THE EQUIVALENCE OF ALMOST BENT AND ALMOST PERFECT NONLINEAR FUNCTIONS AND THEIR GENERALIZATIONS

DISSERTATION

zur Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg

von Dipl. Math. Lilya Budaghyan
geb. am 29.01.1976 in Baku (Azerbaijan)

Gutachter:
Prof. Dr. rer. nat. habil. Alexander Pott
Prof. Dr. rer. nat. habil. Tor Helleseth
Prof. Dr. rer. nat. habil. Yuri Movsisyan

Eingereicht am: 05.10.2005
Verteidigung am: 07.12.2005

Dedication

To my grandparents, Emma and Yakov, my parents, Karina and Mikhail, and my sister and brother, Milena and Yanik.

Acknowledgments

First and formost I thank my family and friends for their constant love, support and encouragement which enabled this work.

I am very grateful to Professor Alexander Pott for having supervised this work while the same time letting me a huge amount of liberty in my research which I appreciated very much. I thank Professor Pott for many mathematical discussions and patience in the first stage of my study, which helped me to get an insight into the field of research in a short time. I am very grateful to the opportunity to cooperate with Professor Claude Carlet from the University of Paris 8. I would like to thank Professor Carlet for the sustained flow of mathematical inspiration, professional advice and for the invaluable experience I gained from our mutual investigations. I would also like to extend my profound gratitude to Professor Yuri Movsisyan from the Yerevan State University who supervised and encouraged my scientific investigations in the field of algebra and logic. The experience of that work played an important role in my further study in discrete mathematics.

I thank the State of Saxony Anhalt for financial support of this research.

Zusammenfassung

Vektorielle boole'sche Funktionen werden in vielen Bereichen der Kryptographie angewendet, insbesondere bei Blockchiffren, siehe [14]. Mächtige Attacken gegen solche Kryptosysteme sind lineare sowie differenzielle Attacken, siehe [4, 48]. Die am stärksten gegen diese Attacken resistenten Funktionen sind die sogenannten fast perfekt nichtlinearen Funktionen ("almost perfect nonlinear", APN) sowie die "almost bent" (AB) Funktionen. Genauer: APN Abbildungen bieten besten Schutz gegen differenzielle Attacken, AB Funktionen gegen lineare Attacken, siehe [19, 53]. Es gab bislang nur wenige Klassen von APN und AB Funktionen, und alle diese Abbildungen sind zu Potenzfunktionen affin äquivalent gewesen [9, 14]. In der vorliegenden Arbeiten werden nun erstmals APN und AB Abbildungen konstruiert, die zu keiner Potenzfunktion affin äquivalent sind. Hierzu habe ich den erweiterten Äquivalenzbegriff aus [15] benutzt. In der Arbeit wird diese Äquivalenz als CCZ-Äquivalenz bezeichnet. Im Fall von AB Abbildungen kann ich sogar zeigen, dass man so unendlich viele verschiedene Klassen finden kann. Eine der konstruierten Klassen liefert ein Gegenbeispiel zu einer bekannten Vermutung, dass alle AB Abbildungen zu Permutationen affin äquivalent sind [15]. Ferner konstruiere ich AB Abbildungen, die auch dann nicht zu einer Potenzfunktion transformiert werden können, wenn man außer affinen Transformationen auch noch "Invertieren" erlaubt. Das zeigt, dass CCZ-Äquivalenz nicht nur ein allgemeinerer Begriff als affine Äquivalenz ist, sondern auch allgemeiner als "affine Äquivalenz plus Invertieren" zusammen.
In der Arbeit werden die Begriffe AB und APN verallgemeinert ("2^δ-uniform, δ-nonlinear"). Es werden einige Resultate über diese neuen Klassen gezeigt, die die Zusammenhänge zwischen APN und AB verallgemeinern, aber auch Unterschiede aufzeigen.

Summary

Vectorial Boolean functions are used in cryptography, in particular in block ciphers [14]. An important condition on these functions is a high resistance to the differential and linear cryptanalyses [4, 48], which are the main attacks on block ciphers. The functions which possess the best resistance to the differential attack are called almost perfect nonlinear (APN). Almost bent (AB) functions are those mappings which oppose an optimum resistance to both linear and differential attacks, see [19, 53]. Up to now only a few classes of APN and AB functions have been known and all these classes happened to be extended affine equivalent (EA-equivalent) to power functions (see for instance [9, 14]). In this work we construct the first classes of APN and AB polynomials EA-inequivalent to power mappings by using the equivalence relation (which we call CCZ-equivalence) presented in [15]. Moreover we show that the number of different classes of AB polynomials EA-inequivalent to power functions is infinite. One of the constructed functions serves as a counterexample for a conjecture about nonexistence of AB functions EA-inequivalent to permutations [15]. Further we show that applying only EA and inverse transformations on an AB permutation F it is possible to construct AB polynomials EA-inequivalent to both functions F and F^{-1}. We also present the notions of differentially 2^{δ}-uniform and s-nonlinear functions which are natural generalizations of the notions of APN and AB mappings, respectively, and we give some results related to these notions.

Contents

Chapter 1

Introduction

Vectorial Boolean functions are used in many cryptographic algorithms. Their properties are responsible for the quality of an algorithm, its resistance to attacks. The linear and differential attacks are the main attacks on block ciphers, where vectorial Boolean functions play an important role [14].

The differential cryptanalysis presented by Biham and Shamir [4] is based on the study of how differences in an input can affect the resultant difference at the output. The resistance to differential attacks for a function F from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$, used as an S-box in the cipher, is high when the value

$$\delta_F = \max_{a,b\in\mathbb{F}_2^m, a\neq 0} |\{x \in \mathbb{F}_2^m : F(x+a) + F(x) = b\}|$$

is small. The functions with the smallest possible differential uniformity [54], that is, with smallest δ_F, oppose an optimum resistance to the differential attack [4]. They are called almost perfect nonlinear (APN).

The linear cryptanalysis introduced by Matsui [48] is based on finding affine approximations to the action of a cipher. The linear attack on a function F is successful if

$$\lambda_F = \max_{a,b\in\mathbb{F}_2^m, b\neq 0} |\sum_{x\in\mathbb{F}_2^m} (-1)^{b\cdot F(x)+a\cdot x}|$$

is large. The functions achieving the maximal possible nonlinearity [19, 53] $NL(F) = 2^{m-1} - \frac{1}{2}\lambda_F$ possess the best resistance to the linear attack [48] and they are called almost bent (AB) or maximum nonlinear.

In this work we introduce the transformation of functions presented in the paper [15] of Carlet, Charpen and Zinoviev as an equivalence relation of functions and we call this equivalence relation Carlet-Charpen-Zinoviev equivalence (CCZ-equivalence). CCZ-equivalence corresponds to the affine equivalence of the graphs of functions, i.e. functions F and F' are CCZ-equivalent if and only if, for some affine permutation, the image of the graph of F is the graph of the function F'. CCZ-equivalent functions have the same linear and differential properties and the same resistance to the algebraic attack.

It was known that the inverse transformation and the extended affine equivalence (EA-equivalence) are the particular cases of CCZ-equivalence [15]. Recall that functions F and F' are called EA-equivalent if $F' = A_1 \circ F \circ A_2 + A$ for some affine functions A, A_1 and A_2, where A_1 and A_2 are permutations. We completely describe the connection between the CCZ-equivalence from one side and the inverse and the EA-transformations on the other side. It could be expected that CCZ-equivalence coincides in practice with both the inverse and the EA-transformations. We prove that CCZ-equivalence is more general. At first we give sufficient conditions for functions to be extended affine inequivalent to power functions. We make some steps to characterize the functions CCZ-equivalent to the Gold power mappings. Then applying CCZ-equivalence to the Gold APN and AB functions we construct classes of APN and AB polynomials which are EA-inequivalent to power functions. This proves that CCZ-equivalence is more general than both the inverse and EA-transformations together. Moreover, the constructed classes are the first classes of APN and AB mappings which are EA-inequivalent to power functions.

The structure of the thesis. Chapter 2 contains all the necessary definitions related to Boolean and vectorial Boolean functions, including EA-equivalence, APN and AB properties, important results related to APN and AB functions. In particular we present by Propositions 16 and 17 sufficient conditions for functions to be EA-inequivalent to power functions. Then we consider vectorial plateaued functions (which we call s-nonlinear) since they are natural generalizations of AB functions. Besides, we define differentially 2^δ-uniform functions which are generalizations of APN mappings. We describe properties of these functions and we study the connections between differentially 2^δ-uniform and s-nonlinear functions.

In Chapter 3, we give the definition of CCZ-equivalence, we describe its main properties and we show its connections with EA-equivalence. Then we give some results related to a classification of functions CCZ-equivalent to the Gold mappings in Section 3.3.

Theorems 6 and 7 in Chapter 4 present two different constructions of APN polynomials which are EA-inequivalent to power functions and Theorem 5, 8 and 9 present different classes of AB functions EA-inequivalent to power mappings. Besides, by Theorem 9 we show that the number of different classes of AB polynomials EA-inequivalent to power mappings is infinite. We also note that some functions from Theorem 5 are EA-inequivalent to any permutation and that disproves the conjecture of [15].

In Chapter 5, applying only the inverse and EA transformations on the Gold AB functions we construct a class of AB polynomials which is EA-equivalent neither to the Gold mappings nor to their inverses.

Finally, it should be noted that the following material from this thesis has either been published, submitted for publication, or is in preparation to be submitted for publication to international journals:

- [Section 2.4] L. Budaghyan and A. Pott. Differentially uniform and nonlinear functions. in preparation.
- [Chapters 3 and 4] L. Budaghyan, C. Carlet, A. Pott. New Constructions of Almost Perfect Nonlinear and Almost Bent Functions. *Proceedings of the Workshop on Coding and Cryptography 2005*, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.
- [Chapters 3 and 4] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Perfect Nonlinear and Almost Bent Functions. submitted to *IEEE Trans. Inform. Theory*, 2005.
- [Chapter 5] L. Budaghyan and C. Carlet. On the equivalence of maximum nonlinear functions. in preparation.

Chapter 2

Differential uniformity and nonlinearity of functions

Let $\mathbb{F}_2^m$ be the m-dimensional vector space over the field $\mathbb{F}_2$. In this work we consider functions from $\mathbb{F}_2^m$ to itself. Obviously, any such function can be viewed as a vectorial Boolean function. In the next section we give necessary notions related to Boolean functions which will be useful for the study of vectorial Boolean functions.

2.1 Boolean functions

A *Boolean function* F in m variables is an $\mathbb{F}_2$-valued function on $\mathbb{F}_2^m$. The unique representation of F as a polynomial over $\mathbb{F}_2$ in m variables of the form

$$F(x_1, ..., x_m) = \sum_{u \in \mathbb{F}_2^m} c(u) \Big(\prod_{i=1}^{m} x_i^{u_i} \Big)$$

is called the *algebraic normal form* of F. The degree of the algebraic normal form of F is denoted by $d^\circ(F)$ and is called the *algebraic degree* of the function F [13].

A Boolean function F is *affine* if $d^\circ(F) \leq 1$. F is called *linear* if it is affine and $F(0) = 0$. The functions of the algebraic degree 2 are called *quadratic* functions.

The *Hamming weight* $wt(F)$ of a Boolean function F is the size of its *support* $\{x \in \mathbb{F}_2^m : F(x) \neq 0\}$. A Boolean function F is called *balanced* if $wt(F) = 2^{m-1}$. The *Hamming distance* $d(F, G)$ between two functions F and G is the size of the set $\{x \in \mathbb{F}_2^m : F(x) \neq G(x)\}$. The minimum distance $\mathcal{NL}(F)$ between F and all affine functions is called the *nonlinearity* of F. The nonlinearity of a Boolean function quantifies the level of confusion put in the system by the function and it must be high to prevent the system from linear attacks [48].

If we consider a Boolean function F as valued in $\{0,1\} \subset \mathbb{Z}$ then the nonlinearity of F can be described by the discrete Fourier transform. The function $\widehat{F} : \mathbb{F}_2^m \to \mathbb{Z}$ defined by

$$\widehat{F}(a) = \sum_{x \in \mathbb{F}_2^m} F(x)(-1)^{a \cdot x}, \qquad a \in \mathbb{F}_2^m,$$

where "$\cdot$" is the usual inner product in $\mathbb{F}_2^m$, is called the *Fourier transform* of F. For the Fourier transform and for any functions F and G the following formulas are true:

$$F(x) = 2^{-m} \sum_{a \in \mathbb{F}_2^m} \widehat{F}(a)(-1)^{a \cdot x},$$

$$(\widehat{F+G})(a) = \widehat{F}(a) + \widehat{G}(a).$$

Obviously, the Fourier transform can be also applied to the function $(-1)^F$, which is called the *sign function* of F. The function λ_F defined for any $a \in \mathbb{F}_2^m$ by

$$\lambda_F(a) = \widehat{(-1)^F}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{F(x)}(-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^m} (-1)^{F(x)+a \cdot x}$$

is called the *Walsh transform* of a Boolean function F.

The equality $(-1)^F = 1 - 2F$ provides the following relationship between Fourier and Walsh transforms of a function:

$$\lambda_F(a) = \widehat{(-1)^F}(a) = \widehat{1} - 2\widehat{F}(a) = 2^m \delta_0(a) - 2\widehat{F}(a),$$

where δ_0 is the Dirac symbol defined by $\delta_0(0) = 1$ and $\delta_0(a) = 1$ if $a \neq 0$.

One can easily note that for any Boolean function F and any element a we have

$$\lambda_F(a) = 2^m - 2wt\big(F(x) + a \cdot x\big) = 2^m - 2d\big(F(x), a \cdot x\big).$$

Then

$$d\big(F(x), a \cdot x\big) = 2^{m-1} - \frac{1}{2}\lambda_F(a), \qquad d\big(F(x), a \cdot x + 1\big) = 2^{m-1} + \frac{1}{2}\lambda_F(a).$$

This gives the connection between the nonlinearity of F and the values of its Walsh transform

$$\mathcal{NL}(F) = 2^{m-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^m} |\lambda_F(a)|.$$

The Walsh transform of a Boolean function F satisfies Parseval's relation

$$\sum_{a\in\mathbb{F}_2^m} \lambda_F(a)^2 = 2^{2m}. \tag{2.1}$$

Indeed,

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^m} \lambda_F(a)^2 &= \sum_{a\in\mathbb{F}_2^m} \big(\sum_{x\in\mathbb{F}_2^m} (-1)^{F(x)+a\cdot x}\big)^2 = \sum_{a\in\mathbb{F}_2^m} \big(\sum_{x,y\in\mathbb{F}_2^m} (-1)^{F(x)+F(y)+a\cdot(x+y)}\big) \\ &= \sum_{x,y\in\mathbb{F}_2^m} (-1)^{F(x)+F(y)} \sum_{a\in\mathbb{F}_2^m} (-1)^{a\cdot(x+y)} = 2^{2m}.\end{aligned}$$

since $\sum_{a\in\mathbb{F}_2^m}(-1)^{a\cdot(x+y)}$ equals 0 when $x\neq y$ and equals 2^m otherwise.

Parseval's relation makes clear that the nonlinearity $\mathcal{NL}(F)$ of any Boolean function F is upper bounded by $2^{m-1} - 2^{\frac{m}{2}-1}$. The functions achieving this bound are called *bent*. They exist only for m even. Obviously, F is bent if and only if $\lambda_F(a) = \pm 2^{\frac{m}{2}}$ for any $a \in \mathbb{F}_2^m$.

The *derivative* of a Boolean function F with respect to $a \in \mathbb{F}_2^m$ is the function

$$D_aF(x) = F(x+a) + F(x).$$

The derivatives of a function determine many cryptographic properties, the most important of which is the resistance to differential attacks. Other properties defined by the mean of the derivatives are the strict avalanche criterion (SAC) and the propagation criterion (PC), which evaluate some kind of diffusion of the function [57]. An element $a \in \mathbb{F}_2^m$ is called a *linear structure* of a Boolean function F if D_aF is a constant. The set of all linear structures of F is a subspace of $\mathbb{F}_2^m$. The existence of nonzero linear structures is considered as a weakness for cryptographic functions (see [31]).

The derivatives can be also used to describe bent functions. Indeed, since for any $a \in \mathbb{F}_2^m$

$$\begin{aligned}\lambda_F(a)^2 &= \sum_{x,y\in\mathbb{F}_2^m} (-1)^{F(x)+F(y)+a\cdot(x+y)} = \sum_{x,y\in\mathbb{F}_2^m} (-1)^{F(x+y)+F(y)+a\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^m} \big(\sum_{y\in\mathbb{F}_2^m} (-1)^{D_xF(y)}\big)(-1)^{a\cdot x} = 2^m + \sum_{x\in\mathbb{F}_2^m, x\neq 0} \big(\sum_{y\in\mathbb{F}_2^m} (-1)^{D_xF(y)}\big)(-1)^{a\cdot x},\end{aligned}$$

then $\lambda_F(a)^2 = 2^m$ for all a if and only if D_xF is balanced for all nonzero elements $x \in \mathbb{F}_2^m$.

Thus, we have the following characterization of bent functions.

Proposition 1 (see [13]) *A Boolean function F on $\mathbb{F}_2^m$ is bent if and only if one of the following conditions holds for any $a \in \mathbb{F}_2^m$:*
(i) $\lambda_F(a) = \pm 2^{\frac{m}{2}}$,
(ii) $wt(D_aF) = 2^{m-1}$ *if* $a \neq 0$.

It is obvious that a function F is balanced if and only if $\lambda_F(0) = 0$. Therefore, none of the bent functions is balanced and, in spite of their optimum nonlinearity, this makes them improper for direct cryptographic use. Hence, it is natural to consider functions which can be balanced and suggest a good nonlinearity.

Let F be a Boolean function on m variables. We denote by

$$N_{\Delta_F} = |\{a \in \mathbb{F}_2^m : \sum_{x \in \mathbb{F}_2^m} (-1)^{D_aF(x)} \neq 0\}|$$

the number of non-balanced derivatives (i.e. the number of nonzero *auto-correlation coefficients*) of F and by

$$N_{\lambda_F} = |\{a \in \mathbb{F}_2^m : \lambda_F(a) \neq 0\}|$$

the number of nonzero values of the Walsh transform of F. Then N_{Δ_F} and N_{λ_F} satisfy the inequality

$$N_{\Delta_F} \times N_{\lambda_F} \geq 2^m,$$

which was conjectured in [56] by B. Preneel and proven in [11] by C. Carlet. In case of equality the function F is called *partially bent.*

Proposition 2 ([11]) *A Boolean function F on $\mathbb{F}_2^m$ is partially bent if and only if one of the following conditions holds:*
(i) *D_aF is either balanced or constant for every $a \in \mathbb{F}_2^m$;*
(ii) *there exist two linear subspaces E (of even dimension) and E' of $\mathbb{F}_2^m$, whose direct sum equals $\mathbb{F}_2^m$, and Boolean functions F_1, bent on E, and F_2, affine on E', such that $F(x+y) = F_1(x) + F_2(y)$ for any $x \in E$ and $y \in E'$.*

It is obviously follows from Proposition 2 that all affine, quadratic and bent functions are partially bent.

Partially bent functions, when they are not bent, have nonzero linear structures and, therefore, they are also cryptographically weak in some sense. The class of plateaued functions is a natural extension of the class of partially bent functions.

A Boolean function F on m variables is called *plateaued* if its Walsh transform takes only three values 0 and $\pm\lambda$, that is, $\lambda_F(a) \in \{0, \pm\lambda\}$ for any $a \in \mathbb{F}_2^m$. The value λ is called the *amplitude* of the plateaued function. Because of (2.1) the amplitude λ cannot be null and must be a power 2^r, $\frac{m}{2} \leq r \leq m$. Bent functions are plateaued and, according to Parseval's relation (2.1), a plateaued function is bent if and only if its Walsh transform never takes the value 0.

A Boolean function F is called *n-th order correlation immune* if it is balanced when any n of the inputs are fixed. F is n-th order correlation immune if and only if $\lambda_F(a) = 0$ for every $a \in \mathbb{F}_2^m$ such that $1 \leq wt(a) \leq n$ (see [67]). Balanced n-th order correlation immune functions are called *n-resilient.* Boolean functions used as combining functions in stream ciphers must have high order of resiliency to resist correlation attacks [62, 63]. It is proven in [59, 64, 69] that the resiliency order n and the nonlinearity of a Boolean function satisfy the relation $\mathcal{NL}(F) \leq 2^{m-1} - 2^{n+1}$. If the nonlinearity of an n-resilient function achieves this bound then it is plateaued, that is, the class of plateaued functions contains the functions which achieve the best possible trade-offs between resiliency and nonlinearity (see [13]); besides, in these cases the algebraic degrees are also optimal [12].

The following proposition gives a characterization of plateaued functions through their second order derivatives

$$D_aD_bF(x) = F(x) + F(x+a) + F(x+b) + F(x+a+b), \qquad a, b \in \mathbb{F}_2^m.$$

Proposition 3 ([17]) *A Boolean function F is plateaued on $\mathbb{F}_2^m$ if and only if there exists σ such that for every $x \in \mathbb{F}_2^m$, $\sum_{a,b\in\mathbb{F}_2^m}(-1)^{D_aD_bF(x)} = \sigma$. If this condition is satisfied then the amplitude λ of the plateaued function F is given by the equality $\sigma = \lambda^2$.*

Obviously, all linear functions are plateaued and the same is true for quadratic functions, since the second order derivatives of any quadratic function are constant.

2.2 Vectorial Boolean functions

Any function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ can be considered as a *vectorial Boolean function*, i.e. F can be presented in the form

$$F(x_1, ..., x_n) = \big(F^1(x_1, ..., x_n), ..., F^m(x_1, ..., x_n)\big),$$

where the Boolean functions $F^1, ..., F^m$ are called the *coordinate* or *component functions* of the function F.

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has a unique representation as a polynomial on n variables with coefficients in $\mathbb{F}_2^m$

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

This representation is called the *algebraic normal form* of F and its degree $d^\circ(F)$ the *algebraic degree* of the function F. The algebraic degree of F is equal to the maximum algebraic degree of the coordinate functions of F (see [14]). The minimum algebraic degree of all nonzero linear combinations of the coordinate functions of F is called the *minimum degree* of the function F and it is denoted by $\min d^\circ(F)$, i.e.

$$\min d^\circ(F) = \min_{c \in \mathbb{F}_2^m, c \neq 0} d^\circ(c \cdot F).$$

If we identify $\mathbb{F}_2^m$ with the finite field $\mathbb{F}_{2^m}$ then a function $F : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$ is also uniquely represented as a univariate polynomial over $\mathbb{F}_{2^m}$ of degree smaller than 2^m

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

If m is a divisor of n then a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ can be viewed as a function from $\mathbb{F}_2^n$ to itself and, therefore, it admits a univariate polynomial representation. More precisely, it can be represented in the form $tr_{n/m}(\sum_{i=0}^{2^n-1} c_i x^i)$, where $tr_{n/m}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ (i.e. $tr_{n/m}(x) = x + x^{2^m} + x^{2^{2m}} + ... + x^{2^{n-m}}$). Indeed, there exists a function G from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ (for example $G(x) = aF(x)$, where $a \in \mathbb{F}_{2^n}$ and $tr_{n/m}(a) = 1$) such that F equals $tr_{n/m} \circ G$.

