr(x^{2^j+1})$. The term $tr(x^{2^i+1})tr(x^{2^j+1})$ is Boolean, then the equation for x, $\varphi(x) = c$, has only two possible solutions, c and $c+1$. If x_0 is a solution for that equation, then $x_0 + 1$ is not a solution: $\varphi(x_0 + 1) = x_0 + 1 + tr(x_0^{2^i+1} + 1)tr(x_0^{2^j+1} + 1) = x_0 + tr(x_0^{2^i+1})tr(x_0^{2^j+1}) + 1 = \varphi(x_0) + 1 \neq \varphi(x_0) = c$, because of the identity $tr(x+1)^{2^k+1} = tr(x^{2^k+1} + 1)$ on F_{2^n}, $\forall k \in \mathbb{N}$, and $tr(1) = 0$. Then the solution for this equation is unique.

Form of the Solution: From our experience with Lemma 2.2.1, we are motivated to consider the following form of the solution, $x = c + tr(c^{2^i+1})tr(c^{2^j+1})$. If $tr(c^{2^i+1})tr(c^{2^j+1}) = 0$, then $\varphi(c + tr(c^{2^i+1})tr(c^{2^j+1})) = \varphi(c) = c + tr(c^{2^i+1})tr(c^{2^j+1}) = c + 0 = c$. On the other hand, if $tr(c^{2^i+1})tr(c^{2^j+1}) = 1$, then $\varphi(c+tr(c^{2^i+1})tr(c^{2^j+1})) = \varphi(c+1) = \varphi(c)+1 = c+tr(c^{2^i+1})tr(c^{2^j+1})+1 = c+1+1 = c$, as in a previous calculation, where $\varphi(x_0 + 1) = \varphi(x_0) + 1$. So in both cases $x = c + tr(c^{2^i+1})tr(c^{2^j+1})$ is the solution for the given equation, $\varphi(x) = c$.

Theorem 2.2.14. [for Product] The family of functions $f(x) = F(x + tr(x^{2^i+1})tr(x^{2^j+1}))$ is *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $j \geq 1$, each $i_k \in \mathbb{N}$, F is *differentially δ-uniform*, over $\mathbb{F}_{2^n}$, where n is even.

Proof:

Given $a \neq 0$, b, both in $\mathbb{F}_{2^n}$, we consider the corresponding differential equation for f to be studied:

$$D_a f(x) = F(x + tr(x^{2^i+1})tr(x^{2^j+1}) + tr(x^{2^i+1})tr(x^{2^j}a + a^{2^j}x + a^{2^j+1}) + tr(x^{2^i}a + a^{2^i}x + a^{2^i+1})tr(x+a)^{2^j+1} + a) - F(x + tr(x^{2^i+1})tr(x^{2^j+1})) = b.$$

The function $tr(x^{2^i+1})tr(x^{2^j}a + a^{2^j}x + a^{2^j+1}) + tr(x^{2^i}a + a^{2^i}x + a^{2^i+1})tr(x+a)^{2^j+1}$ is Boolean, so, for $a = 1$, it is possible that the term $tr(x^{2^i+1})tr(x^{2^j}a+a^{2^j}x+a^{2^j+1})+tr(x^{2^i}a+a^{2^i}x+a^{2^i+1})tr(x+$

$a)^{2^j+1}+a$ becomes zero, with which the equation for $b=0$, $D_1f(x)=0$, is reduced to the equation, $F(x+tr(x^{2^i+1})tr(x^{2^j+1}))-F(x+tr(x^{2^i+1})tr(x^{2^j+1}))=0$.

Case $a\neq 1$. **Subcase** $tr(x^{2^i+1})tr(x^{2^j}a+a^{2^j}x+a^{2^j+1})+tr(x^{2^i}a+a^{2^i}x+a^{2^i+1})tr(x+a)^{2^j+1}=0$: The equation $D_af(x)=b$ becomes:

$$F(x+tr(x^{2^i+1})tr(x^{2^j+1})+a)-F(x+tr(x^{2^i+1})tr(x^{2^j+1}))=b.$$

Because of F is *differentially* δ*-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y=x+tr(x^{2^i+1})tr(x^{2^j+1})$, which will be denoted by $y=y_t$ and $y=y_t+a$, for $1\leq t\leq\frac{\delta}{2}$. In the following, we solve the equations $x+tr(x^{2^i+1})tr(x^{2^j+1})=y$, for each value of y.

The equation $x+tr(x^{2^i+1})tr(x^{2^j+1})=y_t$, by Lemma 2.2.13, has the unique solution $x=y_t+tr(y_t^{2^i+1})tr(y_t^{2^j+1})$, for $1\leq t\leq\frac{\delta}{2}$.
The equation $x+tr(x^{2^i+1})tr(x^{2^j+1})=y_t+a$, by Lemma 2.2.13, has the unique solution $x=y_t+a+tr(y_t+a)^{2^i+1}tr(y_t+a)^{2^j+1}$, for $1\leq t\leq\frac{\delta}{2}$.

Then, there are at most δ solutions.

Subcase $tr(x^{2^i+1})tr(x^{2^j}a+a^{2^j}x+a^{2^j+1})+tr(x^{2^i}a+a^{2^i}x+a^{2^i+1})tr(x+a)^{2^j+1}=1$: The equation $D_af(x)=b$ becomes:

$$F(x+tr(x^{2^i+1})tr(x^{2^j+1})+a+1)-F(x+tr(x^{2^i+1})tr(x^{2^j+1}))=b.$$

Because of F is *differentially* δ*-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y=x+tr(x^{2^i+1})tr(x^{2^j+1})$, which will be denoted by $y=z_t$ and $y=z_t+a+1$, for $1\leq t\leq\frac{\delta}{2}$. In the following, we solve the equations $x+tr(x^{2^i+1})tr(x^{2^j+1})=y$, for each value of y.

The equation $x+tr(x^{2^i+1})tr(x^{2^j+1})=z_t$, by Lemma 2.2.13, has the unique solution $x=z_t+tr(z_t^{2^i+1})tr(z_t^{2^j+1})$, for $1\leq t\leq\frac{\delta}{2}$.
The equation $x+tr(x^{2^i+1})tr(x^{2^j+1})=z_t+a+1$, by Lemma 2.2.13, has the unique solution $x=z_t+a+1+tr(z_t+a+1)^{2^i+1}tr(z_t+a+1)^{2^j+1}=z_t+a+1+tr(z_t+a)^{2^i+1}tr(z_t+a)^{2^j+1}$, because of $tr(1)=0$, for $1\leq t\leq\frac{\delta}{2}$.

Then, there are at most δ solutions.

Case $a = 1$. $D_1 f(x) = F(x + tr(x^{2^i+1})tr(x^{2^j+1}) + 1) - F(x + tr(x^{2^i+1})tr(x^{2^j+1})) = b$, taking into account that $tr(1) = 0$. Such equation can be treated as the equations that appear in the case for $a \neq 1$. So the equation $D_1 f(x) = b$ has at most δ solutions.

In conclusion, for n even, for any $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, the equation $D_a f(x) = b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$.

Lemma 2.2.15. Let $c \in \mathbb{F}_{2^n}$, $i_1, i_2, \cdots, i_j \in \mathbb{N}$, n even, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_j}]$ a polynomial. Then the equation

$$x + \mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1})) = c,$$

has only one solution,

$$x = c + \mathcal{P}(tr(c^{2^{i_1}+1}), \cdots, tr(c^{2^{i_j}+1})).$$

Proof:

Solution Uniqueness: Let $\varphi(x) := x + P(x)$, where $P(x) := \mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$. The term $P(x)$ is Boolean, then the equation for x, $\varphi(x) = c$, has only two possible solutions, c and $c+1$. If x_0 is a solution for that equation, then $x_0 + 1$ is not a solution: $\varphi(x_0 + 1) = x_0 + 1 + P(x_0 + 1) = x_0 + P(x_0) + 1 = \varphi(x_0) + 1 \neq \varphi(x_0) = c$, because of the identity $P(x + 1) = P(x)$ on F_{2^n}, in the next paragraph. Then, the solution for this equation is unique.

Identity $P(x+1) = P(x)$ on $\mathbb{F}_{2^n}$: $P(x+1) = \mathcal{P}(tr(x^{2^{i_1}+1}+1), \cdots, tr(x^{2^{i_j}+1}+1)) = \mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1})) = P(x)$, on $\mathbb{F}_{2^n}$, because of $tr(x+1)^{2^k+1} = tr(x^{2^k+1} + 1)$ on F_{2^n}, $\forall k \in \mathbb{N}$, and $tr(1) = 0$.

Form of the Solution: From our experience with Lemma 2.2.1, we are motivated to consider the following form of the solution, $x = c + P(c)$. If $P(c) = 0$, then $\varphi(c+P(c)) = \varphi(c) = c+P(c) = c+0 = c$. On the other hand, if $P(c) = 1$, then $\varphi(c+P(c)) = \varphi(c+1) = \varphi(c)+1 = c+P(c)+1 = c+1+1 = c$, as in a previous calculation, where $\varphi(x_0 + 1) = \varphi(x_0) + 1$. So in both cases $x = c + P(c)$ is the solution for the given equation, $\varphi(x) = c$.

Then, we obtained the next theorem which can be considered as a major result in the discipline.

Theorem 2.2.16. [for Polynomial] The functions family $f(x) = F(x+\mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1})))$ is *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $j \geq 1$, every $i_k \in \mathbb{N}$, F is *differentially δ-uniform*, n even, over $\mathbb{F}_{2^n}$, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_j}]$ is a polynomial.

Proof:

Given $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, we consider the corresponding differential equation for f:

$$D_a f(x) = F(x + P(x) + P(x+a) - P(x) + a) - F(x + P(x)) = b,$$

where $P(x) := \mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$, the same notation as in Lemma 2.2.15.

$P(x+a) - P(x)$ is a Boolean function, so, for $a = 1$, it is possible that the term $P(x+a) - P(x) + a$ becomes zero, with which the equation for $b = 0$ is reduced to the following equation, $D_1 f(x) = F(x + P(x)) - F(x + P(x)) = 0$, on $\mathbb{F}_{2^n} \cap \{x \in \mathbb{F}_{2^n};\ P(x+1) + 1 = P(x)\}$.

Case $a \neq 1$. **Subcase** $P(x+a) - P(x) = 0$: The equation $D_a f(x) = b$ becomes:

$$F(x + P(x) + a) - F(x + P(x)) = b.$$

Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + P(x)$, which will be denoted by $y = y_t$ and $y = y_t + a$, for $1 \leq t \leq \frac{\delta}{2}$. In the following we solve the equations $x + P(x) = y$, for each value of y.

The equation $x + P(x) = y_t,$ by Lemma 2.2.15, has the unique solution $x = y_t + P(y_t)$, for $1 \leq t \leq \frac{\delta}{2}$. The equation $x + P(x) = y_t + a,$ by Lemma 2.2.15, has the unique solution $x = y_t + a + P(y_t + a)$, for $1 \leq t \leq \frac{\delta}{2}$.

Then there are at most δ solutions.

Subcase $P(x+a) - P(x) = 1$: The equation $D_a f(x) = b$ becomes:

$$F(x + P(x) + a + 1) - F(x + P(x)) = b.$$

Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + P(x)$, which will be denoted by $y = z_t$ and $y = z_t + a + 1$, for $1 \leq t \leq \frac{\delta}{2}$. In the following, we solve the equations $x + P(x) = y$, for each value of y.

The equation $x+P(x)=z_t,$ by Lemma 2.2.15, has the unique solution $x=z_t+P(z_t)$, for $1\leq t\leq \frac{\delta}{2}$. The equation $x+P(x)=z_t+a+1,$ by Lemma 2.2.15, has the unique solution $x=z_t+a+1+P(z_t+a+1)=z_t+a+1+P(z_t+a)$, because of the identity, $P(x+1)=P(x)$, on $\mathbb{F}_{2^n}$, for $1\leq t\leq \frac{\delta}{2}$.

Then there are at most δ solutions.

Case $a=1$. $D_1f(x)=F(x+P(x)+1)-F(x+P(x))=b$, because of the identity, $P(x+1)=P(x)$, on $\mathbb{F}_{2^n}$, this equation can be treated as the equations that appear in the case for $a\neq 1$. So the equation $D_1f(x)=b$ has at most δ solutions.

In conclusion, for n even, for any $a\neq 0,\ b$, both in $\mathbb{F}_{2^n}$, the equation $D_af(x)=b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$.

Corollary 2.2.17. The family of functions $f(x)=x^{2^k+1}+(x^{2^k}+x+1)\mathcal{P}(tr(x^{2^{i_1}+1}),\cdots,tr(x^{2^{i_j}+1}))$, such that $gcd(k,\,n)=1$, n even, and $\mathcal{P}\in\mathbb{F}_2[x_{i_1},x_{i_2},\cdots,x_{i_j}]$ is a polynomial, is at least *differentially* 4-*uniform* over $\mathbb{F}_{2^n}$.

Examples of functions in Corollary 2.2.17 and its nonlinearity calculated by using SAGE:

The entire family of functions $\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^{i_1}+1})tr(x^{2^{i_2}+1});$ for any $k\in\{1,3\}$, i_1 and $i_2\in\{1,2,3\}\}$ are APN over $\mathbb{F}_{2^4}$.

Over $\mathbb{F}_{2^6}$, the family $\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^{\frac{6}{2}}+1})tr(x^{2^j+1});$ for $k\in\{1,5\},\ 1\leq j\leq 5\}\cup\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^1+1})tr(x^{2^5+1});$ for $k\in\{1,5\}\}$ is APN, while the family of functions $\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^i+1})tr(x^{2^j+1});$ for $k\in\{1,5\},\ i\in\{2,4\},\ j\in\{1,2,3,4,5\}-\{\frac{6}{2}\}\}$ is *differentially* 4-*uniform*.

Over $\mathbb{F}_{2^6}$, the family $\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^{\frac{6}{2}}+1})tr(x^{2^j+1})tr(x^{2^l+1});$ for $k\in\{1,5\},\ 1\leq j,\,l\leq 5\}$ is APN, while the family of functions $\{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^i+1})tr(x^{2^j+1})tr(x^{2^l+1});$ for $k\in\{1,5\}$, and three numbers $i<j<l\in\{1,2,3,4,5\}-\{\frac{6}{2}\}\}$ are *differentially* 4-*uniform*.

Corollary 2.2.18. The functions $f(x)=x^{2^{2k}+2^k+1}+(x^{2^{2k}+2^k}+x^{2^{2k}+1}+x^{2^{2k}}+x^{2^k+1}+x^{2^k}+x+1)\mathcal{P}(tr(x^{2^{i_1}+1}),\cdots,tr(x^{2^{i_j}+1}))$ are at least *differentially* 8-*uniform* over $\mathbb{F}_{2^{4k}}$, where $k\in\mathbb{N}$, and $\mathcal{P}\in\mathbb{F}_2[x_{i_1},x_{i_2},\cdots,x_{i_j}]$ is a polynomial.

We focus now to obtain analogous results for fields of odd degree n, $\mathbb{F}_{2^n}$. Therefore, we can involve the *Welch* family.

Theorem 2.2.19. The family $f(x) = F(x + \mathcal{P}(tr(x^{2^{i_1}+1} + x), \cdots, tr(x^{2^{i_j}+1} + x)))$ is *differentially* γ-*uniform*, where $\delta \leq \gamma \leq 2\delta$, $j \geq 1$, every $i_k \in \mathbb{N}$, F is *differentially* δ-*uniform*, n odd, over $\mathbb{F}_{2^n}$, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_j}]$ is a polynomial.

Theorem 2.2.20. For the case n odd, we can write the corresponding versions of Lemma 2.2.15 and Corollary 2.2.17. by adding the term $tr(x)$ to each term for the form $tr(x^{2^i+1})$, resulting in $tr(x^{2^i+1} + x)$.

Theorem 2.2.21. [for Welch] The family functions $f(x) = x^{2^{\frac{n-1}{2}}+3} + (x^{2^{\frac{n-1}{2}}+2} + x^{2^{\frac{n-1}{2}}+1} + x^{2^{\frac{n-1}{2}}} + x^3 + x^2 + x + 1)\mathcal{P}(tr(x^{2^{i_1}+1} + x), \cdots, tr(x^{2^{i_j}+1} + x))$ is at least *differentially* 4-*uniform*, where $j \geq 1$, every $i_k \in \mathbb{N}$, n odd, over $\mathbb{F}_{2^n}$, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_j}]$ is a polynomial.

Proof:

Applying Theorem 2.2.19 for the Welch function, $F(x) = x^{2^{\frac{n-1}{2}}+3}$, over $\mathbb{F}_{2^n}$.

Based on Theorem 2.2.3 the next definition has played a fundamental role in the form of the *differentially* δ-*uniform* families to be created. Also, the form of families from Theorem 2.2.24 conforms to the following definition.

Definition 2.2.1. Two switching neighbours F and $H : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are in the **narrow sense along of the x- axis** with respect to the subgroup U, if $U \leq \mathbb{F}_2^n$ x $\{0\}$ and $dim(U) = 1$.

Lemma 2.2.22. Let $c \in \mathbb{F}_{2^n}$, $\{i, j, k, l\} \subset \mathbb{N} \cup \{0\}$. Then the equation $x + tr(x^{2^i+2^j+1}) = c$ has the solution set

$$\{x_0,\ x_0 + tr(x_0^{2^i+2^j} + x_0^{2^i+1} + x_0^{2^j+1} + x_0 + 1);\ \text{where } x_0 + tr(x_0^{2^i+2^j+1}) = c\}.$$

Lemma 2.2.23. Let $c \in \mathbb{F}_{2^n}$, $\{i,j,k,l\} \subset \mathbb{N} \cup \{0\}$. Then the equation

$$x + tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)tr(x^{2^k+2^l} + x)tr(x^{2^k+1} + x)tr(x^{2^l+1} + x) = c,$$

has the only one solution x, namely,

$$c + tr(c^{2^i+2^j+1}+c^{2^k+2^l+1})tr(c^{2^i+2^j}+c)tr(c^{2^i+1}+c)tr(c^{2^j+1}+c)tr(c^{2^k+2^l}+c)tr(c^{2^k+1}+c)tr(c^{2^l+1}+c).$$

The first member of the aforementioned equation above defines a nonlinear invertible function $\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, which has inverse φ^{-1} with the same formula as φ, i.e. $\varphi o \varphi = \text{Identity}_{\mathbb{F}_{2^n}}$.

Proof:

Solution Uniqueness: We define the Boolean term $B(x) := tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)tr(x^{2^k+2^l} + x)tr(x^{2^k+1} + x)tr(x^{2^l+1} + x)$. Then, the equation for x, $x + B(x) = c$, has only two possible solutions, c and $c+1$. If x_0 is a solution for that equation, then x_0+1 is not a solution: $\varphi(x_0+1) = x_0+1+B(x_0+1) = x_0+1+B(x_0)+tr(x_0^{2^i+2^j}+x_0^{2^i+1}+x_0^{2^j+1}+x_0^{2^k+2^l}+x_0^{2^k+1}+x_0^{2^l+1})tr(x_0^{2^i+2^j}+x_0)tr(x_0^{2^i+1}+x_0)tr(x_0^{2^j+1}+x_0)tr(x_0^{2^k+2^l}+x_0)tr(x_0^{2^k+1}+x_0)tr(x_0^{2^l+1}+x_0)$, because of the last term is cero, we have that, $\varphi(x_0+1) = x_0 + B(x_0) + 1 = \varphi(x_0) + 1 \neq \varphi(x_0) = c$. Then, the solution for this equation is unique.

In the previous paragraph we have used the identity: $tr(x_0^{2^i+2^j} + x_0^{2^i+1} + x_0^{2^j+1} + x_0^{2^k+2^l} + x_0^{2^k+1} + x_0^{2^l+1})tr(x_0^{2^i+2^j} + x_0)tr(x_0^{2^i+1} + x_0)tr(x_0^{2^j+1} + x_0)tr(x_0^{2^k+2^l} + x_0)tr(x_0^{2^k+1} + x_0)tr(x_0^{2^l+1} + x_0) = (tr(x_0^{2^i+2^j} + x_0) + tr(x_0^{2^i+1} + x_0) + tr(x_0^{2^j+1} + x_0) + tr(x_0^{2^k+2^l} + x_0) + tr(x_0^{2^k+1} + x_0) + tr(x_0^{2^l+1} + x_0))tr(x_0^{2^i+2^j} + x_0)tr(x_0^{2^i+1} + x_0)tr(x_0^{2^j+1} + x_0)tr(x_0^{2^k+2^l} + x_0)tr(x_0^{2^k+1} + x_0)tr(x_0^{2^l+1} + x_0)$, which is zero if some of the Boolean factors is zero, and also gives zero if all of them are equals to one.

Form of the Solution: From our experience with Lemma 2.2.1, we are motivated to consider the following form of the solution, $x = c + B(c)$. If $B(c) = 0$, then $\varphi(c+B(c)) = \varphi(c) = c+B(c) = c+0 = c$. On the other hand, if $B(c) = 1$, then $\varphi(c+B(c)) = \varphi(c+1) = \varphi(c)+1 = c+B(c)+1 = c+1+1 = c$, as in the calculation of $\varphi(x_0+1)$. So in both cases $x = c + B(c)$ is the solution for the given equation, $\varphi(x) = c$.

The following theorem shows us a particular technique to obtain *differentially uniform* functions that contains the *trace* of *quadratic* terms of the form $tr(x^{2^i+2^j})$ and $tr(x^{2^i+2^j+1})$.

Theorem 2.2.24. The following two families of functions are *differentially γ-uniform*

$$f_1(x) = F(x + tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j})tr(x^{2^i+1})tr(x^{2^j+1})tr(x^{2^k+2^l})tr(x^{2^k+1})tr(x^{2^l+1})),$$

if n is even.

$$f_2(x) = F(x + tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)tr(x^{2^k+2^l} + x)tr(x^{2^k+1} + x)tr(x^{2^l+1} + x)),$$

where $\delta \leq \gamma \leq 2\delta$, $\{i, j, k, l\} \subset \mathbb{N} \cup \{0\}$, and F is *differentially δ-uniform*, over $\mathbb{F}_{2^n}$.

Proof: for f_2

Given $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, we establish the corresponding differential equation for f_2 to be studied:

$$D_a f_2(x) = F(x + B(x) + \Delta(a, x) + a) - F(x + B(x)) = b,$$

where $\Delta(a, x) := B(x + a) - B(x)$, and $B(x) := tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)tr(x^{2^k+2^l} + x)tr(x^{2^k+1} + x)tr(x^{2^l+1} + x)$, the same notation as in Lemma 2.2.23.

$\Delta(a, x)$ is a Boolean function, then for $a = 1$, it could happen that the Boolean term $\Delta(1, x) + 1$ is zero, with which the corresponding equation $D_1 f_2(x) = F(x + B(x)) - F(x + B(x)) = 0$ would be satisfied for all the elements of $\mathbb{F}_{2^n} \cap \{x \in \mathbb{F}_{2^n};\ \Delta(1, x) + 1 = 0\}$.

Case $a \neq 1$. **Subcase** $\Delta(a, x) = 0$: The equation $D_a f_2(x) = b$ becomes:

$$F(x + B(x) + a) - F(x + B(x)) = b.$$

Because F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + B(x)$, which will be denoted by $y = y_i$ and $y = y_i + a$, for $1 \leq i \leq \frac{\delta}{2}$. In the following, we solve the equations $x + B(x) = y$, for each value of y.

The equation $x + B(x) = y_i$, by Lemma 2.2.23, has the unique solution $x = y_i + B(y_i)$, for $1 \leq i \leq \frac{\delta}{2}$.
The equation $x + B(x) = y_i + a$, by Lemma 2.2.23, has the unique solution $x = y_i + a + B(y_i + a)$, for $1 \leq i \leq \frac{\delta}{2}$.
Then there are at most δ solutions.

Subcase $\Delta(a,x)=1$: The equation $D_af_2(x)=b$ becomes:

$$F(x+B(x)+a+1)-F(x+B(x))=b.$$

Because F is *differentially* δ-*uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y=x+B(x)$, which will be denoted by $y=z_i$ and $y=z_i+a+1$, for $1\leq i\leq \frac{\delta}{2}$. In the following, we solve the equations $x+B(x)=y$, for each value of y.

