# On properties of bent and almost perfect nonlinear functions

Diana Davidova

Thesis for the degree of Philosophiae Doctor (PhD)
University of Bergen, Norway
2021

UNIVERSITY OF BERGEN

# On properties of bent and almost perfect nonlinear functions

Diana Davidova


Thesis for the degree of Philosophiae Doctor (PhD)
at the University of Bergen

Date of defense: 14.09.2021

Year: 2021

Title: On properties of bent and almost perfect nonlinear functions

Name: Diana Davidova

Print: Skipnes Kommunikasjon / University of Bergen

# ACKNOWLEDGEMENTS

> "It takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that."
>
> *Lewis Carroll, Alice in Wonderland*

It is my pleasure to express my gratitude towards all the people who were with me and supported me during the four years of my Ph.D studies at the University of Bergen. The time spent in Bergen was one of the most challenging periods of my life. At the same time, it was full of new experiences. I am grateful to all the people around me for making this time interesting.

First of all, I would like to thank my supervisor Lilya Budaghyan for her support, supervision, and guidance in the new for me world of cryptographic Boolean functions. I always felt her presence and support. At the same time, she allowed me a lot of independence in my research, which I appreciate a lot. I am grateful to her for her invaluable assistance, and for suggesting interesting open problems. I am also grateful to my co-supervisor Claude Carlet for the valuable experience gained from our joint work and discussions, and the incredible amount of knowledge he shared with me. I am grateful to him also for hosting me in Paris during my research visit. I would like to thank Tor Helleseth for our joint work, his warm welcome in the Selmer centre and Bergen in general, and for his encouragement.

I am grateful to all members of the Selmer centre (current and past) for the nice and friendly working atmosphere. My special thanks go to Alessandro, Andrea, Dan, Ermes, George, Irene, Isaac, Marco, Navid, Nikolay, and Sachin for joyful moments. A particularly special thank you goes to my officemate Nikolay for the motivating working environment and, at the same time, for a lot of positive emotions and laughter in the office.

I am grateful to my father Sergey Davidov for imparting to me love for mathematics and for being my first guide in the world of mathematics. I am grateful to Yuri

Movsisyan for the experience I gained during the joint work we did before my move to Bergen, and for his support after that.

I am grateful to all my friends from Armenia for believing in me and for their moral support that I always felt.

Last but not least, I would like to thank my family, my father Sergey, mother Karina and brother Davit, for the biggest gifts in the world: unconditional support and love.

Diana Davidova
Bergen, May 10

# ABSTRACT

(Vectorial) Boolean functions play an important role in all domains related to computer science, and in particular, in cryptography. The safety of a cryptosystem is quantified via some characteristics of (vectorial) Boolean functions implemented in it. The nonlinearity and differential uniformity are among the most important characteristics of cryptographic Boolean functions. Thus, bent and almost perfect nonlinear functions, which have the best possible nonlinearity and differential uniformity, respectively, are optimal cryptographic objects. This thesis is devoted to the investigation of the properties of these functions and is based on published articles.

In Paper I, a special subclass of bent Boolean functions, Niho bent functions, is studded. Boolean functions, and bent functions in particular, are considered up to the so-called EA-equivalence, which is the most general known equivalence relation preserving bentness. However, for Niho bent functions, there is a more general equivalence relation called $o$-equivalence, which is induced from the equivalence of $o$-polynomials (a special type of permutation polynomials). In this paper we study a group of transformations which generates all possible $o$-equivalent Niho bent functions from a given $o$-polynomial, and we exclude all transformations that never produce EA-inequivalent functions. We identify all cases which can potentially lead to pairwise EA-inequivalent Niho bent functions in a same $o$-equivalence class. For all known $o$-monomials, we identify the exact form of transformations which always lead to EA-inequivalent Niho bent functions. For $o$-polynomials, which are not monomials, we identify the exact form of transformations which can potentially lead to EA-inequivalent functions.

Paper II is devoted to the study of two long-standing open problems about APN power functions. The six infinite families of APN power functions are among the oldest known instances of APN functions. It was conjectured in 2000 that there does not exist any APN power function inequivalent to the known ones. This is the first long term open problem we study in Paper II. The functions affine equivalent to a power function $x^i$ have the form $L_1 \circ x^i \circ L_2$, where $L_1, L_2$ are linear transformations. This gives an idea to examine the composition $x^i \circ L \circ x^j$, where $L$ is a linear transformation for providing new APN power functions. So, we investigate compositions $x^i \circ L \circ x^{1/j}$, for a linear polynomial $L$, and show that some of the known APN power functions can be obtained from other known APN power functions through this construction.

Moreover, we compute all APN functions of this form for $n \leq 9$ and for $L$ with binary coefficients, thereby confirming that our theoretical constructions exhaust all possible cases of known APN power functions. In addition, we present observations and data on power functions with exponents $\sum_{i=1}^{k-1} 2^{mi} - 1$ defined over the field $\mathbb{F}_{2^{mk}}$ which generalize the inverse and the Dobbertin families of APN power functions.

Another long-standing open problem is the Walsh spectrum of the Dobbertin APN power family. In Paper II, we derive alternative representations for some of the known families of APN monomials. We show that the Niho and Dobbertin functions can be represented as the composition $x^i \circ x^{1/j}$ of two power functions $x^i$ and $x^j$, and prove that our representations are optimal, i.e. no two power functions $x^{i'}$ and $x^{j'}$ of lesser algebraic degree can produce the same composition. We show as well that the exponents of the Welch functions are optimal in this sense. Based on a computational data performed for $n \leq 35$, we present a conjecture depending on the parity of $n$, which wholly describes the Walsh spectrum of the Dobbertin functions.

In Paper III, we generalize an infinite family of APN binomials, for $n$ divisible by 4, to a family of functions with all derivatives on non-zero directions being $2^t$-to-1 mappings (for some positive integer $t$). The similar result was obtained for the family of APN binomials, for $n$ divisible by 3, in 2012. That is, the family of APN binomials, for $n$ divisible by 3, was generalized to a family of differentially $2^t$-uniform functions with all derivatives on non-zero directions being $2^t$-to-1 functions by relaxing a condition (for some positive integer $t$). We also show that a family of APN quadrinomials obtained as a generalization of a known APN instance over $\mathbb{F}_{2^{10}}$ cannot be generalized to functions with $2^t$-to-1 derivatives by relaxing conditions in a similar way.

# LIST OF PAPERS

The present thesis is based on the following papers.

I. D. Davidova, L. Budaghyan, C. Carlet, T. Helleseth, F. Ihringer, and T. Penttila, "Relation between o-equivalence and EA-equivalence for Niho bent function", *Finite Fields and their Applications*, 72, pp. 1–42 (2021).

   The various aspects of the paper were presented at the *Emil Artin International Conference*, Yerevan, Armenia, 2018, the *3rd International Workshop on Boolean functions and their Applications (BFA 2018)*, Loen, Norway, 2018, and the *4rd International Workshop on Boolean functions and their Applications (BFA 2019)*, Florence, Italy, 2019, under the titles "Magic action and EA-equivalence of Niho bent functions", "Magic action of o-polynomials and EA-equivalence of Niho bent functions", and "Relation between o-equivalence and EA-equivalence for Niho bent functions", respectively.

II. L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. Kaleyski, "On two fundamental problems on APN power functions", *Cryptology ePrint Archive: Report 2020/1359.* Submitted to *IEEE Transactions on Information Theory* in 2020.

   Presented as two talks at the *11th International Conference on Sequences and their Applications (SETA 2020)*, St. Petersburg, Russia, 2020, under the titles "A note on the Walsh spectrum of Dobbertin APN functions", and "On a relationship between Gold and Kasami functions and other power APN functions".

III. D. Davidova, and N. Kaleyski, "Generalization of a class of APN binomials to Gold-like functions", *Lecture Notes in Computer Science*, 12542, pp. 195–206 (2021).

   Presented at the *International Workshop on the Arithmetic of Finite Fields (WAIFI 2020)*, Rennes, France, 2020, under the title "Generalization of a class of APN binomials to Gold-like functions".

# CONTENTS

# CHAPTER 1

# INTRODUCTION

The objects of investigation in this thesis are *discrete functions* defined over finite fields and their properties suitable mainly for cryptographic usage. There are different definitions of discrete functions in different literature. The most general one is as follow: discrete functions are those functions whose both domain and codomain are discrete sets (that is, countable sets). Discrete functions comprise their own branch of mathematics and also have many applications in diverse fields such as statistics, economics, information theory, cryptography, coding theory, projective geometry, combinatorics and sequence design. A particular class of discrete functions, the so-called vectorial Boolean functions, which take as an input a binary sequence[1] of length $n$ and give as an output a binary sequence of length $m$ (for some positive integers $n$ and $m$) play a significant role in all domains related to computer science.

For instance in cryptography, the resistance of a cryptosystem to various cryptographic attacks is measured by certain characteristics of discrete functions implemented in it. Thus, in order to protect a cryptosystem from a particular type of attack, discrete functions implemented in it should satisfy the corresponding property and therefore they are directly responsible for the security of the cryptosystem.

Among the main cryptographic characteristics of functions are differential uniformity and nonlinearity. Bent and almost perfect nonlinear functions are functions which have the best possible *nonlinearity* and *differential uniformity*, respectively. Within the present thesis we will address different problems regarding these functions.

**Structure of the thesis.** The presented dissertation is organized as follow. It consists of three chapters: Introduction (Chapter 1), Papers (Chapter 2) and Conclusions (Chapter 3).

Chapter 1 is divided into four sections. In Section 1.1 we give a brief introduction to cryptography and discuss the role of discrete functions in it. In Section 1.2 we introduce the concept of vectorial Boolean functions, we present different ways of their

[1] A binary sequence is a sequence of 0s and 1s.

representations and the main equivalence notions defined for them. An overview of known up to date results about bent Boolean functions and APN functions as well as how our new results fit into the overall picture of the current knowledge are presented in Sections 1.3 and 1.4.

Chapter 2 is a collection of papers on which this thesis is based on.

In Chapter 3, we give a brief conclusion of our results and present some of the possible directions of future research on the topics we address in this thesis.

## 1.1 Discrete functions in cryptography

Although discrete functions, and in particular (vectorial) Boolean functions, are interesting objects for investigation by themselves, their study has also numerous practical aspects. In this section we will briefly discuss their applications in cryptography (in informal way).

*Crytography* is a branch of science that studies techniques of secure and trustable communication. *Cipher* is a key concept in cryptography. It is a pair of encryption and decryption algorithms. *Encryption algorithm* is a collection of steps whereby an ordinary text (called a plaintext) is converted into unintelligible form (called a ciphertext). *Decryption* does the converse: it converts the ciphertext back into a plaintext. A general scheme of cipher is as follow. A plaintext $P$ is encrypted into a ciphertext $C$ using the so-called encryption key $E_k$, then sent through a communication channel to another user who applies the so-called decryption key $D_K$ and converts the message into the original text (see fig. 1.1).

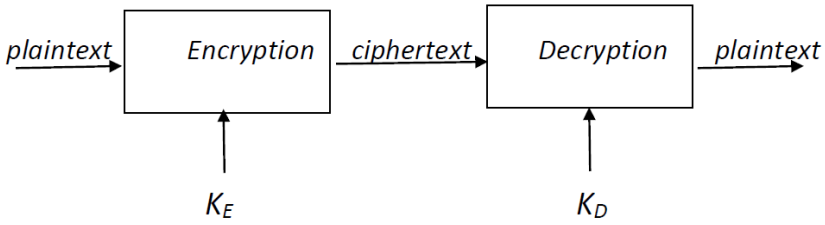


Figure 1.1: Cipher

Secure communication has been playing an important role since the ancient times. The first known cipher is the *Caesar cipher*: each letter in the plaintext is replaced by a letter at some fixed number of positions down the alphabet. The first known cipher device, called the *Scytale*, was employed at the ancient Greece around 400 BC and had been used for secret communications between military commanders. It consisted of a tapered baton around which was spirally wrapped a piece of parchment inscribed with the message. When unwrapped the parchment bore an incomprehensible set of letters, but when wrapped around another baton of identical proportions, the original text reappeared. One of the most well-known cipher machines is the *Enigma*, which played a crucial role in the World War II. In the past, ciphers and cipher machines were

used for military purposes and secret diplomatic communications. Nowadays we need cryptography in our daily life and along with the development of modern technologies, the need in cryptography is becoming more and more vital. The nature of ciphers has also changed due to technological advances and ingrowing computer's power.