For any integer k, $0 \leq k \leq 2^m - 1$, the number $w_2(k)$ of nonzero coefficients k_s, $0 \leq k_s \leq 1$, in the binary expansion $\sum_{s=0}^{m-1} 2^s k_s$ of k is called the 2-weight of k. The algebraic degree of a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is

$$d^\circ(F) = \max_{\substack{0 \leq i \leq 2^m-1 \\ c_i \neq 0}} w_2(i)$$

(see [15]). In particular, F is linear if and only if $F(x)$ is a *linearized polynomial* over $\mathbb{F}_{2^m}$

$$\sum_{i=0}^{m-1} c_i x^{2^i}, \quad c_i \in \mathbb{F}_{2^m}.$$

The sum of a linear function and a constant is called an *affine function.* Obviously, the algebraic degree of any affine function is less than or equal to 1. The functions of the algebraic degree less than or equal to 2 are called quadratic.

Let F be a function from $\mathbb{F}_2^m$ to itself. Then, if F is a permutation the transformation

$$F \mapsto F^{-1}$$

is called the *inverse transformation.* If $A_1,\ A_2 : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ are affine permutations and $A : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ is affine then the following transformations are called the *affine* and *extended affine transformations* respectively:

$$F \mapsto A_1 \circ F \circ A_2,$$

$$F \mapsto A_1 \circ F \circ A_2 + A.$$

In these cases the functions F and $A_1 \circ F \circ A_2$ are called *affine equivalent* and the functions F and $A_1 \circ F \circ A_2 + A$ are called *extended affine equivalent.* If F is not affine then any EA transformation of the function does not change its algebraic degree. If $\min d^\circ(F) > 1$ then the minimum degree of F is also EA invariant. Obviously, the algebraic and minimum degrees of a function are not invariant under the inverse transformation. For example, for a function $F(x) = x^{2^i+1}$ on the field $\mathbb{F}_{2^m}$ we have $d^\circ(F) = \min d^\circ(F) = 2$ and $d^\circ(F^{-1}) = \min d^\circ(F^{-1}) = \frac{m+1}{2}$ when $\gcd(i, m) = 1$ (see [54]).

A function $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is called *balanced* if it takes every value of $\mathbb{F}_2^m$ the same number 2^{n-m} of times. The balanced functions from $\mathbb{F}_2^m$ to itself are the permutations of $\mathbb{F}_2^m$. A function F is balanced if and only if all nonzero linear combinations of the coordinate functions of F are balanced, that is if and only if the Boolean function $c \cdot F$ is balanced for every nonzero $c \in \mathbb{F}_2^m$ (see [14]).

Let $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$. The function $\lambda_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \longrightarrow \mathbb{Z}$ defined by

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_2^m} (-1)^{b \cdot F(x) + a \cdot x}, \quad a \in \mathbb{F}_2^n, \quad b \in \mathbb{F}_2^m,$$

is called the *Walsh transform* of the function F. For any elements $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$ the value $\lambda_F(a, b)$ is called the *Walsh coefficient* of F and the set

$$\Lambda_F = \{\lambda_F(a, b) : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, b \neq 0\}$$

is called the *Walsh spectrum* of F. The Walsh coefficients of F with $b \neq 0$ form a $2^n \times (2^m - 1)$ matrix

$$\Lambda(F) = (\lambda_F(a,b))_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m, b\neq 0}.$$

We also denote

$$\lambda_F = \max_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m, b\neq 0} |\lambda_F(a,b)|.$$

The Walsh transform of a function does not depend on a particular choice of the inner product in $\mathbb{F}_2^m$. If we identify $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$ then we can take $x \cdot y = tr(xy)$, where $tr(x) = x + x^2 + ... + x^{2^{m-1}}$ is the trace function from $\mathbb{F}_{2^m}$ into $\mathbb{F}_2$.

The *nonlinearity* of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the value

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2}\lambda_F = \min_{b\in\mathbb{F}_2^m, b\neq 0} \mathcal{NL}(b \cdot F),$$

which equals the minimum Hamming distance between all nonzero linear combinations of the coordinate functions of F and all affine Boolean functions on n variables. The linear cryptanalysis, introduced by Matsui [48], is based on finding affine approximations to the action of a cipher, therefore the linear attack on a function F is successful if $\mathcal{NL}(F)$ is small.

Obviously, the nonlinearity of any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has the same upper bound $\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ as Boolean functions. This bound is called the *universal bound* and functions achieving it have the optimal nonlinearity and they are called *bent.*

Proposition 4 (see [14]) *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is bent if and only if one of the following conditions holds:*

(i) *for any nonzero $c \in \mathbb{F}_2^m$ the Boolean function $c \cdot F$ is bent;*

(ii) $\Lambda_F = \{\pm 2^{\frac{n}{2}}\}$*;*

(iii) *for any nonzero $a \in \mathbb{F}_2^n$ the function $F(x) + F(x + a)$ is balanced.*

The first statement in this proposition is obvious and the second and third clearly follow from Proposition 1.

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *perfect nonlinear* if for any nonzero $a \in \mathbb{F}_2^n$ the *derivative* D_aF is balanced. Clearly, a function F is bent if and only if it is perfect nonlinear. Bent (perfect nonlinear) functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ exist if and only if n is even and $m \leq \frac{n}{2}$ (see [14]). When $m \geq n$ the inequality

$$\mathcal{NL}(F) \leq 2^{n-1} - \frac{1}{2}\left(3 \cdot 2^n - 2(2^n - 1)(2^{n-1} - 1)/(2^m - 1) - 2\right)^{1/2}$$

gives a better upper bound for nonlinearity of functions as it is proven in [19, 61]. This bound can be achieved only if $n = m$ with n odd. We consider this case in details in the next section.

2.3 APN and AB functions

As we noted above the universal bound is reachable only for functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with n even and $m \leq \frac{n}{2}$. For the case $m = n$, a better bound for the nonlinearity exists [19, 61]:

$$\mathcal{NL}(F) \leq 2^{m-1} - 2^{\frac{m-1}{2}}.$$

In case of equality the function F is called *almost bent* (**AB**) or *maximum nonlinear*. Obviously, AB functions exist only for m odd. When m is even functions with the nonlinearity $2^{m-1} - 2^{\frac{m}{2}}$ are known and it is conjectured that this value is the highest possible nonlinearity for the case m even.

For a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and any elements $a, b \in \mathbb{F}_2^m$ we denote by $\delta_F(a,b)$ the number of solutions of the equation $F(x+a) + F(x) = b$, that is,

$$\delta_F(a,b) = |\{x \in \mathbb{F}_2^m : F(x+a) + F(x) = b\}|,$$

and we call the set

$$\Delta_F = \{\delta_F(a,b) : a, b \in \mathbb{F}_2^m, a \neq 0\}$$

the *differential spectrum* of the function F. We also consider the $(2^m - 1) \times 2^m$ matrix

$$\Delta(F) = \big(\delta_F(a,b)\big)_{a,b \in \mathbb{F}_2^m, a \neq 0}$$

which is called the *table of differences* of F.

For any function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ the value $\delta_F = \max_{a,b \in \mathbb{F}_2^m, a \neq 0} \delta_F(a,b)$ is not less than 2. Indeed, for any $a, b \in \mathbb{F}_2^m$, the number $\delta_F(a,b)$ is even since if x_0 is a solution of the equation $F(x+a) + F(x) = b$ then $x_0 + a$ is a solution too. If $\delta_F = 2$ then the function F is called *almost perfect nonlinear* (**APN**).

APN functions possess the best resistance to the differential attack. The differential cryptanalysis presented by Biham and Shamir [4] is based on the study of how differences in an input can affect the resultant difference at the output. The resistance of a function F, used as an S-box in the cipher, to the differential attack is high when the value δ_F is small.

Proposition 5 ([15, 19, 23]) *A function* $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ *is AB if and only if one of the following conditions is satisfied:*
(i) $\Lambda_F = \{0, \pm 2^{\frac{m+1}{2}}\}$*;*
(ii) *for every* $a, b \in \mathbb{F}_2^m$ *the system of equations*

$$\begin{cases} x + y + z & = & a \\ F(x) + F(y) + F(z) & = & b \end{cases}$$

has $3 \cdot 2^m - 2$ *solutions* (x, y, z) *if* $b = F(a)$*, and* $2^m - 2$ *solutions otherwise;*
(iii) *the function* $\gamma_F : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ *defined by the equality*

$$\gamma_F(a, b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } \delta_F(a, b) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

is bent.

The first statement in this proposition is proven in [19], the second in [23] and the proof of the third statement is given in [15].

Proposition 6 ([15, 39]) *A function* $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ *is APN if and only if one of the following conditions holds:*
(i) $\Delta_F = \{0, 2\}$*;*
(ii) *for any* $a \in \mathbb{F}_2^m \backslash \{0\}$ *the set*

$$H_a = \{F(x + a) + F(x) : x \in \mathbb{F}_2^m\}$$

contains 2^{m-1} *elements, that is* $|H_a| = 2^{m-1}$*;*
(iii) *for every* $(a, b) \neq 0$ *the system*

$$\begin{cases} x + y & = & a \\ F(x) + F(y) & = & b \end{cases}$$

admits 0 *or* 2 *solutions;*
(iv) *for any* $a \in \mathbb{F}_2^m \backslash \{0\}$ *the derivative* $D_a F$ *is a two-to-one mapping;*
(v) *the Boolean function* γ_F *has the weight* $2^{2m-1} - 2^{m-1}$*;*
(vi) F *is not affine on any* 2*-dimensional affine subspace of* $\mathbb{F}_2^m$*.*

The statements (i-iv) in the proposition easily follow from the definition of APN functions and claims (v) and (vi) are proven in [15] and [39] respectively.

For any function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ we have the following inequality

$$\sum_{a,b \in \mathbb{F}_2^m} \lambda_F(a,b)^4 \geq 3 \cdot 2^{4m} - 2^{3m+1}$$

and the equality occurs if and only if F is APN ([19], see also [14]). This implies that every AB function is APN. Indeed, because of Parseval's relation (2.1) the number of nonzero values $\lambda_F(a,b)$ is 2^{m-1} for any fixed $b \in \mathbb{F}_2^m \backslash \{0\}$ when F is AB. Then

$$\sum_{a,b \in \mathbb{F}_2^m} \lambda_F(a,b)^4 = 2^{4m} + \sum_{b \in \mathbb{F}_2^m \backslash \{0\}} \sum_{a \in \mathbb{F}_2^m} \lambda_F(a,b)^4 = 2^{4m} + (2^m - 1) 2^{m-1} 2^{2m+2} = 3 \cdot 2^{4m} - 2^{3m+1}.$$

We know that the bentness of a function implies its perfect nonlinearity and vice versa, that is, $\lambda_F = \{\pm 2^{\frac{n}{2}}\}$ for a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if $D_a F$ is one-to-one for any $a \neq 0$. It is not quite the case with AB and APN functions. Not every APN function is AB. However, every quadratic APN function is AB (see [15]). For the general case the following proposition gives sufficient conditions for APN functions to be AB.

Proposition 7 ([8]) *An APN function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is AB if and only if one of the following conditions is fulfilled:*
(i) *all the values in Λ_F are divisible by $2^{\frac{m+1}{2}}$;*
(ii) *for any $c \in \mathbb{F}_2^m$ the function $c \cdot F$ is plateaued.*

For EA equivalent functions F and F' we have $\Delta_F = \Delta_{F'}$, $\Lambda_F = \Lambda_{F'}$ and if F is a permutation then $\Delta_F = \Delta_{F^{-1}}$, $\Lambda_F = \Lambda_{F^{-1}}$ (see [15]). Therefore, if F is APN (resp. AB) and F' is EA equivalent to either F or F^{-1} (if F is a permutation), then F' is also APN (resp. AB). Moreover, APN and AB functions satisfy the following property of stability, which is considered carefully in Section 3.

Proposition 8 ([15]) *Let F be an APN (resp. AB) function on $\mathbb{F}_2^m$ and L_1, L_2 be two linear functions from $\mathbb{F}_2^{2m}$ to $\mathbb{F}_2^m$. Assume that (L_1, L_2) is a permutation on $\mathbb{F}_2^{2m}$ and that the function $F_1(x) = L_1(x, F(x))$ is a permutation on $\mathbb{F}_2^m$. Then, denoting $F_2(x) = L_2(x, F(x))$, the function $F_2 \circ F_1^{-1}$ is APN (resp. AB).*

There are a few known classes of APN and AB functions (all of them correspond to power functions), but using Proposition 8 one can construct from power functions a huge number of highly nonlinear polynomials. It is proven in [15] that the inverse and EA transformations are particular cases of the transformation of functions given in Proposition 8 and we show in Section 4 that this transformation is more general.

2.3.1 APN permutations and some nonexistence results for APN functions

The existence of APN permutations on $\mathbb{F}_{2^m}$ is an open problem when m is even. It was conjectured by Canteaut, Carlet, Charpin, Dobbertin and Zinoviev that the answer is negative. This conjecture was carefully studied by X.-D. Hou and in the theorem below we give some nonexistence results proven in [39].

Theorem 1 ([39]) *Let $m = 2n$ and a function F be a permutation on $\mathbb{F}_{2^m}$. Then F is not APN if one of the following conditions holds:*
(i) *n is even and $F \in \mathbb{F}_{2^4}[x]$;*
(ii) *F is a polynomial with coefficients in $\mathbb{F}_{2^n}$.*

It obviously follows from this theorem that for m even there exists no APN permutation $F \in \mathbb{F}_2[x]$.

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a function with coefficients in $\mathbb{F}_2^n$, where n is a proper divisor of m. Then clearly if F is not APN on $\mathbb{F}_2^n$ then F is not APN on $\mathbb{F}_2^m$.

The following proof that APN power functions are permutations on $\mathbb{F}_{2^m}\backslash\{0\}$ if m is odd and 3-to-1 if m is even is due to Dobbertin. If $x \neq 1$ then $x = (y+1)/y$ for a unique $y \in \mathbb{F}_{2^m}$, $y \neq 0, 1$. The equality $x^d = 1$ implies

$$(y+1)^d + y^d = 0 = (y^2+1)^d + (y^2)^d.$$

If x^d is APN then $y^2 + y + 1 = 0$, since $y^2 \neq y$. Thus, $y \in \mathbb{F}_4\backslash\{0\}$ and then $x \in \mathbb{F}_4\backslash\{0\}$. Since we assumed that $x \neq 1$ then $\mathbb{F}_4$ must be a subfield of $\mathbb{F}_{2^m}$ and then m is even. For m even d must be divisible by 3, otherwise the restriction of x^d to $\mathbb{F}_4$ is linear and then x^d is not APN.

For m even a more general result can be found in [14].

Proposition 9 (see [14]) *If $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ is the polynomial representation of a function F and $\sum_{j=1}^{(2^m-1)/3} c_{3j} = 0$ then F is not APN when m is even. For a power APN function it means that F is not a permutation.*

The following proposition gives a condition when a function is not APN.

Proposition 10 ([15]) *Let n be a proper divisor of m, a function $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ have the univariate polynomial representation $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ and $c_i \neq 0$ implies $i \equiv 2^j$* mod $(2^n - 1)$. *Then F is not APN.*

Below we give another nonexistence result similar to Proposition 10.

Proposition 11 *Let $n > 2$ be a divisor of m, a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ have the univariate polynomial representation $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ and $c_i \neq 0$ implies either $i \equiv 2^j \mod (2^n-1)$ or $i \equiv 0 \mod (2^n - 1)$. Then F is not APN.*

Proof. Obviously in conditions of the statement $D_1F(x) = D_1F(y)$ for all $x, y \in \mathbb{F}_2^n$, $x, y \notin \{0, 1\}$, and therefore F is not APN when $n > 2$. □

We pay a special attention to power functions with exponents $d = \sum_{i=1}^{k-1} 2^{in} - 1$ on the fields $\mathbb{F}_{2^m}$ where $m = nk$, $k > 1$, $n \geq 1$, because in cases when either $n = 1$ or $k = 5$ we get the only known APN power functions which are not AB. In the next proposition we give some conditions when these functions are not APN. Further we also show (see Corollary 6) that none of these functions is AB, but we leave an open question whether these class of functions provides other cases of APN mappings.

Proposition 12 *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$, $d = \sum_{i=1}^{k-1} 2^{in} - 1$, and $m = nk$ for some integers $n, k > 1$. Then F is not APN if one of the following conditions is fulfilled:*
1. $k = 2^l + 2$ for some integer l;
2. $k = 2$ and $n > 2$.

Proof. If $k = 2^l + 2$ in conditions of this proposition, then $d \mod (2^n - 1) = 2^l$. Thus, F is not APN by Proposition 10. If $k = 2$ then $d \mod (2^n - 1) = 0$ and by Proposition 11 the function F is not APN when $n > 2$. If $k = 2$ and $n = 2$ then we get the APN function $F(x) = x^3$ on $\mathbb{F}_{2^4}$. □

The proposition below gives a condition when a function is neither a permutation nor AB. This result is generalized in this work also for s-nonlinear functions.

Proposition 13 ([15]) *Let $n = 2^m - 1$ and k be a proper divisor of n. If F is a function on $\mathbb{F}_{2^m}$ with the univariate polynomial representation $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ and $c_i \neq 0$ implies $i = kr$ for some r, $0 \leq r \leq n/k$ then F is neither a permutation nor AB.*

Further results related to the nonexistence of APN permutations one can find in [55]. In particular, it is proven there that in m even case there do not exist quadratic APN permutations and, more generally, APN permutations whose coordinate functions are partially bent, as well as all their linear combinations.

2.3.2 Connections with coding theory

Here we consider an interpretation of APN and AB functions in terms of coding theory.

Any linear subspace C of $\mathbb{F}_2^n$ of dimension k is called a *binary linear code of length n and dimension k* and is denoted by $[n,k]$. Any linear code C is associated with its *dual* $[n,n-k]$ code denoted

$$C^\perp = \{x \in \mathbb{F}_2^n : \quad c \cdot x = 0, \quad \forall c \in C\}.$$

The (Hamming) *weight* of any vector $x \in \mathbb{F}_2^n$ is denoted by $wt(x)$. The distance between any two vectors x and y of $\mathbb{F}_2^n$ is denoted $d(x,y)$. The number $d = \min_{c\in C, c\neq 0} wt(c)$ is called the *minimum distance* of the linear code C. A binary code is 2^l *divisible* if the weight of any of its codewords is divisible by 2^l.

Let H be a binary $(r \times n)$ matrix. We say that a linear binary code C of length n is defined by the *parity check matrix* H if $C = \{c \in \mathbb{F}_2^n : cH^t = 0\}$, where H^t is the transposed matrix of H.

APN and AB properties were expressed in terms of codes in [15].

Theorem 2 ([15]) *Let F be a function on $\mathbb{F}_{2^m}$ with $F(0) = 0$. Let C_F be a linear binary code of length $2^m - 1$ defined by the parity-check matrix*

$$H_F = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^m-2}) \end{pmatrix}$$

where each entry is viewed as a binary vector and α is a primitive element of $\mathbb{F}_{2^m}$. Then

(i) *the code C_F is such that* $\dim C_F \geq 2^m - 1 - 2m$ *and* $3 \leq d \leq 5$, *where d is the minimum distance of C_F;*

(ii) *F is APN if and only if the code C_F has the minimum distance* 5*;*

(iii) $\lambda_F = 2^m$ *if and only if* $\dim C_F > 2^m - 1 - 2m$ *or $C_F^\perp$ contains the all-one vector;*

(iv) *if F is APN then* $\dim C_F = 2^m - 1 - 2m$ *and $C_F^\perp$ does not contain the all-one vector;*

(v) *F is AB if and only if the weight of every codeword in $C_F^\perp$ lies in* $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$.

The connection between the weights of codewords of $C_F^\perp$ and the Walsh spectrum of F is given by the equality (cf. the proof of Th. 5 in [15])

$$\{\lambda_F(a,b) : a,b \in \mathbb{F}_2^m\} = \{2^m - 2\omega t(c) : c \in C_F^\perp\}. \tag{2.2}$$

The equality above and Proposition 7 lead to the following result.

Corollary 1 ([8]) *Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and m be odd. Then F is AB if and only if it is APN and the code $C_F^\perp$ is $2^{\frac{m-1}{2}}$-divisible.*

The *covering radius* ρ of a code $C \subseteq \mathbb{F}_2^n$ is the value

$$\rho = \max_{a\in\mathbb{F}_2^n} \min_{c\in C} d(a,c).$$

It is proven in [15] that the covering radius ρ of the code C_F for any APN function F is such that $3 \leq \rho \leq 4$. Recall that a code C is *completely regular* if for any of its coset U,

$$U = a + C = \{a + c : c \in C\},$$

the weight distribution of U is uniquely defined by its minimum weight. If a function F is AB then C_F is a completely regular code [15].

A linear binary code C of length n is *cyclic* if for all codewords $(c_0, ..., c_{n-1})$ in C, the vector $(c_{n-1}, c_0..., c_{n-2})$ is also in C. If we identify a vector $(c_0, ..., c_{n-1})$ of $\mathbb{F}_2^n$ with the polynomial $c(x) = c_0 + c_1x + ... + c_{n-1}x^{n-1}$ then any linear binary cyclic code is an ideal of the ring $\mathbb{F}_2[x]/(x^n - 1)$ of the polynomials over $\mathbb{F}_2$ modulo $(x^n - 1)$. For any such code C there exists a unique monic polynomial $g(x)$, called the *generator polynomial* of C, such that any element $c(x)$ of C can be uniquely expressed in the form $c(x) = a(x)g(x)$. The roots of the generator polynomial are called the *zeros* of the code C. If $n = 2^m - 1$ and α is a primitive element of $\mathbb{F}_2^m$ then the *defining set* of C is the set

$$I(C) = \{i \quad : \quad 0 \leq i \leq 2^m - 2, \quad \alpha^i \text{ is a zero of } C\}.$$

The following theorem due to McEliece reduces the determination of the exact weight divisibility of binary cyclic codes to a combinatorial problem.

Theorem 3 ([49]) *A binary cyclic code is exactly 2^l-divisible if and only if l is the smallest number such that $(l + 1)$ nonzeros of C (with repetitions allowed) have product 1.*

When $F(x) = x^k$, the corresponding code $C_{1,k}$ is a binary cyclic code of length $(2^m - 1)$ whose defining set is the union of two cyclotomic classes of 1 and k. McEliece's theorem was formulated for the duals of this kind of codes in the following way [9].

Theorem 4 ([9]) *The cyclic code $C_{1,k}^{\perp}$ of length $(2^m - 1)$ is exactly 2^l-divisible if and only if for all u such that $0 \leq u \leq 2^m - 1$,*

$$\omega_2(A(u)) \leq \omega_2(u) + m - 1 - l,$$

where $A(u) = uk \mod (2^m - 1)$.

This leads to the following characterization of AB power functions.

Corollary 2 ([9]) *Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$, $F(x) = x^k$, and m be odd. Then F is AB if and only if it is APN and for any u, $1 \leq u \leq 2^m - 1$, the condition $w_2(A(u)) \leq (m-1)/2 + w_2(u)$, where $A(u) = uk \mod (2^m - 1)$, is fulfilled.*

The next proposition is helpful to prove that Dobbertin APN functions (see further) are not AB.