The equation $x+B(x)=z_i,$ by Lemma 2.2.23, has the unique solution $x=z_i+B(z_i)$, for $1\leq i\leq \frac{\delta}{2}$. The equation $x+B(x)=z_i+a+1,$ by Lemma 2.2.23, has the unique solution $x=z_i+a+1+B(z_i+a+1)=z_i+a+1+B(z_i+a)$, because of the identity $\Delta(1,x)=0$ on $\mathbb{F}_{2^n}$, for $1\leq i\leq \frac{\delta}{2}$. Then there are at most δ solutions.

Case $a=1$. $D_1f_2(x)=F(x+B(x)+1)-F(x+B(x))=b$, where $\Delta(1,x)=0$ on $\mathbb{F}_{2^n}$, is the identity used in the proof of Lemma 2.2.23. This equation can be treated as the equations that appear in the case for $a\neq 1$. So the equation $D_1f_2(x)=b$ has at most δ solutions.

In conclusion, for any $a\neq 0,\ b$, both in $\mathbb{F}_{2^n}$, the equation $D_af_2(x)=b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$.

Corollary 2.2.25. The family of functions

$$\varphi(x)=x^{2^m+1}+(x^{2^m}+x+1)tr(x^{2^i+2^j+1}+x^{2^k+2^l+1})tr(x^{2^i+2^j}+x)tr(x^{2^i+1}+x)tr(x^{2^j+1}+x)tr(x^{2^k+2^l}+x)tr(x^{2^k+1}+x)tr(x^{2^l+1}+x)),$$

such that $gcd(m,\,n)=1$, and $\{i,j,k,l\}\subset\mathbb{N}\cup\{0\}$, is at least *differentially* 4-*uniform* over $\mathbb{F}_{2^n}$.

Corollary 2.2.26. The functions $f(x)=x^{2^{2m}+2^m+1}+(x^{2^{2m}+2^m}+x^{2^{2m}+1}+x^{2^{2m}}+x^{2^m+1}+x^{2^m}+x+1)tr(x^{2^i+2^j+1}+x^{2^k+2^l+1})tr(x^{2^i+2^j}+x)tr(x^{2^i+1}+x)tr(x^{2^j+1}+x)tr(x^{2^k+2^l}+x)tr(x^{2^k+1}+x)tr(x^{2^l+1}+x))$, are at least *differentially* 8-*uniform* over $\mathbb{F}_{2^{4m}}$, where $\{i,j,k,l,m-1\}\subset\mathbb{N}\cup\{0\}$.

Proof:

Applying Theorem 2.2.24 for the *differentially* 4-*uniform* function $F(x)=x^{2^{2m}+2^m+1}$ (permutation iff m is odd) over $\mathbb{F}_{2^{4m}}$ [2].

Corollary 2.2.27. The family of functions $f(x) = x^{2^{\frac{n-1}{2}}+3} + (x^{2^{\frac{n-1}{2}}+2} + x^{2^{\frac{n-1}{2}}+1} + x^{2^{\frac{n-1}{2}}} + x^3 + x^2 + x + 1)tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)tr(x^{2^k+2^l} + x)tr(x^{2^k+1} + x)tr(x^{2^l+1} + x))$ are at least *differentially* 4-*uniform* over $\mathbb{F}_{2^n}$, where $j \geq 1$, every $i_k \in \mathbb{N}$, and n is odd.

Proof:

Applying Theorem 2.2.24 for the Welch function, $F(x) = x^{2^{\frac{n-1}{2}}+3}$, over $\mathbb{F}_{2^n}$.

2.3 Generalization

There is a wide variety of counterexamples such that f and g are Boolean functions, $F(x)$ and $F(x+f(x))$ are *differentially* δ-*uniform*, but $F(x+f(x)g(x))$ is *differentially* δ+2-*uniform*, over $\mathbb{F}_{2^n}$. The importance of the following conjecture lies in the detection of *differentially* δ-*uniform* functions close to the *differentially* δ-*uniform* function, $F(x)$, which we call the center of the sphere. It seems like a Sandwich Theorem, about the identification of *differentially* δ-*uniform* functions between $F(x)$ and $F(x + f(x))$. We formulate the following conjecture.

Conjecture 3 [Sphere Differentially Uniform Theorem] Let f and g Boolean functions such that $f(x+a) = f(x)+f(a)$, for all $a \neq 0$, $f(1) = 0$, $g(x+1) = g(x)$, $g(1) = 0$; $F(x)$, $F(x+f(x))$ and $F(x+g(x))$ are *differentially* δ-*uniform*, over $\mathbb{F}_{2^n}$. Then, $F(x+f(x)g(x))$ is *differentially* δ-*uniform*, over $\mathbb{F}_{2^n}$.

In particular, the following ones are candidates to be f and g:

For n even: $f(x) = tr(x^{2^{\frac{n}{2}}+1})$, $tr(x^{2^{\frac{n}{2}}+1} + x)$, $tr(x)$.

For n even: $g(x) = tr(x^{2^i+1})$.

For any n: $g(x) = tr(x^{2^i+1} + x)$, $tr(x^{2^i+2^j+1} + x^{2^k+2^l+1})tr(x^{2^i+2^j} + x)tr(x^{2^i+1} + x)tr(x^{2^j+1} + x)$ $tr(x^{2^k+2^l} + x)$ $tr(x^{2^k+1} + x)tr(x^{2^l+1} + x)$.

Exercise We let the following theorems as exercises (from the previous results you can demonstrate that theorems).

Theorem 2.3.1. Let $u \in \mathbb{F}_2^n$, $u \neq 0$, f a Boolean function, and F a *differentially δ-uniform* function over $\mathbb{F}_2^n$. Then, the function $F(x + u.f(x))$ is at least *differentially 4δ-uniform*.

Corollary 2.3.2. Let $\{u_i \in \mathbb{F}_2^n;\ u_i \neq 0\}$ an additive subgroup of $\mathbb{F}_2^n$, f_i are Boolean functions, and F a *differentially δ-uniform* function over $\mathbb{F}_2^n$. Then, the function $F(x + u_1.f_1(x) + \cdots + u_k.f_k(x))$ is at least *differentially $4^k\delta$-uniform*.

Corollary 2.3.3. Let $\{u_i \in \mathbb{F}_2^n;\ u_i \neq 0\}$ an additive subgroup of $\mathbb{F}_2^n$, f_i are Boolean functions, and F a *differentially δ-uniform* function over $\mathbb{F}_2^n$. Then, the function $F(x) + u_1.f_1(x) + \cdots + u_k.f_k(x)$ is at least *differentially $2^k\delta$-uniform*.

CHAPTER 3

A NEW TECHNIQUE TO DETERMINE THE ALGEBRAIC DEGREE VIA REED-MULLER CODES

All the results about the algebraic degree in this chapter are new. We give news techniques to compute the algebraic degree of families of functions in multivariate polynomial representation by analysis of the corresponding Reed-Muller codes.

3.1 Bent and Almost Bent Functions in the 3rd order Reed-Muller Codes

The frameworks of the *binary Reed-Muller* codes $\mathcal{R}(r,n)$ and the *Euclidean geometry* $\mathbb{EG}(n,2)$ give us another way of thinking about families of functions over $\mathbb{F}_{2^n}$, in particular those that come from Theorem 2.2.3.

$$\text{Let } f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}, \text{ where } f(x)=x^{2^j+1}+(x^{2^j}+x+1)tr(x^{2^i+1}).$$

We can represent $f(x)$ as an n-variable function:

$f:\mathbb{EG}(n,2)\to\mathbb{EG}(n,2)$, where the $n-$coordinate functions of f are in $\mathcal{R}(r,n)$ for some r to be determined.

$\mathbb{EG}(n,2)$ consists of 2^n points that can be labeled by the $n-$tuples of elements in $\mathbb{F}_{2^n}$.

The function f can be seen as tuples of codewords of the 3^{th} *order binary Reed-Muller* code $\mathcal{R}(3,n)^n$, as follows: Let $x=\sum_{k=0}^{n-1}x_k\alpha_k=(x_0,x_1,\cdots,x_{n-1})$ a vectorial Boolean variable in $\mathbb{F}_{2^n}$, where $\{\alpha_0,\cdots,\alpha_{n-1}\}$ is a basis of the $\mathbb{F}_2$- vector space $\mathbb{F}_{2^n}$. Then,

$$f(x)=f(\textstyle\sum_{k=0}^{n-1}x_k\alpha_k)=$$

$$(\textstyle\sum_{k=0}^{n-1}x_k\alpha_k^{2^j})(\sum_{k=0}^{n-1}x_k\alpha_k)+(1+\sum_{k=0}^{n-1}x_k\alpha_k^{2^j}+x_k\alpha_k)tr(\sum_{k=0}^{n-1}x_k\alpha_k^{2^i}\sum_{k=0}^{n-1}x_k\alpha_k)$$

$$\textstyle\sum_{k,l=0}^{n-1}x_kx_l\alpha_k^{2^j}\alpha_l+\sum_{t=0}^{n-1}\sum_{k,l=0}^{n-1}x_kx_l\alpha_k^{2^{i+t}}\alpha_l^{2^t}+\sum_{r,t,k,l=0}^{n-1}x_rx_kx_l(\alpha_r^{2^j}+\alpha_r)\alpha_k^{2^{i+t}}\alpha_l^{2^t}.$$

Making $\alpha_k^{2^j}\alpha_l=\sum_{p=0}^{n-1}a_{k,l,p}\alpha_p$, $\alpha_k^{2^{i+t}}\alpha_l^{2^t}=\sum_{p=0}^{n-1}a_{t,k,l,p}\alpha_p$, $(\alpha_r^{2^j}+\alpha_r)\alpha_k^{2^{i+t}}\alpha_l^{2^t}=\sum_{p=0}^{n-1}a_{r,t,k,l,p}\alpha_p$,

where i, j are fixed values. Then, the explicit representation of $f(x)$ in terms of the considered basis is:

$$f(x) = \sum_{p=0}^{n-1} \left(\sum_{k,l=0}^{n-1} x_k x_l a_{k,l,p} + \sum_{t,k,l=0}^{n-1} x_k x_l a_{t,k,l,p} + \sum_{r,t,k,l=0}^{n-1} x_r x_k x_l a_{r,t,k,l,p}\right) \alpha_p,$$

where it can be seen that the coefficients are up to degree 3.

The vectorial representation of $f(\sum_{k=0}^{n-1} x_k \alpha_k)$ in the $\mathbb{F}_2^n$ has the following form:

$$f(x) =$$
$$\left(\sum_{k,l=0}^{n-1} x_k x_l a_{k,l,0} + \sum_{t,k,l=0}^{n-1} x_k x_l a_{t,k,l,0} + \sum_{r,t,k,l=0}^{n-1} x_r x_k x_l a_{r,t,k,l,0}, \cdots, \sum_{k,l=0}^{n-1} x_k x_l a_{k,l,n-1} + \right.$$
$$\left. \sum_{t,k,l=0}^{n-1} x_k x_l a_{t,k,l,n-1} + \sum_{r,t,k,l=0}^{n-1} x_r x_k x_l a_{r,t,k,l,n-1}\right).$$

From now on we will consider $n \geq 3$. From the expansion of $f(\sum_{k=0}^{n-1} x_k \alpha_k)$, we extract a term of maximum degree (whose monomial term is $x_r x_k x_l$). For example, the sum of all 3! summands that contain $x_0 x_1 x_2$:

$$x_0 x_1 x_2 \sum_{t=0}^{n-1} (\alpha_0^{2^j} + \alpha_0) \alpha_1^{2^i+t} \alpha_2^{2^t} + x_0 x_2 x_1 \sum_{t=0}^{n-1} (\alpha_0^{2^j} + \alpha_0) \alpha_2^{2^i+t} \alpha_1^{2^t} +$$

$$x_1 x_0 x_2 \sum_{t=0}^{n-1} (\alpha_1^{2^j} + \alpha_1) \alpha_0^{2^i+t} \alpha_2^{2^t} + x_1 x_2 x_0 \sum_{t=0}^{n-1} (\alpha_1^{2^j} + \alpha_1) \alpha_2^{2^i+t} \alpha_0^{2^t} +$$

$$x_2 x_0 x_1 \sum_{t=0}^{n-1} (\alpha_2^{2^j} + \alpha_2) \alpha_0^{2^i+t} \alpha_1^{2^t} + x_2 x_1 x_0 \sum_{t=0}^{n-1} (\alpha_2^{2^j} + \alpha_2) \alpha_1^{2^i+t} \alpha_0^{2^t}$$

$$= x_0 x_1 x_2 ((\alpha_0^{2^j} + \alpha_0) tr(\alpha_1^{2^i} \alpha_2 + \alpha_2^{2^i} \alpha_1) +$$

$$(\alpha_1^{2^j} + \alpha_1) tr(\alpha_0^{2^i} \alpha_2 + \alpha_2^{2^i} \alpha_0) +$$

$$(\alpha_2^{2^j} + \alpha_2) tr(\alpha_0^{2^i} \alpha_1 + \alpha_1^{2^i} \alpha_0)), \quad (2)$$

where the existence of the monomial term $x_0x_1x_2$ depends on its coefficient be not zero, which is:

$$C_{012} = (\alpha_0^{2^j} + \alpha_0)tr(\alpha_1^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_1) + (\alpha_1^{2^j} + \alpha_1)tr(\alpha_0^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_0) + (\alpha_2^{2^j} + \alpha_2)tr(\alpha_0^{2^i}\alpha_1 + \alpha_1^{2^i}\alpha_0).$$

Note that the products $(\alpha_r^{2^j} + \alpha_r)tr(\alpha_k^{2^i}\alpha_l + \alpha_l^{2^i}\alpha_k)$ are all nonzero since their factors are nonzero as it will be proved next.

Lemma 3.1.1. For $n \geq 4$, there exist basis vectors $\mathcal{V} = \{\alpha_0, \alpha_1, \alpha_2\}$ such that $1 \notin Span(\mathcal{V})$, and

$$(\alpha_0^{2^j} + \alpha_0)tr(\alpha_1^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_1) + (\alpha_1^{2^j} + \alpha_1)tr(\alpha_0^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_0) + (\alpha_2^{2^j} + \alpha_2)tr(\alpha_0^{2^i}\alpha_1 + \alpha_1^{2^i}\alpha_0) \neq 0.$$

Proof:

By studying the $Kernel(\varphi)$, where $\varphi(x) = x^{2^j} + x$, it can be found that $|Kernel(\varphi)| \leq 2$. Then $Kernel(\varphi) = \{0, 1\}$. Thus, $1 \notin Span(\mathcal{V})$ implies $\varphi(Span(\mathcal{V}) - \{0\}) \nsubseteq Kernel(\varphi)$.

Just consider the term $x^{2^j+2^{i+r}+2^r}$, when $j \notin \{r, i+r\}$. All terms in the expansion of f cannot exceed degree 3. Applying in Equation (2), the fact that $f(x) = x^{2^j+1} + (x^{2^j} + x + 1)tr(x^{2^i+1})$ has algebraic degree 3, it is sufficient to have that the coefficient $C_{012} = (\alpha_0^{2^j} + \alpha_0)tr(\alpha_1^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_1) + (\alpha_1^{2^j} + \alpha_1)tr(\alpha_0^{2^i}\alpha_2 + \alpha_2^{2^i}\alpha_0) + (\alpha_2^{2^j} + \alpha_2)tr(\alpha_0^{2^i}\alpha_1 + \alpha_1^{2^i}\alpha_0)$ is not zero.

Theorem 3.1.2. For $n \geq 4$, there exist basis vectors $\mathcal{V} = \{\alpha_0, \alpha_1, \alpha_2\}$ such that $1 \notin Span(\mathcal{V})$, and

$$tr(\alpha_0^{2^i}\alpha_1 + \alpha_1^{2^i}\alpha_0) = 1.$$

Proof:

The demonstration comes immediately from Lemma 3.1.1.

3.2 Odd order binary Reed-Muller codes

Generalizing the result corresponoding to the 3rd order Reed-Muller codes, using the functions in Corollary 2.2.17, $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)\mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$, we can show that to codewords of *binary Reed-Muller* code of *order* $(2N+1)$, $\mathcal{R}(2N+1, n)^n$, where N is the *algebraic degree* of $\mathcal{P}(x_{i_1}, x_{i_2}, \cdots, x_{i_j})$, i.e. the degree of the term with the maximum number of different factors appearing in $\mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$. Without loss of generality we will consider the subfamily of the form $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1})$. To compute the order of the code, we will concentrate on the terms of maximum degree of $f(\sum_{j=0}^{n-1} x_j\alpha_j)$:

Terms of maximum degree of $f(\sum_{j=0}^{n-1} x_j\alpha_j)$ are,

$$(\sum_{j=0}^{n-1} x_j\alpha_j^{2^k} + x_j\alpha_j)tr(\sum_{j=0}^{n-1} x_j\alpha_j^{2^{i_1}} \sum_{j=0}^{n-1} x_j\alpha_j) \cdots tr(\sum_{j=0}^{n-1} x_j\alpha_j^{2^{i_N}} \sum_{j=0}^{n-1} x_j\alpha_j)$$

$$(\sum_{j=0}^{n-1} x_j(\alpha_j^{2^k} + \alpha_j))(\sum_{t=0}^{n-1} \sum_{j,l=0}^{n-1} x_j x_l \alpha_j^{2^{i_1+t}} \alpha_l^{2^t}) \cdots (\sum_{t=0}^{n-1} \sum_{j,l=0}^{n-1} x_j x_l \alpha_j^{2^{i_N+t}} \alpha_l^{2^t})$$

$$(\sum_{j=0}^{n-1} x_j(\alpha_j^{2^k} + \alpha_j))(\sum_{t_1,j_1,l_1=0}^{n-1} x_{j_1} x_{l_1} \alpha_{j_1}^{2^{i_1+t_1}} \alpha_{l_1}^{2^{t_1}}) \cdots (\sum_{t_N,j_N,l_N=0}^{n-1} x_{j_N} x_{l_N} \alpha_{j_N}^{2^{i_N+t_N}} \alpha_{l_N}^{2^{t_N}})$$

$$(\sum_{j=0}^{n-1} x_j(\alpha_j^{2^k} + \alpha_j))(\sum_{t_1,j_1,l_1,\cdots,t_N,j_N,l_N=0}^{n-1} x_{j_1} x_{l_1} \cdots x_{j_N} x_{l_N} \alpha_{j_1}^{2^{i_1+t_1}} \alpha_{l_1}^{2^{t_1}} \cdots \alpha_{j_N}^{2^{i_N+t_N}} \alpha_{l_N}^{2^{t_N}})$$

$$\sum_{t_1,j_1,l_1,\cdots,t_N,j_N,l_N,j_{N+1}=0}^{n-1} x_{j_1} x_{l_1} \cdots x_{j_N} x_{l_N} x_{j_{N+1}} \alpha_{j_1}^{2^{i_1+t_1}} \alpha_{l_1}^{2^{t_1}} \cdots \alpha_{j_N}^{2^{i_N+t_N}} \alpha_{l_N}^{2^{t_N}} (\alpha_{j_{N+1}}^{2^k} + \alpha_{j_{N+1}})$$

$$\sum_{j_1,l_1,\cdots,j_N,l_N,j_{N+1}=0}^{n-1} x_{j_1} x_{l_1} \cdots x_{j_N} x_{l_N} x_{j_{N+1}} tr(\alpha_{j_1}^{2^{i_1}} \alpha_{l_1}) \cdots tr(\alpha_{j_N}^{2^{i_N}} \alpha_{l_N})(\alpha_{j_{N+1}}^{2^k} + \alpha_{j_{N+1}}),$$

where k, $i_1, \cdots, i_N$ are fixed coefficient indices.

We consider the following expansion in the basis $\{\alpha_0, \cdots, \alpha_{n-1}\}$:

$$tr(\alpha_{j_1}^{2^{i_1}} \alpha_{l_1}) \cdots tr(\alpha_{j_N}^{2^{i_N}} \alpha_{l_N})(\alpha_{j_{N+1}}^{2^k} + \alpha_{j_{N+1}}) = \sum_{p=0}^{n-1} a_{j_1,l_1,\cdots,j_N,l_N,j_{N+1},p}\, \alpha_p.$$

Replacing that last expansion:

Terms of maximum degree of $f(\sum_{j=0}^{n-1} x_j\alpha_j) =$

$$\sum_{p,j_1,l_1,\cdots,j_N,l_N,j_{N+1}=0}^{n-1} x_{j_1} x_{l_1} \cdots x_{j_N} x_{l_N} x_{j_{N+1}} a_{j_1,l_1,\cdots,j_N,l_N,j_{N+1},p}\, \alpha_p.$$

Which contains the non zero terms $x_{j_1} x_{l_1} \cdots x_{j_N} x_{l_N} x_{j_{N+1}}$ of degree $2N+1$.

Because the bases $\{\alpha_0, \cdots, \alpha_{n-1}\}$ are an *linearly independent* set, it only remains to demonstrate that at least some coefficient $a_{j_1,l_1,\cdots,j_N,l_N,j_{N+1},p}$ is not zero. If all the coefficients are zero $\{a_{j_1,l_1,\cdots,j_N,l_N,j_{N+1},p}\}_{p=0}^{n-1} = \{0\}$, then the function f is of a smaller degree, for example, $2N$ and the code of the even order $2N$.

Consider N such that $n \geq 2N+1$. From the expansion of $f(\sum_{k=0}^{n-1} x_k\alpha_k)$ we extract a term of maximum degree, as for example:

The sum of all $(2N+1)!$ summands whose variable part is $x_{j_{1_0}}x_{l_{1_0}} \cdots x_{j_{N_0}}x_{l_{N_0}}x_{j_{(N+1)_0}}$

$= x_{j_{1_0}}x_{l_{1_0}} \cdots x_{j_{N_0}}x_{l_{N_0}}x_{j_{(N+1)_0}}$ by its coefficient $C_{j_{1_0}l_{1_0}\cdots j_{N_0}l_{N_0}j_{(N+1)_0}}$

$$\sum_{(s_1,\cdots,s_{2N+1}) \text{ is a permutation of } (j_{1_0},l_{1_0},\cdots,j_{N_0},l_{N_0},j_{(N+1)_0})} tr(\alpha_{s_1}^{2^{i_1}}\alpha_{s_2}) \cdots tr(\alpha_{s_{2N-1}}^{2^{i_N}}\alpha_{s_{2N}})(\alpha_{s_{2N+1}}^{2^k} + \alpha_{s_{2N+1}}). \quad (3)$$

This implies that there exists a function of high nonlinearity in $\mathcal{R}(2N+1,n)$ which is represented by subfamily of functions $f(x) = x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1})$. Using our result we give explicit examples of functions of high nonlinearity via computational means (see Appendix).

Whether the degree of the field is even or odd depends whether the coefficient $\{a_{j_1,l_1,\cdots,j_N,l_N,j_{N+1},p}\}_{p=0}^{n-1}$ is zero or non-zero.

Algebraic Degree [11], [7] Let $\mathbb{F}_{2^n}$ be the n-dimensional vector space over the field $\mathbb{F}_2$. Any function F from $\mathbb{F}_{2^n}$ to itself can be uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_{2^n}$, whose degree with respect to each coordinate is at most one:

$$F(x_1, \cdots, x_n) = \sum_{u \in \mathbb{F}_2^n} c(u)(\prod_{i=1}^{n} x_i^{u_i}), \;\; c(u) \in \mathbb{F}_2^n.$$

This representation is called the *algebraic normal form* (ANF) of F and its degree d^0F is called the *algebraic degree* of F. The algebraic degree of F, therefore equals the maximal algebraic degree of the coordinate functions of F. It also equals the maximal algebraic degree of the component functions of F. It is a right and left affine invariant (that is, its value does not change when we compose F, on the right or the left, by an affine automorphism).