Typically, a *cryptosystem* consists of three types of algorithms: key generation, encryption and decryption. Depending on encryption and decryption keys, cryptography is divided into two subcategories: *symmetric* and *asymmetric cryptography*. When for decryption and encryption the same key is used (i.e., $E_K = D_K$), we are talking about *symmetric cryptography or private key cryptography*. Thus, for exchanging information by means of a symmetric cipher, two parties should pre-share key in a secure way; this is a drawback. In *asymmetric or public key cryptography*, decryption and encryption keys are different: encryption key is public and decryption key is private. Asymmetric cryptography is a rather new branch of cryptography, it arose only in the fourth quarter of XX century. Asymmetric encryption schemes make possible to securely communicate without having previously shared keys. However, it has some drawbacks as well. For instance, decryption keys should be quite large to ensure security, and the amount of data transmitting per second is quite low in general. Thus, symmetric cryptography is still needed for the confidential transfer of large data and is an active domain of research. Thanks to asymmetric cryptography, the sharing of a private key for symmetric ciphers can be done via insecure channels, such as the internet.

There are two symmetric encryption schemes: *stream ciphers* and *block ciphers*. In stream ciphers, a plain text is considered as a stream of characters, while in block ciphers a plain text is divided into blocks of the same size.

### 1.1.1 Stream ciphers and Boolean functions

In stream ciphers, the plaintext, encryption/decryption key and ciphertext are considered as streams of characters. To obtain the ciphertext stream, each plain-text character is combined one at a time with the corresponding character of the keystream. Stream ciphers are based on the so-called *Vernam cipher* or *one time pad (OTP)*, which was used for secret communications between USA and USSR during the cold war.


Figure 1.2: OTP

Let $P$ be a plaintext of $n$ bits and $E_K$ be a key of $n$ bits, i.e. $P = p_1 p_2 \dots p_n$ and $E_K = k_1 k_2 \dots k_n$. Then the cipher text $C = E_K(P)$ is also a stream of $n$ bits $c_1 \dots c_n$ such that $c_i = p_i \oplus k_i$, for any $i \in \{1, \dots, n\}$ (see fig. 1.2). Decryption is done in the same manner: by adding to each cipherstream bit the corresponding keystream bit.

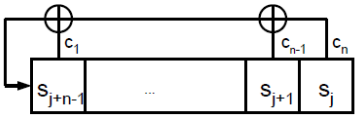


Figure 1.3: LFSR

Assuming that a key is selected every time at random and the same key is not used twice, Vernam cipher gives unconditional security. However, the key stream should have the same length as the plain text stream, which makes Vernam cipher impractical. To make stream ciphers "lighter" and more convenient for usage in practice, a smaller secret key is used to generate a keystream which is combined with the plaintext digits in a similar to the Vernam cipher's way. However, the keystream is now not truly random, it is a pseudorandom and unconditional security no longer holds.

Classical method to generate a pseudorandom key from a secret one are *Linear Feedback Shift Registers* or *LFSRs* (see fig. 1.3). An LFSR of length $n$ is described via a linear recurrence relation $s_i = c_1 s_1 + \ldots c_n s_{n-i}$ ($c_i \in \{0,1\}$, for all $i$). Thus, the inputs and the outputs of the LFSR are linearly dependent. This makes them highly insecure, since linear dependence is relatively easily analysed. To annihilate this weakness, LFSRs are used in combination with Boolean functions, which are as much different from affine functions (that is, linear functions plus constants) as possible. This characteristic is quantified by the nonlinearity of the function. Thus, the security of such cryptosystem entirely depends on the choice of a Boolean function and the nonlinearity of the corresponding Boolean function is one of criteria. Another important cryptographic characteristic of Boolean functions is their balancedness, which prevents from statistical dependence between the inputs and the outputs of the function and high algebraic degree to avoid the so-called Berlekamp-Massey attack [83]. Formal definitions of the nonlinearity, balancedness, and algebraic degree of functions will be given in Sections 1.2.2 and 1.2.3.

### 1.1.2 Block ciphers and vectorial Boolean functions

In a block cipher, a plaintext $P$ is represented by blocks $P_i$ of a fixed length and several blocks are encrypted with the same key.

All known block ciphers are *iterated*, which are designed by repeatedly applying an invertible transformation, called a *round function*. The composition of $N$ round functions can be written as:

$$E_K(\cdot) = F^0_{K_0} \circ F^1_{K_1} \circ \ldots \circ F^{N-1}_{K_{N-1}}(\cdot),$$

where $F^i_{K_i}$ is the $i$-th round function and $K_i$ is the $i$-th round key which is derived from the original key $K$ using the so-called a key schedule algorithm. The two most known models of iterated block ciphers are *Feistel Networks* and *Substitution Permutation*

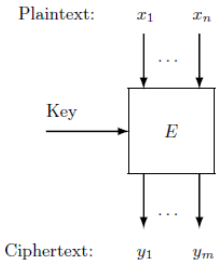


Figure 1.4: Block cipher

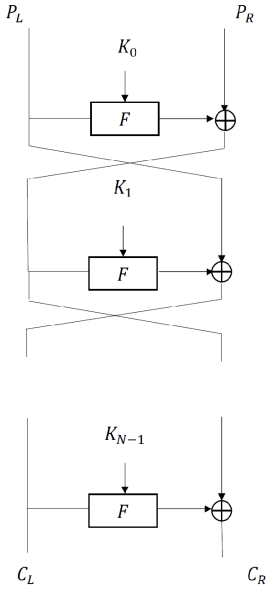


Figure 1.5: Feistel cipher

*Networks*.

*Feistel ciphers* were first published in 1960's by Feistel, for the design of the *Lucifer* block cipher. The famous *Data Encryption Standard (DES)* was released as a modification of the Lucifer in 1977. A Feistel network works by splitting the plaintext block into two equal pieces and applying encryption in multiple rounds. More precisely, a pair $(x_L^i, x_R^i)$ is an internal state of a Feistel cipher, where $x_L^i$ and $x_R^i$ are called the left and right halves of the internal state, respectively. Then the round function of a Feistel

network can be described as follow:

$$\begin{aligned} x_L^{i+1} &= x_R^i \oplus F(x_L^i, K_i); \\ x_R^{i+1} &= x_L^i, \end{aligned}$$

where $F$ is a Feistel function (see fig. 1.5). Using this structure, both encryption and decryption are identical, with the reversed order of round keys. So, Feistel cipher does not need the involved functions to be injective for the encryption to be possible.

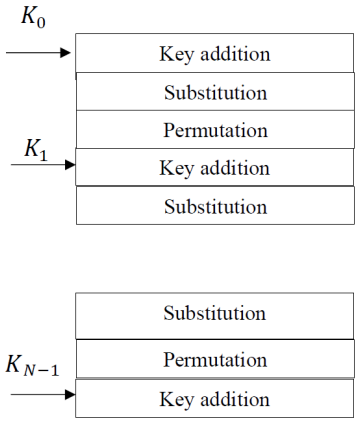


Figure 1.6: SPN

Another model of iterated block ciphers is the *Substitution Permutation Network* (SPN). The round function of SPNs typically consists of a substitution layer, a permutation layer and a key addition layer (see fig. 1.6). The substitution layer is the only nonlinear part in the cipher and it consists from several S-boxes which are nothing else than vectorial Boolean functions. To make decryption possible, the S-boxes (vectorial functions) should be bijective. The permutation layer is a linear transformation (typically the input bits are permuted or shuffled). In the key addition layer, typically, a round key $K_i$ is added bit-wise to the internal state. Thus, the security of SPNs directly depends on the properties of vectorial Boolean functions implemented in it.

The *Advanced Encryption standard (AES)* [47] (see fig. 1.7) is a Substitution Permutation cipher, whose S-boxes are the inverse functions. The reasons behind the choice of the inverse function as an S-box for AES will be explained in Section 1.3. In sequel by block ciphers we will understand the SPN model of block ciphers.

Two most powerful attacks on block ciphers are differential [3] and linear attacks [84], and the corresponding functions characteristics measuring the resistance to these attacks are differential uniformity [90] and nonlinearity.. Some of the other important criteria for vectorial Boolean functions are large enough algebraic degree and balancedness, since they respectively prevent the cryptosystem from the so-called higher order differential attack [74] and avoid statistical dependence between the inputs and outputs of the function.

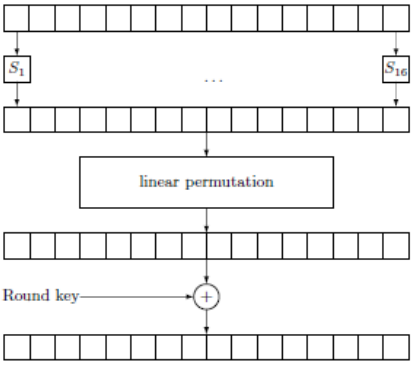


Figure 1.7: A round in the AES

## 1.2 Discrete functions over finite fields. Basic concepts

The concept of Boolean functions was introduced in the second half of the XIX century for the needs of a new branch of fundamental mathematics: mathematical logic. Like many other concepts introduced in mathematics for purely theoretical reasons, Boolean functions found their application in practice. Since the middle of the XX century, with the rapid development of information and communication theory, the theory of Boolean functions has become an important tool for solving problems on the construction and analysis of discrete devices for transforming and processing information. In particular, many cryptographic problems are formulated in the terms of Boolean functions, and techniques from the theory of Boolean functions are essential for solving these problems.

### 1.2.1 Boolean functions and vectorial Boolean functions

*A Boolean function* $f$ is a mapping which takes as an input a sequence of 0s and 1s and gives as an output 0 or 1, i.e. $f : \{0,1\}^n \mapsto \{0,1\}$ [2]. *A vectorial Boolean* function is a generalization of the classical concept of Boolean functions, it is a function whose both the input and the output are sequences of 0s and 1s, i.e. $F : \{0,1\}^n \mapsto \{0,1\}^m$, for some positive integers $n$ and $m$. More strictly, vectorial Boolean functions are discrete functions from the $n$-dimensional vector space $\mathbb{F}_2^n$ over the field $\mathbb{F}_2 = \{0,1\}$ to the $m$-dimensional vector space $\mathbb{F}_2^m$ over $\mathbb{F}_2$, for some positive integers $n$ and $m$. Through the thesis we will assume by default that $m \leq n$. When it is necessary to specify the number of inputs and outputs of vectorial functions, we will call them $(n,m)$-functions; An $n$-variable Boolean function is an $(n,1)$-function. Clearly, any $(n,m)$-function $F$ can be represented via $n$-variable Boolean functions $f_1,\ldots,f_m$, called the *coordinate*

[2] $\{0,1\}^n = \underbrace{\{0,1\} \times \ldots \times \{0,1\}}_{n \text{ times}} = \{(a_1,\ldots a_n) : a_i \in \{0,1\}, i \in \{1,\ldots,n\}\}$.

*functions* of $F$, as follow:

$$F(x) = F(x_1,\ldots,x_n) = (f_1(x_1,\ldots,x_n),\ldots,f_2(x_1,\ldots,x_n)),$$

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

With any $(n,m)$-function $F$ are associated the so-called *component functions*, that is, non-zero linear combinations of the coordinate functions, i.e. the functions of the form $v \cdot F$, where $v \in \mathbb{F}_2^m, v \neq 0$ and $\cdot$ is an inner product in the linear space $\mathbb{F}_2^m$.

There is a huge number of different (vectorial) Boolean functions even in small numbers of inputs and outputs. The number of different $(n,m)$-functions equals $(2^m)^{2^n}$. Thus, for instance, as it can be easily calculated, there are $2^{2^5} = 4.294.967.296$ different Boolen functions in 5 variables and $(2^{2^5})^2 = (4.294.967.296)^2 > 18 \cdot 2^{18}$ different $(5,2)$-functions. The number of (vectorial) Boolean functions grows rapidly with increasing numbers of inputs and outputs. Hence, in order to find functions satisfying certain properties, direct computer searches are not possible. It becomes necessary to find and formulate mathematical properties and characterizations of the functions satisfying these properties, that can be used to reduce the complexity of the search. To analyse properties of functions, we need first a convenient representation of them. (Vectorial) Boolean functions can be represented in several different ways. In the next Section 1.2.2 we shall describe some of them.