Proposition 14 ([9]) *Let m, d be such integers that for some divisor n of m the condition*

$$d \equiv -d_0 \mod \frac{2^m - 1}{2^n - 1},$$

with $0 < d_0 < (2^m - 1)/(2^n - 1)$ and $w_2(d_0) \leq \frac{1}{2}(\frac{m}{n} - 3)$, is satisfied. Then $F(x) = x^d$ is not AB on $\mathbb{F}_{2^m}$.

2.3.3 The case of power functions

There are natural reasons that the main attention in the study of APN and AB functions has been payed to power functions. Maximum nonlinear power functions correspond to binary cyclic codes with two zeros, whose duals are optimal, and to pairs of maximum-length sequences (called M-sequences) with preferred crosscorrelation, which are used for spread-spectrum communications.

A binary sequence which satisfies a linear recurrence relation $s_i = a_1 s_{i-1} + ... + a_m s_{i-m}$ is called *maximum-length* or an *M-sequence* if its period equals $2^m - 1$, which is the maximum possible value. Let $s[1] = (s_0, s_1, s_2, ...s_i, ...)$ denote a binary M-sequence of length $2^m - 1$

and let $s[d] = (s_0, s_d, s_{2d}, ..., s_{id}, ...)$ denote its decimation by an integer d with $\gcd(2^m - 1, d) = 1$. The function

$$C_d(t) = \sum_{i=0}^{2^m-2} (-1)^{s_{id}+s_{i+t}}, \qquad 0 \le t \le 2^m - 2,$$

is called the *crosscorrelation function* between the sequences $s[1]$ and $s[d]$.

The determination of the crosscorrelation spectra for different values of d (with $\gcd(2^m - 1, d) = 1$) is an important problem which has been considered in many papers (see for example [8, 22, 24, 30, 32, 34, 35, 36, 52]). It is proven in [34] that the crosscorrelation function between two (cyclically distinct) M-sequences takes at least three different values. The values of d with three valued crosscorrelation functions are the objects of special interest. A pair of binary M-sequences with three valued crosscorrelation function with values

$$-1, -1 \pm 2^{\lfloor \frac{m+1}{2} \rfloor}$$

is called a *preferred pair.* When $m \equiv 0 \mod 4$ then no pairs of preferred sequences exist as it was conjectured by Sarwate and Pursley [60] and proven by McGuire and Calderbank [50]. There exist pairs of preferred sequences for all other cases (for instance, see the Gold case).

It is well known that for any M-sequence $p = (p_0, ..., p_i, ...)$ there exists a unique $c \in \mathbb{F}_{2^m}^*$ such that $p_i = tr(c\alpha^i)$, $0 \le i \le 2^m - 2$, where α is a primitive element of $\mathbb{F}_{2^m}$. Since the crosscorrelation spectrum only depends on d and not on the choice of M-sequence $s[1]$ we can assume without loss of generality that $s[1]$ is given by $s_i = tr(\alpha^i)$, $0 \le i \le 2^m - 2$. Then $s_{id} = \alpha^{di}$, $0 \le i \le 2^m - 2$, and

$$C_d(t) = \sum_{i=0}^{2^m-2} (-1)^{tr(\alpha^{id}+\alpha^{i+t})} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{tr(x^d+ax)} = -1 + \lambda_F(a, 1),$$

where $F(x) = x^d$ and $a = \alpha^t$. Since $\gcd(2^m - 1, d) = 1$, then the power function F is a permutation and $\lambda_F(a, b) = \lambda_F(ab^{-\frac{1}{d}}, 1)$. Therefore, the crosscorrelation function $C_d(t)$ is three valued if and only if x^d has a three valued Walsh spectrum and if m is odd then the pair of M-sequences with crosscorrelation function $C_d(t)$ is preferred if and only if x^d is AB.

The checking of the APN and AB properties of power functions is easier than in the case of arbitrary polynomials. If F is a power function, that is $F(x) = x^d$, then F is APN if and only if the derivative D_1F is a two-to-one mapping. Indeed, since for any $a \neq 0$

$$D_aF(x) = (x+a)^d + x^d = a^d D_1F(x/a)$$

then D_aF is a two-to-one mapping if and only if D_1F is two-to-one.
Besides, the function $F(x) = x^d$ is AB if and only if $\lambda_F(a,b) \in \{0, \pm 2^{\frac{m+1}{2}}\}$ for $a \in \mathbb{F}_2$, $b \in \mathbb{F}_2^m \backslash \{0\}$, since $\lambda_F(a,b) = \lambda_F(1, a^{-d}b)$ for $a \in \mathbb{F}_2^m \backslash \{0\}$.

Proposition 15 describes the minimum degree of a power function and Proposition 16 gives a sufficient condition for a function to be EA-inequivalent to power functions.

Proposition 15 ([10]) *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$. Then for any $c \in \mathbb{F}_{2^m}^*$ either $tr(cF) = 0$ or $d^\circ\big(tr(cF)\big) = d^\circ(F)$. If F is a permutation then $d^\circ(F) = \min d^\circ(F)$.*

Proposition 16 *Let F be a function from $\mathbb{F}_{2^m}$ to itself. If there exists an element $c \in \mathbb{F}_{2^m}^*$ such that $d^\circ\big(tr(cF)\big) \neq d^\circ(F)$ and $d^\circ\big(tr(cF)\big) > 1$, then F is EA-inequivalent to power functions.*

Proof. By Proposition 15 for any power function x^d and for any $c \in \mathbb{F}_{2^m}$, either the function $tr(cx^d)$ completely vanishes or it has exactly the algebraic degree $w_2(d)$. Thus, for any function F which is affine equivalent to a power function, we have either $tr(cF) = 0$ or $d^\circ\big(tr(cF)\big) = d^\circ(F)$, $c \in \mathbb{F}_{2^m}$. Therefore, if F is EA-equivalent to a power function then either $d^\circ\big(tr(cF)\big) = d^\circ(F)$ or $d^\circ\big(tr(cF)\big) \leq 1$, for every $c \in \mathbb{F}_{2^m}$. □

Since APN power functions are permutations on the fields $\mathbb{F}_{2^m}$ with m odd then the following statement is true.

Proposition 17 *Let F be an APN function on $\mathbb{F}_{2^m}$ with $d^\circ(F) \neq \min d^\circ(F)$ and m be odd. Then F is EA-inequivalent to power functions.*

Propositions 16 and 17 have important applications in Chapter 4.

The exponent d, $0 \leq d < 2^m - 1$, of a power function $F(x) = x^d$ on $\mathbb{F}_{2^m}$ gives an *equivalence class* (d) of exponents

$$(d) = \begin{cases} \{2^i d, \quad 2^i/d \quad : 0 \leq i < m\} & \text{if } x^d \text{ is a permutation} \\ \{2^i d \quad : 0 \leq i < m\} & \text{otherwise} \end{cases},$$

i.e. (d) is a union of 2-cyclotomic cosets of d and $\frac{1}{d}$ modulo $2^m - 1$ if x^d is a permutation, otherwise (d) is the 2-cyclotomic coset of d modulo $2^m - 1$. If d and d' belong to the same equivalence class then we call the power functions x^d and $x^{d'}$ *cyclotomic* equivalent. Obviously, if power functions F and F' are cyclotomic equivalent then $\Delta_F = \Delta_{F'}$ and $\Lambda_F = \Lambda_{F'}$.

Table 1 (resp. Table 2) gives all known values of exponents d (up to cyclotomic equivalence) such that the power function x^d is APN (resp. AB) and Table 3 gives all known values of d that x^d has the best known nonlinearity (that is, $2^{m-1} - 2^{\frac{m}{2}}$) on the field $\mathbb{F}_{2^m}$ with m even.

Table 1

Known APN power functions x^d on $\mathbb{F}_{2^m}$.

	Exponents d	Conditions	$d^\circ(x^d)$	Proven in
Gold functions	$2^i + 1$	$\gcd(i, m) = 1$	2	[33, 54]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1$	$i + 1$	[41, 42]
Welch function	$2^t + 3$	$m = 2t + 1$	3	[27]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$ $2^t + 2^{\frac{3t+1}{2}} - 1$	$m = 2t + 1$, t even $m = 2t + 1$, t odd	$(t + 2)/2$ $t + 1$	[26]
Inverse function	$2^{2t} - 1$	$m = 2t + 1$	$m - 1$	[3, 54]
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$m = 5i$	$i + 3$	[28]

Table 2

Known AB power functions x^d on $\mathbb{F}_{2^m}$, m odd.

	Exponents d	Conditions	Proven in
Gold functions	$2^i + 1$	$\gcd(i, m) = 1$	[33, 54]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1$	[42]
Welch function	$2^t + 3$	$m = 2t + 1$	[8, 9]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$ $2^t + 2^{\frac{3t+1}{2}} - 1$	$m = 2t + 1$, t even $m = 2t + 1$, t odd	[38]

Table 3

Known power permutations x^d with the highest known nonlinearity on $\mathbb{F}_{2^m}$, $m = 2t$.

Exponents d	Conditions	Proven in
$2^i + 1$	$\gcd(i, m) = 2$, t odd	[33]
$2^{2i} - 2^i + 1$	$\gcd(i, m) = 2$, t odd	[42]
$2^{m-1} - 1$		[44]
$2^t + 2^{\frac{t+1}{2}} + 1$	t odd	[22]
$2^t + 2^{t-1} + 1$	t odd	[22]
$2^t + 2^{\frac{t}{2}} + 1$	$t \equiv 2 \mod 4$	[24]
$\sum_{k=0}^{t} 2^{ik}$	$\gcd(i, m) = 1$, t even	[24, 52]

The power functions with the exponents $d = 2^i + 1$ were first considered by Gold within the framework of M-sequences. The proof of APN and AB properties of the Gold functions is easy. If $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$, then

$$D_1F(x) = x^{2^i+1} + (x+1)^{2^i+1} = x^{2^i} + x + 1$$

and, obviously, D_1F is a 2^s-to-one mapping if and only if the kernel of the linear function $x^{2^i} + x$ consists of 2^s elements, that is $\gcd(i, m) = s$. If m/s is odd then F is a permutation and we need to consider only $\lambda_F(a, 1)$, $a \in \mathbb{F}_2^m$, to determine the Walsh spectrum of F. We have

$$\lambda_F(a, 1) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr(x^d)+tr(ax)}$$

and using the Welch's squaring method we get

$$\begin{aligned}
\lambda_F(a, 1)^2 &= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{tr(x^d)+tr(y^d)+tr(a(x+y))} = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(ay)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr(x^d)+tr((x+y)^d)} \\
&= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^d)+tr(ay)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr(x^{2^i}y+xy^{2^i})} \\
&= \sum_{y \in \mathbb{F}_{2^m}} (-1)^{tr(y^d)+tr(ay)} \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr((y^{2^i}+y^{2^{-i}})x)} = 2^m \sum_{y \in \mathbb{F}_{2^s}} (-1)^{tr(y^d)+tr(ay)},
\end{aligned}$$

since $y^{2^i} + y^{2^{-i}} = 0$ means $y^{2^{2i}-1} = 1$ and $y^{2^{\gcd(2i,m)}} = 1$, then $y \in \mathbb{F}_{2^s}$.
The function y^d is linear on $\mathbb{F}_{2^s}$, therefore

$$tr(y^d + ay) = tr(y(1 + a)) = tr_s(y\ tr_{m/s}(1 + a))$$

and since m/s is odd

$$\lambda_F(a,1)^2 = \begin{cases} 2^{m+s} & \text{if} \quad tr_{m/s}(1+a) = 0 \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 2^{m+s} & \text{if} \quad tr_{m/s}(a) = 1 \\ 0 & \text{otherwise} \end{cases} .$$

That completes the proof that if $\gcd(i,m) = s$ then $\Delta_F = \{0, 2^s\}$ and if m/s is odd then $\Lambda_F = \{0, \pm 2^{\frac{m+s}{2}}\}$.

The power functions $F(x) = x^d$ with the exponents $d = 2^{2i} - 2^i + 1$ were first studied in the context of coding theory. In 1971 Kasami showed that when $\gcd(i,m) = s$ and m/s is odd then the Walsh spectrum of F is $\{0, \pm 2^{\frac{m+s}{2}}\}$ (actually this result is due to Welch (1969), but it was never published by him). If m is odd and $\gcd(i,m) = 1$ then, obviously, F is AB and therefore also APN. The APN property of F for m even and $\gcd(i,m) = 1$ was proven by Janva and Wilson [41] by using methods of algebraic geometry. Dobbertin gives another proof of AB property of Kasami functions in [25] and he also gives a direct proof of the APN property of F in [27]. Since $d = 2^{2i} - 2^i + 1 = \frac{2^{3i}+1}{2^i+1}$ then the AB property of the Kasami functions (as well as the Gold functions) can be obtained from the fact proven in [15] that any APN function of the form $F_1 \circ F_2^{-1}$, where the mappings F_1, F_2 are quadratic and F_2 is a permutation, is AB.

It was conjectured by Welch (in terms of M-sequences) that the power function $F(x) = x^d$ with the exponent $d = 2^{(m-1)/2} + 3$ is AB. This conjecture was mentioned in the paper of Golomb [32] in 1968 and only in 2000 the conjecture was proven by Canteaut, Charpin and Dobbertin [8]. The proof is based on the proof of APN property of F given by Dobbertin [27] and on McEliece's theorem on divisible codes [49].

In 1972 Niho conjectured in his thesis [52] that the power function $F(x) = x^{2^{2i}+2^i-1}$ where $4i + 1 \equiv 0 \mod m$, is AB. The APN property of this function was proven by Dobbertin [26] in 1999, and in 2001 the conjecture was proven by Hollman and Xiang [38].

In his proofs of the APN property of Kasami, Welch and Niho functions Dobbertin presents $D_1 F$ as a composition of a two-to-one mapping of the type $x^{2^r} + x$ and a permutation, then the proofs come to showing that certain polynomials are permutations. The proofs are technical and complicated.

The last case of APN power functions was found in 1999 by Canteaut and Dobbertin, and proven by Dobbertin in 2000 by multivariate equation method. It is shown in [9] that this function is not AB.

Let F be the inverse mapping on $\mathbb{F}_{2^m}$, i.e.

$$F(x) = x^{2^m-2} = \begin{cases} \frac{1}{x} & \text{if} \quad x \neq 0 \\ 0 & \text{if} \quad x = 0 \end{cases} .$$

Then the equation $x^{2^m-2} + (x+1)^{2^m-2} = b$ admits 0 and 1 for solutions if and only if $b = 1$. The solutions of this equation, which are different from 0 and 1, are also the solutions of $x^2 + x + b^{-1} = 0$, $b \neq 0$. Therefore, $\delta_F(1, b) \in \{0, 2\}$ for $b \neq 1$ and

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

Indeed, by squaring the equation $x^2 + x + 1 = 0$ and substituting $x^2 = x + 1$ we get the equality $x^4 = x$, which is satisfied only for $x \in \mathbb{F}_{2^2}$. Thus, the inverse function is APN when m is odd and has the differential spectrum $\Delta_F = \{0, 2, 4\}$ when m is even. The inverse APN function is not AB since it has the algebraic degree $m - 1$ while the algebraic degree of any AB function is not greater than $(m + 1)/2$ (see [15]). The Walsh spectrum of the inverse function was determined by Lachaud and Wolfmann in [44]. If m is even then it consists of all integers $s = 0 \mod 4$ in the range $-2^{\frac{m}{2}+1}, ..., 2^{\frac{m}{2}+1}$ and, therefore, the inverse function has the best known nonlinearity for m even.

2.4 Differential uniformity and plateaued mappings

In this section we generalize some results related to APN and AB functions for differentially δ-uniform and vectorial plateaued functions respectively.

Plateaud mappings. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *plateaued* if all nonzero linear combinations of its coordinate functions are plateaued with the same amplitude. Further we consider the class of vectorial plateaued functions from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ which is a natural extension of the class of AB functions.

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called *t-th order correlation immune* if it is balanced when any t of the inputs are fixed. F is t-th order correlation immune if and only if $\lambda_F(a, b) = 0$ for every $a \in \mathbb{F}_2^n$ such that $1 \leq wt(a) \leq r$ and every nonzero $b \in \mathbb{F}_2^m$. Balanced t-th order correlation immune functions are called *t-resilient*. Obviously, F is t-resilient if and only if for any nonzero $b \in \mathbb{F}_2^m$ the Boolean function $b \cdot F$ is t-resilient. The notion of vectorial resilient functions is relevant in cryptography to quantum cryptographic key distribution [2] and pseudo-random sequence generation for stream ciphers.

As we mentioned above the class of plateaued Boolean functions contains the functions which achieve the best possible trade-offs between resiliency, nonlinearity and algebraic degree, and therefore the same is true for the class of vectorial plateaued functions. However, there is another notion of nonlinearity relevant to mappings (S-boxes) used in pseudo-random generators in stream ciphers [68, 18]. The *unrestricted nonlinearity* $\mathcal{UNL}(F)$ of a function F from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$ is the minimum Hamming distance between all non-constant affine functions and all Boolean functions $g \circ F$, where g is any non-costant Boolean function on m variables. In the case of block ciphers, due to their iterative structure, the knowledge of a nonlinear combination of the outputs to F with a low nonlinearity did not lead to a correlation attack, unless its degree was very low. On the contrary, since the structure of the pseudo-random generators using combining or filtering functions is not iterative, all of the m binary sequences prodused by a function can be combined by non-constant m-variable Boolean function g to perform correlation attacks. If $\mathcal{UNL}(F)$ is small then one of the non-constant (linear or nonlinear) combinations of the output bits to F has high correlation to a nonconstant affine function of the input, and a correlation attack is feasible. The unrestricted nonlinearity is unchanged when F is right composed with an affine invertible mapping. Moreover, if A is a surjective affine function from $\mathbb{F}_2^p$ into $\mathbb{F}_2^n$ then $\mathcal{UNL}(F \circ A) = 2^{p-n}\mathcal{UNL}(F)$. Also for every function $G : \mathbb{F}_2^m \to \mathbb{F}_2^p$ we have $\mathcal{UNL}(\mathcal{G} \circ \mathcal{F}) \geq \mathcal{UNL}(F)$ and if G is a permutation on $\mathbb{F}_2^m$ then $\mathcal{UNL}(G \circ F) = \mathcal{UNL}(F)$. Obviously, if F is a permutation on $\mathbb{F}_2^m$ then $\mathcal{UNL}(F) = \mathcal{UNL}(F^{-1} \circ F) = 0$. More information about unrestricted nonlinearity can be found in [14].

Let a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a vectorial plateaued function with the amplitude λ, that is $\Lambda_F = \{0, \pm\lambda\}$. Then λ is equal to $2^{\frac{m+s}{2}}$ for some s, $1 \leq s \leq m$, and we shall say that F is *s-nonlinear*. Obviously, the AB functions correspond to the 1-nonlinear functions.

The proposition below gives a characterization of s-nonlinear functions through their second order derivatives; the proof obviously follows from Proposition 3.

Proposition 18 *A function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is s-nonlinear if and only if there exists σ such that for every $x \in \mathbb{F}_2^m$ and every nonzero $c \in \mathbb{F}_2^m$, $\sum_{a,b\in\mathbb{F}_2^m}(-1)^{D_aD_b[c\cdot F(x)]} = \sigma$. If this condition is satisfied then $\sigma = 2^{m+s}$.*

All linear functions are m-nonlinear. If F is a quadratic mapping on $\mathbb{F}_2^m$ then for all nonzero $c \in \mathbb{F}_2^m$ the Boolean functions $c \cdot F$ are plateaued. However, in these conditions F is not necessarily s-nonlinear. For example, the functions x^{2^i+1}, with $\gcd(i,m) = s$ and m/s even, are not s-nonlinear.

The algebraic degree of any AB function is upper bounded by $\frac{m+1}{2}$ ([15]). It is easy to get an upper bound for s-nonlinear functions using the same argumentation like in the AB case. If all the values of the Walsh transform of a Boolean function are divisible by 2^k then its algebraic degree is at most $m-k+1$ ([46]). The algebraic degree of any function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is equal to the maximum algebraic degree of the Boolean functions $c \cdot F$, $c \in \mathbb{F}_2^m$. If F is s-nonlinear then for any nonzero $c \in \mathbb{F}_2^m$ the values of the Walsh transform of the Boolean function $c \cdot F$ are divisible by $2^{\frac{m+s}{2}}$. Therefore, $d^\circ(c \cdot F) \leq m - \frac{m+s}{2} + 1$, $c \in \mathbb{F}_2^m$, and $d^\circ(F) \leq \frac{m-s}{2} + 1$.

Proposition 19 *Let F be an s-nonlinear function on $\mathbb{F}_2^m$. Then the algebraic degree of F is not greater than $\frac{m-s}{2} + 1$.*

In particular, if a power function x^d is s-nonlinear on $\mathbb{F}_{2^m}$ then $w_2(d) \leq \frac{m-s}{2} + 1$ ([9]).

Some nonexistence results of AB functions can be generalized for s-nonlinear mappings.

Proposition 20 *Let $n = 2^m - 1$ be a composite number and k a proper divisor of n which is not a divisor of $2^s - 1$. If F is a function on $\mathbb{F}_{2^m}$ with the univariate polynomial representation $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ and $c_i \neq 0$ implies $i = kr$ for some r, $0 \leq r \leq n/k$ then F is not s-nonlinear.*

Proof. By hypothesis, there exists a polynomial $P(x)$ such that $F(x) = P(x^k)$. Let $u = n/k$ and $d = \alpha^u$, where α is a primitive element of $\mathbb{F}_{2^m}$. We have $d \neq 1$ and $F(dx) = P(d^k x^k) = P(x^k) = F(x)$. Thus F is a constant on each set

$$\{d^i x : i = 0, ..., k-1\}, \quad x \in \mathbb{F}_{2^m}^*.$$

All these sets have the same cardinality k and define a partition of $\mathbb{F}_{2^m}^*$. Thus the sum

$$\sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{tr(bF(x))}$$

is divisible by k. We deduce that for every b, the integer k is a divisor of $\lambda_F(0,b) \pm 1$. If $\Lambda_F = \{0, \pm 2^{\frac{m+s}{2}}\}$ then k is a divisor of ± 1, $2^{\frac{m+s}{2}} \pm 1$ which is impossible since

$$(2^{\frac{m+s}{2}} + 1)(2^{\frac{m+s}{2}} - 1) = 2^{m+s} - 1 = 2^s(2^m - 1) + (2^s - 1)$$

and k is not a divisor of $2^s - 1$. □

Arguments similar to the ones in the proof of Proposition 20 show that if $F(x) = x^d$ is s-nonlinear on $\mathbb{F}_{2^m}$ then $\gcd(d, 2^m - 1)$ is a divisor of $\gcd(d, 2^s - 1)$. In AB case that means $\gcd(d, 2^m - 1) = 1$.

Differentially uniform mappings. APN property of functions is a particular case of a notion introduced by Nyberg [54]. A function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is called differentially δ-uniform if $\delta_F \leq \delta$. In this work we call a function F *differentially δ-uniform* if $\Delta_F = \{0, \delta\}$. Obviously, APN functions are differentially 2-uniform.