The field $\mathbb{F}_{2^n}$ can be identified with $\mathbb{F}_2^n$ as a vector space over $\mathbb{F}_2$. Then, viewed as a function from this field to itself, F has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$. Let:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \;\; c_i \in \mathbb{F}_{2^n}.$$

For every binary vector $x \in \mathbb{F}_2^n$, we can also denote by x the element $x = \sum_{k=0}^{n-1} x_k \alpha_k$ of $\mathbb{F}_{2^n}$, where $\{\alpha_0, \cdots, \alpha_{n-1}\}$ is a basis of the $\mathbb{F}_2$-vector space $\mathbb{F}_{2^n}$. Let us write the binary expansion of every integer $i \in [0, 2^n - 1]$, $i = \sum_{s=0}^{n-1} i_s 2^s$, $i_s \in \{0, 1\}$. Then we have:

$$F(x) = \sum_{i=0}^{2^n-1} c_i (\sum_{k=0}^{n-1} x_k \alpha_k)^{\sum_{s=0}^{n-1} i_s 2^s}$$

$$F(x) = \sum_{i=0}^{2^n-1} c_i \prod_{s=0}^{n-1} (\sum_{k=0}^{n-1} x_k \alpha_k^{2^s})^{i_s},$$

since the mapping $x \to x^2$ is $\mathbb{F}_2-$ linear over $\mathbb{F}_{2^n}$ and $x_k \in \mathbb{F}_2$. Expanding these last products, simplifying and decomposing again over the basis $(\alpha_1, \cdots, \alpha_n)$ gives the ANF of F.

In the case that F is given as a univariate polynomial over $\mathbb{F}_{2^n}$, $d^0(F) = \max\{\omega_2(i); i \text{ is the exponent of a term in } F\}$, where $\omega_2(i) = \sum_{s=0}^{n-1} i_s$.

By definition, the algebraic degree of the family in Theorem 2.2.3 must be less than or equal to $2N + 1 \leq n$, where N is the number of trace factors.

Theorem 3.2.1. The functions f in the family in Corollary 2.2.17 are not affine equivalent to any power functions nor other members of the family.

Proof:

$d^0(tr(f)) = d^0(x^{2^k+1}) = 2 \notin \{0, 1, d^0(f)\}$ (see [7]). Also, among them are *Extended Affine-inequivalent*, for each additional factor the new one function is *Extended Affine-inequivalent* with the previous ones.

In the functions in the Corollary 2.2.17, $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)\mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$, the *algebraic degree* of $\mathcal{P}(x_{i_1}, x_{i_2}, \cdots, x_{i_j})$ is the degree of the term with the maximum number of different factors appearing in $\mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$. Without loss of generality we will

consider the subfamily of the form $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^{i_1}+1})\cdots tr(x^{2^{i_N}+1})$. To compute the order of the code, we will concentrate in the terms of maximum degree into $f(\sum_{j=0}^{n-1} x_j\alpha_j)$:

We will calculate its algebraic degree from its representation as a function in a single variable, as explained in a previous paragraph in this section [7].

To find the algebraic degree for the family in Theorem 2.2.3, $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^i+1})$, we see that this family contains terms of the following forms:

A) $x^{2^k+1} = x^{1.2^k+1.2^0}$, then $\omega_2(1.2^k + 1.2^0) = 2$.

B) $x^{2^k+2^p(2^i+1)} = x^{1.2^k+1.2^p+1.2^{i+p}}$, then $\omega_2(1.2^k + 1.2^p + 1.2^{i+p}) = 3$, for p such that $k \notin \{p, i+p\}$.

C) $x^{2^0+2^p(2^i+1)} = x^{1.2^0+1.2^p+1.2^{i+p}}$, then $\omega_2(1.2^0 + 1.2^p + 1.2^{i+p}) = 3$, for $p > 0$.

D) $x^{2^p(2^i+1)} = x^{1.2^p+1.2^{i+p}}$, then $\omega_2(1.2^p + 1.2^{i+p}) = 2$.

Then $d^0(x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^i+1})) = \max\{\omega_2(i); i$ is the exponent of a term in the representation of f as a univariate polynomial$\} = 3$.

To find the algebraic degree for the subfamily in Corollary 2.2.17, $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1})\cdots tr(x^{2^{i_N}+1})$, where $1 \leq i_1 < i_2 < \cdots < i_N \leq n-1$ are ordered, it is found that in this family its terms with the highest degrees are in the following forms:

A) $x^{2^k+2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N}} = x^{(2^k+2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N})\, mod(2^n-1)}$,

then $\omega_2((1.2^k + 1.2^{i_1+p_1} + 1.2^{p_1} + \cdots + 1.2^{i_N+p_N} + 1.2^{p_N})\, mod(2^n - 1))$;

B) $x^{2^0+2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N}} = x^{(2^0+2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N})\, mod(2^n-1)}$,

then $\omega_2((1.2^0 + 1.2^{i_1+p_1} + 1.2^{p_1} + \cdots + 1.2^{i_N+p_N} + 1.2^{p_N})\, mod(2^n - 1))$;

C) $x^{2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N}} = x^{(2^{i_1+p_1}+2^{p_1}+\cdots+2^{i_N+p_N}+2^{p_N})\, mod(2^n-1)}$,

then $\omega_2((1.2^{i_1+p_1} + 1.2^{p_1} + \cdots + 1.2^{i_N+p_N} + 1.2^{p_N})\, mod(2^n - 1))$,

where $0 \leq p_t \leq n-1$. Note that the *mod* operation is a *Ring Homomorphism*, so it can be applied in any term or factor involved, especially to the sums of terms of the form $2^{i_t+p_t}$.

Problem Given the parameters k and i_t, where $1 \leq i_1 < i_2 < \cdots < i_N \leq n-1$, find the N values $p_t \in \{0, 1, \cdots n-1\}$ such that the next cardinal attain its maximum value:

$$Card\{2^{i_1}, \cdots, 2^{i_N}, NorN+1; \text{for all } p_t = 0\} \leq Card\{2^k, 2^{i_1+p_1}, 2^{p_1}, \cdots, 2^{i_N+p_N}, 2^{p_N}\},$$

$$Card\{2^0, 2^{i_1+p_1}, 2^{p_1}, \cdots, 2^{i_N+p_N}, 2^{p_N}\} \leq 2N+1 \leq n. \text{ Then } N \leq \tfrac{n-1}{2}.$$

From $1 \leq i_1 < i_2 < \cdots < i_N \leq n-1$, we have that $N \leq n-1$. So in the binary decompositions of N, we have $N_{\{n-1\}} = N_{\{n-2\}} = \cdots = N_{\{1+log_2 N\}} = 0$. Furthermore binary decompositions of N and $N+1$ differ only by one term. Remember that every integer $i \in [0, 2^n - 1]$ has a unique binary decomposition $i = \sum_{s=0}^{n-1} i_s 2^s$, $i_s \in \{0, 1\}$.

The point is to solve the problem for the subfamilies, placing particular conditions on the set of exponents $1 \leq i_1 < i_2 < \cdots < i_N \leq n-1$. And also study the best-case scenario.

A Good Solution

We consider finite sequences of integer numbers $(i_t)_{t=1}^N$, $(p_t)_{t=1}^N$ such that:

$$1 \leq i_t < i_{t+1} < i_N \leq n-1$$

$$0 \leq p_t \leq n-1.$$

From the condition $i_N \leq n-1$, then $N \leq n-1$. From the condition $2N+1 \leq n$, then $N \leq \frac{n-1}{2}$. Then $N \leq \frac{n-1}{2}$.

In this particular case, we search on the subset of $(p_t)_{t=1}^N$ and $(i_t + p_t)_{t=1}^N$ such that:

$$i_t \leq \tfrac{n-1}{2},$$

$$p_t \leq \tfrac{n-1}{2}, \text{ for all } t.$$

Then $2^{p_t} \, mod(2^n - 1) = 2^{p_t}$, for all t.

$i_t + p_t \leq n-1$, then $2^{i_t+p_t} \, mod(2^n - 1) = 2^{i_t+p_t}$, for all t.

Then $Card\{2^{p_t} \, mod(2^n-1), \, 2^{i_t+p_t} \, mod(2^n-1); \, t = 1, \cdots, N\} = Card\{2^{p_t}, \, 2^{i_t+p_t}; \, t = 1, \cdots, N\}$.

$$m+1 = max_t \{i_t\} \leq \tfrac{n-1}{2}, \text{ and}$$

TABLE 9. Sequences $(i_t)_{t=1}^{\frac{m+2}{2}}$, $(p_t)_{t=1}^{\frac{m+2}{2}}$, where m is even.

$i_t:$	1	3	5	$\cdots$	$m-1$	$m+1$
$p_t:$	$\frac{m}{2}$	$\frac{m}{2}-1$	$\frac{m}{2}-2$	$\cdots$	1	0
$i_t+p_t:$	$\frac{m}{2}+1$	$\frac{m}{2}+2$	$\frac{m}{2}+3$	$\cdots$	m	$m+1$

$$\tfrac{m}{2} = max_t\,\{p_t\} \leq \tfrac{n-1}{2}.$$

Then $m+1 \leq \frac{n-1}{2}$, i.e. $m \leq \frac{n-3}{2}$. Let $m = \frac{n-3}{2}$, where m is even (then n has the form $n = 4r+3$, for some $r \in \mathbb{N}$).

Then $Card\{2^{p_t},\, 2^{i_t+p_t};\, t = 1, \cdots,\, N\} = 2(\frac{m+2}{2}) = m+2 = \frac{n-3}{2}+2 = \frac{n+1}{2}$.

Then we obtain the new subfamilies with the maximum possible *algebraic degree*:

$$f(x) = x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^{i_1}+1})\cdots tr(x^{2^{i_N}+1})$$
$$= x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^1+1})tr(x^{2^3+1})tr(x^{2^5+1})\cdots tr(x^{2^{m-1}+1})tr(x^{2^{m+1}+1})$$
$$= x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^1+1})tr(x^{2^3+1})tr(x^{2^5+1})\cdots tr(x^{2^{\frac{n-5}{2}}+1})tr(x^{2^{\frac{n-1}{2}}+1}),$$

where $d^0(f) = \frac{n+1}{2}$.

In general: for m even, such that $m \leq \frac{n-3}{2}$, the subfamily is:

$$f(x) = x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^1+1})tr(x^{2^3+1})tr(x^{2^5+1})\cdots tr(x^{2^{m-1}+1})tr(x^{2^{m+1}+1})$$

where $d^0(f) = m+2$ or $m+3$.

CASE $n = 4r+1$**:**

We consider finite sequences of integer numbers $(i_t)_{t=1}^N$, $(p_t)_{t=1}^N$ such that:

$$1 \leq i_t < i_{t+1} < i_N \leq n-1$$

$$0 \leq p_t \leq n-1$$

subject to:

$$\{i_t,\, p_t\} \leq \tfrac{n-1}{2}, \text{ for all } t.$$

TABLE 10. Sequences $(i_t)_{t=1}^{\frac{m+2}{2}}$, $(p_t)_{t=1}^{\frac{m+2}{2}}$, where m is even.

$i_t:$	2	4	6	$\cdots$	m	$m+2$
$p_t:$	$\frac{m}{2}$	$\frac{m}{2}-1$	$\frac{m}{2}-2$	$\cdots$	1	0
$i_t+p_t:$	$\frac{m}{2}+2$	$\frac{m}{2}+3$	$\frac{m}{2}+4$	$\cdots$	$m+1$	$m+2$

$$m+2 = max_t\{i_t\} \leq \tfrac{n-1}{2}, \text{ and}$$

$$\tfrac{m}{2} = max_t\{p_t\} \leq \tfrac{n-1}{2}.$$

Then $m+2 \leq \frac{n-1}{2}$, i.e. $m \leq \frac{n-5}{2}$. Let $m = \frac{n-5}{2}$, where m is even (then n has the form $n = 4r+5 = 4\bar{r}+1$, for some $\bar{r} \in \mathbb{N}$).

Then $Card\{2^{p_t},\, 2^{i_t+p_t};\, t = 1, \cdots, N\} = 2(\frac{m+2}{2}) = m+2 = \frac{n-5}{2}+2 = \frac{n-1}{2}$ or $\frac{n-1}{2}+1 = \frac{n+1}{2}$, due to the possible presence of the additional term 2^k for the case $Card\{2^k,\, 2^{p_t},\, 2^{i_t+p_t};\, t = 1, \cdots, N\}$, or the presence of the additional term 2^0 for the case $Card\{2^0,\, 2^{p_t},\, 2^{i_t+p_t};\, t = 1, \cdots, N\}$.

Then we obtain the new subfamilies of high *algebraic degree*:

$$\begin{aligned} f(x) &= x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1}) \\ &= x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^2+1})tr(x^{2^4+1})tr(x^{2^6+1}) \cdots tr(x^{2^m+1})tr(x^{2^{m+2}+1}) \\ &= x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^2+1})tr(x^{2^4+1})tr(x^{2^6+1}) \cdots tr(x^{2^{\frac{n-5}{2}}+1})tr(x^{2^{\frac{n-1}{2}}+1}), \end{aligned}$$

where $d^0(f) \in \{\frac{n-1}{2},\, \frac{n+1}{2}\}$.

In general: for m even, such that $m \leq \frac{n-5}{2}$, the subfamily is:

$$f(x) = x^{2^k+1} + (x^{2^k}+x+1)tr(x^{2^2+1})tr(x^{2^4+1})tr(x^{2^6+1}) \cdots tr(x^{2^m+1})tr(x^{2^{m+2}+1}),$$

where $d^0(f) \in \{m+2,\, m+3\}$.

The algebraic degree of f ensures that the sum given in equation (3), $C_{j_{1_0}l_{1_0}\cdots j_{N_0}l_{N_0}j_{(N+1)_0}}$, is not-zero:

Theorem 3.2.2. Let $n \geq 4$, the function $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1})$ has algebraic degree $2N + 1$ if and only if the following items are met:

1. There exist basis vectors $\mathcal{V} = \{\alpha_i\}_i$ such that $1 \notin Span(\mathcal{V})$. In particular, this basis could be $\mathcal{V} \subseteq \{\alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, where α is a primitive element.

2. There exist some non-zero term of maximum degree of variable part (let's say) $x_{j_{1_0}}x_{l_{1_0}} \cdots x_{j_{N_0}}x_{l_{N_0}}x_{j_{(N+1)_0}}$. That is, there is a vector v$= (j_{1_0}, l_{1_0}, \cdots, j_{N_0}, l_{N_0}, j_{(N+1)_0})$ such that the following sum is non-zero:

$$\sum_{(s_1,\cdots,s_{2N+1}) \text{ is a permutation of } (j_{1_0},l_{1_0},\cdots,j_{N_0},l_{N_0},j_{(N+1)_0})} tr(\alpha_{s_1}^{2^{i_1}}\alpha_{s_2}) \cdots tr(\alpha_{s_{2N-1}}^{2^{i_N}}\alpha_{s_{2N}})(\alpha_{s_{2N+1}}^{2^k} + \alpha_{s_{2N+1}}) \neq 0.$$

Proof:

Due to the form of f, its algebraic degree cannot exceed $2N + 1$. By studying the $Kernel(\varphi)$, where $\varphi(x) = x^{2^k} + x$, it we can show that $|Kernel(\varphi)| \leq 2$. Then $Kernel(\varphi) = \{0, 1\}$. Thus, $1 \notin Span(\mathcal{V})$ implies $\varphi(Span(\mathcal{V}) - \{0\}) \nsubseteq Kernel(\varphi)$.

Apply in equation (3), the fact that the families of functions been considered in this section, $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1})$, has algebraic degree $2N + 1$, it is sufficient to have the coefficient $C_{j_{1_0}l_{1_0}\cdots j_{N_0}l_{N_0}j_{(N+1)_0}}$ nonzero.

Corollary 3.2.3. Let $n \geq 4$, the function $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1}) \cdots tr(x^{2^{i_N}+1})$ has algebraic degree $2N + 1$ if and only if the following items are meet:

1. There exist basis vectors $\mathcal{V} = \{\alpha_i\}_i$ such that $1 \notin Span(\mathcal{V})$. In particular, this basis could be $\mathcal{V} \subseteq \{\alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, where α is a primitive element.

2. There exist a vector v$= (j_{1_0}, l_{1_0}, \cdots, j_{N_0}, l_{N_0}, j_{(N+1)_0})$ satisfying the following Boolean identity:

$$\sum_{(s_1,\cdots,s_{2N}) \text{ is a permutation of } v^*=(j_{1_0},l_{1_0},\cdots,j_{N_0},l_{N_0})} tr(\alpha_{s_1}^{2^{i_1}}\alpha_{s_2}) \cdots tr(\alpha_{s_{2N-1}}^{2^{i_N}}\alpha_{s_{2N}}) = 1.$$

Proof:

The demonstration follows immediately from Theorem 3.2.2.

Corollary 3.2.4. Let $n \geq 4$. Then there exist basis vectors $\mathcal{V} = \{\alpha_i\}_i$ such that $1 \notin Span(\mathcal{V})$, and a vector $\mathrm{v}^* = (j_{1_0}, l_{1_0}, \cdots, j_{N_0}, l_{N_0})$ satisfying the following Boolean identity:

$$\sum_{(s_1,\cdots,s_{2N}) \text{ is a permutation of } \mathrm{v}^*=(j_{1_0},l_{1_0},\cdots,j_{N_0},l_{N_0})} tr(\alpha_{s_1}^{2^{i_1}}\alpha_{s_2})\cdots tr(\alpha_{s_{2N-1}}^{2^{i_N}}\alpha_{s_{2N}}) = 1.$$

Proof:

Apply Corollary 3.2.3 to the functions (of algebraic degree $2N+1$) constructed in this section, i.e. $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^{i_1}+1})\cdots tr(x^{2^{i_N}+1})$.

Remark In a vectorial Boolean function F on $\mathbb{F}_2^n$, its $n-$ coordinate functions are codewords in some *binary Reed-Muller* code $\mathcal{R}(r,n)$. The *algebraic degree* of F, d^0(F), which is the maximum *algebraic degree* of its coordinate functions, is the *order* r of $\mathcal{R}(r,n)$.

CHAPTER 4

A NEW TECHNIQUE TO BOUND THE NONLINEARITY

In this chapter, we establish a lower bound on the nonlinearity of the family of functions $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})$ given in Theorem 2.2.16. The techniques developed in the literature are not very helpful for functions we consider (i.e. ones that contain products of the form $tr(x^{2^k+1})tr(x^{2^j+1})$). Here we introduce new techniques. All theorems in this chapter are new.

As a historical background Roy [34] uses some results of Fitzgerald [22] on quadratic functions with two trace terms, $tr_{K/\mathbb{F}_2}(x(x^{2^a} + x^{2^b}))$ where K is a finite extension of $\mathbb{F}_2$, in order to generalize some results of Lahtonen, McGuire and Ward [26] on Gold and Kasami- Welch functions. Then, Roy gets the Walsh spectrum of the sum $tr(x^{2^a+1}) + tr(x^{2^b+1})$ under certain conditions introduced in Lahtonen et al. [26].

4.1 Bounds for the Nonlinearity

The nonlinearity of a function F can be expressed in terms of the maximum modulus of the Walsh Transform, $NL(F) = 2^{n-1} - \frac{1}{2} max_{u\in\mathbb{F}_2^n,\ v\in\mathbb{F}_2^{m*}} |W_F(u, v)|$. Equal exponents in the terms of the Walsh Transform defines the *objective function* to be maximized, in order to calculate the bound. The method discussed here is new and can also be applied to study the Walsh spectrum and the *nonlinearity profile* of other families of functions that contain Boolean terms of the form $tr(bx^{2^k+1})$.

1st-Order Nonlinearity (Nonlinearity)

Simplification of the Walsh Spectrum family in Theorem 2.2.16, $f = F \circ \psi$, where $\psi(x) = x + P(x),\ P(x) := \mathcal{P}(tr(x^{2^{i_1}+1}), \cdots, tr(x^{2^{i_j}+1}))$. Then:

$$W_f(a, b) = \sum_{x\,\in\,\mathbb{F}_{2^n}} (-1)^{tr(b\,F(\psi(x)) + a\,x)} = \sum_{y\,\in\,\mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,\psi^{-1}(y))}$$

$$= \sum_{y\,\in\,\mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,(y + P(y)))} = \sum_{y\,\in\,\mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,y) + tr(a\,P(y))},$$

where, by Lemma 2.2.15, $\psi = \psi^{-1}$ is a permutation on $\mathbb{F}_{2^n}$, such that n is even. P is a Boolean function, if $a \neq 0$ such that $tr(a) = 0$, then $tr(a\,P(y)) = 0$ on $\mathbb{F}_{2^n}$. Then,

$$W_f(a,b) = \sum_{y\,\in\,\mathbb{F}_{2^n}} (-1)^{tr(b\,F(y)\,+\,a\,y)\,+\,tr(a\,P(y))} = W_F(a,b).$$

Then, the Walsh spectrum was verified for all elements ($b \neq 0$, a), such that $tr(a) = 0$:

$$W_f(b,\,a) = W_F(b,\,a).$$

The objective of this section is to obtain a lower bound of the nonlinearity for the class of functions $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})$ which satisfies Corollary 2.2.17. The Walsh coefficient is unknown for $tr(a) = 1$. Without loss of generality, we can assume the number of zeros is larger than or equal the number of ones in the exponents in the Walsh sum. Then, WLOG, looking for a way or the best way to maximize the number of zeros in the range of the function exponent in the Walsh sum for f (using $b+1$ instead b) after the simplification of its Walsh coefficient:

$$tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}).$$

Theorem 4.1.1. Let $n = 2m$, m odd and $gcd(n, k) = 2$. The nonlinearity of the family $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})$ which satisfies Corollary 2.2.17 is bounded by:

$$2^{n-1} - 2^{\frac{n}{2}} \geq NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq |R|,$$

where k is such that x^{2^k+1} has the classic Walsh Spectrum $\mathcal{W}_{x^{2^k+1}} = \{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$ (see Appendix II), and $R = \{x \in \mathbb{F}_{2^n};\ 1 + tr(bx^{2^k+1}) = tr(x^{2^k+1}) = tr(ax)\}$, for some $a, b \neq 0$ in $\mathbb{F}_{2^n}$.

Proof:

Without loss of generality, we can assume the number of zeros is larger than or equal the number of ones in the exponents in the Walsh sum for f. Then, WLOG, maximize the number of zeros (Z) in the range of the function $tr((b+1)f(x)+ax)$. Due to the simplification of the Walsh coefficient of f (based on the application of the permutation in Lemma 2.2.15, $\psi = \psi^{-1}$, $\psi(x) = x + tr(x^{2^k+1})tr(x^{2^j+1}))$, equivalently, we maximize the number of zeros of the function $tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1})$.

Objetive function: $\max_{\{b\neq 1,\, a,\, j\}} |\{x \in \mathbb{F}_{2^n};\ tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$.

First, we will study the case for $b \neq 1$, which will be reduced to the case for $b = 1$.

Let us consider the sets:

$P = \{x \in \mathbb{F}_{2^n};\ tr(bx^{2^k+1}) = tr(ax),\ tr(x^{2^k+1}) = tr(ax)\}$

$Q = \{x \in \mathbb{F}_{2^n};\ tr(bx^{2^k+1}) = 1 + tr(ax),\ tr(x^{2^k+1}) = 1 + tr(ax)\}$

$R = \{x \in \mathbb{F}_{2^n};\ tr(bx^{2^k+1}) = 1 + tr(ax),\ tr(x^{2^k+1}) = tr(ax)\}$

$S = \{x \in \mathbb{F}_{2^n};\ tr(bx^{2^k+1}) = tr(ax),\ tr(x^{2^k+1}) = 1 + tr(ax)\}$.

They define a *partition* of $\mathbb{F}_{2^n}$, denoted by $\mathcal{P}$, with respect to the linear function $tr(ax)$.

By the conditions on n and k, the monomial x^{2^k+1} becomes a permutation [23], [3], [40]. The function $(b+1)x^{2^k+1}$ is a permutation too . Then $(b+1)x^{2^k+1}$ is onto. Then for $b \neq 1$, the term $tr((b+1)x^{2^k+1})$ has 2^{n-1} values equal to zero and 2^{n-1} values equal to one. Then:

$P \cup Q \subseteq \{x \in \mathbb{F}_{2^n};\ tr((b+1)x^{2^k+1}) = 0\}$, then $|P| + |Q| \leq 2^{n-1}$.

$R \cup S \subseteq \{x \in \mathbb{F}_{2^n};\, tr((b+1)x^{2^k+1}) = 1\}$, then $|R| + |S| \leq 2^{n-1}$.

And from $|P| + |Q| + |R| + |S| = |P \cup Q \cup R \cup S| = |\mathbb{F}_{2^n}| = 2^n$, we have the identity:

$$|P| + |Q| = 2^{n-1},\ \ |R| + |S| = 2^{n-1}.$$

In order to maximize the number of zeros, we can assume that $|P| = max\{|P|, |Q|, |R|, |S|\}$. We denote by $Z =$ the number of zeros, $O =$ the number of ones.