### 1.2.2 Representations of (vectorial) Boolean functions

The classical and the most well-known representation of (vectorial) Boolean functions is *the truth-table* (or in the case of vectorial functions – *the look-up table*). The truth table (look-up table) of a given function is simply the list of all ordered pairs such that the first entry of the pair is an element of the domain of the function and the second is the value of the function at this entry. However, in cryptography truth table representations are not much used since the investigation of most of the properties of functions suitable for cryptographic uses via truth-tables is not convenient. The most used representation in cryptography is a polynomial representation. (Vectorial) Boolean functions admit several polynomial representations. The most general one is the so-called *ANF (algebraic normal form)*; any (vectorial) Boolean function can be uniquely represented in the algebraic normal form. The ANF of an $(n,m)$-function $F$ is the unique polynomial of the following form:

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

where $a_u \in \mathbb{F}_2^m$, for any $(x_1,\ldots,x_n) \in \mathbb{F}_2^n$, and the symbol $\sum$ is interpreted here as the component wise addition modulo 2 of vectors from $\mathbb{F}_2^m$. *The algebraic degree of* $F$, denoted by $deg(F)$, is defined as $\max_{a_u \neq 0}\{wt(u) | u \in \mathbb{F}_2^n\}$, where $wt(u) = wt((u_0,\ldots,u_{n-1})) = \sum_{i=0}^{n-1} u_i$ and is called the *weight of vector u*. Functions of algebraic degree 1, resp. 2, resp. 3 are called *affine*, resp. *quadratic*, resp. *cubic* etc. An affine function $F$ such that $F(0) = 0$ is called *linear*.

Due to the fact that the finite field $\mathbb{F}_{2^n}$ of order $2^n$ is an $n$-dimensional vector space over $\mathbb{F}_2$, any $(n,m)$-function $F$ can be considered as a map between fields, i.e. $F:\mathbb{F}_{2^n}\mapsto \mathbb{F}_{2^m}$. Since any function from a finite filed to itself can be represented via the univariate polynomial of degree at most $2^n-1$ over $\mathbb{F}_{2^n}$ in the unique way, any $(n,n)$-function admits such representation:

$$F(x)=\sum_{i=0}^{2^n-1} a_i x^i, \tag{1.1}$$

where the symbol $\sum$ stands for addition in $\mathbb{F}_{2^n}$. Such representation is called *the univariate representation.* When $m$ is a divisor of $n$, any $(n,m)$-function can be considered as a function from the field $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ (since in this case $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$) and therefore, also admits the unique univariate representation. In particular, Boolean functions also can be represented in the form 1.1. The algebraic degree of $F$ ($deg(F)$) in the univariate polynomial representation is $\max\limits_{a_i\neq 0}\{wt(i)|i\in\{0,\ldots,2^n-1\}\}$, where $wt(i)$ corresponds to the weight of $i$ in its bivariate representation (that is, $i=(i_0,\ldots,i_{n-1})$ such that $i=\sum\limits_{k=0}^{n-1} i_k 2^k$), or simply, to the 2-*weight of i*. Thus, an $(n,m)$-function $F$ is

- linear, if $F(x)=\sum\limits_{i=0}^{2^n-1} a_i x^{2^i}$;
- affine, if it is a sum of a linear function and constant;
- quadratic, if $F(x)=\sum\limits_{i,j=0}^{2^n-1} a_{i,j}x^{2^i+2^j}+A(x)$, where A is an affine function.

Functions which have only one term in polynomial representation are called *monomials or power functions*.

If $m$ is a divisor of $n$, and $(n,m)$-function $F$ admits also the so-called *absolute trace representation*.

For any positive integer $m$ dividing $n$, the trace function $\mathrm{Tr}_m^n$ is the mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ defined by

$$\mathrm{Tr}_m^n(x)=\sum_{i=0}^{\frac{n}{m}-1} x^{2^{im}}.$$

For $m=1$, the function $\mathrm{Tr}_1^n:\mathbb{F}_{2^n}\to\mathbb{F}_2$ is called the *absolute trace* over $\mathbb{F}_{2^n}$ and is denoted by $\mathrm{Tr}_n$, i.e.

$$\mathrm{Tr}_n(x)=\sum_{i=0}^{n-1} x^{2^i}. \tag{1.2}$$

For any $(n,m)$ function $F$ ($n$ divisible by $m$) there exists an $(n,n)$-function $G$ such that $F(x)=\mathrm{Tr}_m^n(G(x))$, for all $x\in\mathbb{F}_{2^n}$ (for instance, $G=\lambda F$, where $\mathrm{Tr}_m^n(\lambda)=1$). Hence, every $(n,m)$-function $F$ (for $n$ divisible by $m$) admits the following *univariate absolute trace representation*, which is unfortunately not unique:

$$F(x)=\mathrm{Tr}_m^n\left(\sum_{i=0}^{2^n-1} a_i x^i\right),$$

where $a_i \in \mathbb{F}_{2^n}$.

In particular, any Boolean function admits a univariate absolute trace representation, which is not unique. However, for a Boolean function $f$ in $n$ variables there exists the unique *subfield trace representation*, as well:

$$f(x) = \sum_{j \in \Gamma(n)} \mathrm{Tr}_{n_j}(\beta_j x^j) + \beta_{2^n-1} x^{2^n-1},$$

where $\Gamma(n)$ is a set of representatives of the cyclotomic classes of 2 modulo $2^n-1$, $n_j$ is the size of the cyclotomic class containing $j$ and for any $j \in \Gamma(n)$, $\beta_j \in \mathbb{F}_{2^n j}$, $\beta_{2^n-1} \in \mathbb{F}_2$.

Any $(2m,m)$-function $F$ admits the so-called *bivariate polynomial representation*. Indeed, a linear space $\mathbb{F}_2^{2m}$ can be identified with the Cartesian product of the field $\mathbb{F}_{2^m}$ with itself, i.e. $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and $F$ can be represented in the unique way as a bivariate polynomial over $\mathbb{F}_{2^m}$:

$$F(x,y) = \sum_{i,j=0}^{2^m-1} a_{i,j} x^i y^j.$$

Then the algebraic degree of $F$ ($deg(F)$) is $\max_{a_{i,j} \neq 0} \{wt(i) + wt(j) | i, j \in \{0, \ldots 2^m - 1\}\}$.

A Boolean function in even number of variables also admits the bivariate representation. It can be written via the absolute trace function. A Boolean function $f$ in $2m$ variables can be written in the form $f(x,y) = Tr_m(P(x,y))$, where $P(x,y)$ is some polynomial in two variables over $\mathbb{F}_2^m$. This representation of Boolean functions is not unique.

### 1.2.3 Differential uniformity and nonlinearity of (vectorial) Boolean functions

As we discussed in Section 1.1, the contribution of a function to the resistance of a cryptosystem using it to a particular attack can be quantified through certain characteristics of the functions implemented in it. Some of the main cryptographic criteria of (vectorial) Boolean functions are a sufficiently large algebraic degree (to avoid, for instance, higher order differential attacks on block ciphers [74] and the Berlekamp-Massey attacks for stream ciphers [83]), balancedness (to avoid statistical dependence between inputs and outputs), nonlinearity (to avoid linear attacks on block ciphers [84] and fast correlation attacks on stream ciphers [86]), and differential uniformity [90] (to avoid differential attacks on block ciphers [3]).

Recall from Section 1.2.2 that the *algebraic degree* of an $(n,m)$-function $F$ is the maximum 2-weight of the exponents with non-zero coefficients in the univariate polynomial representation of $F$ given in Relation (1.1) ($m$ is a divisor of $n$). By the definition, the algebraic degree of an $(n,m)$-function is at most $n$.

An $(n,m)$-function $F$ is called *balanced* if it takes every value of $\mathbb{F}_{2^m}$ the same number of times. Or equivalently, a vectorial Boolean function is balanced if and only if all its component functions are *balanced Boolean functions* (that is, take the value 0 the same number of times as the value 1) [82].

Within this thesis, we will focus on the nonlinearity and differential properties mainly.

We fix the notation we will use in sequel. Let $n$ be a positive integer. Then $\mathbb{F}_2^n$ is a linear space over $\mathbb{F}_2$ of dimension $n$, $\mathbb{F}_{2^n}$ denotes the finite field with $2^n$ elements, and $\mathbb{F}_{2^n}^*$ denotes the multiplicative group of $\mathbb{F}_{2^n}$, i.e. $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$.

Let $F$ be an $(n,m)$-function. Then the function $D_aF : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$ defined as $D_aF(x) = F(x+a)+F(x)$ is called *the derivative of $F$ in the direction $a \in \mathbb{F}_{2^n}$*.

**Definition 1.** *An $(n,m)$-function $F$ is called differentially $\delta$-uniform, if the equation $D_aF(x) = b$ admits at most $\delta$ solutions for any $a \in \mathbb{F}_{2^n}$, $a \neq 0$ and any $b \in \mathbb{F}_{2^m}$.*

Differential uniformity introduced by Nyberg in 1990 [90] measures the resistance of a cryptosystem to the differential attacks [3]. One of the crucial parts of differential cryptanalysis introduced by Biham and Shamir is based on studying how the difference in two inputs to a function affects the difference in the corresponding outputs, i.e. it is based on the study of the number of solutions of the equation $D_aF(x) = b$ for any $a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}, a \neq 0$ and a given $(n,m)$-function $F$. Intuitively, the smaller the number of solutions, the more difficult to find a correlation between inputs and outputs, which makes the cryptosystem less vulnerable to the differental attack. Thus, low differential uniformity is a property which protects the corresponding cryptosystem from this type of attacks. The smallest possible value of differential uniformity is 2, since if $x_0$ is a solution of an equation $D_aF(x) = b$ (for some appropriate $a$ and $b$), then $x_0 + a$ is also a solution of the same equation.

**Definition 2.** *Those $(n,n)$-functions whose differential uniformity is 2 are called almost perfect nonlinear or, shortly, APN.*

APN functions provide the cryptosystem with the best possible resistance against differential attacks.

Another important cryptographic property of (vectorial) Boolean functions is the *nonlinearity*. The nonlinearity quantifies how much a given function is different from the functions which are the most simple to analyse: affine functions. The larger the nonlinearity, the better the cryptosystem is protected against this type of attacks. The linear cryptanalysis was introduced by Matsui in 1993 [84].

*The Hamming distance* between two Boolean functions $f$ and $g$ in $n$ variables, denoted by $d_H(f,g)$, is defined as the number of arguments $x \in \mathbb{F}_{2^m}$ such that $f(x) \neq g(x)$, i.e.

$$d_H(f,g) = |\{x \in \mathbb{F}_{2^m} | f(x) \neq g(x)\}|.$$

**Definition 3.** *The minimum Hamming distance between a given Boolean function $f$ in $n$ variables and the set $A_n$ of all affine Boolean functions in $n$ variables is called the nonlinearity of $f$ and is denoted by $\mathcal{NL}(f)$, i.e.*

$$\mathcal{NL}(f) = \min_{a \in A_n} d_H(f,a).$$

The nonlinearity of an $(n,m)$-function $F$ is defined as the minimum nonlinearity of its component functions $v \cdot F$, $v \neq 0$:

$$\mathscr{NL}(F) = \min_{v \in \mathbb{F}_{2^m}, v \neq 0} \mathscr{NL}(v \cdot F).$$

The nonlinearity can be described via the Walsh transform as well.

**Definition 4.** *For a given $(n,m)$-function, the map $W_F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \mapsto \mathbb{Z}$ defined as*

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{a \cdot x + (b \cdot F)(x)},$$

*is called the Walsh transform of $F$ (inner products both in $\mathbb{F}_{2^n}$ and in $\mathbb{F}_{2^m}$ are denoted by the same symbol "$\cdot$"). The value of the Walsh transform on $(a,b)$ is called the Walsh coefficients of $F$ at points $a,b$; The following sets*

$$\{W_F(a,b) | a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}, b \neq 0\}$$

*and*

$$\{|W_F(a,b)| | a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}, b \neq 0\}$$

*are called the Walsh spectrum and the extended Walsh spectrum of $F$, respectively.*

In the case of an $n$-variable Boolean function $f$ we simply have:

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{a \cdot x + f(x)},$$

for any $a \in \mathbb{F}_{2^n}$ (where $\cdot$ is an inner product in $\mathbb{F}_{2^n}$).

The Walsh transform as well as the nonlinearity of a (vectorial) Boolean function does not depend on the choice of the inner product. The most used inner product in $\mathbb{F}_{2^n}$ is: $x \cdot y = Tr_n(xy)$, where $Tr_n$ is the absolute trace function over $\mathbb{F}_{2^n}$ defined by Relation (1.2).