A function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is differentially δ-uniform if and only if the derivative $D_a F$ is a δ-to-one mapping for all nonzero elements $a \in \mathbb{F}_2^m$. Therefore, δ is a divisor of 2^m and equals 2^s for some s, $1 \leq s \leq m$.

It is obvious that a function F is differentially 2^s-uniform if and only if

$$\sum_{(a,b)\neq(0,0)} \delta_F(a,b) = 2^s \sum_{(a,b)\neq(0,0)} \gamma_F(a,b).$$

On the other hand ,

$$\sum_{(a,b)\neq(0,0)} \delta_F(a,b) = 2^m(2^m - 1).$$

Therefore, if F is differentially 2^s-uniform then the sum $\sum_{(a,b)\neq(0,0)} \gamma_F(a,b)$ is equal to $2^{2m-s} - 2^{m-s}$. That implies if F is differentially 2^s-uniform then the Boolean function γ_F has weight $2^{2m-s} - 2^{m-s}$.

If F is differentially 2^s-uniform then for $a \neq 0$

$$\sum_{b\in\mathbb{F}_2^m} \delta_F(a,b) = 2^s \sum_{b\in\mathbb{F}_2^m} \gamma_F(a,b).$$

Since the first sum is equal to 2^m then the function $b \to \gamma_F(a,b)$, $a \neq 0$, takes the value 1 precisely 2^{m-s} times. If F is a permutation then $\gamma_{F^{-1}}(a,b) = \gamma_F(b,a)$ and the function $a \to \gamma_F(a,b)$ takes the value 1 precisely 2^{m-s} times for any nonzero b.

We have the following necessary and sufficient conditions for differentially 2^s-uniform functions.

Proposition 21 *A function F is differentially 2^s-uniform if and only if one of the following conditions holds:*

(i) *for all* $a, b \in \mathbb{F}_2^m$, $a \neq 0$, *the equation* $F(x+a) + F(x) = b$ *has either 0 or* 2^s *solutions;*
(ii) *for any nonzero* $a \in \mathbb{F}_2^m$ *the set* H_a *contains* 2^{m-s} *elements, that is* $|H_a| = 2^{m-s}$*;*
(iii) *for every* $(a, b) \neq 0$ *the system*

$$\begin{cases} x+y & = & a \\ F(x)+F(y) & = & b \end{cases}$$

admits 0 or 2^s *solutions.*

Let n be a proper divisor of m and F be a function on $\mathbb{F}_2^m$ such that in the univariate polynomial representation of F the condition $c_i \neq 0$ implies $i \equiv 2^j \mod 2^n - 1$. Then, obviously, F is linear on $\mathbb{F}_2^n$ and $D_1 F$ is constant on $\mathbb{F}_2^n$. Therefore, if $n > s$ then F cannot be differentially 2^s-uniform. Thus we get the following proposition which is proven for APN case in [15] by using the coding theory approach.

Proposition 22 *Let n be a divisor of m, a function F on $\mathbb{F}_{2^m}$ have the univariate polynomial representation $F(x) = \sum_{i=0}^{2^m-1} c_i x^i$ and $c_i \neq 0$ implies $i \equiv 2^j \mod 2^n - 1$. Then for $s < n$ the function F is not differentially 2^s-uniform.*

2.4.1 Connections between s-nonlinearity and δ-uniformity

The tables below show that s-nonlinearity of a function does not imply that the function is differentially δ-uniform and vice versa. Table 4 (resp. Table 5) gives all known values of exponents d (up to cyclotomic equivalence) that x^d is s-nonlinear (resp. differentially 2^s-uniform). Further we give conditions when a function is both s-nonlinear and differentially δ-uniform (in these cases δ must be equal to 2^s as we prove further).

Table 4

Known s-nonlinear power permutations x^d on $\mathbb{F}_{2^m}$.

Exponents d	Conditions	Linearity	Proven in
2^i+1	$\gcd(i,m)=s$, m/s odd	s	[33, 54]
$2^{2i}-2^i+1$	$\gcd(i,m)=s$, m/s odd	s	[41, 42]
$2^t+2^{\frac{t+1}{2}}+1$	$m=2t$, t odd	2	[22]
$2^t+2^{t-1}+1$	$m=2t$, t odd	2	[22]
2^t+3	$m=2t+1$	1	[8, 9]
$2^t+2^{\frac{t}{2}}-1$ $2^t+2^{\frac{3t+1}{2}}-1$	t even, $m=2t+1$ t odd, $m=2t+1$	1	[38]

Table 5

Known differentially 2^s-uniform power functions x^d on $\mathbb{F}_{2^m}$.

Exponents d	Conditions	Uniformity	Proven in
2^i+1	$\gcd(i,m)=s$	s	[33, 54]
$2^{2i}-2^i+1$	$\gcd(i,m)=s$, m/s odd	s	[37, 41, 42]
2^t+3	$m=2t+1$	1	[27]
$2^t+2^{\frac{t}{2}}-1$	$m=2t+1$, t even	1	[26]
$2^t+2^{\frac{3t+1}{2}}-1$	$m=2t+1$, t odd	1	
$2^{2t}-1$	$m=2t+1$	1	[3, 54]
$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$m=5i$	1	[28]

Proposition 23 *Let F be an s-nonlinear function on $\mathbb{F}_2^m$. If all the values in Δ_F are divisible by 2^s then F is differentially 2^s-uniform.*

Proof. We have $\delta_F(0,0)=2^m$ and $\lambda_F(0,0)=2^m$. Using (2.1) and the equality

$$\sum_{a,b\in\mathbb{F}_2^m}\delta_F(a,b)^2=\frac{1}{2^{2m}}\sum_{a,b\in\mathbb{F}_2^m}\lambda_F(a,b)^4 \tag{2.3}$$

from [19] we get for s-nonlinear function F:

$$\sum_{(a,b)\neq(0,0)}\delta_F(a,b)^2=\frac{1}{2^{2m}}\sum_{(a,b)\neq(0,0)}\lambda_F(a,b)^4=2^{m+s-2m}\sum_{(a,b)\neq(0,0)}\lambda_F(a,b)^2=2^{m+s}(2^m-1),$$

On the other hand, the equality

$$\sum_{(a,b)\neq(0,0)}\delta_F(a,b)=2^m(2^m-1).$$

is true for any function F. Thus

$$\sum_{(a,b)\neq(0,0)}\frac{\delta_F(a,b)}{2^s}=\sum_{(a,b)\neq(0,0)}\left[\frac{\delta_F(a,b)}{2^s}\right]^2.$$

All $\frac{\delta_F(a,b)}{2^s}$ are nonnegative integers since we assumed that they are divisible by 2^s. Therefore, $\Delta_F=\{0,2^s\}$ and F is differentially 2^s-uniform. □

Note that in Proposition 23 the condition that $\delta_F(a,b)$ is divisible by 2^s, for all $a,b\in\mathbb{F}_2^m, a\neq 0$, is automatically satisfied if $s=1$. For $s>1$ there exist s-nonlinear functions which are not differentially 2^s-uniform (see Tables 4 and 5).

Proposition 24 *Let F be a differentially 2^s-uniform function on $\mathbb{F}_2^m$ and $m+s$ be even. If all the values in Λ_F are divisible by $2^{\frac{m+s}{2}}$ then F is s-nonlinear.*

Proof.

$$\sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^4 = 2^{2m} \sum_{(a,b)\neq(0,0)} \delta_F(a,b)^2 = 2^{2m}2^{2s}2^{m-s}(2^m-1) = 2^{2m}2^{m+s}(2^m-1).$$

The first equality follows from (2.3) and the second one from the fact that D_aF is a 2^s-to-one mapping for all $a \neq 0$. Then from (2.1) we get

$$2^{m+s} \sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^2 = 2^{2m}2^{m+s}(2^m-1) = \sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^4.$$

If all values in Λ_F are divisible by $2^{\frac{m+s}{2}}$ then

$$\sum_{(a,b)\neq(0,0)} \lambda_F(a,b)^2 = \sum_{(a,b)\neq(0,0)} [\frac{\lambda_F(a,b)}{2^{\frac{m+s}{2}}}]^2 \lambda_F(a,b)^2.$$

Therefore, $\Lambda_F = \{0, \pm 2^{\frac{m+s}{2}}\}$ and F is s-nonlinear. □

Proposition 25 *Let F be a differentially 2^s-uniform function on $\mathbb{F}_2^m$. Then F is s-nonlinear if and only if the values of the Walsh transform of the function γ_F are 2^{m-s+1} and $2^{m-s+1} - 2^{m+1}$, for $(a,b) \neq (0,0)$.*

Proof. Since F is differentially 2^s-uniform, then $\delta_F(a,b) = 2^m\delta_0 + 2^s\gamma_F$ where δ_0 is the Dirac symbol. For Boolean function γ_F we have

$$(-1)^{\gamma_F} = 1 - 2\gamma_F = 1 - \frac{\delta_F}{2^{s-1}} + 2^{m-s+1}\delta_0.$$

The Fourier transform of the constant function 1 is $2^{2m}\delta_0$ and that of δ_0 is the constant function 1. Therefore,

$$\lambda_{\gamma_F} = \widehat{(-1)^{\gamma_F}} = 2^{2m}\delta_0 - \frac{\widehat{\delta_F}}{2^{s-1}} + 2^{m-s+1},$$

where $\widehat{\delta_F}$ is the Fourier transform of the function δ_F. It is well known that $\widehat{\delta_F}(a,b) = \lambda_F(a,b)^2$ (cf. for instance [19]). Thus, the Walsh transform of the function γ_F is equal to $2^{2m}\delta_0 - \frac{\lambda_F^2}{2^{s-1}} + 2^{m-s+1}$.

When $(a,b) \neq (0,0)$ the Walsh transform of the function γ_F is equal to 2^{m-s+1} or $2^{m-s+1} - 2^{m+1}$ if and only if $\lambda_F^2(a,b)$ is equal to 0 or 2^{m+s}, that is if F is s-nonlinear. □

2.4.2 The coding theory approach

Like in the case of APN and AB functions differentially δ-uniform and s-nonlinear mappings can be described in terms of coding theory.

The proposition below shows that if all nonzero codewords of a $[2^m-1, 2m]$-linear code have Hamming weights in the set $\{2^{m-1}, 2^{m-1} \pm \mu\}$ then the weight distribution of this code is unique as long as its dual has minimum distance at least 3.

Proposition 26 ([9]) *Let C be a $[2^m-1, 2m]$-linear code which does not contain the all-one vector $\mathbf{1} = (1, ..., 1)$. Assume that the minimum distance of the dual code $C^\perp$ is at least 3. Assume that the weight of every codeword in C lies in $\{0, 2^{m-1}, 2^{m-1} \pm \mu\}$. Then μ is divisible by $2^{[\frac{m-1}{2}]}$. Moreover, the weight distribution of C is completely determined:*

w	*Number A_w of words of weight w*
0	1
$2^{m-1}-\mu$	$\frac{2^{m-2}(2^m-1)(2^{m-1}+\mu)}{\mu^2}$
2^{m-1}	$\frac{(2^m-1)((2^m+1)\mu^2-2^{2m-2})}{\mu^2}$
$2^{m-1}+\mu$	$\frac{2^{m-2}(2^m-1)(2^{m-1}-\mu)}{\mu^2}$

In particular the number B_3 (resp. B_4) of codewords of weight 3 (resp. 4) in $C^\perp$ is given by

$$\begin{aligned} B_3 &= \frac{(2^m-1)(\mu^2-2^{m-1})}{3 \cdot 2^{m-1}}, \\ B_4 &= \frac{(2^m-1)(2^{m-2}-1)(\mu^2-2^{m-1})}{3 \cdot 2^{m-1}}. \end{aligned}$$

Using this proposition we describe codes corresponding to s-nonlinear and differentially 2^s-uniform functions by the following proposition.

Proposition 27 *Let F be a function on $\mathbb{F}_{2^m}$ with $F(0) = 0$ and $s < m$. Then*

(i) *if F is s-nonlinear then $\dim C_F = 2^m - 1 - 2m$ and $C_F^\perp$ does not contain the all-one vector;*

(ii) *F is s-nonlinear if and only if the weight of every codeword in $C_F^\perp$ lies in $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m+s}{2}-1}\}$;*

(iii) *if F is differentially 2^s-uniform or s-nonlinear then the number B_3 (resp. B_4) of codewords of weight* 3 *(resp.* 4*) in C_F is given by*

$$B_3 = \frac{1}{3}(2^m - 1)(2^{s-1} - 1),$$
$$B_4 = \frac{1}{3}(2^m - 1)(2^{m-2} - 1)(2^{s-1} - 1);$$

(iv) *if F is s-nonlinear then the weight distribution of $C_F^\perp$ is completely determined:*

w	*Number A_w of words of weight w*
0	1
$2^{m-1} - 2^{\frac{m+s}{2}-1}$	$(2^m - 1)(2^{m-s-1} - 2^{\frac{m-s}{2}-1})$
2^{m-1}	$(2^m - 1)(2^m - 2^{m-s} + 1)$
$2^{m-1} + 2^{\frac{m+s}{2}-1}$	$(2^m - 1)(2^{m-s-1} + 2^{\frac{m-s}{2}-1})$

(v) *if F is differentially 2^s-uniform or s-nonlinear and $s > 1$, then the code C_F has the minimum distance* 3*;*

(vi) *if F is differentially 2^s-uniform then $C_F^\perp$ does not contain the all-one vector.*

Proof. If F is s-nonlinear with $s \neq m$ then $\lambda_F \neq 2^m$. It follows from the statement (iii) of Theorem 2 that $dim\ C_F = 2^m - 1 - 2m$ and $C_F^\perp$ does not contain the all-one vector.

Claim (ii) obviously follows from the equality (2.2).

If F is a differentially 2^s-uniform function, then by the definition of C_F, a codeword $c = (c_0, ..., c_{2^m-1})$ belongs to C_F, if and only if it satisfies

$$\sum_{i=0}^{2^m-1} c_i\alpha^i = 0 \text{ and } \sum_{i=0}^{2^m-1} c_iF(\alpha^i) = 0. \tag{2.4}$$

According to (2.4), the number $B_3 + B_4$ of codewords from C_F with weight 3 and 4 is equal to the number of $\{u, v, u', v'\}$, where u, v, u', v' are distinct elements of $\mathbb{F}_{2^m}$ such that

$$u + v + u' + v' = 0 \text{ and } F(u) + F(v) + F(u') + F(v') = 0. \tag{2.5}$$

If one of the elements u, v, u', v' is 0 then the corresponding codeword has the weight 3, otherwise the weight is 4.

$\{u, v, u', v'\}$ satisfies (2.5) if and only if $\{u, v\}$ and $\{u', v'\}$ are solutions of the equations

$$x + y = a \text{ and } F(x) + F(y) = b \tag{2.6}$$

for some $a, b \in \mathbb{F}_{2^m}$, $a \neq 0$. Moreover, we have three distinct sets $\{\{u, v\}, \{u', v'\}\}$, $\{\{u, v'\}, \{u', v\}\}$ and $\{\{u, u'\}, \{v, v'\}\}$, corresponding to $\{u, v, u', v'\}$ and satisfying (2.6) for different a, b. Therefore, $B_3 + B_4$ is equal to $1/3$ of the number of distinct sets $\{\{u, v\}, \{u', v'\}\}$ satisfying (2.6).
Let for certain $a, b \in \mathbb{F}_{2^m}$, $a \neq 0$, the equations (2.6) have solutions. Therefore, the number of solutions $\{u, v\}$ is exactly 2^{s-1} because F is differentially 2^s-uniform. These solutions form $\frac{2^{s-1}(2^{s-1}-1)}{2}$ distinct sets $\{\{u, v\}, \{u', v'\}\}$, $u \neq v$, $u' \neq v'$. For every $a \neq 0$ there are 2^{m-s} elements b for which (2.6) have solutions. Thus

$$B_3 + B_4 = \frac{1}{3}(2^m - 1)2^{m-s}2^{s-2}(2^{s-1} - 1) = \frac{1}{3}2^{m-2}(2^m - 1)(2^{s-1} - 1).$$

If one of the distinct elements u, v, u', v' satisfying (2.5) is 0 then the pairs $\{u, v\}$ and $\{u', v'\}$ are solutions for (2.6) when $b = F(a)$. For every $a \neq 0$ and $b = F(a)$ the equations (2.6) have 2^{s-1} solutions which give $2^{s-1} - 1$ pairs of distinct unordered pairs $\{\{0, a\}, \{u, v\}\}$, $u \neq v$. Thus,

$$B_3 = \frac{1}{3}(2^m - 1)(2^{s-1} - 1),$$

$$B_4 = \frac{1}{3}2^{m-2}(2^m - 1)(2^{s-1} - 1) - \frac{1}{3}(2^m - 1)(2^{s-1} - 1) = \frac{1}{3}(2^m - 1)(2^{s-1} - 1)(2^{m-2} - 1).$$

Hence, for differentially 2^s-uniform functions (iii) holds for any $s \neq m$.
If $s \neq m$ and F is s-nonlinear then according to the statement (i), (ii) of this theorem and the statement (i) of Theorem 2, F satisfies the conditions of Proposition 26. Replacing μ by $2^{\frac{m+s}{2}-1}$ we complete the proof of (iii) and (iv).

The claim (v) directly follows from (iii).

If F is a differentially 2^s-uniform function then C_F contains some codewords of weight 3 if $s > 1$ and 5 if $s = 1$. Since the vector $\mathbf{1} = (1, ..., 1)$ cannot be orthogonal to any codeword of odd weight, $\mathbf{1}$ is not in $C_F^\perp$. □

Corollary 3 *If a function F is differentially 2^δ-uniform and s-nonlinear then $s = \delta$. In particular, if F is an APN function with three-valued Walsh spectrum $\{0, \pm\lambda\}$ then F is AB and if m is even then there exists no APN function with three valued Walsh spectrum.*

Proposition 26 implies that for any function F with three-valued Walsh spectrum the code C_F has the minimum distance 3 or 5. If m is even then by Corollary 3 the function F is not APN and therefore the minimum distance of the code C_F is precisely 3. Hence, when m is even there exist no s-nonlinear functions with the corresponding code of minimum distance greater than 3. This fact was proven for the case of power functions in [51].

Remark It follows from the proof of statement (iii) of Proposition 27 that a function F, $F(0) = 0$, satisfies the condition $\delta_F(a, F(a)) > 2$ for some $a \neq 0$ if and only if the code C_F has minimum distance 3. If F is a power function then it gives a code C_F with minimum distance 3 if and only if $\delta_F(1, 1) > 2$ (cf. Prop. 2 in [20]). $\diamond$

Remark The function $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$, with Kasami exponent $d = 2^{2k} - 2^k + 1$ has the code C_F with minimum distance 3 if and only if $\gcd(k, m) = s > 1$, otherwise it is equal to 5. Indeed

$$(c+1)^{2^{2k}-2^k+1} + c^{2^{2k}-2^k+1} = (c^{2^{2k}} + 1)(c^{2^k} + 1)^{-1}(c+1) + c^{2^{2k}}(c^{2^k})^{-1}c = 1$$

for any $c \in \mathbb{F}_{2^s}$. Therefore $\delta_F(1, 1) \geq 2^s$. It is proven in [20] (see Theorem 5, the case $u = 2v$) that the number B_3 of the code C_F is equal to $\frac{1}{3}(2^m - 1)(2^{s-1} - 1)$. Thus $\delta_F(1, 1) = 2^s$. $\diamond$

The following proposition provides power functions with corresponding codes of minimum distance greater than 3. Moreover it gives a lower bound on the degree of an s-nonlinear function if $s \neq 1$ and m is prime since such functions have minimum distance 3.

Proposition 28 ([20]) *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^k$, where m is a prime and $1 < k < m + 3$. Then the code C_F has minimum distance $d \geq 4$.*

The statements bellow follow from Proposition 24 and the second statement of Proposition 27.

Corollary 4 *Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and s be a divisor of m such that $m + s$ is even. Then*

- *F is s-nonlinear if F is differentially 2^s-uniform and the code $C_F^\perp$ is $2^{\frac{m+s}{2}-1}$-divisible;*
- *the code $C_F^\perp$ is $2^{\frac{m+s}{2}-1}$-divisible if F is s-nonlinear.*

Applying McEliece's theorem like in the AB case we come to the following statements about s-nonlinear power functions.

Corollary 5 *Let $F(x) = x^k$ be a function on $\mathbb{F}_{2^m}$ and for an integer $s < m$, $m + s$ be even. Then*

- *F is s-nonlinear if F is differentially 2^s-uniform and*
$$\forall u,\ 1 \le u \le 2^m - 1,\ w_2(A(u)) \le \frac{m-s}{2} + w_2(u), \tag{2.7}$$
where $A(u) = uk \mod (2^m - 1)$;

- *the condition (2.7) holds if F is s-nonlinear.*

We prove the next proposition by using Corollary 5.

Proposition 29 *Let m and s be such integers that $m + s$ is even and $s < m$. If there exists a divisor n of m such that d satisfies*

$$d \equiv -d_0 \ mod \ \tfrac{2^m-1}{2^n-1} \ with \ 0 < d_0 < \tfrac{2^m-1}{2^n-1} \ and \ w_2(d_0) < \tfrac{1}{2}(\tfrac{m}{n} + \tfrac{s}{n} - 2)$$

then $F(x) = x^d$ is not s-nonlinear on $\mathbb{F}_{2^m}$.

Proof. Let $u = 2^n - 1$. Then we have

$$A(u) = ud \mod (2^m - 1) = (2^m - 1) - (2^n - 1)d_0,$$

$$w_2(A(u)) = w_2((2^m - 1) - (2^n - 1)d_0) = m - w_2((2^n - 1)d_0).$$

Since $w_2((2^n - 1)d_0) \le w_2(d_0)n$ then

$$w_2(A(u)) \ge m - w_2(d_0)n = n + m - n(w_2(d_0) + 1) > w_2(u) + \frac{m-s}{2},$$

when $w_2(d_0) < \frac{1}{2}(\frac{m}{n} + \frac{s}{n} - 2)$. It follows from Corollary 5 that in conditions of this proposition F cannot be s-nonlinear. □

In particular Proposition 29 gives:

Proposition 30 *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$, and $m = nk$ for some integers n and k. If $d = \sum_{i=1}^{k-1} 2^{in} - 1$ then F is not s-nonlinear when $k \ge 4$.*

Proof. We have $d = (2^{kn} - 1)/(2^n - 1) - 2$. We apply Proposition 29 with $d_0 = 2$. We get $1 = w_2(d_0) < \frac{1}{2}(\frac{m}{n} + \frac{s}{n} - 2)$ when $s > (4 - k)n$. But $s \ge 1 > (4 - k)n$ when $k \ge 4$. Therefore if $k \ge 4$ then F is not s-nonlinear. □

Proposition 30 leads to the following statement about the class of power functions mentioned in Section 2.3.

Corollary 6 *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x^d$, and $m = nk$ for some integers $n, k > 1$. If $d = \sum_{i=1}^{k-1} 2^{in} - 1$ then F is not AB.*

Proof. For $k \ge 4$ the claim follows from the previous proposition and for $k < 4$ see Proposition 12. □

Chapter 3

On CCZ-equivalence of functions

3.1 Carlet-Charpin-Zinoviev equivalence of functions

The transformation of functions presented in Proposition 8 can be introduced as an equivalence relation of functions.