CASE For k such that x^{2^k+1} has Walsh Spectrum $\mathcal{W}_{x^{2^k+1}} \subseteq \{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$:

$Z - O =$	$W_{x^{2^k+1}}(a,b)$
$Z + O =$	2^n

For any $b \neq 0$, $a \in \mathbb{F}_{2^n}$,

$$|P| + |S| = |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) = tr(ax)\}| = \begin{cases} 2^{n-1} + 2^{\frac{n}{2}},\ if\ W_{x^{2^k+1}}(a,b) = 2^{\frac{n+2}{2}} \\ 2^{n-1} + 2^{\frac{n}{2}-1},\ if\ W_{x^{2^k+1}}(a,b) = 2^{\frac{n}{2}} \\ 2^{n-1},\ if\ W_{x^{2^k+1}}(a,b) = 0. \end{cases} \quad (1)$$

Remark For any $c \neq 0$, $a \neq 0$, the set $\{x \in \mathbb{F}_{2^n};\, tr(cx^{2^k+1}) = 0\}$, where x^{2^k+1} is a permutation, not necessarily defines a vector subspace of $\mathbb{F}_2^n$, as the set $\{x \in \mathbb{F}_{2^n};\, tr(ax) = 0\}$. But $tr(cx^{2^k+1})$ can be the same as $tr(ax)$ in $|P| + |S| \in \{2^{n-1} + 2^{\frac{n}{2}}, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-1}\}$ points.

Then, for some pair $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^*$ the maximum number of values equals to zero is $|P|+|S| = |P \cup S| = |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) = tr(ax)\}| = 2^{n-1} + 2^{\frac{n}{2}}$. Later we will only consider b with this requirement. From $\mathcal{P}$, $|Q|+|R| = 2^{n-1} - 2^{\frac{n}{2}}$. From $|P|+|Q| = 2^{n-1}$, $|P| = |R|+2^{\frac{n}{2}}$. From $|P| \leq 2^{n-1}$:

$$|R| \leq 2^{n-1} - 2^{\frac{n}{2}}.$$

Also, from $|P| = 2^{n-1} + 2^{\frac{n}{2}} - |S|$, $|S| \geq 2^{\frac{n}{2}}$. From $|P| = max\{|P|, |Q|, |R|, |S|\}$, $|P| + |Q| = 2^{n-1}$, and $|R| + |S| = 2^{n-1}$, we obtain $|Q| = min\{|P|, |Q|, |R|, |S|\}$.

From now, the parameter j will be used in the maximization process. Moreover, this process depend uniquely on j (independent of b and a).

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	$0 +$	$tr(ax) +$	$tr(ax) \times$	$tr(x^{2^j+1})$
For $x \in Q$:	$0 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$tr(x^{2^j+1})$
For $x \in R$:	$1 +$	$tr(ax) +$	$tr(ax) \times$	$tr(x^{2^j+1})$
For $x \in S$:	$1 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$tr(x^{2^j+1})$

TABLE 11. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

The objective function is simplified such that it only depends on the choice of parameter j:

$$\text{Objetive function: } \max_{tr(x^{2^j+1})} |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|.$$

SUBCASE For j such that x^{2^j+1} has Walsh coefficient $W_{x^{2^j+1}}(a, b) \in \{2^n, 0\}$:

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	$0 +$	$tr(ax) +$	$tr(ax) \times$	$tr(ax)$
	$= 0$			
For $x \in Q$:	$0 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$tr(ax)$
	$= tr(ax)$			
For $x \in R$:	$1 +$	$tr(ax) +$	$tr(ax) \times$	$tr(ax)$
	$= 1$			
For $x \in S$:	$1 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$tr(ax)$
	$= 1 + tr(ax)$			

TABLE 12. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

From:

$$tr(bf(x) + ax) = \begin{cases} 1, \ if \ x \in R \\ 1 + tr(ax), \ if \ x \in S \end{cases} \tag{2}$$

S will be most convenient to get zero values, therefore it will be assumed that $|S| \geq |R|$. Then, the following monotonic sequence on the partition $\mathcal{P}$ is guaranteed:

$$|P| \geq |S| \geq |R| \geq |Q|.$$

That sequence is a key part of solving the optimization problem. Also:

$$|R| + 2^{\frac{n}{2}} = |P| \geq |S| \geq |R|, \text{ so } |R| + 2^{\frac{n}{2}} \geq |S| \geq |R|.$$

From now, on the parameter a will be used in the maximization process. Moreover, this process depend uniquely on a (the three parameters are independent each other $\{b, a, j\}$).

The objective function is simplified such that it only depends on the choice of parameter a:

$$\text{Objective function: } \max_{tr(ax)} |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$$
$$= \max_{tr(ax)} |\{x \in Q \cup S;\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$$

SUBCASE Regarding the parameter a:

The function $tr(ax)$ has up to 2^{n-1} zeros, and 2^{n-1} ones. In the worst case, $\forall x \in Q$, $tr(ax) = 0$, and $\forall x \in S$, $tr(ax) = 1$. Then

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1})$ +	$tr(ax)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
For $x \in P$:	0 +	$tr(ax)$ +	$tr(ax)$ ×	$tr(ax)$
	$= 0$			
For $x \in Q$:	0 +	0 +	$(1+0)$ ×	0
	$= 0$			
For $x \in R$:	1 +	$tr(ax)$ +	$tr(ax)$ ×	$tr(ax)$
	$= 1$			
For $x \in S$:	1 +	1 +	$(1+1)$ ×	1
	$= 1 + 1 = 0$			

TABLE 13. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

$\max_{\{b \neq 1,\, a,\, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}| = 2^n - |R|$

$\geq 2^n - (2^{n-1} - 2^{\frac{n}{2}}) \geq 2^{n-1} + 2^{\frac{n}{2}}$. Then, the new maximum absolute value of Walsh coefficient is:

$$\max_{(a,\, b \neq 0)} |W_{x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})}(a, b)| \geq 2^{\frac{n+2}{2}}$$

Then, the new nonlinearity will be upper bounded by:

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	0			
For $x \in Q$:	0			
For $x \in R$:	1			
For $x \in S$:	0			

TABLE 14. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \leq 2^{n-1} - 2^{\frac{n}{2}}.$$

On the other hand, if we compute the value of $|R|$, the new maximum absolute possible value of Walsh coefficient is attained by:

$$\max_{(a,\, b \neq 0)} |W_{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})}(a, b)| = 2^n - 2|R|.$$

Then, the new nonlinearity will be lower bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq |R|.$$

Using these last two inequalities the new nonlinearity is bounded by:

$$2^{n-1} - 2^{\frac{n}{2}} \geq NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq |R|$$

Where $|R| = |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) = 1 + tr(x^{2^k+1}) = 1 + tr(ax)\}|$. Moreover, to reduce the computational cost, we can be used the more efficient form:

$$|R| = |\{x \in \mathbb{F}_{2^n};\, 1 + tr(bx^{2^k+1}) = tr(x^{2^k+1}) = tr(ax)\}|.$$

SUBCASE For j such that x^{2^j+1} has Walsh the coefficient $W_{x^{2^j+1}}(a, b) \in \{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}\}$:

Then $Z = 2^{n-1} + 2^{\frac{n}{2}}$. We will use these values on $P \cup S$. Then, $tr(x^{2^j+1}) \neq tr(ax)$, so $tr(x^{2^j+1}) = 1 + tr(ax)$ on $Q \cup R$, $|Q \cup R| = 2^{n-1} - 2^{\frac{n}{2}}$. Then,

The objective function is already determined on the sets P and Q.

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	$0 +$	$tr(ax) +$	$tr(ax) \times$	$tr(ax)$
	$= 0$			
For $x \in Q$:	$0 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$(1 + tr(ax))$
	$= 1$			
For $x \in R$:	$1 +$	$tr(ax) +$	$tr(ax) \times$	$(1 + tr(ax))$
	$= 1 + tr(ax)$			
For $x \in S$:	$1 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$tr(ax)$
	$= 1 + tr(ax)$			

TABLE 15. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

The objective function is simplified such that it only depends on the choice of parameter a:

$$\text{Objective function: } \max_{tr(ax)} |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$$
$$= \max_{tr(ax)} |\{x \in R \cup S;\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|.$$

SUBCASE Regarding the parameter a:

The function $tr(ax)$ has up to 2^{n-1} zeros, and 2^{n-1} ones. $|R \cup S| = 2^{n-1}$, then in the worst case, $\forall x \in R \cup S$, $tr(ax) = 1$. Then

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	$0 +$	$tr(ax) +$	$tr(ax) \times$	$tr(ax)$
	$= 0$			
For $x \in Q$:	$0 +$	$tr(ax) +$	$(1 + tr(ax)) \times$	$(1 + tr(ax))$
	$= 1$			
For $x \in R$:	$1 +$	$1 +$	$1 \times$	$(1 + 1)$
	$= 1 + 1 = 0$			
For $x \in S$:	$1 +$	$1 +$	$(1 + 1) \times$	1
	$= 1 + 1 = 0$			

TABLE 16. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

$x \in \mathbb{F}_{2^n}$:	$tr(bx^{2^k+1}) + tr(x^{2^k+1}) +$	$tr(ax) +$	$tr(x^{2^k+1}) \times$	$tr(x^{2^j+1})$
For $x \in P$:	0			
For $x \in Q$:	1			
For $x \in R$:	0			
For $x \in S$:	0			

TABLE 17. $tr(bf(x) + ax)$ on partition $\mathcal{P}$

Then $\max_{\{b \neq 1,\, a,\, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(bx^{2^k+1}) + tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}| = 2^n - |Q|$

If we compute the value of $|Q|$, the new maximum absolute possible value of Walsh coefficient is attained by:

$$\max_{(a,\, b \neq 0)} |W_{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})}(a, b)| = 2^n - 2|Q|.$$

Then, the new nonlinearity will be lower bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq |Q|.$$

But, from $|Q| = min\{|P|, |Q|, |R|, |S|\}$, this last inequality is implied by the before case. In conclusion, for k such that x^{2^k+1} has Walsh Spectrum $\mathcal{W}_{x^{2^k+1}} = \{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$, we have:

$$2^{n-1} - 2^{\frac{n}{2}} \geq NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq |R|,$$

where $|R| = |\{x \in \mathbb{F}_{2^n};\, 1 + tr(bx^{2^k+1}) = tr(x^{2^k+1}) = tr(ax)\}|$.

On the Distribution of Zeros in the Affine Family

For a proof of our following result and its version in higher dimensions we refer to Section 5.1

Theorem 4.1.2. Let $a_1 \neq a_2$ two non-zero elements in $\mathbb{F}_{2^n}$, and $S_{a_1} = \{x \in \mathbb{F}_{2^n};\, tr(a_1 x) = 0\}$ and $S_{a_2} = \{x \in \mathbb{F}_{2^n};\, tr(a_2 x) = 0\}$ its corresponding $\mathbb{F}_2$ - vector subspaces of $\mathbb{F}_{2^n}$. The sets $H_{a_1} = \{x \in \mathbb{F}_{2^n};\, tr(a_1 x) = 1\}$ and $H_{a_2} = \{x \in \mathbb{F}_{2^n};\, tr(a_2 x) = 1\}$ its hyperplanes, respectively. Then the intersections $S_{a_1} \cap S_{a_2}$, $S_{a_1} \cap H_{a_2}$, $H_{a_1} \cap S_{a_2}$, and $H_{a_1} \cap H_{a_2}$ form a partition of $\mathbb{F}_{2^n}$, such that:

$|S_{a_1} \cap S_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = 0\}| = 2^{n-2}$,

$|S_{a_1} \cap H_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = 0,\, tr(a_2x) = 1\}| = 2^{n-2}$,

$|H_{a_1} \cap S_{a_2}| = \{x \in \mathbb{F}_{2^n};\, tr(a_1x) = 1,\, tr(a_2x) = 0\}| = 2^{n-2}$,

$|H_{a_1} \cap H_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = 1\}| = 2^{n-2}$.

Corollary 4.1.3. The number of zeros in the *quadratic function* $tr(a_1x)tr(a_2x)$ ($a_1 \neq a_2$ in $\mathbb{F}_{2^n}^*$) is:

$|\mathcal{O} = \{x \in \mathbb{F}_{2^n};\, tr(a_1x)tr(a_2x) = 0\}| = |(S_{a_1} \cap S_{a_2}) \cup (S_{a_1} \cap H_{a_2}) \cup (H_{a_1} \cap S_{a_2})| = (\frac{3}{4})2^n$.

Remark The following result is useful for knowledge and for a good intuition about the distribution of zeros and ones in the family of linear Boolean functions: $|H_{a_1}| = 2^{n-1}$, but $|\{x \in H_{a_1};\, tr(a_2x) = 0\}| \neq 2^{n-1}$. Exactly, $|\{x \in H_{a_1};\, tr(a_2x) = 0\}| = (\frac{1}{4})2^n$.

Due to potential of application of this Corollary 4.1.3, we call it *Theorem on the distribution of zeros of the quadratic.*

nl(f)	*Ub*	*Lb*	nl(G_1)	d(G_1)	nl(f_1)	d(f_1)	nl(f_{131})	d(f_{131})	nl(f_{1351})	d(f_{1351})	nl(f_{13571})	nl(R_{11})	d(R_{11})
$n=4$	4	0	4	2	4	3	4	–	–	–	–	4	3
$n=6$	24	8	24	2	24	3	24	–	–	–	–	24	3
$n=8$	112	48	112	2	112	3	96	5	–	7	–	104	5
$n=10$	480	224	480	2	480	3	448	5	480	7	–	456	5
$n=12$	1984	180	1984	2	1984	3	1888	5	1912	7	–	1936	5
$n=14$	8064	3968	8064	2	8064	3	7808	5	–	7	–	–	–
$n=16$	32512	16128	32512	2	32512	3	–	5	–	7	–	–	–

FIGURE 1. n = field degree. $NL(f)$ = Nonlinearity of a given function f. Ub= upper bound and Lb= lower bound of $NL(f_{kjk})$, given in Theorems 4.1.1- 4.1.4. Gold $G_k(x) = x^{2^k+1}$. The function of Budaghyan et al. $f_k(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})$. $f_{kjk}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})$ family in Theorems 4.1.1- 4.1.4. $f_{kjuk}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})tr(x^{2^u+1})$. $f_{kjuvk}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})tr(x^{2^u+1})tr(x^{2^v+1})$. $R_{ik}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^i+1})(1 + tr((x + x^8)^{2^i+1}))$ is a variation inspired by families in Corollary 2.2.17. Budaghyan function is EA-inequivalent but CCZ-equivalent to Gold. $d(f)$ = Algebraic degree of f.

Remark A weakness of Gold family is that it has 2nd-*order nonlinearity* equal to 0: $nl_2(G_k) = 0$. Fortunately, for n odd the families given in Corollary 2.2.17 do not necessariy have 2nd-order nonlinearity equal to 0, see Section 4.3. For $n = 7$, $nl_2(f_{kjk}) \geq 9$, where $k = 1$, $j = 2$. For $n = 11$, $nl_2(f) \geq 119$, where f is a function in Corollary 2.2.17.

Theorem 4.1.4. Let $n = 2m$, the family $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})$ belongs to the class of functions given in Corollary 2.2.17, where the Walsh coefficients of x^{2^k+1} satisfy the classic requirement of the Gold family: $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$ (see Appendix II), for any $a_1 \in \mathbb{F}_{2^n}$. Then, the nonlinearity of f has the following lower bound:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq 2^{n-2} - 2^{\frac{n}{2}}.$$

Proof:

CASE $b = 1$. First, we consider the case for n even, later the case for n odd.

Let's $n = 2m$. Without loss of generality, we maximize the number of zeros (Z) in the range of the function $tr(x^{2^k+1}) + tr(ax) + tr(x^{2^k+1})tr(x^{2^j+1})$.

SUBCASE For $\{k, j\}$ such that $W_{x^{2^k+1}}(a_1, 1) = W_{x^{2^j+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$:

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1x)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
For $x \in P$:	0 +	$tr(a_1x)$ ×	$tr(x^{2^j+1})$
For $x \in Q$:	1 +	$(1 + tr(a_1x))$ ×	$tr(x^{2^j+1})$

TABLE 18. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$

The Walsh coefficient $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$, defines the following sets, by solving the linear system:

$Z - O =$	$W_{x^{2^k+1}}(a_1, 1) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(1.x^{2^k+1}) + tr(a_1 x)}$
$Z + O =$	2^n

$P = \{x \in \mathbb{F}_{2^n};\ tr(x^{2^k+1}) = tr(a_1x)\}$, with $|P| = 2^{n-1} + 2^{\frac{n}{2}}$.

$Q = \{x \in \mathbb{F}_{2^n};\ tr(x^{2^k+1}) = 1 + tr(a_1x)\}$, with $|Q| = 2^{n-1} - 2^{\frac{n}{2}}$.

They define the *partition* $P \cup Q = \mathbb{F}_{2^n}$, corresponding to the linear function $tr(a_1x)$.

Now, we pay particular attention to a solution to our optimization problem:

Objective function: $\max\limits_{\{a_1,\, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(x^{2^k+1}) + tr(a_1 x) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$.

Also, since $W_{x^{2^j+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$, then we will ensure at least the $|P| = max\{|P|,\, |Q|\} = 2^{n-1} + 2^{\frac{n}{2}}$ of $2^{n-1}+2^{n-2}$ zero values, if the corollary on the *quadratic function* $tr(a_1 x)tr(a_2 x)$ has been applied.

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1 x)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
For $x \in P$:	0 +	$tr(a_1 x)$ ×	$tr(a_2 x)$
	$tr(a_1 x)tr(a_2 x)$		
For $x \in Q$:	1 +	$(1 + tr(a_1 x))$ ×	$(1 + tr(a_2 x))$
	$tr(a_1 x) + tr(a_2 x) + tr(a_1 x)tr(a_2 x)$		

TABLE 19. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$

It is not convenient for the purpose of getting more zeros, that the quadratic resultant function over the set Q, $tr(a_1 x) + tr(a_2 x) + tr(a_1 x)tr(a_2 x)$, such that $x \notin \mathcal{O}$. Because $x \notin \mathcal{O}$, it implies $tr(a_1 x)+tr(a_2 x)+tr(a_1 x)tr(a_2 x) = 1+1+1 = 1$. Then, we prefer as much as possible for elements in Q that $x \in \mathcal{O}$, which is described in the next table:

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1 x)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
For $x \in P$:	$tr(a_1 x)tr(a_2 x)$		
	$= 0$		
For $x \in Q \cap \mathcal{O}$:	$tr(a_1 x) + tr(a_2 x) + tr(a_1 x)tr(a_2 x)$		
	$= tr(a_1 x) + tr(a_2 x)$		
For $x \in Q \cap \mathcal{O}^c$:	$tr(a_1 x) + tr(a_2 x) + tr(a_1 x)tr(a_2 x)$		
	$= 1 + 1 + 1 = 1$		

TABLE 20. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$

Remark In the probabilistic terms, for $x \in Q \cap \mathcal{O}$, the resultant function, $tr(a_1x) + tr(a_2x)$ is such that $tr(a_1x) = 0 \vee tr(a_2x) = 0$, i.e.:

$$tr(a_1x) + tr(a_2x) = \begin{cases} 0 + 0 = 0, \\ 0 + 1 = 1, \\ 1 + 0 = 1. \end{cases} \tag{3}$$

It is $Pr(1) = \frac{2}{3}$, $Pr(0) = \frac{1}{3}$. But worst case, to get even more zero values, we suppose that $Pr(0) = 1$, i.e. $tr(a_1x) + tr(a_2x) = 0$ on $Q \cap \mathcal{O}$.

Now, $\forall x \in P$, $tr(a_1x)tr(a_2x) = 0$, then $P \subseteq \mathcal{O}$. Taking in account that $P \cup Q = \mathbb{F}_{2^n}$ is a partition, then $P \cup (Q \cap \mathcal{O}) = \mathcal{O}$, $|P \cup (Q \cap \mathcal{O})| = (\frac{3}{4})2^n$, $|Q \cap \mathcal{O}| = (\frac{3}{4})2^n - |P| = 2^{n-2} - 2^{\frac{n}{2}}$, $Q \cap \mathcal{O}^c = \mathcal{O}^c$, and $|Q \cap \mathcal{O}^c| = |Q| - |Q \cap \mathcal{O}| = 2^{n-1} - 2^{\frac{n}{2}} - (2^{n-2} - 2^{\frac{n}{2}}) = 2^{n-2}$.

Then, $\max\limits_{\{a_1, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(x^{2^k+1}) + tr(a_1x) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}| = 2^n - |Q \cap \mathcal{O}^c|$.

The new maximum absolute possible value of Walsh coefficient for $b = 1$, is attained by:

$$\max_{a_1 \in \mathbb{F}_{2^n}} |W_{x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})}(a_1, 1)| = 2^{n-1}.$$

Then, the new "nonlinearity" (with the restriction, $b = 1$) will be lower bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq 2^{n-1} - 2^{n-2}.$$

SUBCASE For $\{k, j\}$ such that $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$, and $W_{x^{2^j+1}}(a_1, 1) = 0$:

Because $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$, we will use the same first table and partition $P \cup Q = \mathbb{F}_{2^n}$ given in the earlier sub-case. Next, the factor $tr(x^{2^j+1})$ takes the main role in the maximization problem, but now with the difference that $W_{x^{2^j+1}}(a_1, 1) = 0$.

Objective function: $\max\limits_{\{a_1, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(x^{2^k+1}) + tr(a_1x) + tr(x^{2^k+1})tr(x^{2^j+1}) = 0\}|$.

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1x)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
For $x \in P$:	0 +	$tr(a_1x)$ ×	$tr(x^{2^j+1})$
For $x \in Q$:	1 +	$(1 + tr(a_1x))$ ×	$tr(x^{2^j+1})$

TABLE 21. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$

From $W_{x^{2^j+1}}(a_1, 1) = 0$, $tr(x^{2^j+1})$ agrees with linear (and affine) functions $tr(a_2x)$ in 2^{n-1} points. In order to satisfy the objective function (maximize the zero values in $tr(1f(x) + ax)$), there are the following four choices:

If $tr(x^{2^j+1}) = tr(a_2x)$, for x in P, then $\eta(x) = tr(a_1x)tr(a_2x) = \begin{cases} 1, \ if \ x \in H_{a_1} \cap H_{a_2} \\ 0, \ if \ x \notin H_{a_1} \cap H_{a_2} \end{cases}$

If $tr(x^{2^j+1}) = tr(a_2x)$, for x in Q, then

$$\kappa(x) = 1 + tr(a_2x) + tr(a_1x)tr(a_2x) = \begin{cases} 1, \ if \ x \in H_{a_1} \cap H_{a_2} \\ 1 + tr(a_2x), \ if \ x \notin H_{a_1} \cap H_{a_2} \end{cases}$$

The best choice is considering $tr(x^{2^j+1}) = tr(a_2x)$, for x in $P \cap (H_{a_1} \cap H_{a_2})^c$. And taking into account that $|P| = 2^{n-1} + 2^{\frac{n}{2}}$ and $(H_{a_1} \cap H_{a_2})^c = (\frac{3}{4})2^n$, it can happen for all the 2^{n-1} points, where $tr(x^{2^j+1})$ agrees with $tr(a_2x)$. Then, we elaborate the next table:

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1x)$ +	$tr(x^{2^k+1})$ ×	$tr(x^{2^j+1})$
2^{n-1} $x's$ in $P = P - (H_{a_1} \cap H_{a_2})$:	0 +	$tr(a_1x)$ ×	$tr(a_2x)$
	$tr(a_1x)tr(a_2x)$		
$2^{\frac{n}{2}}$ $x's$ in $P = P \cap (H_{a_1} \cap H_{a_2})$:	0 +	$tr(a_1x)$ ×	$(1 + tr(a_2x))$
	$tr(a_1x)$ + $tr(a_1x)tr(a_2x)$		
For $x \in Q$:	1 +	$(1 + tr(a_1x))$ ×	$(1 + tr(a_2x))$
	$tr(a_1x) + tr(a_2x) + tr(a_1x)tr(a_2x)$		

TABLE 22. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$, where f in Corollary 2.2.17

There are three types of functions on the partition:

$\eta(x) = tr(a_1x)tr(a_2x)$, $\zeta(x) = tr(a_1x) + tr(a_1x)tr(a_2x)$, $\xi(x) = tr(a_1x) + tr(a_2x) + tr(a_1x)tr(a_2x)$.