It is easy to see that the Walsh transform of a Boolean function $f$ in $n$ variables satisfies Parseval's equation:

$$\sum_{a \in \mathbb{F}_{2^n}} W_f(a)^2 = 2^{2n}. \tag{1.3}$$

Clearly, for any $(n,m)$-function $F$ we have:

$$W_F(a,b) = 2^n - 2d_H((b \cdot F)(x), a \cdot x),$$

therefore

$$d_H((b \cdot F)(x), a \cdot x) = 2^{n-1} - \frac{1}{2} W_F(a,b)$$

and the Hamming distance between an affine Boolean function $a \cdot x + a_0$, where $a_0 \in \{0,1\}$ and any Boolean function of the form $b \cdot F, b \neq 0$ can be either $2^{n-1} - \frac{1}{2}W_F(a,b)$ or $2^{n-1} + \frac{1}{2}W_F(a,b)$. Hence, we have:

$$\mathscr{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}^*} |W_F(a,b)|. \tag{1.4}$$

From (1.3) and (1.4) the upper bound on the nonlinearity of $(n,m)$-function $F$ follows:

$$\mathscr{NL}(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{1.5}$$

If $(n,n)$-function $F$ is a permutation, then $F$ and $F^{-1}$ have the same nonlinearity [33].

**Definition 5.** *Bent functions are those $(n,m)$-functions ($n$ even) with the highest possible nonlinearity, that is $2^{n-1} - 2^{\frac{n}{2}-1}$. Or, equivalently, with Walsh spectrum $\{\pm 2^{\frac{n}{2}}\}$.*

A bent $(n,m)$-function can be defined also as a function whose all component functions are bent Boolean functions (see, for instance, [33]). A bent Boolean function $f$ never can be balanced, since in the case of balancedness $W_f(0) = 0$. Therefore, bent vectorial functions are unbalanced as well. A natural generalization of the class of bent functions is the *class of plateaued functions*. A Boolean function $f$ is called *plateaued* if its Walsh spectrum is a subset of the set $\{0, \pm\lambda\}$, where $\lambda$ is an integer. Because of the Parseval's equation (1.3), $\lambda$ should be of the form $2^j$, where $j \geq \frac{n}{2}$. *A vectorial Boolean function is called plateaued* if all its component functions are plateaued Boolean functions.

The algebraic degree of bent Boolean functions in $n > 2$ variables is at most $\frac{n}{2}$ [96]. The algebraic degree of plateaued functions is bounded above by $\frac{n}{2} + 1$, for $n$ even, and by $\frac{n+1}{2}$, for $n$ odd [33].

It is clear from the definition that bent functions exist only for $n$ even. However, this condition is not sufficient for the existence of bent $(n,m)$-functions: bent $(n,m)$-functions exist only for $m \leq \frac{n}{2}$ ($n$ even) [90]. Thus, in the case $m = n$, bent $(n,m)$-functions do not exist; $(n,n)$-functions with the best possible nonlinearity are called *maximally nonlinear*.

An upper bound on the nonlinearity that is better than (1.5) can be deduced for an $(n,m)$-function $F$ with $m > n$ [41], [99]:

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

This bound can be achieved with equality only for $n = m$, $n$ odd when it takes the form:

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

**Definition 6.** *An $(n,n)$-functions with the highest possible nonlinearity, that is $2^{n-1} - 2^{\frac{n-1}{2}}$ is called almost bent or, shortly, AB.*

AB functions can be characterized by their Walsh spectrum: an $(n,n)$-function $F$ is AB if and only if its Walsh spectrum is $\{0, \pm 2^{\frac{n+1}{2}}\}$.

Clearly AB functions exist only for $n$ odd. Besides, every AB function is APN [41], but converse is not true in general. Thus, AB functions provide an optimal resistance against both differential and linear attacks. For $n$ even, functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$ are known and it is conjectured that this value is the highest possible in this case [97].

In coding theory APN and AB functions define error correcting codes optimal in certain sense (see [36]); AB power functions play significant role in sequence design [63].

### 1.2.4 Equivalence relations for (vectorial) Boolean functions

Equivalence relations are one of the most important and useful tools for the investigation of (vectorial) Boolean functions. Indeed, as it was discussed in Section 1.2.1, there is a huge number of (vectorial) Boolean functions even in a small number of variables. An equivalence relation allows us to make a partition of a set of (vectorial) Boolean functions into equivalence classes and to investigate only one representative from each class, which significantly reduces the complexity. Besides, equivalence relations can be considered as a method of secondary constructions of functions (we will return to this in Sections 1.3 and 1.4).

There are several known equivalence relations on a set of (vectorial) Boolean functions. We shall define the main ones below. Let $F$ and $F'$ be two $(n,m)$-functions, then they are called

- *affine equivalent*, if there are affine permutations $A_1$ and $A_2$ of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively, such that $F' = A_1 \circ F \circ A_2$;
- *extended affine equivalent or EA-equivalent*, if there are affine permutations $A_1$ and $A_2$ of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, and an affine $(n,m)$-function $A$, respectively, such that $F' = A_1 \circ F \circ A_2 + A$;
- *CCZ-equivalent*, if there is an affine permutation $\mathscr{A}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ that maps the graph $\mathscr{G}(F) = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of $F$ to the graph $\mathscr{G}(F')$ of $F'$ [36].

In the case of power functions, another equivalence notion is known. Let $F(x) = x^d$ and $G(x) = x^e$ be two power functions defined over $\mathbb{F}_{2^n}$, then they are called

- *cyclotomic equivalent* if $d \equiv 2^k e \mod (2^n - 1)$ for some positive integer $k$, or if $d^{-1} \equiv 2^k e \mod (2^n - 1)$ in the case that $\gcd(d, 2^n - 1) = 1$, for some positive integer $k$.

The first three equivalence relations are listed in the increasing order of generality. It is obvious that affine equivalence is a particular case of EA-equivalence, it is shown in [36] that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivlent to its inverse. It was proven in [23] that CCZ-equivalence is still more general than EA-equivalence together with taking inverses of permutations. However, CCZ-equivalence and EA-equivalence coincide with each other on some classes of functions:

- on the set of all Boolean functions [23];
- on the set of quadratic APN functions [105];
- on the set of power functions (both CCZ-equivalence and EA-equivalence coincide with cyclotomic equivalence) [104];
- on the set of bent functions [16, 17] (in general, for functions with surjective[3] derivatives, CCZ-equivalence coincides with EA-equivalence [24]).

Moreover,

- a quadratic APN function defined over $\mathbb{F}_{2^n}$ is CCZ-equivalent to a power function if and only if it is EA-equivalent to a function of the form $x^{2^i+1}$, $(i,n)=1$ [104];
- a plateaued APN function defined over $\mathbb{F}_{2^n}, n$ even, is CCZ-equivalent to a power function if and only if are EA-equivalent [103].

The differential uniformity and nonlinearity are preserved by both CCZ-equivalence and EA-equivalence. The algebraic degree of functions is preserved by EA-equivalence, but is not preserved by CCZ-equivalence. Thus, via CCZ-equivalence, functions of larger algebraic degree can be obtained.

The most general currently known equivalence relation on the set of all vectorial Boolean functions that preserves differential uniformity and nonlinearity is CCZ-equivalence. However, for some specific types of functions are known equivalences which are more general. For instance, *o-equivalence* on the set of the so-called *Niho bent functions* [40] and *isotopic equivalence* on the set of the so-called *planar functions* [24] are more general than CCZ-equivalence.

Deciding whether two given functions $F$ and $G$ are CCZ-equivalent is a difficult problem in general. Usually the CCZ-equivalence or inequivalence of functions is decided using code isomorphism. More precisely, any given $(n,n)$-function $F$ can be associated with a linear code $\mathscr{C}_F$ whose generating matrix is

$$\mathscr{C}_F = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \alpha & \dots & \alpha^{2^n-2} \\ F(0) & F(1) & F(\alpha) & \dots & F(\alpha^{2^n-2}) \end{pmatrix},$$

where $\alpha$ is a primitive element of $\mathbb{F}_{2^n}$[4]. Then functions $F$ and $G$ are CCZ-equivalent if and only if their linear codes $\mathscr{C}_F$ and $\mathscr{C}_G$ are isomorphic [8].

It is known that the extended Walsh spectrum is preserved by CCZ-equivalence, and then can potentially allow to verify the inequivalence of functions belonging to distinct CCZ-equivalence classes.

[3] A function $f : X \mapsto Y$ is called surjective if for every element $y \in Y$ there exists at least one $x \in X$ such that $f(x) = y$.

[4] A generator of the multiplicative group of $\mathbb{F}_{2^n}$.

## 1.3 APN functions

Recall that APN functions are $(n,n)$-functions with the lowest possible differential uniformity, that is 2. Classification and investigation of APN functions is important for cryptography, since these functions possess an optimum resistance to differential cryptanalysis. Besides, APN functions define optimal objects also in the theory of commutative semifields, coding theory, sequence design etc.

APN functions have been studied since the early 90's [90] but only a few infinite classes of APN functions are known to date. Complete characterization of APN functions is done only for $n \leq 5$ [7]. Among the currently known infinite families of APN functions are six infinite families of APN power functions and more or less 15 (depending on how we count) infinite families of quadratic APN polynomials. The known families cover only a small percentage of all APN functions found by computer investigations, since only in the field $\mathbb{F}_{2^8}$ more than 20.000 APN functions CCZ-inequivalent to each other are known [1], [101]. Finding new examples of infinite families of APN functions is an intense ongoing research area. All currently known infinite families of APN functions are presented in Tables 1.1 and 1.2.

### 1.3.1 APN power functions

The first known examples of APN functions were power functions (see Table 1.1). The last known case has been constructed in 2000 by H. Dobbertin [53] and it was conjectured that there do not exist APN power functions inequivalent to know cases listed in Table 1.1 [53]. The conjecture has been verified computationally for $n \leq 24$ by Anne Canteaut [53] and later by Yves Edel for $n \leq 34$, $n$ even (unpublished). However, the conjecture is open up to date.

Table 1.1: Known infinite families of APN power functions over $\mathbb{F}_{2^n}$

| Family | Exponent | Conditions | Algebraic degree | Source |
|---|---|---|---|---|
| Gold | $2^i+1$ | $\gcd(i,n)=1$ | 2 | [63, 90] |
| Kasami | $2^{2i}-2^i+1$ | $\gcd(i,n)=1$ | $i+1$ | [68, 71] |
| Welch | $2^t+3$ | $n=2t+1$ | 3 | [55] |
| Niho | $2^t+2^{t/2}-1$, $t$ even<br>$2^t+2^{(3t+1)/2}-1$, $t$ odd | $n=2t+1$ | $(t+2)/2$<br>$t+1$ | [54] |
| Inverse | $2^{2t}-1$ | $n=2t+1$ | $n-1$ | [2, 90] |
| Dobbertin | $2^{4i}+2^{3i}+2^{2i}+2^i-1$ | $n=5i$ | $i+3$ | [53] |

There are a few reasons why power functions were discovered first. The main of them is that most of known APN power functions, for $n$ odd, are AB (except inverse and Dobbertin functions), and AB power functions have been studied in the sequence design and coding theory along before the concept of AB functions was introduced by Chabaud and Vaudenay in 90's. The most part of known APN power functions were discovered in 1960's and early 1970's. AB power functions define sequences with

optimal properties for radar and wireless communication systems (see, for instance, [64], [89]) and correspond to binary cyclic codes with two zeros, whose duals are optimal [36].

*A maximal length sequence or, shortly, an m-sequence* is a binary sequence which can be generated by an LFSR of some degree $n$ (or, equivalently, can be described by a linear recurrence relation $s_i = a_1 s_1 + \ldots a_n s_{n-i}, a_i \in \{0,1\}$, for all $i$) with maximum period $N$ (that is, $2^n - 1$). For any $m$-sequence $s = (s_i)$ of length $2^n - 1$ there exists a unique $\lambda \in \mathbb{F}_{2^n}, \lambda \neq 0$, such that $s_i = Tr_n(\lambda \alpha^i)$, for all $i \in \{0, \ldots, 2^n - 2\}$, where $\alpha$ is some primitive element in $\mathbb{F}_{2^n}$. The autocorrelation value of an $m$-sequence $s$ at non-zero shift $\tau$ $\left(\text{that is, } C_{s_i}(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i \oplus s_{i+\tau}}\right)$ equals to $-1$ [90]. Sequences with the auto-correlation value $-1$ considered optimal for a usage in radars and code division multiple access (CDMA) in telecommunications.

When a communication system uses a set of several signals (usually corresponding to different users), each of these signals should be easily distinguished from any other signal in the set and its time-shifted versions. To achieve this the distance between a sequence $s$ of length $N$ and all cyclic shifts of another sequence $s'$ of the same length $N$ should be large. The distance between two $m$-sequences $s$ and $s'$ is measured via a *crosscorrelation function*: $C_{s_i, s'_i}(\tau) = \sum_{i=0}^{N-1} (-1)^{s_i \oplus s'_{i+\tau}}$.