For a function F from $\mathbb{F}_2^m$ to itself, we denote by G_F the *graph of the function* F:

$$G_F = \{(x, F(x)) : x \in \mathbb{F}_2^m\} \subset \mathbb{F}_2^{2m}.$$

Definition 1 *We say that functions $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ are* Carlet-Charpin-Zinoviev equivalent *(CCZ-equivalent) if there exists a linear permutation $\mathcal{L} : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ such that $\mathcal{L}(G_F) = G_{F'}$.*

Let functions $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be CCZ-equivalent. Then there exists a linear permutation $\mathcal{L} : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ such that $\mathcal{L}(G_F) = G_{F'}$. The linear function $\mathcal{L}$ can be considered as a pair (L_1, L_2) of linear functions $L_1, L_2 : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$. Then $\mathcal{L}(x, F(x)) = (F_1(x), F_2(x))$, where

$$F_1(x) = L_1(x, F(x)), \tag{3.1}$$

$$F_2(x) = L_2(x, F(x)). \tag{3.2}$$

We have

$$\mathcal{L}(G_F) = \{(F_1(x), F_2(x)) : x \in \mathbb{F}_2^m\}.$$

For a given linear permutation $\mathcal{L}$, the set $\mathcal{L}(G_F)$ is the graph of a function if and only if the function F_1 is a permutation; then, $F' = F_2 \circ F_1^{-1}$ and $\mathcal{L}(G_F) = G_{F'}$.

In the proposition below we give a slightly different approach to the CCZ-equivalence. Recall that a set $G \subset \mathbb{F}_2^{2m}$ is *transversal* to a subgroup V of $\mathbb{F}_2^{2m}$ if $|G \cap (u+V)| = 1$ for any $u \in \mathbb{F}_2^{2m}$.

Proposition 31 *Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and $G \subset \mathbb{F}_2^{2m}$. Then the set G is the graph of a function CCZ-equivalent to F if and only if there exists a linear permutation $\mathcal{L} : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ such that $G = \mathcal{L}(G_F)$ and G_F is transversal to $V' = \mathcal{L}^{-1}(V)$, where $V = \{(0,x) : x \in \mathbb{F}_2^m\}$.*

Proof. The condition that there exists a linear permutation $\mathcal{L} : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ such that $G = \mathcal{L}(G_F)$ is clearly necessary. Let us denote $U = \{(x,0) : x \in \mathbb{F}_2^m\}$, $V = \{(0,x) : x \in \mathbb{F}_2^m\}$, $\mathcal{L}^{-1}(U) = U'$ and $\mathcal{L}^{-1}(V) = V'$. Then G is the graph of a function if and only if $|G \cap (u+V)| = 1$ for any $u \in U$; that is, if and only if $|\mathcal{L}^{-1}(G) \cap (u'+V')| = 1$ for any $u' \in U'$. Hence, G is the graph of a function CCZ-equivalent to F if and only if G_F is transversal to V'. □

The subgroup and the linear function approaches give different descriptions to CCZ-equivalence although they are "equivalent".

EA-equivalent functions are CCZ-equivalent and if a function F is a permutation then F is CCZ-equivalent to F^{-1} [15]. Since any permutation is CCZ-equivalent to its inverse then obviously the minimum degree and the algebraic degree of a function are not CCZ-invariant (while they are EA-invariant as noted above). For example, if $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a Gold AB function then

$$\begin{array}{lclcl} \min d^\circ(F) & = & d^\circ(F) & = & 2, \\ \min d^\circ(F^{-1}) & = & d^\circ(F^{-1}) & = & \frac{m+1}{2}, \end{array}$$

as proven in [54].

The property of stability of APN and AB mappings given in [15] can be easily generalized to all functions (not necessarily APN or AB) as follows:

Proposition 32 *Let $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be CCZ-equivalent functions. Then $\Delta_F = \Delta_{F'}$ and $\Lambda_F = \Lambda_{F'}$. In particular, F is an APN (resp. AB) function if and only if F' is APN (resp. AB).*

Proof. If $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ are CCZ-equivalent, then $F' = F_2 \circ F_1^{-1}$ for a certain linear permutation $\mathcal{L} = (L_1, L_2)$, where F_1, F_2 are defined by (3.1) and (3.2). For any $(a,b) \in \mathbb{F}_2^{2m}$

we have

$$\begin{aligned}\delta_F(a,b) &= |\{x \in \mathbb{F}_2^m : F(x+a)+F(x)=b\}| \\ &= |\{(x,y) \in \mathbb{F}_2^{2m} : (x,F(x))+(y,F(y))=(a,b)\}| \\ &= |\{(x,y) \in \mathbb{F}_2^{2m} : (F_1(x),F_2(x))+(F_1(y),F_2(y))=\mathcal{L}(a,b)\}| \\ &= |\{(x,y) \in \mathbb{F}_2^{2m} : (x,F_2\circ F_1^{-1}(x))+(y,F_2\circ F_1^{-1}(y))=\mathcal{L}(a,b)\}| \\ &= \delta_{F'}(\mathcal{L}(a,b))\end{aligned}$$

and

$$\begin{aligned}\lambda_F(a,b) &= \sum_{x\in\mathbb{F}_2^m}(-1)^{b\cdot F(x)+a\cdot x} = \sum_{x\in\mathbb{F}_2^m}(-1)^{(a,b)\cdot(x,F(x))} \\ &= \sum_{x\in\mathbb{F}_2^m}(-1)^{(a,b)\cdot\mathcal{L}^{-1}(F_1(x),F_2(x))} = \sum_{x\in\mathbb{F}_2^m}(-1)^{\mathcal{L}^{-1*}(a,b)\cdot(x,F_2\circ F_1^{-1}(x))} \\ &= \lambda_{F'}(\mathcal{L}^{-1*}(a,b)),\end{aligned}$$

where $\mathcal{L}^{-1*}$ is the adjoint operator of $\mathcal{L}^{-1}$ (i.e. $x\cdot\mathcal{L}^{-1}(y)=\mathcal{L}^{-1*}(x)\cdot y$, for any $(x,y)\in\mathbb{F}_2^{2m}$; if "$\cdot$" is the usual inner product, then $\mathcal{L}^{-1*}$ is the linear permutation whose matrix is transposed of that of $\mathcal{L}^{-1}$). Hence, $\Delta_F=\Delta_{F'}$ and $\Lambda_F=\Lambda_{F'}$. □

Remark Obviously, CCZ-equivalence can be defined for functions between any two groups H_1 and H_2. For a function $F : H_1 \to H_2$ we can consider the set of the values $\delta_F(a,b)=|\{x\in H_1 : F(x+a)-F(x)=b\}|$, $a\in H_1\backslash\{0\}$, $b\in H_2$, and if the groups H_1 and H_2 are Abelian, then the discrete Fourier transform of F can also be defined. In this more general case CCZ-equivalent functions again have the same differential properties and in the case of finite fields also the same linear properties. One can find results related to nonlinear functions on Abelian groups in [16, 58]. ◇

Since CCZ-equivalent functions have the same differential uniformity and the same nonlinearity, then the resistance of a function to linear and differential attacks is CCZ-invariant. CCZ-equivalent functions have also the same weakness/strength with respect to algebraic attacks. Indeed, let functions $F,F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be CCZ-equivalent. Then $F'=F_2\circ F_1^{-1}$, where F_1,F_2 are defined by (3.1) and (3.2) for a certain linear permutation $\mathcal{L}=(L_1,L_2)$. If there exists a nonzero function $\psi : \mathbb{F}_2^{2m}\to\mathbb{F}_2$ of low degree such that

$$\psi(x,F(x))=0, \forall x\in\mathbb{F}_2^m,$$

then ψ could be used in an algebraic attack [21]. The function $\psi \circ \mathcal{L}^{-1}$ has the same degree as ψ and

$$\psi \circ \mathcal{L}^{-1}(F_1(x), F_2(x)) = 0, \forall x \in \mathbb{F}_2^m,$$

implies

$$\psi \circ \mathcal{L}^{-1}(x, F'(x)) = 0, \forall x \in \mathbb{F}_2^m.$$

Hence, $\psi \circ \mathcal{L}^{-1}$ could be used in an algebraic attack on F', and *vice versa.* Therefore, the resistance of a function to algebraic attacks is also CCZ-invariant.

3.2 CCZ-equivalence and EA-equivalence

If we want to classify all functions CCZ-equivalent to a given one F, then we should characterize all permutations of the form $L \circ F + L'$, where L, L' are linear. Indeed, we need to know which linear mapping $L_1 \ : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ is such that the function $F_1(x) = L_1(x, F(x))$ is a permutation. Clearly, L_1 can be written uniquely in the form $L_1(x, y) = L(y) + L'(x)$. If F_1 is a permutation then there exists a linear function $L_2(x, y)$ such that the linear function $(L_1, L_2)(x, y)$ is a permutation too. Indeed, $L_1(x, F(x))$ being a permutation, L_1 is onto and the kernel of L_1 has then dimension m. We can take for L_2 any linear permutation between $Ker(L_1)$ and $\mathbb{F}_2^m$, extended to $\mathbb{F}_2^{2m}$ by $L_2(x + y) = L_2(x)$ for all $x \in Ker(L_1)$, $y \in E$, where E is an m-dimensional subspace of F_2^{2m} such that $E \oplus Ker(L_1) = \mathbb{F}_2^{2m}$. Conversely, any linear function L_2 such that (L_1, L_2) is a permutation has this form. Indeed, L_2 being onto, it has also an m-dimensional kernel, and (L_1, L_2) being one to one, the kernels of L_1 and L_2 have trivial intersection. This proves that $Ker(L_1) \oplus Ker(L_2) = \mathbb{F}_2^{2m}$ and that we can take $E = Ker(L_2)$.

Proposition 33 *Let $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^m$. The function F' is EA-equivalent to the function F or to the inverse of F (if it exists) if and only if there exists a linear permutation $\mathcal{L} = (L_1, L_2)$ on $\mathbb{F}_2^{2m}$ such that $\mathcal{L}(G_F) = G_{F'}$ and the function L_1 depends only on one variable, i.e. $L_1(x, y) = L(x)$ or $L_1(x, y) = L(y)$.*

Proof. Let $\mathcal{L}(G_F) = G_{F'}$ for some linear permutation $\mathcal{L} = (L_1, L_2) : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ and $L_1(x, y) = L(y)$, $L_2(x, y) = R_1(x) + R_2(y)$, where L, R_1, $R_2 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ are linear. Then

$$F_1(x) = L_1(x, F(x)) = L \circ F(x),$$

$$F_2(x) = L_2(x, F(x)) = R_1(x) + R_2 \circ F(x).$$

The function F_1 is a permutation, since $\mathcal{L}(G_F)$ is the graph of a function. Therefore, L and F have to be permutations. On the other hand, the system

$$\begin{cases} L(y) & = & 0 \\ R_1(x) + R_2(y) & = & 0 \end{cases}$$

has only $(0, 0)$ solution, since $\mathcal{L} = (L_1, L_2)$ is a permutation. But L is also a permutation. Therefore, the linear function R_1 has to be a permutation too.

We have

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) = R_1 \circ F^{-1} \circ L^{-1}(x) + R_2 \circ F \circ F^{-1} \circ L^{-1}(x) \\ &= R_1 \circ F^{-1} \circ L^{-1}(x) + R_2 \circ L^{-1}(x). \end{aligned}$$

Thus, F' is EA-equivalent to F^{-1}.

The proof that F' is EA-equivalent to F, when $L_1(x, y) = L(x)$, is similar.

Conversely, let $F' = R_1 \circ F \circ R_2 + R$ or $F' = R_1 \circ F^{-1} \circ R_2 + R$ for some linear permutations R_1, R_2 and for some linear function R. Then take $\mathcal{L}(x, y) = (R_2^{-1}(x), R_1(y) + R \circ R_2^{-1}(x))$ in the first case and in the second case take $\mathcal{L}(x, y) = (R_2^{-1}(y), R \circ R_2^{-1}(y) + R_1(x))$. Obviously, all conditions are satisfied. □

Proposition 34 *Let $\mathcal{L} = (L_1, L_2)$, $\mathcal{L}' = (L_1, L_2')$ be such linear permutations on $\mathbb{F}_2^{2m}$ that for a function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ the function $L_1(x, F(x))$ is a permutation. Then the functions defined by the graphs $\mathcal{L}(G_F)$ and $\mathcal{L}'(G_F)$ are EA-equivalent.*

Proof. Let

$$L_1(x, y) = R_1(x) + R_2(y), \quad L_2(x, y) = T_1(x) + T_2(y), \quad L_2'(x, y) = T_1'(x) + T_2'(y),$$

for some linear functions R_1, R_2, T_1, T_2, T_1', T_2' from $\mathbb{F}_2^m$ to itself. We can consider the linear functions $\mathcal{L}$, $\mathcal{L}'$ and $\mathcal{L}^{-1}$ as $(2m) \times (2m)$ matrices

$$\mathcal{L} = \begin{pmatrix} R_1 & R_2 \\ T_1 & T_2 \end{pmatrix}, \quad \mathcal{L}' = \begin{pmatrix} R_1 & R_2 \\ T_1' & T_2' \end{pmatrix}, \quad \mathcal{L}^{-1} = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}.$$

Then

$$\mathcal{L} \circ \mathcal{L}^{-1} = \begin{pmatrix} R_1 & R_2 \\ T_1 & T_2 \end{pmatrix} \times \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} R_1A_1 + R_2A_3 & R_1A_2 + R_2A_4 \\ T_1A_1 + T_2A_3 & T_1A_2 + T_2A_4 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix},$$

$$\mathcal{L}'\circ\mathcal{L}^{-1} = \begin{pmatrix} R_1 & R_2 \\ T_1' & T_2' \end{pmatrix} \times \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = \begin{pmatrix} R_1A_1+R_2A_3 & R_1A_2+R_2A_4 \\ T_1'A_1+T_2'A_3 & T_1'A_2+T_2'A_4 \end{pmatrix},$$

where I is the identity matrix and 0 is the 0-matrix of order m. Thus, $R_1A_2 + R_2A_4 = 0$ and $R_1A_1 + R_2A_3 = I$ and we can consider the linear function $\mathcal{L}'\circ\mathcal{L}^{-1}$ as a pair $(S_1(x,y), S_2(x,y))$ of linear functions, where

$$\begin{aligned} S_1(x,y) &= R_1\circ A_1(x) + R_2\circ A_3(x) + R_1\circ A_2(y) + R_2\circ A_4(y) = x, \\ S_2(x,y) &= T_1'\circ A_1(x) + T_2'\circ A_3(x) + T_1'\circ A_2(y) + T_2'\circ A_4(y). \end{aligned}$$

For the linear permutation $\mathcal{L}'\circ\mathcal{L}^{-1} = (S_1, S_2)$ we have $(\mathcal{L}'\circ\mathcal{L}^{-1})\circ\mathcal{L}(G_F) = \mathcal{L}'(G_F)$ and S_1 depends only on x. It follows from Proposition 33 that the functions with the graphs $\mathcal{L}(G_F)$ and $\mathcal{L}'(G_F)$ are EA-equivalent. □

Proposition 33 shows that if we want to construct functions F' which are CCZ-equivalent to a function F and EA-inequivalent to both F and F^{-1} (if F^{-1} exists), then we have to use a linear function $L_1(x,y)$ depending on both variables. However, this condition is not sufficient as the following example shows.

Example Let $m = 2n+1$ and $s \equiv n$ [mod 2]. Then the linear function

$$\mathcal{L}(x,y) = (x + tr(x) + \sum_{j=0}^{n-s} y^{2^{2j+s}}, y + tr(x))$$

is a permutation on $\mathbb{F}_{2^m}^2$ since the kernel of $\mathcal{L}$ is $\{(0,0)\}$ (this can be checked by considering the cases $tr(x) = 0$ and $tr(x) = 1$). For the Gold AB function x^3 the function

$$F_1(x) = x + tr(x) + \sum_{j=0}^{n-s} (x^3)^{2^{2j+s}}$$

is a permutation on $\mathbb{F}_{2^m}$. Indeed, denoting $L(y) = \sum_{j=0}^{n-s} y^{2^{2j+s}}$ we have $L(y+y^2) = y+tr(y)$ and $L((y+1)^3) = L(y^3) + y + tr(y) + 1$ since $L(1) = 1$. Thus $F_1(x) = L((x+1)^3) + 1$ and F_1 is a permutation if L is bijective. The equation $z = L(y)$ implies $z + z^2 = y + tr(y)$ and $tr(z) = tr(y)$. Therefore, L is a permutation and $L^{-1}(x) = x + x^2 + tr(x)$, $F_1^{-1}(x) = [L^{-1}(x+1)]^{\frac{1}{3}} + 1$. Finally, we get

$$\begin{aligned} F'(x) &= F_2\circ F_1^{-1}(x) = ([L^{-1}(x+1)]^{\frac{1}{3}} + 1)^3 + tr([L^{-1}(x+1)]^{\frac{1}{3}} + 1) \\ &= L^{-1}(x+1) + [L^{-1}(x+1)]^{\frac{2}{3}} + [L^{-1}(x+1)]^{\frac{1}{3}} + tr([L^{-1}(x+1)]^{\frac{1}{3}}) \\ &= L^{-1}(x+1) + L^{-1}([L^{-1}(x+1)]^{\frac{1}{3}}). \end{aligned}$$

Thus, both functions L_1 and L_2 depend on two variables, but the function F' is EA-equivalent to the inverse of x^3.
This example can be generalized for any Gold AB function by replacing $L^{-1}(x) = x + x^{2^i} + tr(x)$ and x^3 by x^{2^i+1}. ◇

3.3 Gold functions and CCZ-equivalence

In propositions below we give a characterization of permutations $L \circ F + L'$ when F is a Gold function. This characterization is not complete but it is useful for constructions of new APN and AB polynomials.

Proposition 35 *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = L(x^{2^i+1}) + L'(x)$, where L, L' are linear and* $\gcd(m, i) = 1$. *Then F is a permutation if and only if, for every $u \neq 0$ in $\mathbb{F}_{2^m}$ and every v such that $tr(v) = tr(1)$, the condition $L(u^{2^i+1}v) \neq L'(u)$ holds.*

Proof. For any $u \in \mathbb{F}^*_{2^m}$ we have

$$\begin{aligned} F(x) + F(x+u) &= L(x^{2^i+1}) + L'(x) + L((x+u)^{2^i+1}) + L'(x+u) \\ &= L\left(ux^{2^i} + u^{2^i}x + u^{2^i+1}\right) + L'(u) = L\left(u^{2^i+1}\left((x/u)^{2^i} + x/u + 1\right)\right) + L'(u). \end{aligned}$$

When x ranges over $\mathbb{F}_{2^m}$ then $(x/u)^{2^i} + x/u + 1$ ranges over the subset of $\{v \in \mathbb{F}_{2^m} : tr(v) = tr(1)\}$. Hence, F is a permutation if $L(u^{2^i+1}v) \neq L'(u)$ for every $u \neq 0$ and every v such that $tr(v) = tr(1)$. If $\gcd(m, i) = 1$ then this condition is also necessary for F to be a permutation. □

Remark If m is even then without loss of generality we can consider only permutations $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ of the type $F(x) = L(x^{2^i+1}) + x$. Indeed, if $F(x) = L(x^{2^i+1}) + L'(x)$ is a permutation on $\mathbb{F}_{2^m}$ and m is even, then it follows from the Proposition 35 that L' must be a permutation (take $v = 0$). ◇

Recall that for any divisor n of m we denote $tr_{m/n}(x) = x + x^{2^n} + x^{2^{2n}} + ... + x^{2^{m-n}}$ the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^n}$ and $tr_n(x) = x + x^2 + ... + x^{2^{n-1}}$.

Corollary 7 *Let n be a divisor of m and $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x + tr_{m/n}(L'(x)) + tr_{m/n}(L(x^{2^i+1}))$, where L and L' are linear functions with coefficients in $\mathbb{F}_{2^n}$. Then F is a permutation if and only if for every $u, w \in \mathbb{F}_{2^n}^*$, $tr_n(w) = tr(1)$ the condition $L(u^{2^i+1}w) \neq u + tr_{m/n}(1)L'(u)$ is satisfied. In particular, if m is odd or n is even then F is a permutation if and only if the function $x + tr_{m/n}(1)L'(x) + L(x^{2^i+1})$ is a permutation on $\mathbb{F}_{2^n}$.*

Proof. If m is divisible by n, and $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = x + tr_{m/n}(L'(x)) + tr_{m/n}(L(x^{2^i+1}))$, where L, L' are linear functions with coefficients in $\mathbb{F}_{2^n}$, then by Proposition 35 the function F is a permutation if and only if for every $v \in \mathbb{F}_{2^m}$ such that $tr(v) = tr(1)$ and every $u \in \mathbb{F}_{2^m}^*$ the condition $tr_{m/n}(L(u^{2^i+1}v)) \neq u + tr_{m/n}(L'(u))$ holds. Obviously, if $u \notin \mathbb{F}_{2^n}^*$ then $u + tr_{m/n}(L'(u)) \notin \mathbb{F}_{2^n}^*$ and $tr_{m/n}(L(u^{2^i+1}v)) \neq u + tr_{m/n}(L'(u))$. Therefore, F is a permutation if and only if for every $v \in \mathbb{F}_{2^m}$ such that $tr(v) = tr(1)$ and every $u \in \mathbb{F}_{2^n}^*$ the condition $L(u^{2^i+1}tr_{m/n}(v)) \neq u + tr_{m/n}(1)L'(u)$ holds. Then F is a permutation if and only if for every $u, w \in \mathbb{F}_{2^n}^*$, $tr_n(w) = tr(1)$ the condition $L(u^{2^i+1}w) \neq u + tr_{m/n}(1)L'(u)$ is satisfied.

If m is odd or n is even then by Proposition 35 the function F is a permutation if and only if $x + tr_{m/n}(1)L'(x) + L(x^{2^i+1})$ is a permutation on $\mathbb{F}_{2^n}$. □

The examples below are used for constructions in Chapter 4.