For example, for the function ξ: If $x \in H_{a_1} \cap H_{a_2}$, then $\xi(x) = 1 + 1 + 1 = 1$. Then, we prefer that x is not in $H_{a_1} \cap H_{a_2}$, to increase the chances of obtaining zero values, $\xi(x) = 0$.

To sum up all possible values:

$$\eta(x) = \begin{cases} 1, \ if \ x \in H_{a_1} \cap H_{a_2} \\ 0, \ if \ x \notin H_{a_1} \cap H_{a_2} \end{cases} \tag{4}$$

$$\zeta(x) = \begin{cases} 0, \ if \ x \in H_{a_1} \cap H_{a_2} \\ tr(a_1 x), \ if \ x \notin H_{a_1} \cap H_{a_2} \end{cases} \tag{5}$$

$$\xi(x) = \begin{cases} 1, \ if \ x \in H_{a_1} \cap H_{a_2} \\ tr(a_1 x) + tr(a_2 x), \ if \ x \notin H_{a_1} \cap H_{a_2}. \end{cases} \tag{6}$$

To get the best number of zeros, it is convenient to apply Theorem 4.1.2, $|H_{a_1} \cap H_{a_2}| = 2^{n-2}$.

$x \in \mathbb{F}_{2^n}$:	$tr(x^{2^k+1}) + tr(a_1 x) +$ | $tr(x^{2^k+1}) \times$ | $tr(x^{2^j+1})$
2^{n-1} $x's$ in $P = P - (H_{a_1} \cap H_{a_2})$:	$\eta(x)$
	0
$2^{\frac{n}{2}}$ $x's$ in $P = P \cap (H_{a_1} \cap H_{a_2})$:	$\zeta(x)$
	0
2^{n-2} $x's$ in $Q = Q - (H_{a_1} \cap H_{a_2})$:	$\xi(x)$
	$tr(a_1 x) + tr(a_2 x)$
$2^{n-2} - 2^{\frac{n}{2}}$ $x's$ in $Q = Q \cap (H_{a_1} \cap H_{a_2})$:	$\xi(x)$
	1

TABLE 23. $tr(1f(x) + ax)$ on partition $P \cup Q = \mathbb{F}_{2^n}$

In the worst case, to get even more zero values, we assume that $\xi(x) = tr(a_1 x) + tr(a_2 x) = 0$ on the $Q \cap \mathcal{O}$.

Then $\max\limits_{\{a_1, j\}} |\{x \in \mathbb{F}_{2^n};\, tr(x^{2^k+1}) + tr(a_1 x) + tr(x^{2^k+1}) tr(x^{2^j+1}) = 0\}| = 2^n - |Q \cap (H_{a_1} \cap H_{a_2})|$.

The new maximum absolute possible value of Walsh coefficient for $b = 1$, is attained by:

$$\max_{a_1 \in \mathbb{F}_{2^n}} |W_{x^{2^k+1}+(x^{2^k}+x+1)tr(x^{2^k+1})tr(x^{2^j+1})}(a_1,1)| = 2^{n-1} + (2)2^{\frac{n}{2}}.$$

Then, the new "nonlinearity" (with the restriction, $b = 1$) will be lower bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq 2^{n-2} - 2^{\frac{n}{2}}.$$

Summarizing the two sub cases for $b = 1$, and $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq \begin{cases} 2^{n-2},\ if\ W_{x^{2^j+1}}(a_1,1) = 2^{\frac{n+2}{2}} \\ 2^{n-2} - 2^{\frac{n}{2}},\ if\ W_{x^{2^j+1}}(a_1,1) = 0. \end{cases} \quad (7)$$

Note that the case $W_{x^{2^j+1}}(a_1, 1) = 0$ is always present.

CASE For $b \neq 1$ from $b = 1$:

In order to satisfy the objective function we will consider the subcase for $b = 1$, which is the one with the maximum number of zero values corresponding to $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$ and $W_{x^{2^j+1}}(a_1, 1) = 0$. From that, we address the case for $b \neq 1$:

$$W_f(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(bf(x)+ax)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr((b+1)\,x^{2^k+1}) + tr(x^{2^k+1}) + tr(a_1 x) + tr(x^{2^k+1})tr(x^{2^j+1})}$$

$$= \sum_{x \notin Q \cap (H_{a_1} \cap H_{a_2})} (-1)^{tr((b+1)\,x^{2^k+1})+0} + \sum_{x \in Q \cap (H_{a_1} \cap H_{a_2})} (-1)^{tr((b+1)\,x^{2^k+1})+1}.$$

Taking in account the following facts: $tr((b+1)\,x^{2^k+1}$ is a permutation, that is $|T| = 2^{n-1}$, where $T = \{x \in \mathbb{F}_{2^n};\, tr((b+1)\,x^{2^k+1}) = 0\}$, $|\mathbb{F}_{2^n} - (Q \cap (H_{a_1} \cap H_{a_2}))| = 2^{n-1} + 2^{n-2} + 2^{\frac{n}{2}}$, $|Q \cap (H_{a_1} \cap H_{a_2})| = 2^{n-2} - 2^{\frac{n}{2}}$. Then, in order to get the maximum number of zeros, the worst case occurs with the following choice:

$$W_f(a,b) \leq \sum_{x \notin Q \cap (H_{a_1} \cap H_{a_2}) \cap T} (-1)^{0+0} + \sum_{x \notin Q \cap (H_{a_1} \cap H_{a_2}) \cup T} (-1)^{1+0} + \sum_{x \in Q \cap (H_{a_1} \cap H_{a_2}) - T} (-1)^{1+1}$$

$$W_f(a,b) \leq 2^{n-1} + (2^{n-2} - 2^{\frac{n}{2}}) - (2^{n-2} + 2^{\frac{n}{2}}) = 2^{n-1} - (2)2^{\frac{n}{2}}.$$

Where: $|\mathbb{F}_{2^n} - (Q \cap (H_{a_1} \cap H_{a_2}) \cap T)| = 2^{n-1}$, $|\mathbb{F}_{2^n} - (Q \cap (H_{a_1} \cap H_{a_2}) \cup T)| = 2^{n-2} + 2^{\frac{n}{2}}$, $|Q \cap (H_{a_1} \cap H_{a_2}) - T| = 2^{n-2} - 2^{\frac{n}{2}}$.

Then, the new "nonlinearity" (with the restriction, $b \neq 1$) will be lower bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq 2^{n-2} + 2^{\frac{n}{2}}.$$

In summary, for $W_{x^{2^k+1}}(a_1, 1) = 2^{\frac{n+2}{2}}$, the nonlinearity is under bounded by:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq \begin{cases} 2^{n-2} - 2^{\frac{n}{2}}, \ if \ b = 1 \\ 2^{n-2} + 2^{\frac{n}{2}}, \ if \ b \neq 1 \end{cases} \tag{8}$$

Then, in the worst case:

$$NL(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \geq 2^{n-2} - 2^{\frac{n}{2}}.$$

Remark This method can also be applied to study the Walsh spectrum and the *nonlinearity profile* of other families of functions that contain the Boolean terms $tr(bx^{2^k+1})$. Moreover, because the bounds depend on the Walsh spectrum of functions, the new family of functions with the same Walsh spectrum could have the same bounds according to their formula.

4.2 Simplification of the Walsh Spectrum of the Family in Theorem 2.2.24, $f_2 = F \circ \varphi$, where $\varphi(x) = x + B(x)$. Then:

$$W_{f_2}(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(\varphi(x)) + a\,x)} = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,\varphi^{-1}(y))}$$

$$= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,(y + B(y)))} = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,y) + tr(a\,B(y))},$$

where $\varphi = \varphi^{-1}$ is a permutation. B is a Boolean function, considering a, such that $tr(a) = 0$, then $tr(a\,B(y)) = 0$ on $\mathbb{F}_{2^n}$. There are a lot of candidates, exactly $|\{a \neq 0 \in \mathbb{F}_{2^n};\, tr(a) = 0\}| = 2^{n-1} - 1$.

Then, $W_{f_2}(a, b) = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,y) + tr(a\,B(y))} = W_F(a, b)$, for $a \neq 0$, with $tr(a) = 0$. Then, the Walsh spectrum was verified for all elements ($b \neq 0$, a), such that $tr(a) = 0$:

$$W_{f_2}(b,\, a) = W_F(b,\, a).$$

Using the previous technique in order to increase the chances of achieving a high nonlinearity for the family, from the nonlinearity of one of the two functions that have participated in its composition.

4.3 Bounds for the 2nd-Order Non-linearity

2nd-Order Nonlinearity

The same concept $d(f, \mathcal{R}(1,n))$ works in general for $\mathcal{R}(r,n)$, $\forall r \geq 2$.

$$nl_2(f) = min_{h \in \mathcal{R}(2,n)}\, d_H(f,h) = min_{h \in \mathcal{R}(2,n)}(f+h).$$

Applying the concepts from Reed-Muller Codes Section 1.2 to $f+g$, where $deg(g)=2$, we get a formula for the 2nd- order nonlinearity based on the Walsh Transform with the extra quadratic term :

$$\mathrm{d}_H\{\boldsymbol{f},\, \boldsymbol{g} + \varepsilon + \textstyle\sum_{i=1}^{n} u_i v_i\} = \mathrm{d}_H\{\boldsymbol{f} + \boldsymbol{g},\, \varepsilon + \textstyle\sum_{i=1}^{n} u_i v_i\} = \frac{1}{2}\{2^n \pm \sum\limits_{v \in \mathbb{F}_{2^n}} (-1)^{u.v+(f+g)(v)}\}$$

$$nl_2(f) = \tfrac{1}{2}\{2^n - \max_{u \in \mathbb{F}_2^n,\, g \in \mathcal{R}(2,n)} |\sum_{v \in \mathbb{F}_{2^n}} (-1)^{b.f(v)+u.v+g(v)}|\},$$

where ε could be 0 or 1, and $Q(v) = \boldsymbol{g} + \varepsilon + \sum_{i=1}^{n} u_i v_i$ means an arbitrary quadratic function in the vector $v = (v_1, v_2, \cdots, v_n) \in \mathbb{F}_2^n$.

$$W_{2,f}((a_i)_{i=0}^{\frac{n}{2}}, b) = |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(bf(x)) + tr(\sum\limits_{i=1}^{\frac{n}{2}} a_i x^{2^i+1}) + tr(ax)}| = |\sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(bf(x)) + tr(\sum\limits_{i=0}^{\frac{n}{2}} a_i x^{2^i+1})}|.$$

Objective function: $\max\limits_{\{b \neq 0,\, (a_i)_i,\, a_i \in \mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\, tr(bf(x)) + tr(\sum\limits_{i=0}^{\frac{n}{2}} a_i x^{2^i+1}) = 0\}|$

Considering a family of Corollary 2.2.17, $f = F \circ \psi$, where $\psi(x) = x + P(x)$, $P(x) = tr(x^{2^k+1})tr(x^{2^j+1})$, $Q(x) = ax + g(x) = \sum\limits_{i=0}^{\frac{n}{2}} a_i x^{2^i+1}$

$$W_{2,f}((a_i)_i, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(\psi(x)) + a\,x + g(x))} = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + a\,\psi^{-1}(y) + g(\psi^{-1}(y)))}$$

$$= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y) + Q(y + P(y)))} = \sum_{y \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(y)) + tr(\sum\limits_{i=0}^{\frac{n}{2}} a_i (y + P(y))^{2^i+1})}.$$

We begin the maximization process with the exponent in the exponential sum $W_{2,f}((a_i)_i, b)$:

$$e(x) = tr(b\,x^{2^k+1}) \; + \; tr(b\,(x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \; + \; tr(\sum_{i=0}^{\frac{n}{2}} a_i x^{2^i+1}).$$

Taking into account that in general the sum $tr(\sum_{i=0}^{\frac{n}{2}} a_i x^{2^i+1})$ contains the term $tr(b\,x^{2^k+1})$. Then, the objective function is simplified to:

$$\max_{\{b\neq 0,\,(a_i)_i,\,a_i\,\in\,\mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\; tr(b\,(x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \; + \; \sum_{i=0}^{\frac{n}{2}} tr(a_i x^{2^i+1}) = 0\}|.$$

For $b = 1$ for n even, $tr(b\,(x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) = 0$ on $\mathbb{F}_{2^n}$. Then, the maximization problem is reduced to the knowledge of the *weight distribution* of $\mathcal{R}(2, n)$ (quadratics more general than a Gold function):

$$\max_{\{b=1,\,(a_i)_i,\,a_i\,\in\,\mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\; \sum_{i=0}^{\frac{n}{2}} tr(a_i x^{2^i+1}) = 0\}| = 2^n - \textit{ minimum weight} \text{ in } \mathcal{R}(2, n)$$

where, $\min_{\{b=1,\,(a_i)_i,\,a_i\,\in\,\mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\; \sum_{i=0}^{\frac{n}{2}} tr(a_i x^{2^i+1}) = 1\}| = \textit{minimum weight} \text{ in } \mathcal{R}(2, n) = \min\{2^n,\, 2^{n-1} \pm 2^{n-2},\, \cdots,\, 2^{n-1} \pm 2^{\frac{n}{2}},\, 2^{n-1} \pm 2^{\frac{n}{2}-1},\, 2^{n-1}\} = 2^{n-1} - 2^{n-2}$

Also, we are looking for non-trivial solutions, so just considering the cases where the element 0 is not in the *weight distribution* of $\mathcal{R}(2, n)$.

On the other hand, for $b \neq 1$ there may be fewer number of ones. Then, there is an *upper bound*:

$$nl_2(f) = d(f, \mathcal{R}(2, n)) = \min_{\{b\neq 0,\,(a_i)_i,\,a_i\,\in\,\mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\; tr(b\,(x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \; + \; \sum_{i=0}^{\frac{n}{2}} tr(a_i x^{2^i+1}) = 1\}| \leq \min_{\{b=1,\,(a_i)_i,\,a_i\,\in\,\mathbb{F}_{2^n}\}} |\{x \in \mathbb{F}_{2^n};\; \sum_{i=0}^{\frac{n}{2}} tr(a_i x^{2^i+1}) = 1\}| = 2^{n-1} - 2^{n-2}$$

$$nl_2(x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^k+1})tr(x^{2^j+1})) \leq 2^{n-1} - 2^{n-2}.$$

Theorem 4.3.1. [14]

All the weights in $\mathcal{R}(r, n)$ are multiples of $2^{[\frac{n-1}{r}]}$.

Proposition [Carlet [11], recursive lower bounds on the $r-$ nonlinearity]:

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

Corollary 4.3.2. [Corollary 2, Carlet [9]]:

Assuming some K, k, $\in \mathbb{N} \cup \{0\}$, with $\forall a \in \mathbb{F}_{2^n}^*$, $nl_{r-1}(D_a f) \geq 2^{n-1} - K2^k$.

Then:

$$nl_r(f) \geq 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n-1)K2^{k+1} + 2^n}.$$

It is approximately:

$$nl_r(f) \geq 2^{n-1} - \sqrt{K}2^{\frac{n+k-1}{2}}.$$

Example For $n = 6 = 2(3)$, $\frac{n}{2} = 3$ even, by application of Corollary 4.3.2:

The subfamily $f(x) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})$, where i, $j \in \{1, 2, 3\}$.

$nl_1(D_a f) = 0$, $\forall a \neq 0$. $0 = 32 - K2^k$, then $K = 1$, $k = 5$. Then $nl_2(f) \geq 32 - 2^5 = 0$.

On the other hand, by J. Schatz [35], $18 = \rho(RM(2,6)) \geq nl_2(f)$. Then $18 \geq nl_2(f) \geq 0$.

Example For $n = 8 = 2(4)$, $\frac{n}{2} = 4$ not even, by application of Corollary 4.3.2 for lower bound:

The sub family $f(x) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})$, where i, $j \in \{1, 2, 3, 4\}$.

$nl_1(D_a f) = 0$, constant $\forall a \neq 0$. $0 \geq 2^{8-1} - K2^k$, then $K = 1$, $k = 7$.

Then $nl_2(f) \geq 2^{8-1} - \frac{1}{2}\sqrt{(2^8-1)2^8 + 2^8}$, $nl_2(f) \geq 0$.

Example For $n = 7$, by application of Corollary 4.3.2 for lower bound:

The sub family $f(x) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})$, where $i = 1$, $j = 2$.

$nl_1(D_1 f) = 24$, and $nl_1(D_a f) = 16$, constant, $\forall a \notin \{0, 1\}$.

$r = 2$, $\min\limits_{a \in \mathbb{F}_{2^n}^*} nl_{r-1}(D_a f) = 16 = 2^{7-1} - K2^k$, then $K = 3$, $k = 4$.

Then $nl_r(f) \geq 2^{7-1} - \frac{1}{2}\sqrt{(2^7-1)(3)2^5 + 2^7} \geq 8.5$. Then $nl_2(f) \geq 9$.

Example For $n = 9$, by application of Corollary 4.3.2 for lower bound:

The sub family $f(x) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1})tr(x^{2^j+1})$, where $i = 1$, $j = 3$.

$nl_1(D_a f) = \{112, 64, 0\}$, $\forall a \neq 0$.

$r = 2$, $\min\limits_{a \in \mathbb{F}_{2^n}^*} nl_{r-1}(D_a f) = 0 = 2^{9-1} - K2^k$, then $K = 1$, $k = 8$.

Then $nl_r(f) \geq 2^{9-1} - \frac{1}{2}\sqrt{(2^9 - 1)(1)2^9 + 2^9} = 0$. Then $nl_2(f) \geq 0$.

Example For $n = 11$, by application of Corollary 4.3.2 for lower bound:

$nl_1(D_1 f) = 480$, and $nl_1(D_a f) \in \{256, 224, calculating\}$, $\forall a \neq 0$.

$r = 2$, $\min\limits_{a \in \mathbb{F}_{2^n}^*} nl_{r-1}(D_a f) = 224 = 2^{11-1} - K2^k$, then $K = 5^2$, $k = 5$.

Then $nl_r(f) \geq 2^{11-1} - \frac{1}{2}\sqrt{(2^{11} - 1)(5^2)2^6 + 2^{11}} = 118.8$. Then $nl_2(f) \geq 119$.

CHAPTER 5

NEW SIMPLE DIFFERENTIALLY δ- UNIFORM BOOLEAN FACTORS BASED FAMILIES

5.1 New Differentially $\{4, 6, 8\}$-Uniform Permutations with Optimal Algebraic Degree

In the whole discussion of this theory, we identify the vector space $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$.

The AES (advanced encryption standard) uses the inverse function, which is a differential 4-uniform function. Finding differential 4- uniform permutation functions with high nonlinearity on even degree fields is a big challenge. In view of these reasons, in [2], Bracken and Leander listed an open problem:

Problem To find more highly nonlinear permutations of even degree fields with differential uniformity of 4.

It is known that if f is an *permutation* on $\mathbb{F}_{2^n}$, then $deg(f) \leq n-1$. If it attains the equality Zha [40] calls it *optimal algebraic degree (oad)*. To read about a class of sporadic binomials permutations with low differential uniformity ($\delta = 4, 6$) see the work of Charpin and Kyureghyan (2017) in [13]. Yu and Wang built differential 6 and 4- uniform permutations from the inverse function [39]. Then Qu et al. [33] gives us a survey of differentially 4-uniform permutations families, even without the requirement of high nonlinearity see the Carlet [10], and also Zha [40].

We construct new families of 4-uniform functions in this Chapter. All our functions have much simpler forms than the ones given by the authors mentioned above. It is important to underline that the functions given by a group of authors are defined implicitly, or are given as a piecewise function. While our functions are given through an explicit formula in polynomial representation.

Theorem 5.1.1. [Differentially $\{4, 6, 8\}$-Uniform Permutations]

There is a *linearly independent set* of $\mathbb{F}_2^n$, $(a_i)_{i=1}^{n-1}$, whith $tr(a_1) = \cdots = tr(a_{n-1}) = 0$, such that:

1) If n odd and $gcd(n, k) = 1$, then, the family of functions:

$$f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x) \cdots tr(a_{n-1}x),$$

is *differentially* 4*-uniform permutation* on $\mathbb{F}_{2^n}$, $nl(f) \geq nl(x^{2^k+1}) - 2 = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$, and optimal algebraic degree $d^0(f) = n - 1$.

2) If $n = 2m$, where m is odd and $gcd(n, k') = 2$, then, the family of functions:

$$\mathcal{G}(x) = x^{2^{k'}+1} + (x^{2^{k'}} + x + 1)tr(a_1x), \cdots, tr(a_{deg}x),$$

is *differentially* γ*-uniform permutation* on $\mathbb{F}_{2^n}$, where $\gamma \in \{4, 6, 8\}$, $d^0(\mathcal{G}) = deg \in \{n - 2, n - 1\}$. Moreover:

If $deg = n - 1$ (optimal algebraic degree), then $nl(\mathcal{G}) \geq nl(x^{2^{k'}+1}) - 2$.

If $deg = n - 2$ (almost optimal algebraic degree), then $nl(\mathcal{G}) \geq nl(x^{2^{k'}+1}) - 4$.

3) If n odd and $gcd(n, i) = 1$, then, the *Kasami based* family of functions:

$$\mathcal{K}(x) = x^{2^{2i}-2^i+1} + (x^{2^{2i}-2^i} + x^{2^{2i}-(2)2^i+1} + x^{2^{2i}-(2)2^i} + x^{2^{2i}-(3)2^i+1} + x^{2^{2i}-(3)2^i} + \cdots + x^{2^i+1} + x^{2^i} + x + 1)tr(a_1x), \cdots, tr(a_{n-1}x),$$

is *differentially* 4*-uniform permutation* on $\mathbb{F}_{2^n}$, $nl(\mathcal{K}) \geq nl(F) - 2 = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$, $F(x) = x^{2^{2i}-2^i+1}$, and optimal algebraic degree $d^0(\mathcal{K}) = n - 1$.

Proof:

We will first demonstrate more general results. Then we will obtain our results as consequences as particular cases. Following the sequence of propositions in this section.

Lemma 5.1.2. There exists a *linearly independent set* of $\mathbb{F}_2^n$, $(a_i)_{i=1}^{n-1}$, such that $tr(a_1) = \cdots = tr(a_{n-1}) = 0$.

Proof:

Let $\mathcal{B} = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ be a *basis* over $\mathbb{F}_{2^n}$ with α a *primitive element* of the field. If we select $\mathcal{B}$ such that it contains elements whose trace is 1 then we can consider the maximal subsets of $\mathcal{B}$: $\{\alpha^{e_1}, \cdots, \alpha^{e_p}\}$ and $\{\alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$, such that $tr(\alpha^{e_i}) = 1$, for $i \leq p$, and $tr(\alpha^{e_i}) = 0$, for $p < i$, for some p.

Thus the set of $n-1$ vectors $\{\alpha^{e_1} + \alpha^{e_2}, \cdots, \alpha^{e_1} + \alpha^{e_p}, \alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$ are *linearly independent* (because of definition of linear independence) and have trace 0.

Lemma 5.1.3. There exist a *basis* in $\mathbb{F}_2^n$, $(a_i)_{i=1}^{n}$, where its basis vectors have trace 1.

Proof:

Half of the elements in the vector space $\mathbb{F}_2^n$ have trace equal to 1. Any vector v of trace 1 can be spanned by a linear combination of basis vectors because taking the trace of v is the same as taking the trace of the basis vectors. As such, there must exist at least one vector $\alpha^{e_1} \in \mathcal{B}$ such that $tr(\alpha^{e_1}) = 1$.

Consider the maximal subsets of $\mathcal{B}$: $\{\alpha^{e_1}, \cdots, \alpha^{e_p}\}$ and $\{\alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$, such that $tr(\alpha^{e_i}) = 1$, for $i \leq p$, and $tr(\alpha^{e_i}) = 0$, for $p < i$, for some p. Then the set of n vectors $\{\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_p}, \alpha^{e_1} + \alpha^{e_{p+1}}, \cdots, \alpha^{e_1} + \alpha^{e_n}\}$ is also a *basis* in $\mathbb{F}_2^n$ where its elements have trace 1.