For any two $m$-sequences $s$ and $s'$ of the same length $2^n - 1$, there exists an integer $d \in \{0, \ldots, 2^n - 2\}$ and a pair $(\lambda, \lambda')$ of elements from $\mathbb{F}_{2^n}^*$ such that $s_i = Tr_n(\lambda \alpha^i)$ and $s'_i = Tr_n(\lambda' \alpha^{di})$. When $\lambda = \lambda'$, $s'$ is called the *d-decimated sequence of s*. Then the crosscorrelation between two sequences $s$ and $s'$ is

$$C_{s_i, s'_i}(\tau) = \sum_{i=0}^{2^n-2} (-1)^{Tr_n(\alpha^{i+j} + \alpha^{di+j'+\tau})} = \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{Tr_n(\alpha^{\tau'}(\alpha^{j-\tau'} x + x^d))},$$

where $\tau' = j' + \tau$, $\lambda = \alpha^j$, $\lambda' = \alpha^{j'}$, for some $j, j' \in \{0, \ldots, 2^n - 2\}$.

Thus, $C_{s_i, s'_i}$ does not depends on $\lambda' = \alpha^{j'}$ and therefore, in order to find the cross-correlation between two different sequences of the same length, it is enough to study the crosscorrelation between sequence $s$ and its $d$-decimated sequences. The values of the crosscorrelation function between a sequence and its $d$-deciminated sequence are the values of the Walsh transform of the power function $x^d$ define over $\mathbb{F}_{2^n}$ (since $\gcd(d, 2^n - 1) = 1$, then $F(x) = x^d$ is a permutation and $W_F(a,b) = W_F\left(ab^{-\frac{1}{d}}, 1\right)$). Thus, AB power functions (maximally nonlinear) define decimations with the lowest possible crosscorrelation, which is of great importance in CDMA.

A relationship between APN and AB functions and properties of related codes has been observed in [68] and developed further in [36], [31]. Any linear subspace $\mathscr{C}$ of $\mathbb{F}_2^n$ of dimension $k$ is called a *binary linear code of length n and dimension k* and is denoted by $[n,k,d]$, where $d = \min_{c \in \mathscr{C}, c \neq 0} wt(c)$ and is the *minimum distance of* $\mathscr{C}$. The numbers $n, k$ and $d$ are called *parameters of* $\mathscr{C}$. The elements of $\mathscr{C}$ are called *codewords*. Any linear code $\mathscr{C}$ is associated with its *dual linear code* $\mathscr{C}^\perp = [n, n-k, d^\perp]$:

$$\mathscr{C}^\perp = \{x \in \mathbb{F}_2^n | c \cdot x = 0, \forall c \in \mathscr{C}\},$$

where $\cdot$ is an inner product in $\mathbb{F}_2^n$.

A linear code is called $2^l$-*divisible*, if the weight of any of its codewords $wt(c)$ is divisible by $2^l$ (for a positive integer $l$). Two linear codes with the same parameters are called *isomorphic* if they coincide, up to the order of codewords.

A linear code $\mathscr{C}$ of length $n$ can be defined by the so-called *parity-check matrix* $H$ (a binary matrix of the size $r \times n$):

$$\mathscr{C} = \{c \in \mathbb{F}_2^n | cH^T = 0\},$$

where $H^T$ is the transposed matrix of H.

A linear binary code $\mathscr{C}$ of length $m$ is called *cyclic* if, for any codeword $(c_0, \ldots, c_{n-1})$ from $\mathscr{C}$, $(c_{n-1}, \ldots, c_0)$ is also a codeword in $\mathscr{C}$. If we identify a vector $(c_0, \ldots, c_{n-1})$ of $\mathbb{F}_2^n$ with the polynomial $c(x) = c_0x^0 + c_1x^1 + \ldots + c_{n-1}x^{n-1}$, 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 $\mathscr{C}$ there exists a unique polynomial $g$, called the generator polynomial of $\mathscr{C}$, such that any codeword $c$ of $\mathscr{C}$ can be uniquely expressed as $c(x) = a(x)g(x)$. The roots of the generator polynomial are called the zeros of the code $\mathscr{C}$. If $n = 2^m - 1$ and $\alpha$ is a primitive element of $\mathbb{F}_2^m$ then the *defining set of* $\mathscr{C}$ is

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

Since $\mathscr{C}$ is a binary code, its defining set is a union of 2-cyclotomic cosets modulo $2^m - 1$: $Cl(a) = \{2^j a \mod (2^m-1)\}$. The defining set of a binary cyclic code of length $2^m - 1$ is usually identified with the representatives of the corresponding 2-cyclotomic cosets modulo $2^m - 1$.

Vectorial Boolean functions define linear codes and the APN and AB properties of functions can be characterized via the corresponding linear codes.
Let $F$ be a function defined on $\mathbb{F}_{2^m}$ such that $F(0) = 0$. Let $\mathscr{C}_F$ be a binary linear $[2^m-1, k, d]$-code defined by the following parity-check matrix:

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

where $\alpha$ is a primitive element of $\mathbb{F}_{2^m}$. Then [36]

- $3 \leq d \leq 5$ and $dim\, C_F \geq 2^m - 2m - 1$;
- If $F$ is APN then $dim\, C_F = 2^m - 2m - 1$ and $C_F^{\perp}$ does not contain the all-one vector;
- $F$ is APN if and only if $d = 5$;
- $F$ is AB if the weight of every codeword of the dual code $\mathscr{C}_F^{\perp}$ belongs to the set $\{0, 2^{m-1}, 2^{m-1} \pm 2^{\frac{m-1}{2}}\}$.

Binary linear codes of length $2^m - 1$ and dimension $2m$ are optimal, in certain sense. These optimal codes correspond to AB functions [36]. In particular, if $F$ is an AB power function $x^d$ defined over $\mathbb{F}_{2^m}$, the corresponding code $\mathscr{C}_F$ is a binary cyclic code of length $2^m - 1$ with two zeros: $\alpha$ and $\alpha^d$ whose dual is optimal.

Besides, the Walsh spectrum of function $F$ defined over $\mathbb{F}_{2^m}$ can be characterized by the dual code of $\mathscr{C}_F$ [36]:

$$\{W_F(a,b) : a,b \in \mathbb{F}_{2^n}\} = \{2^n - 2wt(c) : c \in \mathscr{C}^{\perp}\}.$$

Another characterization of the AB property was obtained in [30]: an $(m,m)$-function $F$, for $m$ odd, is AB if and only if $F$ is APN and the dual code of $\mathscr{C}_F$ is $2^{\frac{m-1}{2}}$-divisible. This statement was used in the proof that the Dobbertin APN power functions are not AB (we will return to this further).

Thus, cyclic codes with two zeros, whose dual is optimal are related to highly nonlinear power functions over finite fields; they also correspond to pairs of maximum-length sequences with optimal crosscorrelation values.

Another reasons why in the beginning main attention was paid to APN power functions is that power functions, in general, are simpler to analyse. Indeed, the APN property in the case of power functions is simpler to check. Let $F(x) = x^d$ be a function defined over the field $\mathbb{F}_{2^n}$, then for any $a \in \mathbb{F}_{2^n}$, $a \neq 0$, we have:

$$D_aF(x) = F(x+a) + F(x) = (x+a)^d + x^d = a^d\left(\left(\frac{x}{a}+1\right)^d + \left(\frac{x}{a}\right)^d\right) = a^d D_1\left(\frac{x}{a}\right).$$

Thus, the number of solutions of the equation $D_aF(x) = b$ is equal to the number of solutions of the equation $D_1F\left(\frac{x}{a}\right) = \frac{b}{a^d}$, for any $a,b \in \mathbb{F}_{2^n}$, $a \neq 0$ and therefore, in the case of power functions it is enough to check whether the equation $D_1F(y) = c$ admits at most 2 solutions for any $c \in \mathbb{F}_{2^n}$.

Computing the Walsh spectrum of power functions is also simpler than in the general case. Indeed, for $F(x) = x^d$ we have

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_n(ax+bF(x))} = \sum_{x \in \in \mathbb{F}_{2^n}} (-1)^{Tr_n(x+b(a^{-d}x)^d)} = W_F(1, ba^{-d}),$$

therefore $\{W_F(a,b) | a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m}, b \neq 0\} = \{W_F(1,c) | c \in \mathbb{F}_{2^m}, c \neq 0\}$.

Besides, power functions are considered up to cyclotomic equivalence, which is significantly simpler to test than both EA- and CCZ-equivalence.

An important property of APN power functions due to Dobbertin [53] (for proof see [33]): power APN functions are permutations when defined over a field of odd dimension and are 3-to-1, otherwise. Thus, APN power permutations do not exist over $\mathbb{F}_{2^n}$, for n even, and in the case of power permutations, the optimal value of differential uniformity is 4.

Determining the Walsh spectrum of a (vectorial) Boolean function and, in particular, of a power function characterizes many of its important properties. Moreover as we discussed above, there is a correspondence between the Walsh coefficients of a power function and the weight distribution of an associated linear code [36] and the crosscorelation values of $m$-sequences [89]. It is also known that the extended Walsh spectrum is invariant under CCZ-equivalence [36], and knowing the Walsh spectrum of two functions can potentially allow to verify their CCZ-inequivalence, that is, the fact that they belong to distinct CCZ-equivalence classes.

Although the exponents of Gold, Kasami, Welch and Niho power functions from Table 1.1 were discovered and investigated within the sequence theory since 1960's, not all of them have been proven to be maximally nonlinear at that time.

The Walsh spectrum of the Gold and Kasami functions (for $n$ odd) was determined in 1968 and 1971 by Gold and Kasami[5], respectively [63], [72]. As all AB functions, they have Walsh spectrum $\{0, \pm 2^{\frac{n-1}{2}}\}$ (for $n$ odd). Another proof of the AB property of the Kasami functions is done in [56] by Dobbertin. The APNness of Kasami functions in the even case was proven in [68]. The Walsh spectrum of the Gold and Kasami functions coincide also in the even case and has the form: $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$.

The optimal nonlinearity of the Welch functions (that is, in contemporary terms, their property of being AB) was conjectured by Welch in 1968[6]. The common Walsh spectrum of the Welch and Niho functions was conjectured in 1972 by Niho [90]. These conjectures remained open for almost 30 years. The progress in solving them became possible after the invention of the APN property. First, Dobbertin has proved that the Welch and Kasami functions are APN in [54], [55] and then the Walsh spectrum of these functions which is $\{0, \pm 2^{\frac{n-1}{2}}\}$ was determined using their APNness and applying methods of coding theory (via cyclic codes) [30, 31, 67].

The Walsh spectrum of the inverse function was determined by Lachaud and Wolfmann in [76], it consists of all integers divisible by 4 from the interval $[-2^{\frac{n}{2}+1} + 1; 2^{\frac{n}{2}+1} + 1]$. For $n$ odd, the inverse functions are APN, but they are not AB (since the algebraic degree of the inverse function is $n-1$, while AB functions have algebraic degree not more than $\frac{n+1}{2}$ [36]). For $n$ even, APN power functions could not be permutations, therefore the optimal value of differential uniformity in even case is 4. For cryptographic uses, $n$ even is preferred because it allows to decompose the elements of $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^{n/2}}$ and to express the operations in the half field. The inverse function, for $n$ even, is a permutation with differential uniformity 4 and has the best known nonlinearity (for $n$ even), that is $2^{n-1} - 2^{\frac{n}{2}}$. Thus, it is an optimal function for cryptographic uses and due to this, it was chosen as the S-box for AES [47]. The problem of finding APN permutations in even number of variables is one of the most attractive problems in the theory of Boolean functions. It was long believed that such functions did not exist. The conjecture was disproved by Dillon et al. when they constructed an APN permutation over $\mathbb{F}_{2^6}$ [9]. To date this function is the only known APN permutation in even number of variables.

The last known case of APN power functions was found in 1999 by Canteaut and Dobbertin independently, and proven by Dobbertin in 2000 [53]. To date, the Walsh spectrum and even the nonlinearity of the Dobbertin family of power functions remain unknown. This problem has already been open for 20 years, and without any progress since the seminal work of Canteaut, Charpin and Dobbertin from 2000, in which they proved that all Walsh coefficients of the Dobbertin function over $\mathbb{F}_{2^n}$ are divisible by $2^{\frac{n}{5}}$, but not all of them are divisible by $2^{\frac{n}{5}+1}$ [31]. The latter non divisibility result shows that the Dobbertin functions are not AB, for $n$ odd. It follows from the weight divisibility of the duals of cyclic codes with two zeros of length $2^n - 1$ (for more details

[5] As stated in [89] the Walsh spectrum of the Kasami function was computed by Welch in 1969 [102], however the result was never published.