Example Let m be even. Then by Corollary 7 the function $x + tr(x^{2^i+1})$ is a permutation of $\mathbb{F}_{2^m}$ if $x + tr_2(x^{2^i+1})$ is a permutation on $\mathbb{F}_{2^2}$. But on $\mathbb{F}_{2^2}$ the function $x + tr_2(x^{2^i+1})$ is equal to either x or x^2. Therefore, $x + tr(x^{2^i+1})$ is a permutation for any i and any m even. Using Corollary 7 it is easy to confirm by a computer that for m even and not divisible by 3 and $n \leq 13$ this is the only permutation of the type $x + tr_{m/n}(L(x^{2^i+1}))$, where L is a linear function with coefficients in $\mathbb{F}_2$ and $\gcd(i, m) = 1$. For m divisible by 3 we could find two more permutations $x + tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)})$ and $x + tr_{m/3}(x^{2^i+1} + x^{2^i(2^i+1)})$. If m is odd, then by Corollary 7 the function $x + tr_{m/n}(x) + tr_{m/n}(x^{2^i+1})$ is a permutation if $x + x + x^{2^i+1} = x^{2^i+1}$ is a permutation on $\mathbb{F}_{2^n}$ and that is always true since $\gcd(i, n) = \gcd(2i, n)$ for m odd. As it was checked by a computer, for m odd and $n \leq 13$ these give the only permutation of the kind $x + c\, tr(x) + tr_{m/n}(L(x^{2^i+1}))$, where $\gcd(i, m) = 1$, $c \in \mathbb{F}_2$ and L is a linear function with coefficients in $\mathbb{F}_2$. For m divisible by 3 we get also the permutations $x + tr_{m/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})$ and $x + tr(x) + tr_{m/3}(x^{2^i(2^i+1)})$. ◇

Proposition 36 *Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $F(x) = L(x^{2^i+1}) + x$, where L is linear, m even and $\gcd(m,i) = 1$. Let L^* be the adjoint operator of L. Then F is a permutation if and only if, for every $v \in \mathbb{F}_{2^m}$ such that $L^*(v) \neq 0$, there exists $u \in \mathbb{F}_{2^m}$ such that $L^*(v) = u^{2^i+1}$ and $tr_{m/2}(\frac{v}{u}) \neq 0$, where $tr_{m/2}$ is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^2}$.*

Proof. The function F is a permutation if and only if, for every $v \neq 0$, the Boolean function $tr(v(L(x^{2^i+1}) + x))$ is balanced (see e.g. [14]). Let L^* be the adjoint operator of L, then we have

$$tr(v(L(x^{2^i+1}) + x)) = tr(L^*(v)x^{2^i+1} + vx).$$

If $L^*(v) = 0$, then the function $tr(v(L(x^{2^i+1}) + x))$ is balanced. If $L^*(v) \neq 0$, the quadratic function $tr(L^*(v)x^{2^i+1} + vx)$ has associated symplectic form :

$$\varphi(x,y) = tr(L^*(v)x^{2^i}y + L^*(v)xy^{2^i}) = tr((L^*(v)x^{2^i} + (L^*(v)x)^{2^{m-i}})y) \ ,$$

which has kernel :

$$\mathcal{E} = \{x \in \mathbb{F}_{2^m} : L^*(v)x^{2^i} + (L^*(v)x)^{2^{m-i}} = 0\} =$$

$$= \{x \in \mathbb{F}_{2^m} : L^*(v)^{2^i}x^{2^{2i}} + L^*(v)x = 0\} = \{0\} \cup \{x \in \mathbb{F}_{2^m} : L^*(v)^{2^i-1}x^{2^{2i}-1} = 1\}.$$

A quadratic function is balanced if and only if its restriction to the kernel of its associated symplectic form is not constant [10, 13]. The restriction of $tr(L^*(v)x^{2^i+1})$ to $\mathcal{E}$ is null. Indeed, $L^*(v)^{2^i-1}x^{2^{2i}-1} = 1$ implies that the order of $L^*(v)x^{2^i+1}$ divides $2^i - 1$ and since $\gcd(i,m) = 1$ then $L^*(v)x^{2^i+1} \in \mathbb{F}_2$ and the trace function is null on $\mathbb{F}_2$, since m is even. Hence, the function $L(x^{2^i+1}) + x$ is a permutation if and only if every v such that $L^*(v) \neq 0$ lies outside the dual of $\{0\} \cup \{x \in \mathbb{F}_{2^m} : L^*(v)^{2^i-1}x^{2^{2i}-1} = 1\}$. Equivalently, the function $L(x^{2^i+1}) + x$ is a permutation if and only if, for every v such that $L^*(v) \neq 0$ the following two conditions hold:

1) $L^*(v)^{2^i-1}$ belongs to $\{x^{2^{2i}-1} : x \in \mathbb{F}_{2^m}\}$ (otherwise, $\mathcal{E}$ would be trivial), say $L^*(v)^{2^i-1} = u^{2^{2i}-1}$, i.e. $L^*(v) = u^{2^i+1}$ (since the mapping $y \to y^{2^i-1}$ is a permutation); in this case $\mathcal{E} = \{0\} \cup \{x \in \mathbb{F}_{2^m} : (ux)^{2^{2i}-1} = 1\} = \frac{1}{u}\{y \in \mathbb{F}_{2^m} : y^{2^{2i}} = y\} = \frac{1}{u}\mathbb{F}_{2^j}$, where $j = \gcd(2i,m) = 2$, hence $\mathcal{E} = \frac{1}{u}\mathbb{F}_4$;

2) v lies outside the dual of $\mathcal{E}$, that is, $tr(vx) \neq 0$ for some $x \in \mathcal{E}$.

For every $z \in \mathbb{F}_{2^m}$ and every $y \in \mathbb{F}_{2^2}$ we have

$$tr(z\frac{1}{u}y) = tr_2(tr_{m/2}(\frac{z}{u}y)) = tr_2(y\, tr_{m/2}(\frac{z}{u})).$$

Hence, the function $L(x^{2^i+1})+x$ is a permutation if and only if every v such that $L^*(v) \neq 0$ satisfies $L^*(v) = u^{2^i+1}$ for some u and $tr_{m/2}(\frac{v}{u}) \neq 0$. □

The existence of APN permutations on $\mathbb{F}_{2^m}$ is an open problem when m is even. In particular it is not known whether there exist permutations EA equivalent to known APN functions. We show below that the answer is no for the Gold APN functions. More general result that there exist no quadratic APN permutations one can find in [55].

Corollary 8 *For m even, there exist no permutations EA-equivalent to the Gold APN functions.*

Proof. Let $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be affine equivalent to $F(x) = x^{2^i+1}$, $\gcd(m,i) = 1$. Then, without loss of generality we can assume that $F'(x) = L_1 \circ F \circ L_2(x) + L_3(x)$, where L_1, L_2, L_3 are linear and L_1, L_2 are permutations. Assume that F' is a permutation. Then $F' \circ L_2^{-1}(x) = L_1 \circ F(x) + L_3 \circ L_2^{-1}(x)$ is a permutation too. Using the remark on page 45, we can assume that $L_3 \circ L_2^{-1} = id$. Thus $L_1(x^{2^i+1}) + x$ is a permutation and by Proposition 36, for every $v \in \mathbb{F}_{2^m}^*$ the condition $L_1^*(v) = u^{2^i+1}$ must be satisfied for some $u \in \mathbb{F}_{2^m}^*$, because L_1 is a permutation and therefore $L_1^*(v) \neq 0$ when $v \neq 0$. On the other hand, x^{2^i+1} is a 3-to-1 mapping for m even, hence neither L_1^* nor L_1 is a permutation, a contradiction. Therefore, there exists no permutation F' affine equivalent to F. □

However, nonexistence of permutations EA-equivalent to a certain function F does not mean yet that there are no permutations CCZ-equivalent to F. In the next section we give such an example of an APN function $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, m odd, that F is CCZ-equivalent to a permutation and there exist no permutations EA-equivalent to F.

The existence of a permutation CCZ-equivalent to the Gold function x^{2^i+1} (for m even) would mean that there exist such linear functions L, $L' :\in \mathbb{F}_2^m \to \mathbb{F}_2^m$ that the functions $x + L(x^{2^i+1})$, $x + L'(x^{2^i+1})$ and $(x + L(y), x + L'(y))$ are permutations. The linear function $(x + L(y), x + L'(y))$ is a permutation if and only if the system

$$\begin{cases} x + L(y) &= 0 \\ x + L'(y) &= 0 \end{cases}$$

has the only solution $(0,0)$ and, therefore, if and only if the linear function $L(y) + L'(y)$ is a permutation. Some permutations of the type $x + L(x^{2^i+1})$ are given in the examples on page 46. There are no such pair of functions $x + L(x^{2^i+1})$, $x + L'(x^{2^i+1})$ among them that $L(y) + L'(y)$ is a permutation.

Chapter 4

New cases of AB and APN mappings

4.1 The first APN and AB polynomials

The next theorems show that CCZ-equivalent functions are not necessarily EA-equivalent (including the equivalence to the inverse). They lead to infinite classes of almost bent and almost perfect nonlinear polynomials, which are EA-inequivalent to power functions.

Theorem 5 *The function $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $m > 3$ odd,*

$$F'(x) = x^{2^i+1} + (x^{2^i} + x)tr(x^{2^i+1} + x), \ \ \gcd(m, i) = 1,$$

is an AB function which is EA-inequivalent to any power function.

Proof. The linear function

$$\mathcal{L}(x, y) = (L_1(x), L_2(x)) = (x + tr(x) + tr(y), y + tr(y) + tr(x))$$

is an involution on $\mathbb{F}_{2^m}^2$:

$$\mathcal{L} \circ \mathcal{L}(x, y) = \mathcal{L}(x + tr(x) + tr(y), y + tr(y) + tr(x))$$
$$= (x + tr(x) + tr(y) + tr(x + tr(x) + tr(y)) + tr(y + tr(y) + tr(x)), y + tr(y) + tr(x)$$
$$+tr(y + tr(y) + tr(x)) + tr(x + tr(x) + tr(y))) = (x, y)$$

The function $F_1(x) = L_1(x, F(x)) = x + tr(x) + tr(x^{2^i+1})$ is an involution too:

$$\begin{aligned} F_1 \circ F_1(x) &= x + tr(x) + tr(x^{2^i+1}) + tr(x + tr(x) + tr(x^{2^i+1})) \\ &+ tr((x + tr(x) + tr(x^{2^i+1}))^{2^i+1}) = x + 3tr(x) + 2tr(x^{2^i+1}) \\ &+ tr(x^{2^i+1} + (x^{2^i} + x + 1)(tr(x) + tr(x^{2^i+1}))) = x + tr(x) + tr(x^{2^i+1}) \\ &+ tr(1)(tr(x) + tr(x^{2^i+1})) = x, \end{aligned}$$

since

$$\begin{aligned}(x+tr(x)+tr(x^{2^i+1}))^{2^i+1} &= (x+tr(x)+tr(x^{2^i+1}))(x^{2^i}+tr(x)+tr(x^{2^i+1}))\\ &= x^{2^i+1}+(x^{2^i}+x+1)(tr(x)+tr(x^{2^i+1})).\end{aligned}$$

We have

$$F_2(x)=L_2(x,F(x))=x^{2^i+1}+tr(x^{2^i+1})+tr(x),$$

then

$$\begin{aligned}F_2\circ F_1^{-1}(x) &= (x+tr(x)+tr(x^{2^i+1}))^{2^i+1}+tr((x+tr(x)+tr(x^{2^i+1}))^{2^i+1})\\ &+tr(x+tr(x)+tr(x^{2^i+1}))=x^{2^i+1}+(x^{2^i}+x+1)(tr(x)+tr(x^{2^i+1}))\\ &+tr(x^{2^i+1}+(x^{2^i}+x+1)(tr(x)+tr(x^{2^i+1})))+tr(x^{2^i+1})\\ &= x^{2^i+1}+(x^{2^i}+x)tr(x+x^{2^i+1}).\end{aligned}$$

By Proposition 32 the function F' is AB.
For $m>3$ the algebraic degree of F' is 3. Indeed, let us take $i=1$ for simplicity. Then

$$\begin{aligned}&(x+x^2)tr(x^3)=(x+x^2)(x^{2+1}+x^{2^2+2}+...+x^{2^{m-1}+2^{m-2}}+x^{2^m+2^{m-1}})\\ &=[x^{2^2}+x^{2^2+2+1}+x^{2^3+2^2+1}+...+x^{2^{m-1}+2^{m-2}+1}+x^{2^{m-1}+2}]\\ &+[x^{2^2+1}+x^{2^3}+x^{2^3+2^2+2}+...+x^{2^{m-1}+2^{m-2}+2}+x^{2^{m-1}+2+1}]\\ &=x^{2^2}+x^{2^{m-1}+2}+\sum_{j=1}^{m-2}x^{2^{j+1}+2^j+1}+x^{2^2+1}+x^{2^3}+\sum_{j=2}^{m-2}x^{2^{j+1}+2^j+2}+x^{2^{m-1}+2+1}.\end{aligned}$$

All exponents in $\sum_{j=1}^{m-2}x^{2^{j+1}+2^j+1}$ and $\sum_{j=2}^{m-2}x^{2^{j+1}+2^j+2}$ are different and smaller than 2^m; moreover they have the weight 3. Obviously all items in this sum vanish (cancel with $x^{2^{m-1}+2+1}$) if and only if $m\le 3$. Therefore, $d^\circ(F')=3$ for $m>3$.

On the other hand $tr(F'(x))=tr(x^{2^i+1})$ and $d^\circ(tr(F'(x)))=2$. It follows from Proposition 16 that F' is EA-inequivalent to any power function. □

Remark It was conjectured in [15] that any AB function is EA-equivalent to a permutation. The AB function from Theorem 1 serves as a counterexample for this conjecture. It was checked by the help of a computer, that for no linear function L on $\mathbb{F}_{2^5}$ the sum $F'+L$ is a permutation for the AB function $F'(x)=x^{2^i+1}+(x^{2^i}+x)tr(x^{2^i+1}+x)$, $\gcd(5,i)=1$. Thus, F' is EA-inequivalent to any permutation but it is CCZ-equivalent to the permutation x^{2^i+1}. ◇

Theorem 6 *The function $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $m \geq 4$ even,*

$$F'(x) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1}), \;\; \gcd(m, i) = 1,$$

is an APN function which is EA-inequivalent to any power function.

Proof. The linear mapping

$$\mathcal{L}(x, y) = (L_1, L_2)(x, y) = (x + tr(y), y)$$

is obviously an involution. The function $F_1 = L_1(x, F(x)) = x + tr(x^{2^i+1})$ is also an involution:

$$\begin{aligned} F_1 \circ F_1(x) &= x + tr(x^{2^i+1}) + tr((x + tr(x^{2^i+1}))^{2^i+1}) = x + tr(x^{2^i+1}) \\ &+ tr(x^{2^i+1} + x^{2^i} tr(x^{2^i+1}) + xtr(x^{2^i+1}) + tr(x^{2^i+1})) \\ &= x + 2tr(x^{2^i+1}) + tr(x^{2^i} + x + 1)tr(x^{2^i+1}) = x. \end{aligned}$$

For $F_2(x) = L_2(x, F(x)) = x^{2^i+1}$ we have

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) = (x + tr(x^{2^i+1}))^{2^i+1} = x^{2^i+1} + x^{2^i} tr(x^{2^i+1}) \\ &+ xtr(x^{2^i+1}) + tr(x^{2^i+1}) = x^{2^i+1} + (x^{2^i} + x + 1)tr(x^{2^i+1}). \end{aligned}$$

Hence, F' is CCZ-equivalent to F and it is APN by Proposition 32. The algebraic degree of F' is 3 and $d^\circ(tr(F')) = 2$ since $tr(F'(x)) = tr(x^{2^i+1})$. Therefore, F' is EA-inequivalent to power functions by Proposition 16. □

Remark Note that the proofs of Theorems 5 and 6 do not depend on the condition $\gcd(i, m) = 1$. When $\gcd(i, m) = s$ then the functions F' have the same differential and linear properties as x^{2^i+1} and, therefore, if m/s is odd they can be considered as the first polynomials with three valued Walsh spectrum $\{0, \pm 2^{\frac{m+s}{2}}\}$, which are EA-inequivalent to power functions.

4.2 The case m divisible by 3

Theorem 7 *The function $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, m divisible by 6,*

$$F'(x) = [x + tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr(x)tr_{m/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1},$$

with $\gcd(m, i) = 1$, is an APN function.

Proof. The linear function $\mathcal{L} : \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}^2$,

$$\mathcal{L}(x, y) = (L_1, L_2)(x, y) = (x + tr_{m/3}(y^2 + y^4), y)$$

is obviously a permutation. For m divisible by 6 the function

$$F_1(x) = L_1(x, F(x)) = x + tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)})$$

is a permutation (see the example on page 46).

We show below that $F_1^{-1} = F_1 \circ F_1 \circ F_1 \circ F_1 \circ F_1$.

We denote

$$T(x) = tr_{m/3}(x^{2^i+1}),$$

then

$$F_1(x) = x + T(x)^2 + T(x)^4.$$

Since every element of $\mathbb{F}_8$ is equal to its 8 power and the function $tr_{m/3}(x)$ is 0 on $\mathbb{F}_8$, then

$$\begin{aligned} & T \circ F_1(x) = tr_{m/3}[(x + tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)}))^{2^i+1}] \\ = {} & tr_{m/3}[(x + tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)}))(x^{2^i} + tr_{m/3}(x^{2^{i+1}(2^i+1)} \\ + {} & x^{2^{i+2}(2^i+1)}))] = tr_{m/3}[x^{2^i+1} + xtr_{m/3}(x^{2^{i+1}(2^i+1)} + x^{2^{i+2}(2^i+1)}) \\ + {} & x^{2^i} tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)})] = tr_{m/3}(x) tr_{m/3}(x^{2^{s+1}(2^i+1)} + x^{2^{s+2}(2^i+1)}) \\ + {} & tr_{m/3}(x^{2^s}) tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr_{m/3}(x^{2^i+1}). \end{aligned}$$

Therefore,

$$\begin{aligned} & F_1 \circ F_1(x) = F_1(x) + [T \circ F_1(x))]^2 + [T \circ F_1(x))]^4 \\ = {} & x + 2tr_{m/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr_{m/3}(x^2) tr_{m/3}(x^{2^{s+2}(2^i+1)} \\ + {} & x^{2^s(2^i+1)}) + tr_{m/3}(x^{2^{s+1}}) tr_{m/3}(x^{4(2^i+1)} + x^{2^i+1}) \\ + {} & tr_{m/3}(x^4) tr_{m/3}(x^{2^s(2^i+1)} + x^{2^{s+1}(2^i+1)}) + tr_{m/3}(x^{2^{s+2}}) tr_{m/3}(x^{2^i+1} + x^{2(2^i+1)}) \end{aligned}$$

Considering separately the cases $s = 1$ and $s = 2$ we get

$$\begin{aligned} F_1 \circ F_1(x) &= x + tr_{m/3}(x + x^2 + x^4) tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)}) \\ &= x + tr(x) tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)}) = x + (T(x) + T(x)^{2^s}) tr(x). \end{aligned}$$

Like this we get

$$F_1 \circ F_1 \circ F_1 \circ F_1 \circ F_1(x) = x + T(x)^2 + T(x)^4 + tr(x)(T(x) + T(x)^{2^{2s}}),$$

$$F_1 \circ F_1 \circ F_1 \circ F_1 \circ F_1 \circ F_1(x) = x.$$

Thus,

$$\begin{aligned} F'(x) &= F_2 \circ F_1^{-1}(x) = [x + T(x)^2 + T(x)^4 + tr(x)(T(x) + T(x)^{2^{2s}})]^{2^i+1} = x^{2^i+1} + T(x)^{2^s+1} \\ &+ tr(x^{2^i+1})T(x)^{2^{2s}} + tr(x)(T(x) + T(x)^4) + xtr(x)(T(x) + T(x)^{2^s}) \\ &+ x^{2^i} tr(x)(T(x) + T(x)^{2^{2s}}) + x(T(x) + T(x)^{2^{2s}}) + x^{2^i}(T(x)^2 + T(x)^4), \end{aligned}$$

where $F_2(x) = L_2(x, F(x)) = x^{2^i+1}$.

The function F' is CCZ-equivalent to the APN function x^{2^i+1}, therefore F' is APN.

F' has the algebraic degree 4. Indeed,

$$\begin{aligned} F'(x) &= [x^{2^i+1} + tr(x)(T(x) + T(x)^4) + x(T(x) + T(x)^{2^{2s}}) + x^{2^i}(T(x)^2 + T(x)^4)] \\ &+ [T(x)^{2^s+1} + tr(x^{2^i+1})T(x)^{2^{2s}} + xtr(x)(T(x) + T(x)^{2^s}) + x^{2^i} tr(x)(T(x) + T(x)^{2^{2s}})], \end{aligned}$$

and we have to consider only the polynomial in the second bracket since the function in the first bracket has the algebraic degree smaller than 4. For simplicity we shall consider the case $i = 1$. Replacing $T(x) = tr_{m/3}(x^{2^i+1})$ and $tr(x^3) = tr_{m/3}(x^3) + (tr_{m/3}(x^3))^2 + (tr_{m/3}(x^3))^4$ we get

$$\begin{aligned} &[(tr_{m/3}(x^3))^3 + (tr_{m/3}(x^3))^5 + (tr_{m/3}(x^3))^6] + tr_{m/3}(x^3) \\ &+[xtr(x)tr_{m/3}(x^3 + x^6) + x^2 tr(x)tr_{m/3}(x^3 + x^{12})]. \end{aligned}$$

Obviously, all the items in the second bracket have the form $x^{2^j+2^k+2^l+2^r}$, where $r \leq l \leq k \leq j \leq m-1$, $r \leq 1$. Therefore, if we find an item of algebraic degree 4 in the first bracket of the form $x^{2^j+2^k+2^l+2^r}$, where $2 \leq r < l < k < j \leq m-1$, which does not cancel, then this item does not vanish in the whole sum.

$$\begin{aligned} tr_{m/3}(x^3) &= x^{2+1} + x^{2^4+2^3} + ... + x^{2^{m-5}+2^{m-6}} + x^{2^{m-2}+2^{m-3}} = \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}} \\ (tr_{m/3}(x^3))^2 &= x^{2^2+2} + x^{2^5+2^4} + ... + x^{2^{m-4}+2^{m-5}} + x^{2^{m-1}+2^{m-2}} = \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+2}+2^{3k+1}} \\ (tr_{m/3}(x^3))^4 &= x^{2^3+2^2} + x^{2^6+2^5} + ... + x^{2^{m-3}+2^{m-4}} + x^{2^m+2^{m-1}} = \sum_{k=0}^{\frac{m}{3}-2} x^{2^{3k+3}+2^{3k+2}} + x^{2^{m-1}+1} \end{aligned}$$

$$(tr_{m/3}(x^3))^3 = (tr_{m/3}(x^3))^2 tr_{m/3}(x^3) = \sum_{i,k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}+2^{3i+2}+2^{3i+1}} \tag{4.1}$$

$$(tr_{m/3}(x^3))^5 = \sum_{j=0}^{\frac{m}{3}-2} \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+1}+2^{3k}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+1}+2^{3k}} \tag{4.2}$$

$$(tr_{m/3}(x^3))^6 = \sum_{j=0}^{\frac{m}{3}-2} \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+2}+2^{3k+1}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+2}+2^{3k+1}} \tag{4.3}$$

Note that all exponents of weight 4 in (4.1), (4.2), (4.3) are smaller than 2^m. If $m \geq 12$ then it is obvious that the item $x^{2^6+2^5+2^4+2^3}$ does not vanish in (4.2) and it definitely differs from all items in (4.1) and (4.3). Hence, for $m \geq 12$ the function F' has the algebraic degree 4 and for $m = 6$ it can be easily checked by a computer.