Lemma 5.1.4. Let $c \in \mathbb{F}_{2^n}$, $i_1, i_2, \cdots, i_l \in \mathbb{N}$, $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{j+l}}]$ a polynomial with coefficients in $\mathbb{F}_2$, and $tr(a_1) = \cdots = tr(a_j) = 0$. Then, the equation

$$x + \mathcal{P}(tr(a_1 x), \cdots, tr(a_j x), tr(x^{2^{i_1}+1} + x\, tr(1)), \cdots, tr(x^{2^{i_l}+1} + x\, tr(1))) = c,$$

has only one solution,

$$x = c + \mathcal{P}(tr(a_1 c), \cdots, tr(a_j c), tr(c^{2^{i_1}+1} + c\, tr(1)), \cdots, tr(c^{2^{i_l}+1} + c\, tr(1))).$$

Proof:

Uniqueness: Let $\varphi(x) := x + P(x)$, where $P(x) := \mathcal{P}(tr(a_1x), \cdots, tr(a_jx), tr(x^{2^{i_1}+1} + x\,tr(1)), \cdots, tr(x^{2^{i_l}+1} + x\,tr(1)))$. The equation for x, $\varphi(x) = c$, implies $x = c + P(x)$, where the algebraic expression $P(x)$ is Boolean, i.e. $P(x) \in \{0, 1\}, \forall x \in \mathbb{F}_{2^n}$. Then, the equation $\varphi(x) = c$, has only two possible solutions, c and $c + 1$. If x_0 is a solution for that equation, then $x_0 + 1$ is not a solution: $\varphi(x_0 + 1) = x_0 + 1 + P(x_0 + 1) = x_0 + P(x_0) + 1 = \varphi(x_0) + 1 \neq \varphi(x_0) = c$, because of the identity $P(x + 1) = P(x)$ on $\mathbb{F}_{2^n}$, in the next paragraph. Then the solution for this equation is unique.

Identity $P(x + 1) = P(x)$ on $\mathbb{F}_{2^n}$: $P(x + 1) = \mathcal{P}(tr(a_1x), \cdots, tr(a_jx), tr(x^{2^{i_1}+1} + 1 + xtr(1) + tr(1)), \cdots, tr(x^{2^{i_l}+1}+1+xtr(1)+tr(1))) = \mathcal{P}(tr(a_1x), \cdots, tr(a_jx), tr(x^{2^{i_1}+1}+x\,tr(1)), \cdots, tr(x^{2^{i_l}+1}+x\,tr(1))) = P(x)$, on $\mathbb{F}_{2^n}$, because of $tr(a_1) = \cdots = tr(a_j) = 0$, and $tr(x + 1)^{2^k+1} = tr(x^{2^k+1} + 1)$ on $\mathbb{F}_{2^n}$, $\forall k \in \mathbb{N}$.

Form of the Solution: Along the lines of the proof of Lemma 2.2.1, we consider the following form of the solution, $x = c + P(c)$. If $P(c) = 0$, then $\varphi(c + P(c)) = \varphi(c) = c + P(c) = c + 0 = c$. On the other hand, if $P(c) = 1$, then $\varphi(c + P(c)) = \varphi(c + 1) = \varphi(c) + 1 = c + P(c) + 1 = c + 1 + 1 = c$, as in a previous calculations, where $\varphi(x_0 + 1) = \varphi(x_0) + 1$. Therefore in both cases $x = c + P(c)$ is the solution for the given equation, $\varphi(x) = c$.

Theorem 5.1.5. [Differentially γ-Uniform Polynomial] Let $tr(a_1) = \cdots = tr(a_j) = 0$ over $\mathbb{F}_{2^n}$, F a *differentially δ-uniform* function, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{j+l}}]$ a polynomial with coefficients in $\mathbb{F}_2$. Then, the family of functions:

$$f(x) = F(x + \mathcal{P}(tr(a_1x), \cdots, tr(a_jx), tr(x^{2^{i_1}+1} + x\,tr(1)), \cdots, tr(x^{2^{i_l}+1} + x\,tr(1))))$$

is *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $j + l \geq 1$, and each $i_k \in \mathbb{N}$.

Proof:

Given $a \neq 0$, b, both in $\mathbb{F}_{2^n}$, considering the corresponding differential equation for f to be studied:

$$D_af(x) = F(x + P(x) + P(x + a) - P(x) + a) - F(x + P(x)) = b,$$

where $P(x) := \mathcal{P}(tr(a_1x), \cdots, tr(a_jx), tr(x^{2^{i_1}+1} + x\,tr(1)), \cdots, tr(x^{2^{i_l}+1} + x\,tr(1)))$, the same notation as in the previous Lemma.

Since $P(x+a)-P(x)$ is a Boolean function, for $a=1$, it is possible that the term $P(x+a)-P(x)+a$ becomes zero, then the equation for $b=0$ is reduced to the following equation, $D_1f(x)=F(x+P(x))-F(x+P(x))=0$, on $\mathbb{F}_{2^n}\cap\{x\in\mathbb{F}_{2^n};\, P(x+1)+1=P(x)\}$.

Case $a\neq 1$. **Subcase** $P(x+a)-P(x)=0$: The equation $D_af(x)=b$ becomes:

$$F(x+P(x)+a)-F(x+P(x))=b$$

Because F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y=x+P(x)$, which will be denoted by $y=y_t$ and $y=y_t+a$, for $1\leq t\leq\frac{\delta}{2}$. In the following steps we solve the equations in x, $x+P(x)=y$, for each value of y.

The equation $x+P(x)=y_t,$ by Lemma 5.1.2, has the unique solution $x=y_t+P(y_t)$, for $1\leq t\leq\frac{\delta}{2}$.
The equation $x+P(x)=y_t+a,$ by Lemma 5.1.2, has the unique solution $x=y_t+a+P(y_t+a)$, for $1\leq t\leq\frac{\delta}{2}$.

Then, there are at most δ solutions.

Subcase $P(x+a)-P(x)=1$: The equation $D_af(x)=b$ becomes:

$$F(x+P(x)+a+1)-F(x+P(x))=b$$

Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y=x+P(x)$, which will be denoted by $y=z_t$ and $y=z_t+a+1$, for $1\leq t\leq\frac{\delta}{2}$. In the following we will try to solve the equations in x, $x+P(x)=y$, for each value of y.

The equation $x+P(x)=z_t,$ by Lemma 5.1.2, has the unique solution $x=z_t+P(z_t)$, for $1\leq t\leq\frac{\delta}{2}$.
The equation $x+P(x)=z_t+a+1,$ by Lemma 5.1.2, has the unique solution $x=z_t+a+1+P(z_t+a+1)=z_t+a+1+P(z_t+a)$, because of the identity, $P(x+1)=P(x)$, on $\mathbb{F}_{2^n}$, for $1\leq t\leq\frac{\delta}{2}$.

Then, there are at most δ solutions.

Case $a=1$. $D_1f(x)=F(x+P(x)+1)-F(x+P(x))=b$, because of the identity, $P(x+1)=P(x)$, on $\mathbb{F}_{2^n}$, this equation can be treated as the equations that appear in the case for $a\neq 1$. So the equation $D_1f(x)=b$ has at most δ solutions.

In conclusion, for any $a \neq 0,\ b$, both in $\mathbb{F}_{2^n}$, the equation $D_a f(x) = b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$.

Remark Apply this Theorem to the *differentially* $\{2,4\}$-*uniform* permutations F (Gold and Kasami subfamilies), refer to Gold in [23], Janwa and Wilson in [24], Nyberg in [30], and others in [33], [40], [11].

For any $a \in \mathbb{F}_{2^n}$, let $S_a = \{x \in \mathbb{F}_{2^n};\ tr(ax) = 0\}$ its corresponding $\mathbb{F}_2$- vector subspace of $\mathbb{F}_{2^n}$, and the set $H_a = \{x \in \mathbb{F}_{2^n};\ tr(ax) = 1\}$ its hyperplane, respectively. For $a \neq 0$, $\dim S_a = n - 1$.

Lemma 5.1.6. Let $a_1 \neq a_2$ two nonzero elements in $\mathbb{F}_{2^n}$. Then:

$|S_{a_1} \cap S_{a_2}| = |\{x \in \mathbb{F}_{2^n};\ tr(a_1 x) = tr(a_2 x) = 0\}| = 2^{n-2}$.

Proof:

S is a 1-1 transformation: $S : \mathbb{F}_{2^n}^* \to \mathcal{L}_{n-1}(\mathbb{F}_2^n)$ where $\mathcal{L}_{n-1}(\mathbb{F}_2^n)$ represents the set of all linear

$$a \qquad S_a$$

subspaces of dimension $n-1$ of the linear space $\mathbb{F}_2^n$.

Let $a_1 \neq a_2$. If we have $S_{a_1} = S_{a_2}$, then:

$$\forall x \in \mathbb{F}_{2^n}, tr(a_1 x) = 0 \Longleftrightarrow tr(a_2 x) = 0$$

$$\forall x \in \mathbb{F}_{2^n}, tr(a_1 x) \neq 0 \Longleftrightarrow tr(a_2 x) \neq 0$$

$$\forall x \in \mathbb{F}_{2^n}, tr((a_1 + a_2)x) = tr(a_1 x) + tr(a_2 x) = 0.$$

Thus for $a_1 + a_2 \neq 0$ we have $|S_{a_1+a_2}| = 2^n$. This contradicts that the cardinality of proper subspaces S_a (for each $a \in \mathbb{F}_{2^n}^*$) is $|S_a| = 2^{n-1}$. Thus $S_{a_1} \neq S_{a_2}$.

If $a_1 \neq a_2 \in \mathbb{F}_{2^n}^*$ we know that $dim(S_{a_1}) = dim(S_{a_2}) = n - 1$. Let $\mathcal{B} = (x_i)_{i=1}^{n-1}$ be a basis for S_{a_1}, and $x_n \in \mathbb{F}_{2^n}$ such that $\mathcal{B} \cup \{x_n\}$ is a basis for $\mathbb{F}_{2^n}$. Furthermore, let $\mathcal{B}' = (x_i')_{i=1}^{n-1}$ be a basis for S_{a_2}, and $x_n' \in \mathbb{F}_{2^n}$ such that $\mathcal{B}' \cup \{x_n'\}$ is a basis for $\mathbb{F}_{2^n}$.

Now lets consider $S_{a_1} \neq S_{a_2}$, $dim(S_{a_1}) = dim(S_{a_2})$, and $dim(S_{a_1}) + 1 = dim(\mathbb{F}_{2^n})$, then there exist a unique vector (say x_{n-1}) in $\mathcal{B}$ that we cannot obtain from a linear combination of vectors in $\mathcal{B}'$, and vice versa.

We know that $k(\in \mathbb{N})$ *linearly independent* vectors can generate (via linear combinations) sets of exactly k *linearly independent* vectors (since the space generated by their span is the same up to isomorphism). Since $\mathcal{B}'$ does not generate x_{n-1} it must then generate the $n-1$ *linearly independent* vectors in $\mathcal{B} \cup \{x_n\} - \{x_{n-1}\}$. As a consequence, $\mathcal{B}'$ generate the $n-2$ vectors in $\mathcal{B}$, $x_1, .., x_{n-2}$, i.e. $\mathcal{B} \cap S_{a_2} = \{x_1, \cdots, x_{n-2}\}$. Thus the subspace $S_{a_2} \cap S_{a_2}$ is such that $Span(\{x_1, \cdots, x_{n-2}\}) \subseteq S_{a_2} \cap S_{a_2}$.

Let $x \neq 0 \in S_{a_1} \cap S_{a_2}$, then $\sum_{i=1}^{n-2} c_i x_i + c_{n-1}x_{n-1} = x = \sum_{i=1}^{n-1} c'_i x'_i$. Since $\forall x_i (1 \leq i \leq n-2) \in Span(\mathcal{B}')$, then $c_{n-1}x_{n-1} = \sum_{i=1}^{n-1} c''_i x'_i \in Span(\mathcal{B}')$. Since $x_{n-1} \notin Span(\mathcal{B}')$, then $c_{n-1} = 0$. Thus, $x = c_1x_1 + \cdots + c_{n-2}x_{n-2} + 0x_{n-1} = c_1x_1 + \cdots + c_{n-2}x_{n-2}$, i.e. $x \in Span(\{x_1, \cdots, x_{n-2}\})$.

This means that $S_{a_1} \cap S_{a_2}$ is an $\mathbb{F}_2$ - vector subspace of S_{a_1} (and S_{a_2}) of one dimension less, $dim(S_{a_1} \cap S_{a_2}) = n-2$ and $|S_{a_1} \cap S_{a_2}| = 2^{n-2}$.

Remark To prove the Lemma 5.1.6 we can also apply the theorem for the dimension of a sum of subspaces of a finite dimensional vector space.

Lemma 5.1.7. Let $a_1 \neq a_2$ two nonzero elements in $\mathbb{F}_{2^n}$. Then the intersections $S_{a_1} \cap S_{a_2}$, $S_{a_1} \cap H_{a_2}$, $H_{a_1} \cap S_{a_2}$, and $H_{a_1} \cap H_{a_2}$ form a partition of $\mathbb{F}_{2^n}$, such that:

$|S_{a_1} \cap S_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = 0\}| = 2^{n-2}$,

$|S_{a_1} \cap H_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = 0,\, tr(a_2x) = 1\}| = 2^{n-2}$,

$|H_{a_1} \cap S_{a_2}| = \{x \in \mathbb{F}_{2^n};\, tr(a_1x) = 1,\, tr(a_2x) = 0\}| = 2^{n-2}$,

$|H_{a_1} \cap H_{a_2}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = 1\}| = 2^{n-2}$.

Proof:

The previous Lemma states that, $S_{a_1} \cap S_{a_2}$ is an $\mathbb{F}_2$ - vector subspace of S_{a_1} such that, $dim(S_{a_1} \cap S_{a_2}) = n-2$ and $|S_{a_1} \cap S_{a_2}| = 2^{n-2}$. From $|S_{a_1}| = 2^{n-1}$, and that $\{S_{a_1} \cap S_{a_2},\, S_{a_1} \cap H_{a_2}\}$ defines a partition for S_{a_1}, then $|S_{a_1} \cap H_{a_2}| = 2^{n-2}$.

Let $a = a_1 + a_2$. Then $|S_a| = |\{x \in \mathbb{F}_{2^n};\, tr(ax) = 0\}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x)\}| = 2^{n-1}$, is the number of points where the two linear functions, $tr(a_1x)$ and $tr(a_2x)$, agree, that is $|S_{a_1} \cap S_{a_2}| + |H_{a_1} \cap H_{a_2}|$. Then $|H_{a_1} \cap H_{a_2}| = 2^{n-2}$. On the other hand, $|H_a| = |\{x \in \mathbb{F}_{2^n};\, tr(ax) = 1\}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) \neq tr(a_2x)\} = 2^{n-1}$, is the number of points where the two linear functions are different, that is $|S_{a_1} \cap H_{a_2}| + |H_{a_1} \cap S_{a_2}|$. Then $|H_{a_1} \cap S_{a_2}| = 2^{n-2}$.

Lemma 5.1.8. Let $\{a_i \in \mathbb{F}_{2^n};\, i = 1, 2, 3\}$ be a $\mathbb{F}_2$- *linearly independent* set of $\mathbb{F}_2^n$, such that $|S_{a_i} \cap S_{a_j}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_ix) = tr(a_jx) = 0\}| = 2^{n-2}$, for all $i \neq j$. Then, the intersections $S_{a_1} \cap S_{a_2} \cap S_{a_3}$, $S_{a_i} \cap S_{a_j} \cap H_{a_k}$, $S_{a_i} \cap H_{a_j} \cap H_{a_k}$, and $H_{a_1} \cap H_{a_2} \cap H_{a_3}$ form a partition of $\mathbb{F}_{2^n}$, such that:

$|S_{a_1} \cap S_{a_2} \cap S_{a_3}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = tr(a_3x) = 0\}| = 2^{n-3}$,

$|S_{a_i} \cap S_{a_j} \cap H_{a_k}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_ix) = tr(a_jx) = 0,\, tr(a_kx) = 1\}| = 2^{n-3}$,

$|S_{a_i} \cap H_{a_j} \cap H_{a_k}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_ix) = 0,\, tr(a_jx) = tr(a_kx) = 1\}| = 2^{n-3}$,

$|H_{a_1} \cap H_{a_2} \cap H_{a_3}| = |\{x \in \mathbb{F}_{2^n};\, tr(a_1x) = tr(a_2x) = tr(a_3x) = 1\}| = 2^{n-3}$, for all i, j, k different from each other.

Proof: We denote by $\tilde{t}_{i,j,k} = \{x \in \mathbb{F}_{2^n};\, tr(a_1x) = i,\, tr(a_2x) = j,\, tr(a_3x) = k\}$, and $t_{i,j,k} = |\tilde{t}_{i,j,k}|$, for any $(i,\, j,\, k) \in \mathbb{F}_2^3$. From $\{a_i\}_{i=1}^3$ linearly independent, $a_1 + a_2 + a_3 \neq 0$, $|S_{a_1+a_2+a_3} = \{x \in \mathbb{F}_{2^n};\, tr(a_1x) + tr(a_2x) = tr(a_3x)\}| = 2^{n-1}$. The set $\{\tilde{t}_{0,0,0},\, \tilde{t}_{0,1,1},\, \tilde{t}_{1,0,1},\, \tilde{t}_{1,1,0}\}$ defines a partition of $S_{a_1+a_2+a_3}$, then $t_{0,0,0} + t_{0,1,1} + t_{1,0,1} + t_{1,1,0} = |S_{a_1+a_2+a_3}| = 2^{n-1}$.

Also, the set $\{\tilde{t}_{0,0,1},\, \tilde{t}_{0,1,0},\, \tilde{t}_{1,0,0},\, \tilde{t}_{1,1,1}\}$ defines a partition of $H_{a_1+a_2+a_3} = \{x \in \mathbb{F}_{2^n};\, tr(a_1x) + tr(a_2x) = tr(a_3x) + 1\}$, then $t_{0,0,1} + t_{0,1,0} + t_{1,0,0} + t_{1,1,1} = |H_{a_1+a_2+a_3}| = 2^n - |S_{a_1+a_2+a_3}| = 2^{n-1}$.

From the hypothesis $|S_{a_i} \cap S_{a_j}| = 2^{n-2}$, as in the demonstration of the previous Lemma, we have a common cardinality: $|S_{a_i} \cap H_{a_j}| = |H_{a_i} \cap S_{a_j}| = |H_{a_i} \cap H_{a_j}| = 2^{n-2}$, for all $i \neq j$ in $\{1,\, 2,\, 3\}$.

Then, taking into account the partitions, we have the following system of 14 linear equations in the 8 variables, $t_{i,j,k}$:

$t_{0,0,0} + t_{0,0,1} = |S_{a_1} \cap S_{a_2}| = 2^{n-2}$, $t_{0,0,0} + t_{1,0,0} = |S_{a_2} \cap S_{a_3}| = 2^{n-2}$,

$t_{0,0,0} + t_{0,1,0} = |S_{a_1} \cap S_{a_3}| = 2^{n-2}$, $t_{0,1,1} + t_{0,1,0} = |S_{a_1} \cap H_{a_2}| = 2^{n-2}$,

$t_{0,1,1} + t_{1,1,1} = |H_{a_2} \cap H_{a_3}| = 2^{n-2}$, $t_{0,1,1} + t_{0,0,1} = |S_{a_1} \cap H_{a_3}| = 2^{n-2}$,

$t_{1,0,1} + t_{1,0,0} = |H_{a_1} \cap S_{a_2}| = 2^{n-2}$, $t_{1,0,1} + t_{0,0,1} = |S_{a_2} \cap H_{a_3}| = 2^{n-2}$,

$t_{1,0,1} + t_{1,1,1} = |H_{a_1} \cap H_{a_3}| = 2^{n-2}$, $t_{1,1,0} + t_{1,1,1} = |H_{a_1} \cap H_{a_2}| = 2^{n-2}$,

$t_{1,1,0} + t_{0,1,0} = |H_{a_2} \cap S_{a_3}| = 2^{n-2}$, $t_{1,1,0} + t_{1,0,0} = |H_{a_1} \cap S_{a_3}| = 2^{n-2}$,

$t_{0,0,0} + t_{0,1,1} + t_{1,0,1} + t_{1,1,0} = |S_{a_1+a_2+a_3}| = 2^{n-1}$, $t_{0,0,1} + t_{0,1,0} + t_{1,0,0} + t_{1,1,1} = |H_{a_1+a_2+a_3}| = 2^{n-1}$.

$S_{a_1} \cap S_{a_2} \cap S_{a_3}$ is an $\mathbb{F}_2$ - vector subspace of $S_{a_i} \cap S_{a_j}$, for any $i \neq j$, of one less or same dimension, i.e. $|S_{a_1} \cap S_{a_2} \cap S_{a_3}| = 2^{n-2}$ (or 2^{n-3}). Then, from the first three equations, $t_{0,0,1} = t_{1,0,0} = t_{0,1,0} = 0$ or 2^{n-3}, respectively. Substituting in the equation (14): $t_{1,1,1} = 2^{n-1}$ or 2^{n-3}, respectively. Now, substituting $t_{1,1,1} = 2^{n-1}$ in the equation (5):

$t_{0,1,1} = 2^{n-2} - 2^{n-1}$ (contradiction with $t_{0,1,1} \in \mathbb{N} \cup \{0\}$). Then $t_{1,1,1} = 2^{n-3}$ and $t_{0,1,1} = 2^{n-2} - 2^{n-3} = 2^{n-3}$. Also, from the equation (14), $3\,t_{0,0,1} + 2^{n-3} = 2^{n-1}$, i.e. $t_{0,0,1} = t_{1,0,0} = t_{0,1,0} = 2^{n-3}$.

Doing back substitution. From the first equation, $t_{0,0,0} = 2^{n-3}$. From equations (7), (12):

$t_{1,0,1} = |H_{a_1} \cap S_{a_2}| - t_{1,0,0} = 2^{n-3}$, $t_{1,1,0} = |H_{a_1} \cap S_{a_3}| - t_{1,0,0} = 2^{n-3}$. All the equations are satisfied. In summary $t_{i,j,k} = 2^{n-3}$.

Theorem 5.1.9. [On the Distribution of Zeros in Affine Functions] Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set* of $\mathbb{F}_2^n$, the sets $S_{a_i} = Kernel(tr(a_i x)) = \{x \in \mathbb{F}_{2^n};\, tr(a_i x) = 0\}$ its corresponding $\mathbb{F}_2$ - vector subspaces of $\mathbb{F}_{2^n}$, and $H_{a_i} = \{x \in \mathbb{F}_{2^n};\, tr(a_i x) = 1\}$ its hyperplanes. Then, the intersections of the form $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-1}}}$, $H_{a_{i_1}} \cap S_{a_{i_2}} \cap \cdots \cap S_{a_{i_{n-1}}}$, $H_{a_{i_1}} \cap H_{a_{i_2}} \cap S_{a_{i_3}} \cap \cdots \cap S_{a_{i_{n-1}}}$,$\cdots$, and $H_{a_{i_1}} \cap \cdots \cap H_{a_{i_{n-1}}}$ form a partition of $\mathbb{F}_{2^n}$. Also, $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = 2^{n-(n-1)} = 2^1$, where $U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}$ denotes any partition element.

Proof: It is sufficient to demonstrate that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_k}}| = 2^{n-k}$, for all $U_{a_{i_1}}, \cdots U_{a_{i_k}}$, for all $1 \leq k \leq n-1$. In particular it follows the theorem. Proceeding by *induction*:

We use the Lemmas 5.1.7 and 5.1.8 for some beginning values for n:

For $n = 2$: $|U_{a_{i_1}}| = 2^{n-1} = 2^1$.

For $n = 3$: $|U_{a_{i_1}}| = 2^{n-1} = 2^2$; $|U_{a_{i_1}} \cap U_{a_{i_2}}| = 2^{n-2} = 2^1$.

For $n = 4$: $|U_{a_{i_1}}| = 2^{n-1} = 2^3$; $|U_{a_{i_1}} \cap U_{a_{i_2}}| = 2^{n-2} = 2^2$; $|U_{a_{i_1}} \cap U_{a_{i_2}} \cap U_{a_{i_3}}| = 2^{n-3} = 2^1$.

The induction hypothesis: Supposing true up to $K = n-2$, i.e. let $\{a_{i_1}, \cdots, a_{i_{n-2}}\}$ a *linearly independent set*, such that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_k}}| = 2^{n-k}$, for all $1 \leq k \leq n-2$.