[6] The conjecture was mentioned in [64].

see [55], [31]) and does not clarify the internal structure of the functions. In 2020 we presented two new results on the Dobbertin functions [14]. Based on computational data, we presented a conjecture fully describing the Walsh spectrum of the Dobbertin power functions defined over $\mathbb{F}_{2^{5m}}$. Depending on the parity of $m$, it has the following possible forms:

- $\{0, 2^{2m}(2^m+1), \pm 2^{5k-2}, \pm a \cdot 2^{2m} \mid 1 \leq a \leq k \cdot (k+1), a \text{ odd}\}$, for $m = 2k-1, k \in \mathbb{N}$;
- $\{0, -2^{2m}(2^m+1), \pm 2^{5k}, \pm 2^{5k+1}, \pm a \cdot 2^{2m} \mid 1 \leq a \leq k \cdot (k+2), a \text{ odd}\}$, for $m = 2k, k \in \mathbb{N}$.

Motivated by [36], we obtained alternative representations for the Niho and Dobbertin exponents: they can be represented as the composition $x^i \circ x^{1/j}$ of two power functions $x^i$ and $x^j$ of smaller algebraic degree than the original functions. The Niho power functions defined over $\mathbb{F}_{2^{2t+1}}$ can be represented in the form $x^i \circ x^{1/j}$, where $i = 3$ and $j \in \{2^{\frac{3t}{2}} + 2^t + 1, 2^{t+1} + 2^{\frac{t}{2}} + 1, 2^{t+1} + 2^{\frac{t}{2}+1} + 1\}$, for $t$ even and $j \in \{2^{\frac{3(t+1)}{2}} + 2^{\frac{t+1}{2}} + 1, 2^{\frac{3t+1}{2}} + 2^{t+1} - 1, 2^t + 2^{\frac{t-1}{2}} + 1\}$, for $t$ odd; The Dobbertin power functions defined over the field $\mathbb{F}_{2^{5m}}$ can be represented in the form $x^i \circ x^{1/j}$, where the ordered pair of exponents $(i, j)$ is one of the following 4 pairs: $(2^{2m} + 2^m + 1, 2^m + 1)$, $(2^{3m} + 2^{2m} + 1, 2^{2m} + 1)$, $(2^{3m} + 2^m + 1, 2^{3m} + 1)$, $(2^{2m} + 2^m + 1, 2^{4m} + 1)$ [14]. Moreover, we prove that our representations are optimal, i.e. no two power functions $x^{i'}$, and $x^{j'}$ of smaller algebraic degree can produce the corresponding functions in the similar way. A natural continuation of our work is to find a proof of the conjecture about the Walsh spectrum of the Dobbertin functions. We believe that alternative representations of the Doobertin exponent found in [14] can be a useful tool for approaching this problem.

The conjecture about non-existence of APN power functions inequivalent to known six classes was studied in [14]. In a view of this conjecture, two constructions $x^i \circ L \circ x^{1/j}$, where $L$ is a linear polynomial and power functions $x^d$ with exponent of the form $d = \sum_{i=1}^{k-1} 2^{mi} - 1$ over $\mathbb{F}_{2^{mk}}$ were examined in [14]. An initial motivation to study the first construction is the observation that the Kasami power functions (in odd case) can be obtained from Gold functions via such construction. This suggests that this construction may be a source for new APN power functions constructed from known ones. The second construction can also be potentially helpful for approaching that conjecture, since the exponents of both the inverse and the Dobbertin functions are special cases of this form [12].

### 1.3.2 Non-power APN functions

There are two main types of constructions of functions: primary (when functions are constructed from the scratch) and secondary (when functions are constructed from already known functions in the same or other number of variables). In this section we will describe some of the known methods of the secondary construction of APN functions and will give an overview on the known infinite families of non-power APN functions.

For a long time it was widely accepted that all APN functions are EA-equivalent to power functions. The first infinite family of APN functions EA-inequivalent to power functions was constructed only in 2006 [23]. In [23] it was shown that, for the Gold APN functions, CCZ-equivalence is more general than EA-equivalence and taking the inverse. As a result, the first classes of APN and AB functions EA-inequivalent to power functions were constructed. However, based on computational data on small dimensions it is conjectured in [15] that for non-Gold APN power functions, CCZ-equivalence coincides with EA-equivalence taken together with the inverse transformation. Recently this conjecture was confirmed for the inverse function [75]. Nonetheless in [20, 15] was shown also that for quadratic APN polynomials and for APN polynomials CCZ-inequivalent to both quadratic and power functions, CCZ-quivalence can be more general than EA-equivalence together with the inverse transformation.

Table 1.2: Known infinite families of quadratic APN polynomials over $\mathbb{F}_{2^n}$

| Family | Functions | Conditions | Source |
|---|---|---|---|
| F1-F2 | $x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$ | $n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$ | [22] |
| F3 | $sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$ | $q=2^m, n=2m$, $gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution $x$ s.t. $x^{q+1}=1$ | [18] |
| F4 | $x^3+a^{-1}\mathrm{Tr}_1^n(a^3x^9)$ | $a\neq 0$ | [20] |
| F5 | $x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$ | $3\|n$, $a\neq 0$ | [21] |
| F6 | $x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$ | $3\|n, a\neq 0$ | [21] |
| F7-F9 | $ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$ | $n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\|(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$ | [5, 4] |
| F10 | $(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$ | $n=2m, m\geqslant 2$ even, $\gcd(k,m)=1$ and $i\geqslant 2$ even, $u$ primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube | [106] |
| F11 | $a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$ | $n=3m, m$ odd, $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [13] | [13] |
| F12 | $u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$ | $q=2^m, n=2m, \gcd(i,m)=1, x^{2^i+1}+ax+b$ has no roots in $\mathbb{F}_{2^m}$ | [100] |
| F13 | $x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$ | $n=2m=10, (a,b,c)=(\beta,0,0), i=3, k=2, \mathbb{F}_4=<\beta>$ | [26] |
| | | $n=2m$, $m$ odd, $3\nmid m$, $(a,b,c)=(\beta,\beta^2,1), \mathbb{F}_4=<\beta>, i\in\{m-2,m,2m-1,(m-1)^{-1} \bmod m$ | |
| F14 | $u[(u^qx+x^qu)^{2^i+1}+(u^qx+x^qu)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]+(u^qx+x^qu)^{2^{2i}+1}+(u^qx+x^qu)^{2^{2i}}(x^q+x)+(x^q+x)^{2^{2i}+1}$ | $q=2^m, n=2m, \gcd(3i,m)=1, u$ primitive in $\mathbb{F}_{2^m}^*$ | [65] |
| F15 | $u[(u^qx+x^qu)^{2^i+1}+(u^qx+x^qu)(x^q+x)^{2^i}+(x^q+x)^{2^i+1}]+(u^qx+x^qu)^{2^{3i}}(x^q+x)+(u^qx+x^qu)(x^q+x)^{2^{3i}}$ | $q=2^m$, $m$ odd, $n=2m$, $\gcd(3i,m)=1$, $u$ primitive in $\mathbb{F}_{2^m}^*$ | [65] |

So, the first class of non-power APN and AB functions were constructed via CCZ-equivalence. This shows that equivalence relations are important tools not only for the investigation of functions, but also for their construction. Besides, the first and the only known up to date APN permutation in even dimension was constructed by employing CCZ-equivalence [9].

By construction, the APN and AB polynomials from [23] are CCZ-equivalent to power functions. Thus, the question of the existence of non-power APN and AB functions up to CCZ-equivalence was still open. The first examples of APN functions CCZ-inequivalent to power functions were found in [59]. These were the binomials $x^3+wx^{528}$ over $\mathbb{F}_{2^{12}}$ and $x^3+wx^{36}$ over $\mathbb{F}_{2^{10}}$. The idea leading to these examples was to consider the sum of two Gold APN functions. Later, as a generalization of the polynomial $x^3+wx^{528}$, the first infinite classes of APN binomials CCZ-inequivalent to power functions were constructed in [22] (classes F1-F2 in Table 1.2). Class F1, for $n$ divisible by 3 is an AB permutation, for $n$ odd. These classes of binomials proved the existence of AB functions CCZ-inequivalent to power functions. Besides, they disproved the conjecture from [36] about the non-existence of quadratic AB functions inequivalent to the Gold functions. Applying the same idea of constructing new functions by adding new quadratic terms to a known APN functions, the family of APN binomials F1, for $n$ divisible by 3, was generalized to trinomials and quadrinomials [5], [4]. Recently, an infinite class of APN quadrinomials containing the binomial $x^3+wx^{36}$ over $\mathbb{F}_{2^{10}}$ was constructed in [26], using the same approach of adding new quadratic terms to known functions.

In 2012, the family F1-F2 of APN binomials, for $n$ divisible by 3, was generalized to functions with $2^t$-to-1 derivatives in all non-zero directions with nonlinearity equal to $2^{n-1}-2^{(n+t)/2}$ for $n+t$ even, and $2^{n-1}-2^{(n+t-1)/2}$ for $n+t$ odd by relaxing the condition $\gcd(s,n)=1$ (see the conditions in Table 1.2) to $\gcd(s,n)=t$, for some positive integer $t$; these functions are permutations if and only if $n/t$ is odd [6]. The question of the possibility of such generalization for the second family ($n$ divisible by 4) remained open till 2020. In [48], we prove that by relaxing the condition $\gcd\left(s,\frac{n}{2}\right)=1$ to $\gcd\left(s,\frac{n}{2}\right)=t$ (for some positive integer $t$), the family F1-F2, for $n$ divisible by 4, can be also generalized to a family of functions with all derivatives in non-zero directions being $2^t$-to-1 mappings and with the nonlinearity at least $2^{n-1}-2^{\frac{n}{2}+t-1}$; these functions are permutations if and only if $n/\gcd(s,n)$ is odd (which is possible if and only if they are EA-equivalent to power permutations $x^{2^s+1}$).

The simplest example of functions which can be generalized to a function with all derivatives in non-zero directions being $2^t$-to-1 mappings is the Gold function. Indeed, let $x^{2^i+1}$ be the Gold function defined over $\mathbb{F}_{2^n}$. Relaxing the condition $\gcd(i,n)=1$ to $\gcd(i,n)=t$, for some positive integer $t$, the functions of the form $x^{2^i+1}$ become differentially $2^t$-uniform, with all derivatives in non-zero direction being $2^t$-to-1 functions. These functions are permutations if and only if $n/\gcd(i,n)=n/t$ is odd [90], and are $(2^t+1)$–to–1 functions otherwise. Their nonlinearity is $2^{n-1}-2^{(n+t)/2}$ when $n/t$ is odd, and $2^{n-1}-2^{(n+2t)/2}$ otherwise.

Thus, the APN binomials F1-F2 behave in the same way as the Gold functions from the point of view of the differential uniformity, nonlinearity and being permutations. These classes are not the only ones that can be generalized to functions with all derivatives in non-zero direction being $2^t$-to-1 mappings. Another example is the family of

hexanomials F3 constructed in [18]. In the same paper the authors prove that this family can be generalized to a family which consists of $2^t$-difrentially uniform functions (for some positive integer $t$) with all derivatives in non-zero directions being $2^t$-to-1 mappings. However, not all APN functions allow such generalization. For instance, the class of quadrinomials F13 can not be generalized to $2^t$-differentially uniform functions in the similar way, as shown in [48].

The family of hexanomials F3 was obtained by a generalization of a method of the construction of APN polynomials introduced by J. Dillon in [50]; the original method is to consider quadratic polynomials of the form $F(x) = x(Ax^2 + Bx^q + Cx^{2q}) + x^2(Dx^q + Ex^{2q}) + Gx^{3q}$ over $\mathbb{F}_{2^{2m}}$, where $q = 2^m$. The original approach gave new examples of quadratic APN functions in 6 and 8 variables which are CCZ-inequivalent to power functions [8].

It was observed in [20] that functions of the form $F + f$, where $F$ is an APN function and $f$ is a Boolean function can have differential uniformity at most 4. This leads to a new family of APN and AB functions F4. Note that F4 is the only currently known family of APN functions inequivalent to power functions defined for all values of $n$.

Constructions of the form $L_1(x^3) + L_2(x^9)$ for linear functions $L_1$ and $L_2$ gave two more infinite families of APN and AB functions F5 and F6 (see Table 1.2). The family F11 from Table 1.2 was obtained via the so-called isotopic shift construction [13]. The authors tried to adapt the isotopic equivalence of planar functions (that is, functions defined over the field $\mathbb{F}_{p^n}$ , for prime $p > 2$) to vectorial functions and to obtain a more general equivalence relation than CCZ-equivalence. Instead, they found a new construction method of APN functions inequivalent to power functions. The so-called the bivariate construction of APN functions introduced in [35] is a very fruitful method of the contraction of new APN functions. Applying this method, several infinite families of APN functions, namely, F10, F12, F14 and F15 were introduced (see [34],[65], [100], [106]).