Thus, F' is EA-inequivalent to other known APN functions since for m divisible by 6 we have no known APN functions of algebraic degree 4. □

Theorem 8 *Let $m \geq 9$ be odd and divisible by* 3 *and* $T(x) = tr_{m/3}(x^{2^i+1})$, *with* $\gcd(m, i) = 1$. *Then the function* $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$,

$$\begin{aligned} F'(x) = {} & x^{2^i+1} + tr(x^{2^i+1}) + T(x)^6 + T(x)^2 tr(x) + x tr(x) tr_{m/3}(x)^{2^{i+1}} \\ & + tr(x) tr_{m/3}(x)^{2(2^i+1)} + xT(x)(tr_{m/3}(x)^6 + tr_{m/3}(x) + 1) + x^{2^i} tr(x) tr_{m/3}(x)^2 \\ & + T(x)^{2^i+1}(x + tr_{m/3}(x)) + x^{2^i} T(x)^{2^{i+1}} (tr_{m/3}(x)^4 + tr_{m/3}(x)^3 + 1) \\ & + T(x)(tr_{m/3}(x)^4 + tr_{m/3}(x)^{2^{i-1}}) + x^{2^i} T(x)^{2^{i-1}} (tr_{m/3}(x)^5 + tr_{m/3}(x)^2 + 1) \\ & + T(x)^{2^{2i}+1}(x^{2^i} + tr_{m/3}(x)^{2^i}) + T(x)^4 (tr_{m/3}(x) + tr_{m/3}(x)^{2^i} + tr_{m/3}(x)^{4(2^i+1)}) \\ & + xT(x)^{2^i} (tr_{m/3}(x)^{2^i+1} + tr_{m/3}(x)^{2^{2i}} + 1), \end{aligned}$$

is an AB function which is EA-inequivalent to any power function.

Proof. Let m be odd and divisible by 3. Then the linear functions

$$\mathcal{L}(x, y) = (L_1, L_2)(x, y) = (x + tr(x) + tr_{m/3}(y^{2^s}), y + tr(x)), \qquad 1 \leq s \leq 2,$$

are obviously permutations on $\mathbb{F}_{2^m}^2$. The function $F_1(x) = x + tr(x) + tr_{m/3}(x^{2^s(2^i+1)})$, $s = i$ $[mod\ 3]$, $\gcd(m, i) = 1$, is a permutation on $\mathbb{F}_{2^m}$ as it is shown in the example on page 46. We have

$$F_1(x) = \sum_{\epsilon \in \mathbb{F}_2, w \in \mathbb{F}_8} (tr(x) + \epsilon + 1)((tr_{m/3}(x^{2^s(2^i+1)}) + w)^7 + 1)(x + \epsilon + w).$$

Hence,

$$\begin{aligned} F_1^{-1}(x) = &\sum_{\epsilon\in\mathbb{F}_2, w\in\mathbb{F}_8} (tr(x+\epsilon+w)+\epsilon+1)((tr_{m/3}((x+\epsilon+w)^{2^s(2^i+1)})+w)^7+1)(x+\epsilon+w) \\ &= tr_{m/3}(x^{2^i+1})^{2^{2s}+1} + tr_{m/3}(x^{2^i+1})^{2^{s+2}}(tr_{m/3}(x)^5 + tr_{m/3}(x)^2+1) \\ &+ tr_{m/3}(x^{2^i+1})^{2^{s+1}}(tr_{m/3}(x)^3 + tr_{m/3}(x)^4+1) + tr(x)tr_{m/3}(x)^2 + x. \end{aligned}$$

The last equality we get by routine computations with the help of a computer as well as the following:

$$\begin{aligned} F'(x) = F_2 \circ F_1^{-1}(x) &= x^{2^i+1} + tr(x^{2^i+1}) + T(x)^6 + T(x)^2 tr(x) + xtr(x)tr_{m/3}(x)^{2^{s+1}} \\ &+ tr(x)tr_{m/3}(x)^{2(2^s+1)} + xT(x)(tr_{m/3}(x)^6 + tr_{m/3}(x)+1) + x^{2^i}tr(x)tr_{m/3}(x)^2 \\ &+ T(x)^{2^s+1}(x+tr_{m/3}(x)) + x^{2^i}T(x)^{2^{s+1}}(tr_{m/3}(x)^4 + tr_{m/3}(x)^3+1) \\ &+ T(x)(tr_{m/3}(x)^4 + tr_{m/3}(x)^{2^{s-1}}) + x^{2^i}T(x)^{2^{s-1}}(tr_{m/3}(x)^5 + tr_{m/3}(x)^2+1) \\ &+ T(x)^{2^{2s}+1}(x^{2^i} + tr_{m/3}(x)^{2^s}) + T(x)^4(tr_{m/3}(x) + tr_{m/3}(x)^{2^s} + tr_{m/3}(x)^{4(2^s+1)}) \\ &+ xT(x)^{2^s}(tr_{m/3}(x)^{2^s+1} + tr_{m/3}(x)^{2^{2s}}+1), \end{aligned}$$

where $F_2(x) = L_2(x, F(x)) = x^{2^i+1} + tr(x)$ and $T(x) = tr_{m/3}(x^{2^i+1})$. The function F' is CCZ-equivalent to the AB function x^{2^i+1}, then F' is AB by Proposition 32. Obviously, $d^\circ(F) \leq 5$ and it is possible to show that not all the items of the algebraic degree 5 vanish in F' using the same methods like in Theorem 7. Thus, the algebraic degree of F' is 5 but $d^\circ(tr(F'(x))) \leq 4$. Indeed, we have $F'(x) = U(x) + V(x)$, where $V(x)$ has the algebraic degree smaller than 5 and

$$\begin{aligned} U(x) &= xT(x)tr_{m/3}(x)^6 + T(x)^{2^s+1}(x+tr_{m/3}(x)) + x^{2^i}T(x)^{2^{s+1}}tr_{m/3}(x)^3 \\ &+ x^{2^i}T(x)^{2^{s-1}}tr_{m/3}(x)^5 + T(x)^{2^{2s}+1}(x^{2^i} + tr_{m/3}(x)^{2^s}) + xT(x)^{2^s}tr_{m/3}(x)^{2^s+1}. \end{aligned}$$

We have

$$\begin{aligned} tr(U(x)) &= tr_3(T(x)tr_{m/3}(x)^7) + 2tr_3(T(x)^{2^s+1}tr_{m/3}(x)) + tr_3(T(x)^{2^{s+1}}tr_{m/3}(x))^{2^s+3}) \\ &+ tr_3(T(x)^{2^{s-1}}tr_{m/3}(x)^{2^s+5}) + 2tr_3(T(x)^{2^{2s}+1}tr_{m/3}(x)^{2^s}) + tr_3(T(x)^{2^s}tr_{m/3}(x)^{2^s+2}) \\ &= tr_3(T(x)tr_{m/3}(x)^{2^s+1}) + tr_3(T(x)^{2^{s+1}}tr_{m/3}(x)). \end{aligned}$$

Hence, $d^\circ(tr(F')) \leq 4$. By Proposition 17 the function F' is EA-inequivalent to power functions. □

4.3 m odd case

The next theorem shows that the number of different classes of AB polynomials EA-inequivalent to power functions is infinite.

Theorem 9 *The function $F' : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, where m is odd and divisible by n, $m \neq n$ and* $\gcd(m, i) = 1$,

$$\begin{aligned} F'(x) &= x^{2^i+1} + tr_{m/n}(x^{2^i+1}) + x^{2^i} tr_{m/n}(x) + x\ tr_{m/n}(x)^{2^i} \\ &+ [tr_{m/n}(x)^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x)]^{\frac{1}{2^i+1}}(x^{2^i} + tr_{m/n}(x)^{2^i} + 1) \\ &+ [tr_{m/n}(x)^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x)]^{\frac{2^i}{2^i+1}}(x + tr_{m/n}(x)), \end{aligned}$$

is an AB function which is EA-inequivalent to any power function.

Proof. Let m be odd and divisible by n. Obviously, the linear function

$$\mathcal{L}(x,y) = (L_1, L_2)(x,y) = (x + tr_{m/n}(x) + tr_{m/n}(y), y + tr_{m/n}(x))$$

is a permutation on $\mathbb{F}_{2^m}^2$. We have

$$F_1(x) = x + tr_{m/n}(x) + tr_{m/n}(x^{2^i+1}),$$

$$F_2(x) = x^{2^i+1} + tr_{m/n}(x).$$

The function F_1 is one of the permutations from the example on page 46. We need the inverse of the function F_1 to construct $F' = F_2 \circ F_1^{-1}$.
For any fixed element $x \in \mathbb{F}_{2^m}$ we have

$$y = x + tr_{m/n}(x) + tr_{m/n}(x^{2^i+1}) = x + u,$$

for some $u \in \mathbb{F}_{2^n}$, and, therefore, $x = y + u$. Then

$$y = (y+u) + tr_{m/n}(y+u) + tr_{m/n}((y+u)^{2^i+1})$$

which yields

$$u^{2^i+1} + u^{2^i} tr_{m/n}(y) + u(tr_{m/n}(y))^{2^i} + tr_{m/n}(y^{2^i+1}) + tr_{m/n}(y) = 0. \tag{4.4}$$

If $tr_{m/n}(y) \neq 0$ then we denote $v = u/tr_{m/n}(y)$ and we get

$$v^{2^i+1} + v^{2^i} + v + \frac{tr_{m/n}(y^{2^i+1}) + tr_{m/n}(y)}{(tr_{m/n}(y))^{2^i+1}} = 0.$$

Since $v^{2^i+1}+v^{2^i}+v=(v+1)^{2^i+1}+1$ then

$$v+1=\left[\frac{tr_{m/n}(y^{2^i+1})+tr_{m/n}(y)}{(tr_{m/n}(y))^{2^i+1}}+1\right]^{\frac{1}{2^i+1}}.$$

Replacing v by $u/tr_{m/n}(y)$ we have

$$u=[(tr_{m/n}(y))^{2^i+1}+tr_{m/n}(y^{2^i+1})+tr_{m/n}(y)]^{\frac{1}{2^i+1}}+tr_{m/n}(y).$$

If $tr_{m/n}(y)=0$ then from the equality (4.4) we get $u=[tr_{m/n}(y^{2^i+1})]^{\frac{1}{2^i+1}}$ and we observe that u equals again $[(tr_{m/n}(y))^{2^i+1}+tr_{m/n}(y^{2^i+1})+tr_{m/n}(y)]^{\frac{1}{2^i+1}}+tr_{m/n}(y)$. Thus, in all cases, we have

$$F_1^{-1}(y)=y+u=y+[(tr_{m/n}(y))^{2^i+1}+tr_{m/n}(y^{2^i+1})+tr_{m/n}(y)]^{\frac{1}{2^i+1}}+tr_{m/n}(y)$$

and

$$\begin{aligned}F'(x) &= F_2\circ F_1^{-1}(x)=[x+[(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x)]^{\frac{1}{2^i+1}}+tr_{m/n}(x)]^{2^i+1}\\ &+ tr_{m/n}[x+[(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x)]^{\frac{1}{2^i+1}}+tr_{m/n}(x)]\\ &= x^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x)+x^{2^i}tr_{m/n}(x)+x(tr_{m/n}(x))^{2^i}\\ &+ [(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x)]^{\frac{1}{2^i+1}}(x^{2^i}+(tr_{m/n}(x))^{2^i}+1)\\ &+ [(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x)]^{\frac{2^i}{2^i+1}}(x+tr_{m/n}(x)).\end{aligned}$$

We show below that the function F' has the algebraic degree $n+2$. It means that the number of functions CCZ-equivalent to a Gold AB function and EA-inequivalent to it is not smaller than the number of divisors of m.

The inverse of x^{2^i+1} on F_{2^n} is x^d, where

$$d=\sum_{k=0}^{\frac{n-1}{2}}2^{2ik},$$

and x^d has the algebraic degree $\frac{n+1}{2}$ (see [54]). Obviously, $((tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})+tr_{m/n}(x))^d$ has the algebraic degree $n+1$ if and only if $((tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1}))^d$ has this algebraic degree.

We assume that $m\neq n$ and $n\neq 1$ since when $m=n$ we get $F'(x)=x^{\frac{1}{2^i+1}}+x$ and Theorem 5 gives the case $n=1$.

We have

$$tr_{m/n}(x)=\sum_{k=0}^{\frac{m}{n}-1}x^{2^{kn}}$$

and

$$(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})=\sum_{k=0}^{\frac{m}{n}-1}x^{2^{kn}}\sum_{k=0}^{\frac{m}{n}-1}x^{2^{kn+i}}+\sum_{k=0}^{\frac{m}{n}-1}(x^{2^i+1})^{2^{kn}}$$

$$=\sum_{k,j=0}^{\frac{m}{n}-1}x^{2^{kn}+2^{jn+i}}+\sum_{k=0}^{\frac{m}{n}-1}x^{2^{kn}+2^{kn+i}}=\sum_{\substack{k,j=0\\k\neq j}}^{\frac{m}{n}-1}x^{2^{kn}+2^{jn+i}}.$$

Note that we have

$$[(tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1})]^{2^{2i}+1}=\sum_{\substack{k,j=0\\k\neq j}}^{\frac{m}{n}-1}x^{2^{kn}+2^{jn+i}}\sum_{\substack{k,j=0\\k\neq j}}^{\frac{m}{n}-1}x^{2^{kn+2i}+2^{jn+3i}}$$

$$=\sum_{\substack{k,j,s,t=0\\k\neq j,s\neq t}}^{\frac{m}{n}-1}x^{2^{kn}+2^{jn+i}+2^{sn+2i}+2^{tn+3i}}.$$

Similarly, we have

$$((tr_{m/n}(x))^{2^i+1}+tr_{m/n}(x^{2^i+1}))^d=\sum_{(k_0,\dots,k_n)\in I}x^{\sum_{s=0}^{n}2^{k_sn+si}},\tag{4.5}$$

where $I=\{(l_0,...,l_n):\quad 0\le l_t\le\frac{m}{n}-1,\quad l_{2t}\neq l_{2t+1}\}$.

The equality $k_sn+si=k_tn+ti$ is possible for $0\le s<t\le n$ only for $s=0$ and $t=n$. Indeed, if $k_sn+si=k_tn+ti$ then $(k_s-k_t)n=(t-s)i$. Since $\gcd(n,i)=1$ and $0\le t,s\le n$ then $t=n$, $s=0$ and $k_s-k_t=i$.

For simplicity we consider now the equality (4.5) in the case $i=1$. In the sum $\sum_{s=0}^{n}2^{k_sn+s}$ the largest possible item is $2^{(\frac{m}{n}-1)n+n}=2^m$. Therefore, when $k_n\neq\frac{m}{n}-1$ the sum is smaller than 2^m-1. Besides, all items in the sum are different modulo 2^m-1 except the case when $k_0=0$ and $k_n=\frac{m}{n}-1$ and in the cases where $k_0=k_n+1$. Therefore, when $k_0=k_n=1$ the number $\sum_{s=0}^{n}2^{k_sn+s}$ has the weight $n+1$. On the other hand, when $k_0=k_n=1$ and $k_1=k_{n-1}=0$ the term

$$x^{\sum_{s=0}^{n}2^{k_sn+s}}$$

does not vanish in (4.5). Indeed, if

$$\sum_{s=0}^{n} 2^{k_s n+s} \equiv \sum_{p=0}^{n} 2^{t_p n+p} \mod (2^m - 1)$$

then we have only two possibilities:
1) for any s there exists p such that $k_s n+s = t_p n+p$ (and vice versa). Then $(k_s - t_p)n = p-s$ and since $0 \le s, p \le n$ then $k_0 = t_n + 1$, $t_0 = k_n + 1$ and $k_s = t_s$ for $s \ne 0, n$. If $k_0 = k_n = 1$ then $t_n = 0$, $t_0 = 2$. But in our case $k_0 = k_n = 1$, $t_1 = k_1 = 0$, $t_{n-1} = k_{n-1} = 0$ and, therefore, $t_n \ne 0$ since $t_{n-1} \ne t_n$.
2) if $t_n = \frac{m}{n} - 1$ then k_0 must be equal to 0 or $k_n = \frac{m}{n} - 1$, but $k_0 = k_n = 1$.

Thus, when $k_0 = k_n = 1$ and $k_1 = k_{n-1} = 0$ (for permissible k_s, $1 < s < n-1$) the term

$$x^{\sum_{s=0}^{n} 2^{k_s n+s}}$$

has the algebraic degree $n + 1$ and it does not vanish in (4.5).

If $n \ge 5$ we can also take $k_2 = 1, k_3 = k_4 = 0$ and then we get

$$\sum_{s=0}^{n} 2^{k_s n+s} = 2^n + 2 + 2^{n+2} + 2^3 + 2^4 + ... + 2^{2n}. \tag{4.6}$$

We have

$$((tr_{m/n}(x))^3 + tr_{m/n}(x^3))^d (x^2 + tr_{m/n}(x)^2) + ((tr_{m/n}(x))^3 + tr_{m/n}(x^3))^{2d} (x + tr_{m/n}(x))$$

$$= \sum_{(k_0,...,k_n)\in I} x^{\sum_{s=0}^{n} 2^{k_s n+s}} \sum_{1\le k\le m/n-1} x^{2^{nk+1}} + \sum_{(k_0,...,k_n)\in I} x^{\sum_{s=0}^{n} 2^{k_s n+s+1}} \sum_{1\le j\le m/n-1} x^{2^{nj}}$$

$$= \sum_{\substack{(k_0,...,k_n)\in I \\ 1\le k\le m/n-1}} x^{2^{nk+1}+\sum_{s=0}^{n} 2^{k_s n+s}} + \sum_{\substack{(k_0,...,k_n)\in I \\ 1\le j\le m/n-1}} x^{2^{nj}+\sum_{s=0}^{n} 2^{k_s n+s+1}}. \tag{4.7}$$

We consider the item with the exponent

$$2^n + 2 + 2^{n+2} + 2^3 + 2^4 + ... + 2^{2n} + 2^{nk+1} \tag{4.8}$$

from the first sum in (4.7). It is easy to see that $2^n + 2 + 2^{n+2} + 2^3 + 2^4 + ... + 2^{2n} + 2^{nk+1} < 2^m$ since $k \le m/n - 1$. In this sum $nk + 1 = k_s n + s$ only if $s = 1$. But then $k = k_1 = 0$ which is in contradiction with $1 \le k$. Thus, the number given by this sum has the weight $n + 2$.

The item with the exponent (4.8) does not vanish. Indeed, if there is another item in the first sum of (4.7) with this exponent then

$$2^n + 2 + 2^{n+2} + 2^3 + 2^4 + ... + 2^{2n} + 2^{nk+1} = 2^{nj+1} + \sum_{s=0}^{n} 2^{k_s n+s}.$$

If $k = j$ then (4.6) is equal to another sum $\sum_{s=0}^{n} 2^{k_s n+s}$ and we already showed that it is impossible. If $k \neq j$ then $k_1 = k$ and $j = 0$ while $1 \leq j$.
Assume there exists an item in the second sum of (4.7) with the exponent (4.8) then

$$2^n + 2 + 2^{n+2} + 2^3 + 2^4 + ... + 2^{2n} + 2^{nk+1} = 2^{nj} + \sum_{s=0}^{n} 2^{k_s n+s+1}$$

for some j, $1 \leq j \leq m/n - 1$ and $(k_0, ..., k_n) \in I$. We have $3 = k_s n + s + 1 \mod m$ for some s, $0 \leq s \leq n$. Then $k_s n = 2 - s$ or $k_s n = m - (s - 2)$ and this is possible only if $k_2 = 0$ or $k_2 = m/n$, but since $0 \leq k_s \leq m/n - 1$, then $3 = k_s n + s + 1 \mod m$ only if $k_2 = 0$. The same arguments show that $4 = k_s n + s + 1 \mod m$ only if $k_3 = 0$ and that is in contradiction with the condition $k_{2t} \neq k_{2t+1}$. Therefore the item with the exponent (4.8) does not vanish in (4.7) and then it does not vanish in the sum presenting the function F'. This completes the proof that F' has the algebraic degree $n + 2$.

The algebraic degree of the function $tr(F'(x))$ is not greater than $n + 1$ since

$$\begin{aligned} tr(F'(x)) &= tr(x^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x) + x^{2^i} tr_{m/n}(x) + x(tr_{m/n}(x))^{2^i}) \\ &+ tr_n([(tr_{m/n}(x))^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x)]^{\frac{1}{2^i+1}} tr_{m/n}(x^{2^i} + (tr_{m/n}(x))^{2^i} + 1)) \\ &+ tr_n([(tr_{m/n}(x))^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x)]^{\frac{2^i}{2^i+1}} tr_{m/n}(x + tr_{m/n}(x))) \\ &= tr(x) + tr(x^{2^i} tr_{m/n}(x)) + tr(x(tr_{m/n}(x))^{2^i}) \\ &+ tr([(tr_{m/n}(x))^{2^i+1} + tr_{m/n}(x^{2^i+1}) + tr_{m/n}(x)]^{\frac{1}{2^i+1}}). \end{aligned}$$

Therefore, the function F' is EA-inequivalent to any power function by Proposition 17.□

Chapter 5

On the inverse and EA transformations

CCZ-equivalence gives rise to some interesting problems. One of them is whether Gold, Kasami, Welch and Niho functions are CCZ-inequivalent. The aim of this chapter is to show that it is also a question whether these functions are inequivalent in respect to the inverse and EA transformations. Applying only the inverse and EA transformations on the Gold AB functions we construct a class of AB polynomials which are EA equivalent neither to the Gold mappings nor to their inverses.

We should note that the classes of functions constructed in the previous chapter completely differ from the one constructed below. Indeed, when m is even then for any quadratic APN function F on $\mathbb{F}_{2^m}$ some linear combinations of the coordinate functions are bent [55]. This implies that all functions EA equivalent to the Gold mapping are not permutations (see [14, 55]) and it is impossible to apply the inverse transformation. Therefore, the functions presented in the previous section cannot be constructed from the Gold functions only by applying the inverse and EA transformations. In case m odd the remark on page 52 can serve as an evidence that those functions cannot be constructed from the Gold mappings only by applying the inverse and EA transformations, but we do not have an exact proof.

The questions about equivalences do not occur in the cases of the inverse and Dobbertin APN functions because of their unique nonlinearities [9, 44].

If a function F' is EA-equivalent to a function F or the inverse of F then either $d^\circ(F') = d^\circ(F)$ or $d^\circ(F') = d^\circ(F^{-1})$. It could be used as a tool to show that the classes of AB power functions are inequivalent in respect to the inverse and EA transformations. But the theorem below shows that this property does not hold if we apply the inverse and EA transformations in consecutive order several times.

Theorem 10 *Let $m \geq 9$ be odd and divisible by 3. Let $F(x) = x^{2^i+1}$ and*

$$F'(x) = x^{2^i+1} + (tr_{m/3}(x^{2^i+1}))^6 + (tr_{m/3}(x^{2^i+1}))^5 + (tr_{m/3}(x^{2^i+1}))^3 + (tr_{m/3}(x^{2^i+1}))^4$$
$$+x^{2^i} tr_m(x) tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + x\ tr_m(x) tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)}) + x^{2^i} tr_{m/3}(x^{2(2^i+1)}$$
$$+x^{2^{2s+1}(2^i+1)}) + x\ tr_{m/3}(x^{2(2^i+1)} + x^{2^{s+1}(2^i+1)}) + tr_m(x) tr_{m/3}(x^{2^i+1} + x^{4(2^i+1)})$$

be functions on $\mathbb{F}_{2^m}$ with $\gcd(i,m) = 1$. Then F^{-1} and F'^{-1} are EA-equivalent and $d^\circ(F) \neq d^\circ(F') \neq d^\circ(F^{-1})$.