Induction Step: To demonstrate for $K+1 = n-1$, $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = 2^{n-(n-1)} = 2^1$, for all $U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}$:

To define by $\tilde{t}_{l_{i_1},\cdots,l_{i_k}} := \{x \in \mathbb{F}_{2^n};\, tr(a_{i_1}x) = l_{i_1}, \cdots,\, tr(a_{i_k}x) = l_{i_k}\}$, and $t_{l_{i_1},\cdots,l_{i_k}} = |\tilde{t}_{l_{i_1},\cdots,l_{i_k}}|$, $\forall$ $(l_{i_1}, \cdots, l_{i_k}) \in \mathbb{F}_2^k$, where $1 \leq k \leq n-1$. Systems of equations:

Those that add to zero: By the induction hypothesis $\{a_i\}_{i=1}^{n-1}$ are linearly independent, $a_1 + \cdots + a_{n-1} \neq 0$. Then $2^{n-1} = |S_{a_1+\cdots+a_{n-1}} = \{x \in \mathbb{F}_{2^n};\, tr((a_1+\cdots+a_{n-1})x) = tr(a_1x)+\cdots+tr(a_{n-1}x) = l_1 + \cdots + l_{n-1} = 0\}| = t_{0_{i_1},\cdots,0_{i_{n-1}}} + \sum_{(l_{i_1},\cdots,l_{i_{n-1}}) \in \mathbb{F}_2^{n-1} \text{ has even } 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}}$.

Those that add to one: Also, $2^{n-1} = 2^n - |S_{a_1+\cdots+a_{n-1}}| = |H_{a_1+\cdots+a_{n-1}} = \{x \in \mathbb{F}_{2^n};\, tr((a_1 + \cdots + a_{n-1})x) = l_1 + \cdots + l_{n-1} = 1\}| = \sum_{(l_{i_1},\cdots,l_{i_{n-1}}) \in \mathbb{F}_2^{n-1} \text{ has odd } 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}}$.

To define by $\bar{t}_{l_{i_{k+1}},\cdots,l_{i_{n-1}}} := t_{l_{i_1},\cdots,l_{i_k},l_{i_{k+1}},\cdots,l_{i_{n-1}}}$, where $l_{i_1}, \cdots, l_{i_k}$ are the fixed values, $l_{i_{k+1}}, \cdots, l_{i_{n-1}}$ are the free values. Then we have the identity $\sum_{(l_{i_{k+1}},\cdots,l_{i_{n-1}}) \in \mathbb{F}_2^{n-1-k}} \bar{t}_{l_{i_{k+1}},\cdots,l_{i_{n-1}}} = t_{l_{i_1},\cdots,l_{i_k}}$. The induction hypothesis yields the following systems of equations:

From $n-1$ factors $(U_{a_{i_j}})$, $n-2$ fixed values, and 1 free value:

$$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = |U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-2}}}| = 2^{n-(n-2)} = 2^2.$$

From $n-1$, $n-3$ fixed values, and 2 free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^{n-(n-3)} = 2^3.$$

From $n-1$, $n-4$ fixed values, and 3 free values:

$$\bar{t}_{0_{i_{n-3}}0_{i_{n-2}}0_{i_{n-1}}} + \sum_{(l_{i_{n-3}},l_{i_{n-2}},l_{i_{n-1}})\in\mathbb{F}_2^3 \, has\, one\, entry\, 1} \bar{t}_{l_{i_{n-3}}l_{i_{n-2}}l_{i_{n-1}}} + \sum_{(l_{i_{n-3}},l_{i_{n-2}},l_{i_{n-1}})\in\mathbb{F}_2^3 \, has\, two\, entry\, 1's} \bar{t}_{l_{i_{n-3}}l_{i_{n-2}}l_{i_{n-1}}} + \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 2^{n-(n-4)} = 2^4.$$

...

From $n-1$, $n-(\mu+1)$ fixed values, and μ free values:

$$\bar{t}_{0_{i_{n-\mu}}\cdots 0_{i_{n-1}}} + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu} \, has\, one\, entry\, 1} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu} \, has\, two\, entry\, 1's} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \cdots + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu} \, has\, \mu-1\, entry\, 1's} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \bar{t}_{1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = 2^{n-(n-(\mu+1))} = 2^{\mu+1}.$$

...

From $n-1$, 1 fixed value, and $n-2$ free values:

$$\bar{t}_{0_{i_2}\cdots 0_{i_{n-1}}} + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{n-2} \, has\, one\, entry\, 1} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{n-2} \, has\, two\, entry\, 1's} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \cdots + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{n-2} \, has\, n-3\, entry\, 1's} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^{n-1}.$$

The intersection $(S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}) \cap S_{a_{i_{n-1}}}$ is a $\mathbb{F}_2$ - vector subspace of $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}$, then, it has one less or the same dimension that of the space $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}$. Then:

$$t_{0_{i_1}\cdots 0_{i_{n-1}}} = |\bigcap_{j=1}^{n-1} S_{a_{i_j}}| = \begin{cases} |\bigcap_{j=1}^{n-2} S_{a_{i_j}}| = 2^{n-(n-2)} = 2^2, & \text{if } dim(\bigcap_{j=1}^{n-1} S_{a_{i_j}}) = dim(\bigcap_{j=1}^{n-2} S_{a_{i_j}}) \\ 2^{-1}|\bigcap_{j=1}^{n-2} S_{a_{i_j}}| = 2^1, & \text{if } dim(\bigcap_{j=1}^{n-1} S_{a_{i_j}}) = dim(\bigcap_{j=1}^{n-2} S_{a_{i_j}}) - 1 \end{cases} \tag{9}$$

Case If $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$: Substituting in the last system of equations:

From $n-1$, $n-2$ fixed values, in particular to be 0, and 1 free value:

$$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = 2^2,\ \bar{t}_{0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}},\ \text{then } \bar{t}_{1_{i_{n-1}}} = 2^2 - 2^1 = 2^1.$$

From $n-1$, $n-3$ fixed values, in particular to be 0, and 2 free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3,$$

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}}, \quad \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}}, \quad \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}},$$

$$\text{then:} \quad \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3 - 3(2^1) = 2^1.$$

...

From $n-1$, $n-\mu-1$ fixed values, in particular to be 0, and μ free values, for $1 \leq \mu \leq n-2$ (from the inductive hypothesis):

$$\sum_{j=0}^{\mu} \binom{\mu}{j} \bar{t}_{\substack{l_{i_{n-\mu}}\cdots l_{i_{n-1}} \\ ((l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \\ \text{has } j \text{ entries } 1's)}} = 2^{\mu+1}.$$

We obtain the constant sequence: $\bar{t}_{1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = \cdots = \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^1$.

Case If $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^2$: Again substituting in the system of equations:

From $n-1$, $n-2$ fixed values, in particular to be 0, and 1 free value:

$$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = 2^2, \; \bar{t}_{0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}}, \text{ then } \bar{t}_{1_{i_{n-1}}} = 2^2 - 2^2 = 0, \text{ for } \bar{t}_{1_{i_{n-1}}} \text{ arbitrary.}$$

From $n-1$, $n-3$ fixed values, in particular to be 0, and 2 free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3,$$

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}}, \quad \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}} = 0, \text{ substituting the last identity}$$

$$\text{then:} \quad \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3 - 2^2 = 2^2, \text{ for } \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} \text{ arbitrary.}$$

From $n-1$, $n-4$ fixed values, in particular to be 0, and 3 free values:

$$2^2 + 3(0) + 3(2^2) + \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 2^4,$$

$$\text{then:} \quad \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 0, \text{ for } \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} \text{ arbitrary.}$$

We obtain the alternating sequence:

$$\bar{t}_{\substack{l_{i_{n-\mu}}\cdots l_{i_{n-1}} \\ ((l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \\ \text{has } \mu \text{ free values})}} = \begin{cases} 0, \; if\,(l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \text{ contains an odd number of 1's} \\ 4, \; if\,(l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \text{ contains an even number of 1's,} \end{cases} \tag{10}$$

$\forall\, 1 \leq \mu \leq n-2$.

Substituting in the equation:

$$2^{n-1} = |H_{a_1+\cdots+a_{n-1}}| = \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ odd\ 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}} =$$

$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ one\ entry\ 1} \bar{t}_{1_{i_{n-1}}} + \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ three\ entry\ 1's} \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} + \cdots +$$

$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ n-3\ entry\ 1's} \bar{t}_{1_{i_3}\cdots 1_{i_{n-1}}} \text{ or } \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ n-2\ entry\ 1's} \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} +$$

$$\text{possibly } t_{\substack{1_{i_1}\cdots 1_{i_{n-1}} \\ (\text{all } n-1 \text{ places} \\ \text{are } 1's)}} = 2^{n-1}.$$

I.e.:

$$0 + \cdots + 0 + \text{possibly } t_{\substack{1_{i_1}\cdots 1_{i_{n-1}} \\ (\text{all } n-1 \text{ places} \\ \text{are } 1's)}} = 2^{n-1}.$$

Then term $t_{1_{i_1}\cdots 1_{i_{n-1}}}$ needs to be present and can't be 0; it is $t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^{n-1}$.

From the inductive hypothesis we have:

$$t_{l_{i_1}\cdots l_{i_{n-2}}} = |U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-2}}}| = 2^{n-(n-2)} = 2^2$$

In particular:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}} = |H_{a_{i_1}} \cap \cdots \cap H_{a_{i_{n-2}}}| = 2^2.$$

By definition:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} + t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-2}}}$$

Then substituting the last equations:

$$2^{n-1} = t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^2 - t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} \leq 2^2, \text{ where } t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} \geq 0, \ \forall n \geq 4.$$

For $n \leq 3$ the theorem is true, from the previous lemmas, Lemma 5.1.7 and 5.1.8.

Then $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^2$ is not true. Then, $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$, then for this case we have the corresponding *constant sequence*:

$$\bar{t}_{1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = \cdots = \bar{t}_{\substack{1_{i_{n-\mu}}\cdots 1_{i_{n-1}} \\ ((l_{i_1},\cdots,l_{i_{n-1}})\ \text{has}\ \mu\ \text{entry}\ 1's)}} = \cdots = \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^1$$

Equivalently:

$$t_{0_{i_1}\cdots 0_{i_{n-2}}1_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = \cdots = t_{0_{i_1}\cdots 0_{i_{n-\mu-1}}1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = \cdots = t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = 2^1,$$

for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$ places, $1 \leq \mu \leq n-2$.

It remains to see what happens in the case of $n-1$ ones, $t_{1_{i_1}\cdots 1_{i_{n-1}}}$. By back substitution, this is by substituting the last equation (which has $n-2$ ones and 1 zero) of the constant sequence, $t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = 2^1$, for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$ places (then also $t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} = 2^1$), into the equation:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} + t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-2}}}$$

$$t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = 2^2 - 2^1 = 2^1.$$

Then, with the last equation $t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^1$, and $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$, the *constant sequence* is completed:

$$t_{0_{i_1}\cdots 0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-2}}1_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = \cdots = t_{0_{i_1}\cdots 0_{i_{n-\mu-1}}1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = \cdots =$$
$$t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^1,$$

for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$ places, $1 \leq \mu \leq n-2$.

Which means that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = t_{l_{i_1}\cdots l_{i_{n-1}}} = 2^1$, $\forall\ l_{i_1}\cdots l_{i_{n-1}}$, $(l_{i_1}, \cdots, l_{i_{n-1}})$ contains any number of ones, from 0 up to $n-1$. Then $|U_{a_1} \cap \cdots \cap U_{a_{n-1}}| = 2^1$, for all $U_{a_1}, \cdots, U_{a_{n-1}}$.

Corollary 5.1.10. Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set* of $\mathbb{F}_2^n$, and φ a function on $\mathbb{F}_{2^n}$, define the sets $\widetilde{H}_{a_i} := \{x \in \mathbb{F}_{2^n};\ tr(a_i\varphi(x)) = 1\}$. Then

$$|\widetilde{H}_{a_{i_1}} \cap \cdots \cap \widetilde{H}_{a_{i_{n-1}}}| = |\varphi^{-1}[\{v_0,\, v_1\}]|, \text{ where } H_{a_1} \cap \cdots \cap H_{a_{n-1}} = \{v_0,\, v_1\}.$$

In particular, if φ is a *permutation*, then $|\widetilde{H}_{a_{i_1}} \cap \cdots \cap \widetilde{H}_{a_{i_{n-1}}}| = 2^1$.

Corollary 5.1.11. Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set*, and be $0 \notin (h_i)_{i=1}^{l}$ a sequence of different elements, on $\mathbb{F}_{2^n}$. Defining $a_i^{(j)} := a_i h_j$, where each $h_j \neq 1$, then

$$\{x \in \mathbb{F}_{2^n};\ tr(a_1x), \cdots tr(a_{n-1}x) + tr(a_1^{(1)}x)\cdots tr(a_{n-1}^{(1)}x) + tr(a_1^{(l)}x)\cdots tr(a_{n-1}^{(l)}x) = 1\}$$

$$\subset (H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup \ \cdots \ \cup (H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}}), \text{ and}$$

$$|(H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup \cdots \cup (H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}})| \leq 2(l+1).$$

Also, one can use the *affine* transformation $a_i^{(j)} := a_i + h_j$.

Moreover, if $H_{a_1} \cap \cdots \cap H_{a_{n-1}}, \cdots, H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}}$ are disjoints, then the following equality is achieved:

$$|\{x \in \mathbb{F}_{2^n};\, tr(a_1 x) \cdots tr(a_{n-1}x) + tr(a_1^{(1)}x) \cdots tr(a_{n-1}^{(1)}x) + tr(a_1^{(l)}x) \cdots tr(a_{n-1}^{(l)}x) = 1\}$$

$$= (H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup \cdots \cup (H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}})| = 2(l+1).$$

Example Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set* on $\mathbb{F}_{2^n}$, define $a_i^{(1)} := a_i h_1$, where $h_1 \neq 0, 1$, moreover $(H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cap (h_1 H_{a_1} \cap \cdots \cap H_{a_{n-1}}) = \emptyset$. Then

$$|\{x \in \mathbb{F}_{2^n};\, tr(a_1 x) \cdots tr(a_{n-1}x) + tr(a_1^{(1)}x) \cdots tr(a_{n-1}^{(1)}x) = 1\}$$

$$= (H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup (H_{a_1^{(1)}} \cap \cdots \cap H_{a_{n-1}^{(1)}})| = 4.$$

Theorem 5.1.6 implies that $|H_{a_1} \cap \cdots \cap H_{a_{n-1}}| = 2^1$, i.e. only two pre images will change, from x to $x+1$, that means: $H_{a_1} \cap \cdots \cap H_{a_{n-1}} = \{x_0, x_1\}$, for some $x_i \in \mathbb{F}_{2^n}^*$.

The given families in the hypothesis of the main theorem (Theorem 5.1.1) belong to the more general family $f(x) = F(x + tr(a_1 x) \cdots tr(a_{n-1}x))$. For f we will make a approximation of its nonlinearity through the nonlinearity for F (which is known):

$$W_f(a,b) = (-1)^{tr(b\,F(x_0+1) + a\,x_0)} + (-1)^{tr(b\,F(x_1+1) + a\,x_1)} + \sum_{x \in \mathbb{F}_{2^n} - \{x_0, x_1\}} (-1)^{tr(b\,F(x) + a\,x)}$$

$$= (-1)^{tr(b\,F(x_0+1) + a\,x_0)} - (-1)^{tr(b\,F(x_0) + a\,x_0)} + (-1)^{tr(b\,F(x_1+1) + a\,x_1)} - (-1)^{tr(b\,F(x_1) + a\,x_1)} + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr(b\,F(x) + a\,x)}$$

$$= (-1)^{tr(b\,F(x_0+1) + a\,x_0)} - (-1)^{tr(b\,F(x_0) + a\,x_0)} + (-1)^{tr(b\,F(x_1+1) + a\,x_1)} - (-1)^{tr(b\,F(x_1) + a\,x_1)} + W_F(a,b)$$

Then:

$$W_f(a,b) - W_F(a,b) = (-1)^{tr(b\,F(x_0+1) + a\,x_0)} - (-1)^{tr(b\,F(x_0) + a\,x_0)} + (-1)^{tr(b\,F(x_1+1) + a\,x_1)} - (-1)^{tr(b\,F(x_1) + a\,x_1)}$$

$$W_f(a,b) - W_F(a,b) = r \in \{0, \pm 2, \pm 4\}.$$

Then we have the following *bounds* for the nonlinearity of f:

$$nl(f) = 2^{n-1} - \tfrac{1}{2} \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_f(a,b)| = 2^{n-1} - \tfrac{1}{2} \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b) + r|.$$

$$nl(F) - \tfrac{|r|}{2} = 2^{n-1} - \tfrac{1}{2}(|r| + \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b)|) \leq nl(f) \leq$$
$$2^{n-1} - \tfrac{1}{2}(-|r| + \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b)|) = nl(F) + \tfrac{|r|}{2}$$
$$nl(f) - nl(F) = \tfrac{r}{2} \in \{0, \pm 1, \pm 2\}.$$

In particular: $nl(f) \geq nl(F) - 2$. Apply this inequality to the functions F (subfamilies of Gold and Kasami), whose nonlinearities are shown on in Table 1 in Section 1.2, we can apply the result of Kaisa Nyberg [30]. The Walsh spectrum of Gold subfamilies can be found in the paper of Edel [21].

Examples *Gold* and *Kasami based permutations*. From Theorem Differentially δ-Uniform polynomial, $\mathcal{G}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x), \cdots, tr(a_jx)$ and $\mathcal{K}(x) = x^{2^{2i}-2^i+1} + (x^{2^{2i}-2^i} + x^{2^{2i}-(2)2^i+1} + x^{2^{2i}-(2)2^i} + x^{2^{2i}-(3)2^i+1} + x^{2^{2i}-(3)2^i} + \cdots + x^{2^i+1} + x^{2^i} + x + 1)tr(a_1x), \cdots, tr(a_jx)$, where $tr(a_1) = \cdots = tr(a_j) = 0$. Cryptographic properties: $\Delta(f) =$ its differential δ uniformity. $nl(f) =$ its nonlinearity, depending on which family they are, they satisfy the inequalities: $nl(f) \geq nl(F) - 2$ (or $nl(f) \geq nl(F) - 4$), where $nl(F)$ is the high nonlinearity of the Gold or Kasami. $d^0(f) =$ its algebraic degree. For the computer programs see Appendix I.

n	$f(x)$	$\Delta(f)$	*1 to 1*	$nl(f)$	$d^0(f)$
6	Gold x^5	4	yes	24	2
$= 2(3)$	$x^5 + (x^4 + x + 1)tr(x)tr(ax)$	6	yes	22	5
3 *odd*	$tr(a^2x)tr(a^4x)tr(a^5x)$				
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)$	6	yes	20	5
	$tr(a^2x)tr(a^4x)$				
	Kasami x^{13}	4	yes	24	3
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x +$	6	yes	22	5
	$1)tr(x)tr(ax)tr(a^2x)tr(a^4x)tr(a^5x)$				
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x +$	$\mathbf{8}$	yes	20	5
	$1)tr(x)tr(ax)tr(a^2x)tr(a^4x)$	$4 \leq \mathbf{8} \leq 2(4)$			
7	Kasami x^{13}	2	yes	56	3
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1)$	4	yes	54	6
	$tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1)$	4	yes	52	6
	$tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^9	2	yes	56	2
	$x^9 + (x^8 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^9 + (x^8 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^5	2	yes	56	2
	$x^5 + (x^4 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^5 + (x^4 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^3	2	yes	56	2
	$x^3 + (x^2 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^3 + (x^2 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				

TABLE 24. *Gold* and *Kasami based permutations* with *optimal algebraic degree* (oad). Where $a = \alpha$ is a primitive element such that the trace of each power of a appearing in f is zero, and see Appendix II for the properties of Gold functions.

n	$f(x)$	$\Delta(f)$	*1 to 1*	$nl(f)$	$d^0(f)$
10	Gold x^{17}	4	yes	480	2
$= 2(5)$	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	478	9
5 *odd*	$tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	476	9
	$tr(a^4x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	Gold x^5	4	yes	480	2
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	478	9
	$tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	**8**	yes	476	9
	$tr(a^4x)tr(a^6x)tr(a^8x)tr(a^9x)$				
12	Gold x^{17}	**16**	yes	1920	2
	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)$	18	yes	1918	11
	$tr(a^3x)tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)$	where			
	$tr((a^5 + a^9)x)tr((a^9 + a^{10})x)tr(a^{11}x)$	$16 \leq 18 \leq 2(16)$			
	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)$	18	yes	1916	11
	$tr(a^3x)tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)$				
	$tr((a^5 + a^9)x)tr(a^{11}x)$				

TABLE 25. *Gold* and *Kasami based permutations* with *optimal algebraic degree* (oad). Where $a = \alpha$ is a primitive element such that the trace of each power of a appearing in f is zero, and see Appendix II for the properties of Gold functions.

Remark The Galois field $\mathbb{F}_{2^{10}}$ is often used in Cryptography research, see [27], [16], [17], [18]. Xu and Qu in their Theorem 3.2 in [38](2020) have obtained a differentialy 4-uniform permutation family piecewise defined on the field $\mathbb{F}_{2^{10}}$, whose nonlinearities run from 462 up to 476. Our permutation with the lowest nonlinearity has nonlinearity 476, surpassing them. Furthermore, our permutations reach an *optimal algebraic degree*, and theirs do not. Other set of authors Peng, Tan, and Wang in [32](2016), Tang D., Carlet, and Tang X. in [36](2015), Qu, Tan Y., Tan C., and Li in [33](2013) have obtained differentialy 4-uniform permutation families on the field $\mathbb{F}_{2^{10}}$, whose nonlinearities run from 442 up to 454.

Furthermore, on the field $\mathbb{F}_{2^{12}}$ our function $R_{ik}(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(x^{2^i+1})(1 + tr((x + x^8)^{2^i+1}))$ (which is inspired by families from our Corollary 2.2.17) has a better nonlinearity $nl(R_{ik}) = 1936$ than the nonlinearities of the functions givens by groups of authors, whose nonlinearities run from 1888 up to 1928, in [32]. The *Preferred functions* discovered by Qu, Tan Y., Tan C., and Li, $PF(x) = x^{3(2^t+1)}$, where $2 \leq t \leq \frac{n}{2} - 1$ (n even), defined in Lemma 4.1(2) shown in Table IV in [33], have a nonlinearity that is between 1884 and 1900. While their functions given by range of Theorem 5.6 shown in Table III, in [33], $G(x) = x^{-1} + \text{tr}_1^n(\frac{x^2}{x+1})$, have nonlinearity equal to 1928.

Remark We can sacrifice a little in the size of the function. Taking the function an almost permutation, but obtaining a better differentiability uniform (low) $\Delta(f)$.

From results in this section it can be proved our following good corollary.

Corollary 5.1.12. [On the Distribution of Zeros in Affine Functions] Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set* of $\mathbb{F}_2^n$, the sets $S_{a_i} = Kernel(tr(a_i x)) = \{x \in \mathbb{F}_{2^n};\, tr(a_i x) = 0\}$ its corresponding $\mathbb{F}_2$ - vector subspaces of $\mathbb{F}_{2^n}$, $H_{a_i} = \{x \in \mathbb{F}_{2^n};\, tr(a_i x) = 1\}$ its hyperplanes, and $1 \leq r \leq n-1$. Then, the intersections of the form $S_{a_1} \cap \cdots \cap S_{a_r}$, $H_{a_1} \cap S_{a_2} \cap \cdots \cap S_{a_r}$, $H_{a_1} \cap H_{a_2} \cap S_{a_3} \cap \cdots \cap S_{a_r}, \cdots$, and $H_{a_1} \cap \cdots \cap H_{a_r}$ form a partition of $\mathbb{F}_{2^n}$. Also, $|U_{a_1} \cap \cdots \cap U_{a_r}| = 2^{n-r}$, where $U_{a_1} \cap \cdots \cap U_{a_r}$ denotes any partition element.

5.2 Simple Differentially δ-Uniform Families

Based on Section 2.2 and 4.1, and the techniques used in the proof of the main theorem presented in Section 5.1, allows us to write the following new differentially δ-uniform functions with a simple polynomial formula:

Theorem 5.2.1. [Cubic Boolean Based I] Let $gcd(k,\, n) = 1$, and $tr(a_1) = tr(a_2) = tr(a_3) = 0$. The family of functions:

$$f(x) = x^{2^k+1} + (x^{2^k} + x + 1 + tr(1))tr(a_1 x)tr(a_2 x)tr(a_3 x)$$

are at least *differentially* 4- *uniform* over $\mathbb{F}_{2^n}$.