Note that almost all currently known APN polynomials (CCZ-inequivalent to monomials) are quadratic. The only example of a non-quadratic and non-power APN function is known in dimension 6. It is a $(6,6)$-function of the form [7, 60]:

$$x^3 + a^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + Tr_2(x^{21}) + Tr_3(a^{18}x^9) + a^{14}Tr_6(a^{52}x^3 + a^6x^5 + a^{19}x^7 + a^{28}x^{11} + a^2x^{13}).$$

For more details about constructions of APN functions see, for instance, [11, 10, 11, 29, 33].

## 1.4 Bent Boolean functions

Recall that bent functions are functions with the highest possible nonlinearity. Bent Boolean functions were invented and named by Oscar Rothaus in 1966 as optimal combinatorial objects[7]. A natural extension of bent Boolean functions are bent vectorial functions, i.e. functions with all component functions being bent Boolean functions [90]. The investigation of bent functions was stimulated along with the development

[7] The work was published in May 1976.

of computer science. Bent functions have applications in coding theory, cryptography, sequence design, projective geometry. Bent Boolean functions play a role in coding theory since they allow to construct good codes and, in particular, Kerdock codes [72], and in the other domains of communications (for instance, in telecommunications, see [93]). Bent vectorial functions can be used in block ciphers at the coast of additional diffusion, compression, expansion layers, or as building blocks for the construction of S-boxes. They are also used to construct algebraic manipulation detection codes [69, 70].

Despite their simple and natural definition, bent functions admit a very complicated structure in general. The general structure of bent functions over $\mathbb{F}_{2^n}$ is not yet clear. The complete classification of bent functions is a hard open problem; it was done only for $n \leq 8$ [77]. Therefore, an important focus of research is to find constructions of bent functions leading to infinite families of bent functions.

Bent functions always occur in pairs with their duals. The function $\tilde{f}$ is called the dual of an $n$ variable bent Boolean function $f$ if $W_f(x) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(x)}$, for every $x \in \mathbb{F}_{2^n}$. The dual of a bent function is again bent and its own dual is $f$ itself [51].

Several primary constructions of bent functions in bivariate form have been introduced in [51, 85]. Some are more principles of constructions than explicit (since they need conditions which are difficult to achieve) like the *PS* class, other lead to explicit bent functions: Maiorana-McFarland construction and the partial spread subclass $PS_{ap}$.

*The Maiorana-McFarland class or, shortly, MM class* is the collection of all $n = 2m$-variable Boolean functions $f$ of the form:

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

where $\cdot$ is an inner product in $\mathbb{F}_2^m$, $\pi$ is a permutation over $\mathbb{F}_2^m$ and $g$ is a Boolean function over $\mathbb{F}_2^m$. A necessary and sufficient condition for $f$ being bent is the bijectivity of $\pi$. *The completed Maiorana-McFarland class* consists of all functions which are EA-equivalent to functions from Maiorana-McFarland functions. The completed *MM* class contains all quadratic bent Boolean functions [51].

The $PS_{ap}$ class is the set of $n = 2m$ variable Boolean functions $f$ over the field $\mathbb{F}_{2^{2m}}$ of the following form:

$$f(x,y) = g\left(xy^{2^m-2}\right),$$

where $g$ is a balanced Boolean function on $\mathbb{F}_{2^m}$ such that $g(0) = 0$ (with the convention $\frac{1}{0} = 0$). The dual of the function $g\left(xy^{2^m-2}\right)$ from the class $PS_{ap}$ is $g(yx^{2^m-2})$. In general, for every balanced function $g$, the dual of the bent function $g(\frac{x}{y})$ is $g(\frac{y}{x})$ [37].

Functions from the class $H$ of bent Boolean functions introduced by Dillon in his PhD thesis [51] have the following bivariate form:

$$f(x,y) = Tr_m\left(y + xF\left(yx^{2^m-2}\right)\right),$$

where $x, y \in \mathbb{F}_{2^m}$, $F$ is a permutation of $\mathbb{F}_{2^m}$ s.t. $F(x) + x$ does not vanish and for any $\beta \in \mathbb{F}_{2^m} \setminus \{0\}$, the function $F(x) + \beta x$ is 2-to-1. Dillon did not manage to find a bent function in the class $H$ that would not belong to the completed *MM* class. For a long time it was unknown whether every function from $H$ is EA-equivalent to a function from *MM*. Later, when in [40] the explicit form of functions in the Dillon's class $H$ was

derived (by relating it to the notion of $o$-polynomials), the question was answered negatively in [25]: the $MM$ class and Dillon's class $H$ are different up to EA-equivalence.

Bent functions can also be viewed in their univariate form. Finding explicit bent functions in the univariate polynomial representation is more difficult than in the bivariate. A first step towards this is to focus on *monomial bent functions*, that is, the bent functions of the form $Tr_n(ax^d)$, for some positive integer $d$, and $a \in \mathbb{F}_{2^n}$; then the exponent $d$ is called a *bent exponent*. Note that a function of the form $Tr_n(ax^d)$ with a bent exponent is bent not for every non-zero $a$. There are only a few exponents $d$ known that allow the construction of bent functions. The list of currently known monomial bent functions is presented in Table 1.3. As stated in [78], this list is complete for $n \leq 24$ up to equivalence.

Table 1.3: The known monomial bent functions of the form $Tr_n(ax^d)$ over $\mathbb{F}_{2^n}$

| Exponent $d$ | Conditions | Family | Reference |
|---|---|---|---|
| $2^i+1$ | $\gcd(i,n)=1, a \notin < \alpha^{\gcd(d,2^{n-1})} >$, | $MM$ | [63] |
| $s(2^{\frac{n}{2}}-1)$ | $\gcd(s,2^{\frac{n}{2}}+1)=1$, $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, $\sum_{x \in \mathbb{F}^*_{2^{n/2}}} (-1)^{(ax+x^{-1})} = -1$ | $PS_{ap}$ | [42, 51] |
| $2^{2i}-2^i+1$ | $\gcd(3,n)=\gcd(3,n)=1, a \notin < \alpha^3 >$ | | [52] |
| $(2^s+1)^2$ | $n=4s$, $s$ odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot < \alpha^{2^s+1} >$ | $MM$ | [43, 79] |
| $2^{2s}+2^s+1$ | $n=5s$, $a \in \{r \in \mathbb{F}_{2^{\frac{n}{2}}} \mid Tr_s^{n/2}(r)=0\} \cdot < \alpha^d >$ | $MM$ | [32] |

### 1.4.1 Niho bent functions

An important case of bent Boolean functions are the so-called *Niho bent functions*. There are a few reasons why this class is of particular interest. First, some of the constructions of non-monomial bent functions in univariate polynomial form are done via Niho power functions (see for instance, [58]). Besides, it is known that Boolean functions, and bent functions in particular, are considered up to EA-equivalence, which is the most general known equivalence relation preserving bentness [16, 17]. However, for Niho bent functions, a more general equivalence relation preserving bentness is known [40]. In addition, Niho bent functions have an important property: every Niho bent function defines a vectorial bent function. This property was first observed in [88], however in [49] we provide the simpler proof of this statement. Moreover, Niho bent functions played the central role in a proof that the class $H$ introduced by Dillon in [51] does not coincide with the completed $MM$ class [40, 25].

The name of Niho exponent comes from a theorem dealing with power functions by Niho [89]. Later, in [58] linear combinations of such power functions were considered and the class of Niho bent functions was introduced.

A positive integer $d$ (always understood modulo $2^n-1$) is said to be a *Niho exponent* and $x^d$ a *Niho power function* if the restriction of $x^d$ to $\mathbb{F}_{2^m}$ ($n=2m$) is linear or, in other words, $d \equiv 2^j \mod (2^m-1)$, for some $j<n$. As we consider $tr_n(ax^d)$ with $a \in \mathbb{F}_{2^n}$,

without loss of generality, we can assume that $d$ is in the normalized form, i.e., with $j = 0$. Then we have a unique representation $d = (2^m - 1)s + 1$.

Table 1.4: The known Niho bent function over $\mathbb{F}_{2^n}, n = 2m$

| Family | Function | Conditions | | Reference |
|---|---|---|---|---|
| Monomials | $Tr_m(ax^{2^m+1})$ | $a \in \mathbb{F}^*_{2^m}$ | | [63] |
| Binomials | $Tr_n(a_1x^{d_1} + a_2x^{d_2})$ | $2d_1 \equiv 2^m + 1 \pmod{2^n - 1}$, $a_1, a_2 \in \mathbb{F}^*_{2^n}$, $(a_1 + a_1^{2^m})^2 = a_2^{2^m+1}$ | | [58], [66] |
| | | Case 1: | $d_2 = 3(2^m - 1) + 1$ | |
| | | Case 2: | $d_2 = \frac{1}{4}(2^m - 1) + 1$, $m$ odd | |
| | | Case 3: | $d_2 = \frac{1}{6}(2^m - 1) + 1$, $m$ even | |
| Leander-Kholosha | $Tr_n\left(a^2x^{2^m+1} + (a + a^{2^m})\sum_{i=1}^{2^{r-1}-1} x^{d_i}\right)$ | $1 < r < m$, $\gcd(r,m) = 1$, $2^r d_i = (2^m - 1)i + 2^r$, $a \in \mathbb{F}_{2^n}$, $a + a^{2^m} \neq 0$ | | [80, 81] |
| | Niho bent functions in bivariate form obtained from $o$-polynomials | | | See for instance, [40] |

A few examples of infinite families of Niho bent functions are known. The corresponding list is presented in Table 1.4.

The simplest example of Niho bent functions is *the quadratic function* of the form $Tr_m(ax^{2^m+1})$ (note that $s = 2^{m-1} + 1$) defined over the field $\mathbb{F}_{2^n}, n = 2m$ (see Table 1.4).

Another known families of Niho bent functions are *the binomial Niho bent functions* from Table 1.4. The binomial Niho bent functions can be written in an alternative form, as

$$f(x) = \mathrm{Tr}_m(ax^{2^m+1}) + \mathrm{Tr}_n(bx^{d_2}),$$

where $a = (a_1 + a_1^{2^m})^2$, $b = a_2$, $a = b^{2^m+1} \in \mathbb{F}^*_{2^m}$, $d_2 \in \{3(2^m - 1) + 1, \frac{2^m-1}{4} + 1 (m \text{ odd}), \frac{2^m-1}{6} (m \text{ even})\}$. Note that if $b = 0$ and $a \neq 0$ then $f$ is the quadratic Niho bent function from Table 1.4. These functions, for $d_2 = 3(2^m - 1) + 1$ and $6d_2 = (2^m - 1) + 6$, have algebraic degree $m$ and do not belong to the completed $MM$ class; the function for $4d_2 = (2^m - 1) + 4$ has algebraic degree 3 [38, 25]. Originally, the family of Niho bent binomials, for $d_2 = 3(2^m - 1) + 1$, was introduced under an assumption that if $m \equiv 2 \mod 4$, then $b = c^5$, for some $c \in \mathbb{F}^*_{2^n}$; otherwise, $b$ could be any element from $\mathbb{F}^*_{2^n}$. Thanks to an observation made in [40] (we will return to this observation later in this Section), it was shown in [66] that even for $m \equiv 2 \mod 4$ the value of $b$ can be arbitrary. In [40], the bivariate representation of the family of binomial Niho bent functions, for $4d_2 = (2^m - 1) + 4$, and the bivariate expression of its dual was found. It has been shown that the dual of this function has algebraic degree $\frac{m+3}{2}$ and belongs to

the completed *MM* class (since the duals of functions from the *MM* class belong to the *MM* class).

The family of binomal Niho bent functions, for $4d_2 = (2^m - 1) + 1, m$ odd, was generalized by Leander and Kholosha into a function with $2^r$ Niho exponents [80] (the *Leander-Kholosha family* in Table 1.4). The algebraic degree of these functions is $r+1$ [28] and they belong to the completed *MM* class [38]. The duals of functions belonging to the Leander-Kholosha family were found and their algebraic degree has been computed in [25] and [38].