Proof. We use CCZ-equivalence to prove this theorem.

If m is odd and divisible by 3 then the linear function $L(x,y) = (x + tr_{m/3}(y + y^{2^{2s}}), y)$, $1 \leq s \leq 2$, is a permutation on $\mathbb{F}_{2^m}^2$ since its kernel is $\{(0,0)\}$. It is shown in the example on page 46 that the function

$$F_1(x) = x + tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)}),$$

with $s = i$ [mod 3] and $\gcd(i,m) = 1$, is a permutation. Therefore, the function $F'(x) = F_2 \circ F_1^{-1}(x) = [F_1^{-1}(x)]^{2^i+1}$, where $F_2(x) = x^{2^i+1}$, is an AB permutation CCZ-equivalent to F and

$$F'^{-1}(x) = F_1(x^{\frac{1}{2^i+1}}) = x^{\frac{1}{2^i+1}} + tr_{m/3}(x + x^{2^{2s}}).$$

Thus, the functions F'^{-1} and F^{-1} are EA equivalent.

We have $d^\circ(F) = 2$ and it is proven in [54] that $d^\circ(F^{-1}) = \frac{m+1}{2}$. We show below that $d^\circ(F') = 4$ for $m \geq 9$.

To get the function F' we need the inverse of the function F_1. The following computations are helpful to show that $F_1^{-1} = F_1 \circ F_1$.

$$tr_{m/3}[(x + tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)}))^{2^i+1}] = tr_{m/3}(x^{2^i+1}) + tr_{m/3}(x^{2^s}) tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)})$$
$$+tr_{m/3}(x) tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)}) + tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)}),$$

since

$$tr_{m/3}((x^{2^i+1} + x^{2^{2s}(2^i+1)})^{2^i}) = tr_{m/3}((x^{2^i+1} + x^{2^{2s}(2^i+1)})^{2^s})$$
$$= tr_{m/3}(x^{2^s(2^i+1)} + x^{2^{3s}(2^i+1)}) = tr_{m/3}(x^{2^s(2^i+1)} + x^{2^i+1}).$$

Then

$$\begin{aligned}
&tr_{m/3}[(x+tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^i+1}+(x+tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{2s}(2^i+1)}]\\
&=tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+tr_{m/3}(x^{2^s})tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&+tr_{m/3}(x)tr_{m/3}(x^{2^{2s}(2^i+1)}+x^{2^s(2^i+1)})+tr_{m/3}(x)tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&+tr_{m/3}(x^{2^{2s}})tr_{m/3}(x^{2^{2s}(2^i+1)}+x^{(2^i+1)})+tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&+tr_{m/3}(x^{2^{2s}(2^i+1)}+x^{2^s(2^i+1)})tr_{m/3}(x^{2^{2s}(2^i+1)}+x^{(2^i+1)})=tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&+tr_{m/3}(x+x^{2^s}+x^{2^{2s}})tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2\\
&=tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2
\end{aligned}$$

and

$$F_1\circ F_1(x)=x+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2$$

and, since $tr_m(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))=0$,

$$\begin{aligned}
&(F_1\circ F_1)\circ F_1(x)=x+tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+tr_m(x)[tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2]+[tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2]^2\\
&=x+tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^4\\
&=x+tr_3(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))=x+tr_m(x^{2^i+1}+x^{2^{2s}(2^i+1)}))=x.
\end{aligned}$$

Therefore,

$$F_1^{-1}(x)=F_1\circ F_1(x)=x+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^2.$$

Thus, we have

$$\begin{aligned}
&F'(x)=F_2\circ F_1^{-1}(x)=[F_1^{-1}(x)]^{2^i+1}=[x+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+(tr_{m/3}(x^{2^i+1}\\
&+x^{2^{2s}(2^i+1)}))^2]^{2^i+1}=x^{2^i+1}+tr_m(x)(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+1}\\
&+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2(2^s+1)}+x^{2^i}tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\
&+x\ tr_m(x)(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s}+x^{2^i}tr_{m/3}(x^{2(2^i+1)}+x^{2^{2s+1}(2^i+1)})\\
&+x\ (tr_{m/3}(x^{2(2^i+1)}+x^{2^{2s+1}(2^i+1)}))^{2^s}+tr_m(x)(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+2}\\
&+tr_m(x)(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{s+1}+1}=x^{2^i+1}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2(2^s+1)}\\
&+x^{2^i}tr_m(x)(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+x\ tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\
&+x^{2^i}tr_{m/3}(x^{2(2^i+1)}+x^{2^{2s+1}(2^i+1)})+x\ tr_{m/3}(x^{2(2^i+1)}+x^{2^{s+1}(2^i+1)})+tr_m(x)[(tr_{m/3}(x^{2^i+1}\\
&+x^{2^{2s}(2^i+1)}))^{2^s+1}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+2}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{s+1}+1}].
\end{aligned}$$

The only item in this sum which can give algebraic degree greater than 4 is the last item. We have

$$\begin{aligned}&(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+1}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+2}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{s+1}+1}\\ &= (tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+1}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{4(2^s+1)}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{2s}},\end{aligned}$$

since

$$2^s+2=\begin{cases}4 \text{ if } s=1\\ 6 \text{ if } s=2\end{cases}, \qquad 4(2^s+1)=\begin{cases}12=5 \pmod{2^3-1} \text{ if } s=1\\ 20=6 \pmod{2^3-1} \text{ if } s=2\end{cases},$$

$$2^{s+1}+1=\begin{cases}5 & \text{if } s=1\\ 9=2 \pmod{2^3-1} & \text{if } s=2\end{cases}, \quad 2^{2s}=\begin{cases}4 & \text{if } s=1\\ 16=2 \pmod{2^3-1} & \text{if } s=2\end{cases}.$$

On the other hand,

$$\begin{aligned}&(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+1} = tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\ &= tr_{m/3}(x^{2^i+1})^2+(tr_{m/3}(x^{2^i+1}))^{2^{2s}+1}+(tr_{m/3}(x^{2^i+1}))^{2^s+1}+(tr_{m/3}(x^{2^i+1}))^{2^{2s}+2^s}\\ &= (tr_{m/3}(x^{2^i+1}))^6+(tr_{m/3}(x^{2^i+1}))^5+(tr_{m/3}(x^{2^i+1}))^3+(tr_{m/3}(x^{2^i+1}))^2 \qquad (5.1)\end{aligned}$$

Using (5.1) we get

$$\begin{aligned}&(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^s+1}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{4(2^s+1)}+(tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)}))^{2^{2s}}\\ &= (tr_{m/3}(x^{2^i+1}))^6+(tr_{m/3}(x^{2^i+1}))^5+(tr_{m/3}(x^{2^i+1}))^3+(tr_{m/3}(x^{2^i+1}))^2+[(tr_{m/3}(x^{2^i+1}))^3\\ &+(tr_{m/3}(x^{2^i+1}))^6+(tr_{m/3}(x^{2^i+1}))^5+tr_{m/3}(x^{2^i+1})]+(tr_{m/3}(x^{2^i+1}))^2+(tr_{m/3}(x^{2^i+1}))^4\\ &= tr_{m/3}(x^{2^i+1})+(tr_{m/3}(x^{2^i+1}))^4. \qquad (5.2)\end{aligned}$$

Hence, applying (5.1) and (5.2) we get

$$\begin{aligned}F'(x) &= x^{2^i+1}+[(tr_{m/3}(x^{2^i+1}))^6+(tr_{m/3}(x^{2^i+1}))^5+(tr_{m/3}(x^{2^i+1}))^3+(tr_{m/3}(x^{2^i+1}))^2]^2\\ &+x^{2^i}tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})+x\ tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})\\ &+x^{2^i}tr_{m/3}(x^{2(2^i+1)}+x^{2^{2s+1}(2^i+1)})+x\ tr_{m/3}(x^{2(2^i+1)}+x^{2^{s+1}(2^i+1)})\\ &+tr_m(x)[tr_{m/3}(x^{2^i+1})+(tr_{m/3}(x^{2^i+1}))^4] = x^{2^i+1}+(tr_{m/3}(x^{2^i+1}))^6+(tr_{m/3}(x^{2^i+1}))^5\\ &+(tr_{m/3}(x^{2^i+1}))^3+(tr_{m/3}(x^{2^i+1}))^4+x^{2^i}tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^{2s}(2^i+1)})\\ &+x\ tr_m(x)tr_{m/3}(x^{2^i+1}+x^{2^s(2^i+1)})+x^{2^i}tr_{m/3}(x^{2(2^i+1)}+x^{2^{2s+1}(2^i+1)})\\ &+x\ tr_{m/3}(x^{2(2^i+1)}+x^{2^{s+1}(2^i+1)})+tr_m(x)tr_{m/3}(x^{2^i+1}+x^{4(2^i+1)}).\end{aligned}$$

Below we consider all items in the sum presenting the function F' which may give the algebraic degree 4:

$$[(tr_{m/3}(x^{2^i+1}))^6 + (tr_{m/3}(x^{2^i+1}))^5 + (tr_{m/3}(x^{2^i+1}))^3]$$

$$+[x^{2^i} tr_m(x)(tr_{m/3}(x^{2^i+1} + x^{2^{2s}(2^i+1)}) + x\ tr_m(x)(tr_{m/3}(x^{2^i+1} + x^{2^s(2^i+1)})].$$

For simplicity we take $i = 1$. Obviously, all the items in the second bracket of the algebraic degree 4 have the form $x^{2^j+2^k+2^l+2^r}$, where $r < l < k < j \leq m-1$, $r \leq 1$. Therefore, if we find an item of algebraic degree 4 in the first bracket of the form $x^{2^j+2^k+2^l+2^r}$, where $2 \leq r < l < k < j \leq m-1$, which does not cancel, then this item does not vanish in the whole sum.

We have

$$tr_{m/3}(x^3) = x^{2+1} + x^{2^4+2^3} + ... + x^{2^{m-5}+2^{m-6}} + x^{2^{m-2}+2^{m-3}} = \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}},$$

$$(tr_{m/3}(x^3))^2 = x^{2^2+2} + x^{2^5+2^4} + ... + x^{2^{m-4}+2^{m-5}} + x^{2^{m-1}+2^{m-2}} = \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3k+2}+2^{3k+1}},$$

$$(tr_{m/3}(x^3))^4 = x^{2^3+2^2} + x^{2^6+2^5} + ... + x^{2^{m-3}+2^{m-4}} + x^{2^m+2^{m-1}} = \sum_{k=0}^{\frac{m}{3}-2} x^{2^{3k+3}+2^{3k+2}} + x^{2^{m-1}+1},$$

then

$$(tr_{m/3}(x^3))^3 = (tr_{m/3}(x^3))^2 tr_{m/3}(x^3) = \sum_{i,k=0}^{\frac{m}{3}-1} x^{2^{3k+1}+2^{3k}+2^{3i+2}+2^{3i+1}}, \tag{5.3}$$

$$(tr_{m/3}(x^3))^5 = \sum_{j=0}^{\frac{m}{3}-2} \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+1}+2^{3k}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+1}+2^{3k}}, \tag{5.4}$$

$$(tr_{m/3}(x^3))^6 = \sum_{j=0}^{\frac{m}{3}-2} \sum_{k=0}^{\frac{m}{3}-1} x^{2^{3j+3}+2^{3j+2}+2^{3k+2}+2^{3k+1}} + \sum_{k=0}^{\frac{m}{3}-1} x^{2^{m-1}+1+2^{3k+2}+2^{3k+1}}. \tag{5.5}$$

Note that all exponents of weight 4 in (5.3), (5.4), (5.5) are smaller than 2^m. If $m \geq 9$ then it is obvious that the item $x^{2^6+2^5+2^4+2^3}$ does not vanish in (5.4) and it definitely differs from all items in (5.3) and (5.5).

Hence, the function F' has the algebraic degree 4 when $m \geq 9$ and that completes the proof of Theorem 1. □

Chapter 6

Conclusion

In this thesis we consider the questions of the existence of classes of APN and AB functions which are inequivalent to power mappings. We pay a special attention to CCZ-equivalence presented in [15]. We carefully study connections between CCZ- and EA-equivalences and we give a sufficient condition for a function to be EA-inequivalent to power functions. Applying the CCZ-equivalence to the Gold power functions we construct the first classes of APN and AB polynomials which are EA-inequivalent to power functions and we show that in the AB case the number of such classes is infinite while there are only four classes of AB power functions known, see [8, 27]. By that we show that CCZ-equivalence is more general than EA-equivalence together with the inverse transformation. However because of time constraints we have to leave many questions for our future research. In particular our results lead to a question whether four known classes of AB power functions are CCZ-inequivalent. It means that we need more invariants for CCZ-equivalence. It is also interesting to find a criterion for a function to be CCZ-inequivalent to power functions. Besides we have no examples of functions CCZ-equivalent to power APN mappings different from the Gold functions which are EA-inequivalent to power mappings.

Further we also prove that applying only the inverse and EA transformations on a permutation F it is possible to construct a class of functions which is EA-inequivalent to both F and F^{-1} while it was expected that all the functions constructed from F by using the inverse and EA transformations are EA-equivalent to either F or F^{-1}.

Bibliography

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions and distance-regular graphs. *Electron. J. Comb.*, 5(R34), 14, 1998.

[2] C. H. Bennett, G. Brassard and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Computing 17*, pp. 210-229, 1988.

[3] T. Beth and C. Ding. On almost perfect nonlinear permutations. *Advances in Cryptology–EUROCRYPT'93, Lecture Notes in Computer Science*, 765, Springer-Verlag, New York, pp. 65-76, 1993.

[4] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.

[5] L. Budaghyan, C. Carlet, A. Pott. New Constructions of Almost Perfect Nonlinear and Almost Bent Functions. *Proceedings of the Workshop on Coding and Cryptography 2005*, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.

[6] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Perfect Nonlinear and Almost Bent Functions. submitted to *IEEE Trans. Inform. Theory* (also available on http://arxiv.org), 2005.

[7] A. Canteaut, P. Charpin and H. Dobbertin. A new characterization of almost bent functions. *Fast Software Encryption 99, Lecture Notes in Computer Science* 1636, L. Knudsen edt, pp. 186-200. Springer-Verlag, 1999.

[8] A. Canteaut, P. Charpin and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.

[9] A. Canteaut, P. Charpin, H. Dobbertin. Weight divisibility of cyclic codes , highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105-138, 2000.

[10] C. Carlet. Codes de Reed-Muller, codes de Kerdock et de Preparata. PhD thesis, Publication of LITP, Institut Blaise Pascal, Université Paris 6, 90.59, 1990.

[11] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3, pp. 135-145, 1993.

[12] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. *Proceedings of SETA'01*, Discrete Mathematics and Theoretical Computer Science, New York, Springer Verlag, pp. 131-144, 2001.

[13] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Methods and Models*, Yves Crama and Peter Hammer eds, Cambridge University Press, to appear (winter 2005-2006).

[14] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Yves Crama and Peter Hammer eds, Cambridge University Press, to appear (winter 2005-2006).

[15] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[16] C. Carlet and C. Ding. Highly Nonlinear Mappings. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 205-244, 2004.

[17] C. Carlet and E. Prouff. On plateaued functions and their constructions. Proceedings of *Fast Software Encryption 2003, Lecture Notes in Computer Science* 2887, pp.54-73, 2003.

[18] C. Carlet and E. Prouff. On a new notion of nonlinearity relevant to multi-output pseudo-random generators. *Proceeding of Selected Areas in Cryptography 2003, Lecture Notes in Computer Science* 3006, to appear, 2004.

[19] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. *Advances in Cryptology–EUROCRYPT'94, Lecture Notes in Computer Science*, Springer-Verlag, New York, 950, pp. 356-365, 1995.

[20] P. Charpin, A. Tietavainen and V. Zinoviev. On binary cyclic codes with $d = 3$. *Problems of Information Transmission*, Vol. 33, No. 3, 1997.

[21] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *Advances in cryptology–ASIACRYPT 2002, Lecture Notes in Computer Science* 2501, pp. 267-287, Springer, 2003.

[22] T. Cusick and H. Dobbertin. Some new 3-valued crosscorrelation functions of binary m-sequences. *IEEE Trans. Inform. Theory*, 42, pp.1238-1240, 1996.

[23] E. R. van Dam, D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions. *Eur. J. Comb.* 24(1), pp. 85-98, 2003.

[24] H. Dobbertin. One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. *Appl. Algebra Eng. Commun. Comput.* 9 (2), pp. 139-152, 1998.

[25] H. Dobbertin. Another prof of Kasami's Theorem. *Designs, Codes and Cryptography* 17, pp. 177-180, 1999.

[26] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Niho case. *Inform. and Comput.*, 151, pp. 57-72, 1999.

[27] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45, pp. 1271-1275, 1999.

[28] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. D. Jungnickel and H. Niederreiter eds. *Proceedings of Finite Fields and Applications FQ5*, Augsburg, Germany, Springer, pp. 113-121, 2000.

[29] H. Dobbertin, private communication, 2004.

[30] H. Dobbertin, P. Felke, T. Helleseth, P. Rosendahl. Niho-type crosscorrelation-functions via Dickson Polynomials and Kloosterman Sums. *IEEE, Trans. Inform. Theory.*

[31] J. H. Evertse. Linear structures in block ciphers. In *Advances in Cryptology, EUROCRYPT‘87, Lecture Notes in Computer Science*, Springer-Verlag, No 304, pp. 249-266, 1988.

[32] S. W. Golomb. Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences. *Inform. Sci.*, vol. 1, pp. 87-109, 1968.

[33] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14, pp. 154-156, 1968.

[34] T.Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, vol. 16, pp. 209-232, 1976.

[35] T.Helleseth. A note on the cross-correlation function between two maximal linear sequences. *Discrete Math.*, vol. 23, pp. 301-307, 1978.

[36] T.Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of Coding Theory*, V. Pless and W. C. Hoffman eds., Amsterdam, The Netherlands: Elsevier, vol. II, pp. 1765-1854, 1998.

[37] D. Hertel, private communication, 2005.

[38] H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and Their Applications 7*, pp. 253-286, 2001.

[39] X.-D. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Proceedings of the Workshop on the Coding and Cryptography 2003*, Augot, Charpin and Kabatianski eds, pp. 273-280, 2003.

[40] T. Jakobsen and L. R. Knudsen. The interpolation attack on block ciphers. *Fast Software Encription'97, Lecture Notes in Computer Science* 1267, pp. 28-40, 1997.

[41] H. Janwa and R. Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. *Proceedings of AAECC-10, Lecture Notes in Computer Science*, vol. 673, Berlin, Springer-Verlag, pp. 180-194, 1993.

[42] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Inform. and Control*, 18, pp. 369-394, 1971.

[43] T. Kasami. Weight distribution formula for some class of cyclic codes. *Technical Report R-285 (AD 632574), Coordinated Science Laboratory, University of Illinois, Urbana* (April 1966).

[44] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[45] X. Lai.Higher order derivatives and differential cryptanalysis. *Proc. of the "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday.* 1994.

[46] P. Langevin. Covering radius of $RM(1,9)$ in $RM(3,9)$. *Eurocode'90, Lecture Notes in Computer Science* 514, Springer-Verlag, pp. 51-59, 1991.

[47] R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachusetts, 1983.

[48] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, pp. 386-397, 1994.

[49] R. McEliece. Weight congruence for p-ary cyclic codes. *Discrete Math.* 3, pp.177-192, 1972.

[50] G. McGuire and A. R. Calderbank. Proof of a conjecture of Sarwate and Pursley regarding pairs of binary m-sequences. *IEEE Trans. Inform. Theory*, vol. 41, pp. 1153-1155, 1995.

[51] G. McGuire. On three weights in cyclic codes with two zeros. preprint, 2003.

[52] Y. Niho. Multi-valued cross-correlation functions between two maximal linear recursive sequences. Ph.D. dissertation, Dept. Elec. Eng., Univ. Southern California. [*USCEE* Rep. 409], 1972.

[53] K. Nyberg. On the construction of highly nonlinear permutations. *Advances in Cryptography, EUROCRYPT'92, Lecture Notes in Computer Science*, Springer-Verlag, 658, pp. 92-98, 1993.

[54] K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science*, Springer-Verlag, New York, 765, pp. 55-64, 1994.

[55] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.

[56] B. Preneel, R. Govaerts and J. Vandevalle. Boolean functions satisfying higher order propagation criteria. *Advances in Cryptology, EUROCRYPT'91, Lecture Notes in Computer Science*, Springer-Verlag, No 547, pp. 141-152, 1991.

[57] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandevalle. Propagation characteristics of Boolean functions. *Advances in Cryptology, EUROCRYPT'90, Lecture Notes in Computer Science*, Springer-Verlag, No 473, pp. 161-173, 1991.

[58] A. Pott. Nonlinear functions in Abelian groups and relative difference sets. *Discrete Applied Math.* 138, pp. 177-193, 2004.

[59] P. Sarkar, S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. *Advances in Cryptology, Crypto 2000, Proceedings, Lecture Notes in Computer Science*, v. 1880, pp. 515-532, 2000.

[60] D. V. Sarwate and M. B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proc. IEEE* 68, pp. 593-619, 1980.

[61] V. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12, pp. 197-201, 1971.

[62] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, vol. IT-30, No 5, pp. 776-780, 1984.

[63] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Inform. Theory*, vol. C-34, No 1, pp. 81-85, 1985.

[64] Y. Tarannikov. On resilient Boolean functions with maximum nonlinearity. *Proceedings of Indocrypt 2000, Lecture Notes in Computer Science*, Springer-Verlag, v. 1977, pp. 19-30, 2000.

[65] H. M. Trachtenberg. On the cross-correlation functions of maximal linear recurring sequences. PhD Thesis, University of Southern California, 1970.

[66] Q. Xiang. Maximally Nonlinear Functions and Bent Functions. *Designs, Codes and Cryptography*, 17, pp. 211-218, 1999.

[67] G.-Z. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, vol. IT-34, No 3, pp.569-571, 1988.

[68] M. Zhang and A. Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. *Advances in Cryptology - CRYPTO 2000, Lecture Notes in Computer Science*, v. 1880, Springer, Berlin, pp. 501-514, 2000.

[69] Y. Zheng, X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Lecture Notes in Computer Science*, Springer-Verlag, v. 2012, pp. 264-274, 2001.

RESUME

Lilya Budaghyan

Date of Birth: January 29, 1976
Place of Birth: Baku, Azerbaijan
Citizienship: Armenia

1983-1993 Attended a Russian Secondary School

1993 Graduated with Excellent Grades a Russian Secondary School, Yerevan, Armenia

1993-1998 Study in the Mathematics Department of the Yerevan State University, Armenia

1998 Diploma with Honors in Mathematics of the Yerevan State University

1998-2003 Scientific Research in the Higher Algebra and Geometry Chair, Mathematics Department, Yerevan State University

2003-2005 Ph.D. Study in the Institute of Agebra and Geometry, Otto-von-Guericke University Magdeburg, Germany;
Ph.D Fellowship of the State of Saxony Anhalt