Remark The exponent 2^k+1 is the simplest such that the cubics $tr(a_1x)tr(a_2x)tr(a_3x)$ "survive", i.e. such that the functions $f(x) = x^{2^k+1}+(x^{2^k}+x+1)tr(a_1x)tr(a_2x)tr(a_3x)$ have strong cryptographic properties, such as differential δ- uniformity, nonlinearity and algebraic degree.

The 2nd-Order Nonlinearity of $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x)tr(a_2x)tr(a_3x)$:

$tr(bf(x)) + tr(Q(x)) = tr(bx^{2^k+1}) + tr(b(x^{2^k} + x + 1)tr(a_1x)tr(a_2x)tr(a_3x)) + tr(Q(x))$

$= tr(Bx)tr(a_1x)tr(a_2x)tr(a_3x)+ tr(b)tr(a_1x)tr(a_2x)tr(a_3x) + tr(Q(x))$, where $B = b + b^{\frac{1}{2^k}}$, $Q(x)$ is any quadratic function.

For $b = 1 = tr(1)$, for n odd, then $tr(bf(x))+tr(Q(x)) = tr(a_1x)tr(a_2x)tr(a_3x)+tr(Q(x))$. Subject to $(a_i)_{i\in\mathbb{F}_{2^n}}$ be a *linearly independent* set of vectors in $\mathbb{F}_2^n$, we have:

$$nl_2(x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x)tr(a_2x)tr(a_3x)) \leq |H_{a_1} \cap H_{a_2} \cap H_{a_3}| = 2^{n-2} - 2^{n-3}.$$

Theorem 5.2.2. [Cubic Boolean Based II] Let $gcd(k, n) = 1$, and $tr(a_1) = 0$. The family of functions:

$$f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x)tr(x^{2^j+1} + x\,tr(1))$$

are at least *differentially* 4- *uniform* over $\mathbb{F}_{2^n}$.

Remark The 2nd- Order Walsh exponents of $f(x) = x^{2^k+1} + (x^{2^k} + x + 1)tr(a_1x)tr(x^{2^j+1} + x)$:

$tr(bf(x)) + tr(Q(x)) = tr(bx^{2^k+1}) + tr(b(x^{2^k} + x + 1)tr(a_1x)tr(x^{2^j+1} + x\,tr(1))) + tr(Q(x))$

$= tr(Bx)tr(a_1x)tr(x^{2^j+1} + x\,tr(1))+ tr(b)tr(a_1x)tr(x^{2^j+1} + x\,tr(1)) + tr(Q(x))$, where $B = b + b^{\frac{1}{2^k}}$, $Q(x)$ is any quadratic function.

For $b = 1 = tr(1)$, for n odd, then $tr(bf(x)) + tr(Q(x)) = tr(a_1x)tr(x^{2^j+1} + x) + tr(Q(x)) = tr(a_1x)tr(x^{2^j+1}) + tr(a_1x)tr(1x) + tr(Q(x))$, where $tr(a_1) = 0$ and $tr(1) \neq 0$.

Theorem 5.2.3. Let F be a *Gold differentially δ-uniform* function over $\mathbb{F}_{2^n}$, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{n-1}}]$ a polynomial with coefficients in $\mathbb{F}_2$. Then there exist a *linearly independent set* of $\mathbb{F}_2^n$, $(a_i)_{i\in\mathbb{F}_{2^n}}^{n-1}$, and $tr(a_1) = \cdots = tr(a_{n-1}) = 0$, such that the family of functions:

$$f(x) = F(x + \mathcal{P}(tr(a_1x), \cdots, tr(a_{n-1}x)))$$

are *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $d^0(f) = n-1$, and $nl(f) \geq nl(F) - 2$.

Theorem 5.2.4. Let F be a *Gold differentially δ-uniform* function over $\mathbb{F}_{2^n}$, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{n-2}}]$ a polynomial with coefficients in $\mathbb{F}_2$. Then there is a *linearly independent set* of $\mathbb{F}_2^n$, $(a_i)_{i\in\mathbb{F}_{2^n}}^{n-2}$, and $tr(a_1) = \cdots = tr(a_{n-2}) = 0$, such that the family of functions:

$$f(x) = F(x + \mathcal{P}(tr(a_1 x), \cdots, tr(a_{n-2}x)))$$

is *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $d^0(f) = n-1$, and $nl(f) \geq nl(F) - 4$.

The following theorem was proved in Section 5.1.

Theorem 5.2.5. [Differentially γ-Uniform Polynomial] Let $tr(a_1) = \cdots = tr(a_j) = 0$ over $\mathbb{F}_{2^n}$, F a *differentially δ-uniform* function, and $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{j+l}}]$ a polynomial with coefficients in $\mathbb{F}_2$. Then the family of functions:

$$f(x) = F(x + \mathcal{P}(tr(a_1 x), \cdots, tr(a_j x),\, tr(x^{2^{i_1}+1} + x\, tr(1)), \cdots, tr(x^{2^{i_l}+1} + x\, tr(1))))$$

is *differentially γ-uniform*, where $\delta \leq \gamma \leq 2\delta$, $j + l \geq 1$, and every $i_k \in \mathbb{N}$.

References

[1] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. On the Walsh spectrum of a new APN function. In *Cryptography and coding*, volume 4887 of *Lecture Notes in Comput. Sci.*, pages 92–98. Springer, Berlin, 2007.

[2] Carl Bracken and Gregor Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields Appl.*, 16(4):231–242, 2010.

[3] Carl Bracken, Chik How Tan, and Yin Tan. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields Appl.*, 18(3):537–546, 2012.

[4] Lilya Budaghyan. The equivalence of almost bent and almost perfect nonlinear functions and their generalizations. 2005.

[5] Lilya Budaghyan, Marco Calderini, and Irene Villa. On equivalence between known families of quadratic apn functions. *Finite Fields and Their Applications*, 66:101704, 2020.

[6] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields Appl.*, 15(2):150–159, 2009.

[7] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Trans. Inform. Theory*, 52(3):1141–1152, 2006.

[8] Marco Calderini. Differentially low uniform permutations from known 4-uniform functions. *arXiv preprint arXiv:1910.14337*, 2019.

[9] Claude Carlet. Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications. *IEEE Trans. Inform. Theory*, 54(3):1262–1272, 2008.

[10] Claude Carlet. On known and new differentially uniform functions. In *Australasian Conference on Information Security and Privacy*, pages 1–15. Springer, 2011.

[11] Claude Carlet, Yves Crama, and Peter L Hammer. Vectorial boolean functions for cryptography., 2010.

[12] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Advances in cryptology—EUROCRYPT '94 (Perugia)*, volume 950 of *Lecture Notes in Comput. Sci.*, pages 356–365. Springer, Berlin, 1995.

[13] Pascale Charpin and Gohar M. Kyureghyan. On sets determining the differential spectrum of mappings. *Int. J. Inf. Coding Theory*, 4(2-3):170–184, 2017.

[14] Gérard Cohen, Iiro Honkala, Simon Litsyn, and Antoine Lobstein. *Covering codes*, volume 54 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, 1997.

[15] Gérard D. Cohen, Mark G. Karpovsky, H. F. Mattson, Jr., and James R. Schatz. Covering radius—survey and recent results. *IEEE Trans. Inform. Theory*, 31(3):328–343, 1985.

[16] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. *Proposal*, 1999.

[17] Joan Daemen and Vincent Rijmen. *The design of Rijndael*. Information Security and Cryptography. Springer-Verlag, Berlin, 2002. AES—the advanced encryption standard.

[18] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: The Advanced Encryption Standard (AES)*. Springer Nature, 2020.

[19] John F Dillon. Apn polynomials and related codes. In *Banff Conference, Nov. 2006*, 2006.

[20] John F Dillon. Apn polynomials: an update. In *International Conference on Finite fields and applications-Fq9*, 2009.

[21] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3(1):59–81, 2009.

[22] Robert W. Fitzgerald. Invariants of trace forms over finite fields of characteristic 2. *Finite Fields Appl.*, 15(2):261–275, 2009.

[23] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE transactions on Information Theory*, 14(1):154–156, 1968.

[24] H. Janwa and R. M. Wilson. Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993)*, volume 673 of *Lecture Notes in Comput. Sci.*, pages 180–194. Springer, Berlin, 1993.

[25] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18:369–394, 1971.

[26] Jyrki Lahtonen, Gary McGuire, and Harold N. Ward. Gold and Kasami-Welch functions, quadratic forms, and bent functions. *Adv. Math. Commun.*, 1(2):243–250, 2007.

[27] Arjen Lenstra, Eran Tromer, Adi Shamir, Wil Kortsmit, Bruce Dodson, James Hughes, and Paul Leyland. Factoring estimates for a 1024-bit RSA modulus. In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 55–74. Springer, Berlin, 2003.

[28] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II*. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[29] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[30] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 55–64. Springer, 1993.

[31] Kaisa Nyberg. On the construction of highly nonlinear permutations. In *Advances in cryptology—EUROCRYPT '92 (Balatonfüred, 1992)*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 92–98. Springer, Berlin, 1993.

[32] Jie Peng, Chik How Tan, and QiChun Wang. A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k. *Sci. China Math.*, 59(6):1221–1234, 2016.

[33] Longjiang Qu, Yin Tan, Chik How Tan, and Chao Li. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. *IEEE Trans. Inform. Theory*, 59(7):4675–4686, 2013.

[34] Sankhadip Roy. Generalization of some results on Gold and Kasami-Welch functions. *Finite Fields Appl.*, 18(5):894–903, 2012.

[35] James R. Schatz. The second order Reed-Muller code of length 64 has covering radius 18. *IEEE Trans. Inform. Theory*, 27(4):529–530, 1981.

[36] Deng Tang, Claude Carlet, and Xiaohu Tang. Differentially 4-uniform bijections by permuting the inverse function. *Des. Codes Cryptogr.*, 77(1):117–141, 2015.

[37] Irene Villa. On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2. *Cryptogr. Commun.*, 11(1):3–20, 2019.

[38] Guangkui Xu and Longjiang Qu. Two classes of differentially 4-uniform permutations over f 2n with n even. *Advances in Mathematics of Communications*, 14(1), 2020.

[39] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. Constructing differentially 4 uniform permutations from known ones. *Chinese Journal of Electronics*, 22(3):495–499, 2013.

[40] Zhengbang Zha, Lei Hu, and Siwei Sun. Constructing new differentially 4-uniform permutations from the inverse function. *Finite Fields Appl.*, 25:64–78, 2014.

Appendix I

This Computational Library (CL) collects a programming experience using *symbolic software*, in particular SAGE. This CL contains the implementation of the new Theorems, Algorithms in this research work. Also it can be applied to several purposes in Technology and Defense.

```
# SWITCHING NEIGHBOURS OF F(X) IN THE NARROW SENSE:
from sage.crypto.sbox import SBox

n=4; K.<a> = GF(2^n); pm= a^4+a+1; F2p= Set(K);  # cubics roots of the unit: a^2 + a, a^2 + a+ 1
#n=5; K.<a> = GF(2^n); pm= a^5+a^2+1; F2p= Set(K);
#n=6; K.<a> = GF(2^n); pm= a^6+a+1; F2p= Set(K);   # cubics roots of the unit: a^3 + a^2 + a,   a^3 + a^2 + a + 1
#n=7; K.<a> = GF(2^n); pm= a^7+a+1; F2p= Set(K);  # cubics roots of the unit:
#n=8; K.<a> = GF(2^n); pm= a^8+a^4+a^3+a^2+1; F2p= Set(K);  # cubics roots of the unit: a^7 + a^6 + a^4 + a^2 + a, a^7 + a^6
#n=9; K.<a> = GF(2^n); pm= a^9+a^4+1; F2p= Set(K);   # cubics roots of the unit:
#n=10; K.<a> = GF(2^n); pm= a^(10)+a^3+1; F2p= Set(K);  # cubics roots of the unit: a^5 + a^3 + a, a^5 + a^3 + a + 1

#U =[ x^3+ (x^(3)).trace() for x in F2p];
#U =[ x^3+ (x^(3)).trace()+ (x^(9)).trace() for x in F2p];
#U =[ x^3+ (a*x^(9)).trace() for x in F2p];
#U =[ x^3+ (a*x^(9)).trace()+ a*(x^(9)).trace() for x in F2p];
#U =[ x^3+ (a*x^(9)).trace()+ (x^(3)).trace() for x in F2p];
#U =[ x^3+ (x^(5)).trace() for x in F2p];
#U =[ x^3+ (x^(5)).trace()+ (x^(9)).trace() for x in F2p];
U =[ x^3+ (a*x^9).trace()+ (a^2 + a+ 1)*(x^9).trace() for x in F2p];

S_Box = [p.integer_representation() for p in U]; S = SBox(S_Box); UNIF=S.differential_uniformity();
print 'The differential uniformity of the neighbour x^3+ trace(a*x^9)+ (a^2 + a+ 1)*trace(x^9) is =', UNIF;
```

```
The differential uniformity of the neighbour x^3+ trace(a*x^9)+ (a^2 + a+ 1)*trace(x^9) is = 2
```

FIGURE 2. Switching Neighbors in the Narrow Sense: $\Gamma_i(x) = x^3 + \mu tr(G(x)) + \bar{\mu} tr(x^r)$, where $G(x)$ is any function, and $r = 9, 3$ (see Tables in section 2.1).

```
######## GOLD POLYNOMIAL BASED- 1 ORDER NONLINEARITY:
from sage.crypto.sbox import SBox
n=10; K.<a> = GF(2^n); k=4; B=a^0 ; C=a ; D=a^2; E=a^4; F=a^3; G=a^6; H=a^8; R=a^9; J=a^5+a^7; pm= a^10+a^3+1; F2p= Set(K);
# And {a, a^2, a^3} is an linearly independent in F_2^n, for any n>= 3.
# And {a, a^2, a^4} is an linearly independent in F_2^n, for any n>= 4, and if tr(a)=0 then also tr(a)=tr(a^2)=tr(a^4)=0.

U =[(x + (B*x).trace()*(C*x).trace()*(D*x).trace()*(E*x).trace()*(F*x).trace()*(G*x).trace()
    *(H*x).trace()*(R*x).trace()*(J*x).trace())^(2^k+1) for x in F2p];
S_Box = [p.integer_representation() for p in U]; S = SBox(S_Box); NL=S.nonlinearity(); DG=S.max_degree();
UNIF=S.differential_uniformity();

print 'Function f(x) = x^17+ (x^16+x+1)tr(x)tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr((a^5+a^7)x)tr(a^6x)tr(a^8x)tr(a^9x)', ',',
print 'Its nonlinearity = ', NL, ',', 'Its algebraic degree = ', DG, ',', 'Its differential uniformity = ', UNIF, ',',
print 'Its cardinality of the range = ', len(Set(U)), '.';
```

```
Function f(x) = x^17+ (x^16+x+1)tr(x)tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr((a^5+a^7)x)tr(a^6x)tr(a^8x)tr(a^9x) , Its nonlinearity
=  478 , Its algebraic degree =  9 , Its differential uniformity =  6 , Its cardinality of the range =  1024 .
```

FIGURE 3. Gold and Kasami based permutations with *optimal algebraic degree*. Where $a = \alpha$ is a primitive element, also the trace of each power of a appearing in f is zero (see Tables in section 5.1).

Appendix II

The following tables include the Walsh Spectrum and other cryptographic properties of the Gold family (to read about *Classical Walsh Spectrum* see [21]). Unusual values that are not mentioned in the papers, and that these values represent a weakness of the Gold family, as for example $\Delta = 8$ and 16, Wlash Spectrum of the forms $\{\mathbf{2^{n-3}}, 2^{\frac{n}{2}}, 0\}$, $\{\mathbf{2^{n-4}}, 2^{\frac{n}{2}}, 0\}$, $\{\mathbf{2^{\frac{n+3}{2}}}, 0\}$ and $\{\mathbf{2^{\frac{n+5}{2}}}, 0\}$ are highlighted in bold letter. A complete information about it, up to the finite field of degree 15, is a matter of interest for authors in this research area:

Examples Let us n an even number. Monomials x^{2^d+1}, Δ = its differential δ uniformity. These permit us to see the variety of cases that can occur. The programs given in Appendix I can be adapted to obtain the following table.

n even	x^{2^d+1}	Δ	*permutation*	*Walsh coeff.* $\lvert W_{x^{2^d+1}}(a,b)\rvert$	$\lvert\mathcal{W}_{x^{2^d+1}}\rvert$ *form*
$n=2$	x^3	2	not perm	[(0, 3), (4, 1)]; [(2, 4)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$n=4$	x^5	4	not perm	[(0, 15), (16, 1)]; [(4, 16)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^3	2	not perm	[(0, 12), (8, 4)]; [(4, 16)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n=6$	x^9	8	not perm	[(0, 63), (64, 1)]; [(8, 64)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$=2(3)$	x^5	4	permutation	[(0, 48), (16, 16)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
3 *odd*	x^3	2	not perm	[(0, 48),(16, 16)]; [(8, 64)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n=8$	x^{17}	16	not perm	[(0, 255), (256, 1)]; [(16, 256)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^9	2	not perm	[(0, 192), (32, 64)]; [(16, 256)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	not perm	[(0, 240), (64, 16)]; [(16, 256)]	$\{\mathbf{2^{n-2}}, 2^{\frac{n}{2}}, 0\}$
	x^3	2	not perm	[(0, 192), (32, 64)]; [(16, 256)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n=10$	x^{33}	32	not perm	[(0, 1023), (1024, 1)], [(32, 1024)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$=2(5)$	x^{17}	4	permutation	[(0, 768), (64, 256)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
5 *odd*	x^9	2	not perm	[(0, 768), (64, 256)]; [(32, 1024)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	permutation	[(0, 768), (64, 256)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
	x^3	2	not perm	[(0, 768), (64, 256)]; [(32, 1024)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n=12$	x^{65}	64	not perm	[(0, 4095), (4096, 1)], [(64, 4096)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^{33}	2	not perm	[(0, 3072), (128, 1024)], [(64, 4096)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^{17}	**16**	permutation	[(0, 3840), (256, 256)] cte.	$\{\mathbf{2^{n-4}}, 0\}$
	x^9	**8**	not perm	[(0, 4032), (512, 64)], [(64, 4096)]	$\{\mathbf{2^{n-3}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	not perm	[(0, 3840), (256, 256)], [(64, 4096)]	$\{\mathbf{2^{n-4}}, 2^{\frac{n}{2}}, 0\}$
	x^3	2	not perm	[(0, 3072), (128, 1024)], [(64, 4096)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n=14$	x^{129}	–	not perm	[(0, 16383), (16384, 1)], [(128, 16384)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$=2(7)$	x^{65}	4	permutation	[(0, 12288), (256, 4096)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
7 *odd*	x^{33}	2	not perm	[(0, 12288), (256, 4096)], [(128, 16384)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^{17}	4	permutation	[(0, 12288), (256, 4096)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
	x^9	2	not perm	[(0, 12288), (256, 4096)], [(128, 16384)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	permutation	[(0, 12288), (256, 4096)] cte.	$\{2^{\frac{n+2}{2}}, 0\}$
	x^3	2	not perm	[(0, 12288), (256, 4096)], [(128, 16384)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$

TABLE 26. A variety of extended Walsh Spectrum $\lvert\mathcal{W}_{x^{2^d+1}}\rvert$

Examples Let us n an odd number. Monomials x^{2^d+1}, Δ = its differential δ uniformity. These permit us to see the variety of cases that can occur. For computer programs see the Appendix I.

n odd	x^{2^d+1}	Δ	*permutation*	*Walsh coeff.* $\lvert W_{x^{2^d+1}}(a,b)\rvert$	$\lvert\mathcal{W}_{x^{2^d+1}}\rvert$ *form*
$n=3$	x^3	2	permutation	[(0, 4), (4, 4)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=5$	x^5	2	permutation	[(0, 16), (8, 16)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	2	permutation	[(0, 16), (8, 16)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=7$	x^9	2	permutation	[(0, 64), (16, 64)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^5	2	permutation	[(0, 64), (16, 64)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	2	permutation	[(0, 64), (16, 64)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=9$	x^{17}	2	permutation	[(0, 256), (32, 256)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^9	**8**	permutation	[(0, 448), (64, 64)] cte.	$\{\mathbf{2^{\frac{n+3}{2}}},0\}$
	x^5	2	permutation	[(0, 256), (32, 256)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	2	permutation	[(0, 256), (32, 256)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=11$	x^{33}	2	permutation	[(0, 1024), (64, 1024)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^{17}	2	permutation	[(0, 1024), (64, 1024)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^9	2	permutation	[(0, 1024), (64, 1024)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^5	2	permutation	[(0, 1024), (64, 1024)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	2	permutation	[(0, 1024), (64, 1024)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=13$	x^{65}	2	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^{33}	2	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^{17}	2	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^9	2	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^5	2	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	–	permutation	[(0, 4096), (128, 4096)] cte.	$\{2^{\frac{n+1}{2}},0\}$
$n=15$	x^{129}	–	permutation	[(0, 16384), (256, 16384)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^{65}	–	permutation	[(0, 28672), (512, 4096)] cte.	$\{\mathbf{2^{\frac{n+3}{2}}},0\}$
	x^{33}	–	permutation	[(0, 31744), (1024, 1024)] cte.	$\{\mathbf{2^{\frac{n+5}{2}}},0\}$
	x^{17}	–	permutation	[(0, 16384), (256, 16384)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^9	–	permutation	[(0, 28672), (512, 4096)] cte.	$\{\mathbf{2^{\frac{n+3}{2}}},0\}$
	x^5	–	permutation	[(0, 16384), (256, 16384)] cte.	$\{2^{\frac{n+1}{2}},0\}$
	x^3	–	permutation	[(0, 16384), (256, 16384)] cte.	$\{2^{\frac{n+1}{2}},0\}$

TABLE 27. A variety of extended Walsh Spectrum $\lvert\mathcal{W}_{x^{2^d+1}}\rvert$

Appendix III

List of the primitive polynomials $p(x)$ used in this research work:

$\mathbb{F}_{2^n}$	$p(x)$
$\mathbb{F}_{2^2}$	x^2+x+1
$\mathbb{F}_{2^3}$	x^3+x+1
$\mathbb{F}_{2^4}$	x^4+x+1
$\mathbb{F}_{2^5}$	x^5+x^2+1
$\mathbb{F}_{2^6}$	x^6+x+1, $x^6+x^4+x^3+x+1$ [SAGE]
$\mathbb{F}_{2^7}$	x^7+x+1
$\mathbb{F}_{2^8}$	$x^8+x^4+x^3+x^2+1$
$\mathbb{F}_{2^9}$	x^9+x^4+1
$\mathbb{F}_{2^{10}}$	$x^{10}+x^3+1$, $x^{10}+x^6+x^5+x^3+x^2+x+1$ [SAGE]
$\mathbb{F}_{2^{11}}$	$x^{11}+x^2+1$
$\mathbb{F}_{2^{12}}$	$x^{12}+x^6+x^4+x+1$, $x^{12}+x^7+x^6+x^5+x^3+x+1$ [SAGE]
$\mathbb{F}_{2^{13}}$	$x^{13}+x^4+x^3+x+1$
$\mathbb{F}_{2^{14}}$	$x^{14}+x^5+x^3+x+1$, $x^{14}+x^7+x^5+x^3+1$ [SAGE]
$\mathbb{F}_{2^{15}}$	$x^{15}+x+1$, $x^{15}+x^5+x^4+x^2+1$ [SAGE]

TABLE 28. $p(x)$ is a primitive polynomial over $\mathbb{F}_{2^n}$.

```
# Given a positive integer n, the following program returns the primitive polynomial (pr) used by
# SAGE to construct the finite field of 2^n elements:
from sage.crypto.sbox import SBox
n=5; K.<x> = GF(2^n); pr= K.polynomial(); print 'primitive polynomial= ', pr;
```

```
primitive polynomial=  x^5 + x^2 + 1
```

FIGURE 4. Given a positive integer n, the following program returns the primitive polynomial used by SAGE to construct the finite field of degree n.

Contact: roberto.reyes@upr.edu robertoruv@gmail.com