Table 1.5: The known $o$-polynomials over $\mathbb{F}_{2^m}$

| Family | Function | Conditions | Reference |
|---|---|---|---|
| Translation | $x^{2^i}$ | $\gcd(i,n) = 1$ | [98] |
| Serge | $x^6$ | $m$ odd | [98] |
| Glynn I | $x^{3\cdot 2^k+4}$ | $m = 2k-1$ | [61] |
| Glynn II | $x^{2^k+2^{2k}}$ | $m = 4k-1$ | [61] |
| Glynn III | $x^{2^{2k+1}+2^{3k+1}}$ | $m = 4k+1$ | [61] |
| Cherewitzo | $x^{2^k}+x^{2^k+2}+x^{3\cdot 2^k+4}$ | $m = 2k-1$ | [44] |
| Payne | $x^{\frac{1}{6}}+x^{\frac{1}{2}}+x^{\frac{5}{6}}$, | $m$ odd | [94] |
| Subiaco | $\frac{\delta^2(x^4+x)+\delta^2(1+\delta+\delta^2)(x^3+x^2)}{x^4+\delta^2x^2+1} + x^{\frac{1}{2}}$, | $Tr_m(\frac{1}{\delta}) = 1$ (if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$) | [46] |
| Adelaide | $\frac{1}{Tr_m^n}(v)\left(Tr_m^n(v^r)(x+1)+(x+Tr_m^n(v)x^{\frac{1}{2}}+1)^{1-r}Tr_m^n(vx+v^{2^m})^r\right)+x^{\frac{1}{2}}$ | $m$ even, $r = \pm\frac{2^m-1}{3}$, $v \in F_{2^{2m}}, v^{2^m+1} \neq 1, v \neq 1$ | [45] |
| O'Keefe-Penttila | $F(x) = x^4+x^{16}+x^{28}+\omega^{11}(x^6+x^{10}+x^{14}+x^{18}+x^{22}+x^{26})+\omega^{20}(x^8+x^{20})+\omega^6(x^{12}+x^{24})$ | $\omega^5 = \omega^2+1$ and $m = 5$ | [92] |

In [40] the authors observed that there is a one-to-one correspondence between Niho bent functions and a special type of permutation polynomials, the so-called *o-polynomials*. A permutational polynomial $G$ over $\mathbb{F}_{2^m}$ is called an *o-polynomial* if the functions $P_\gamma, \gamma \in \mathbb{F}_{2^m}$ defined over $\mathbb{F}_{2^m}$ as follow

$$P_\gamma(z) = \begin{cases} \frac{G(\gamma+z)+G(\gamma)}{z} & \text{if } z \neq 0; \\ 0 & \text{if } z = 0 \end{cases}$$

are permutations, for all $\gamma \in \mathbb{F}_{2^m}$. Then every Niho bent function in $2m$ variables is EA-equivalent to a function $g$ defined in a bivariate form as follow:

$$g(x,y) = \begin{cases} Tr_m(x\psi(\frac{y}{x})) & \text{if } x \neq 0; \\ Tr_m(\mu y) & \text{if } x = 0 \end{cases} \tag{1.6}$$

where $\psi$ is a mapping from $\mathbb{F}_{2^m}$ such that $G(z) = \psi(z) + \mu z$ is an $o$-polynomial [40]. The class of functions defined by (1.6) is exactly the Dillon's class $H$ up to addition of a linear term. Therefore, the class of Niho bent functions and the Dillon's class $H$ are the same up to EA-equivalence. Note that, since functions from the families of binomial Niho bent functions, for $d = (2^m-1)3+1$ and $6d_2 = (2^m-1)+6$, do not belong to the completed $MM$ class, the Dillon's class $H$ and $MM$ are different up to EA-equivalence.

Originally, the notion of $o$-polynomial comes from projective geometry and it took around 50 years for geometers to construct 9 classes of inequivalent o-polynomials. The list of all known $o$-polynomials can be found in Table 1.4.1. This table consists of 5 quadratic and one cubic power functions, two trinomials, 2 families of $o$-polynomials of more complicated form and 1 $o$-polynomial in dimension $2^5$. It is conjectured that the list of o-monomials is complete up to equivalence [61]. The conjecture is computationally verified for $n \leq 28$ in [62].

The o-polynomials corresponding to the functions from the Leander-Kholosha family of Niho bent functions are equivalent to the Frobenius map [80]. In [66], a relation between Niho bent functions belonging to the families of binomial Niho bent functions, for $d = (2^m-1)3+1$ and $6d_2 = (2^m-1)+6$, and the Subiaco and Adelaide $o$-polynomials, respectively, was found. This allowed to expand the class of binomial Niho bent functions, for $d = (2^m-1)3+1$, in the case $m \equiv 2 \mod 4$ [66].

In [27] it was shown that any Niho bent function in univariate form defined over the field $\mathbb{F}_{2^n}$ can be obtained as a sum of Leander-Kholosha functions taken with particular non-zero coefficients from $\mathbb{F}_{2^n}$. More precisely, any Niho bent function in a univariate representation (defined over the field $\mathbb{F}_{2^n}$), up to EA-equivalence, is obtained as a sum of functions of the following form:

$$Tr_n\left(A_{2^{r-1}}x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} A_i x^{(2^m-1)(2^{m-r}i+1)+1}\right),$$

where $0 < r < m$, $A_i \in \mathbb{F}_{2^n}^*$ (for $r = 1$, replace the last sum with zero). In particular, every $o$-monomial corresponds to a bent function of Leander-Kholosha type with particular coefficients of power terms.

In [40] the authors observed that the equivalence between $o$-polynomials induces an equivalence relation of Niho bent functions, the so-called $o$-equivalence. Equivalence of $o$-polynomials implies EA-equivalence of the corresponding Niho bent functions. However, this new equivalence relation is more general than EA-equivalence, since Niho bent functions generated by equivalent $o$-polynomials $F$ and $F^{-1}$ are EA-inequivalent in general. Later, in [19] $o$-equivalence was successfully employed as a method of the construction of new Niho bent functions from known ones. A group of transformations (introduced in [44]) of order 24 preserving o-equivalence was studied. It was shown that these transformations can generate up to three EA-inequivalent Niho bent functions from a given one (including its inverse). However the group of transformations from [44] does not cover all possible transformations which applied to

Niho bent functions preserves their $o$-equivalence. A more general group of transformations preserving the equivalence of $o$-polynomials was introduced in [91]. In [49], we studied this group of transformations together with the inverse map, and proved that EA-inequivalent Niho bent functions can arise only from a transformation of specific form (composed by specific transformations of the group in a special order and involving the inverse map). We derived the number of Niho bent functions induced by a given $o$-polynomial and, in the case of $o$-monomials, we identified the exact transformations always leading to EA-inequivalent Niho bent functions. For $o$-polynomials which are not monomials, the question of identifying such transformations which can be guaranteed to lead to EA-inequivalent Niho bent functions remains open and it is an interesting problem to study.

More information on constructions of bent functions can be found in [33, 39, 73, 87].

# BIBLIOGRAPHY


[1] C. Beierle, and G. Leander, "New Instances of Quadratic APN Functions", arXiv:2009.07204 (2020).

[2] T. Beth, and C. Ding, "On almost perfect nonlinear permutations", *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg (1993).

[3] E. Biham, and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, 4(1), pp. 3–72 (1991).

[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "A Few More Quadratic APN Functions", *Cryptography and Communications*, 3(1), pp. 43–53 (2011).

[5] C. Bracken, E. Byrne, N. Markin, and G. McGuire, " New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials", *Finite Fields and Their Applications*, 14(3), pp. 703–714 (2008).

[6] C. Bracken, C.Tan, Y. Tan, " Binomial differentially 4 uniform permutations with hight nonlinearity", *Finite Fields and Their Applications*, 18, pp. 537–546 (2012).

[7] M. Brinkman, and G. Leander, "On the classification of APN functions up to dimension five", *Proceedings of the International Workshop on Coding and Cryptography 2007*, France, pp. 39–48 (2007).

[8] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan, "APN Polynomials and Related Codes", *Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday*, 34(1–4), pp. 135–159 (2009).

[9] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, "An APN Permutation in Dimension Six", *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS*, 518, pp. 33-42 (2010).

[10] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer Verlag, 2015.

[11] L. Budaghyan, *The Equivalence of AB and APN Functions and Their Generalization*, VDM Verlag, 2008.

[12] L. Budaghyan, *The equivalence of bent and almost perfect nonlinear functions and their generalizations*, Ph.D. Thesis, Otto-von-Guericke University Magdeburg, Germany, 2005.

[13] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa, "Constructing APN functions through isotopic shift", *IEEE Trans. Inform. Theory*, 66(8), pp. 5299–5309 (2020).

[14] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. Kaleyski, "On two fundamental problems on APN power functions", *IACR Cryptol. ePrint Arch. 2020: ia.cr/2020/1359*. Submitted to *IEEE Transactions on Information Theory* in 2020.

[15] L. Budaghyan, M. Calderini, and I. Villa, "On relations between CCZ- and EA-equivalences", *Cryptography and Communications*, 12, pp. 85–100 (2020).

[16] L. Budaghyan, and C. Carlet, "CCZ-equivalence of bent vectorial functions and related constructions", *Designs, Codes and Cryptography*, 59(1–3), pp. 69–87 (2011).

[17] L. Budaghyan, and C. Carlet, "On CCZ-equivalence and its use in secondary constructions of bent functions", *Proceedings of International Workshop on Coding and Cryptography WCC 2009 and IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2009/42 (2009).

[18] L. Budaghyan, and C. Carlet, "Classes of Quadratic APN Trinomials and Hexanomials and Related Structures", *IEEE Transactions on Information Theory* 54(5), pp. 2354–2357 (2008).

[19] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, "On o-equivalence of Niho Bent functions", *International Workshop on the Arithmetic of Finite Fields 2014, Lecture Notes in Computer Science*, 9061, pp. 155-168 (2015).

[20] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones", *Finite Fields and Their Applications*, 15(2), pp. 150–159 (2009).

[21] L. Budaghyan, C. Carlet, and G. Leander, "On a construction of quadratic APN functions", *P*roceedings of IEEE Information Theory Workshop ITW'09, pp. 374–378 (2009).

[22] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions", *IEEE Transactions on Information Theory*, 54(9), pp. 4218–4229 (2008).

[23] L. Budaghyan, C. Carlet, and A. Pott, " New Classes of Almost Bent and Almost Perfect Nonlinear Functions", *IEEE Transactions on Information Theory*, 52(3), pp. 1141–1152 (2006).

[24] L. Budaghyan, and T. Helleseth, " New commutative semifields defined by new PN multinomials", *Cryptography and Communications* 3(1), pp. 1–16 (2011).

[25] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "Further results on Niho bent functions," *IEEE Transactions on Information Theory*, 58(11), pp. 6979–6985 (2012).

[26] L. Budaghyan, T. Helleseth, and N. Kaleyski, " A new family of APN quadrinomials", *IEEE Transactions on Information Theory*, 66(11), pp. 7081-7087 (2020).

[27] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Univariate Niho Bent Functions From o-Polynomials", *IEEE Information Theory workshop ITW'09*, 60(4), pp. 2254–2265 (2016).

[28] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, "Niho bent functions from quadratic o-monomials", *Proceedings of the 2014 IEEE International Symposium on Information Theory, ISIT 2014*, Honolulu, HI, USA, July 2014.

[29] M. Calderini, L. Budaghya, and C. Carlet, " On known constructions of APN and AB functionsand their relation to each other ", *Rad HAZU, Matematičke znanosti* (2021), to appear.

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

[31] A. Canteaut, P. Charpin, and H. Dobbertin, "Weight divisibility by cyclic codes, highly-nonlinear functions on $\mathbb{F}_2^n$, and crosscorelation of maximum-weight sequences", *SIAM Journal of Discrete Mathematics*, 13(1), pp. 105–138 (2000).

[32] A. Canteaut, P. Charpin, and G. M. Kyureghyan,"A new class of monomial bent functions", *Finite Fields and Their Applications*, 14(1), pp. 221–241 (2008).

[33] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge: Cambridge University Press, 2021.

[34] C. Carlet, " More constructions of APN and differentially 4-uniform functions by concatenation", *Science China Mathematics*, 56(7), 1373–1384 (2013).

[35] C. Carlet, "Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions", *Designs, Codes and Cryptography*, 59, pp. 8–109 (2011).

[36] 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).

[37] C. Carlet and P. Guillot, " A characterization of binary bent functions", *Journal of Combinatorial Theory*, Series A, 76(2), pp. 328–335 (1996).

[38] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "On the dual of bent functions with $2^r$ Niho exponents", in *Proceedings of the 2011 IEEE International Symposium on Information Theory*. IEEE, Jul./Aug, pp. 657–661 (2011).

[39] C. Carlet, and S. Mesnager, "Four decades of research on bent functions", *Designs, Codes and Cryptography* 78(1), pp. 5–50, (2016).

[40] C. Carlet, and S. Mesnager, "On Dillon's class $H$ of bent functions, Niho bent functions and o-polynomials", *Journal of Combinatorial Theory, Series A*, 118(8), pp. 2392–2410 (2011).

[41] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science*, 950, pp. 356–365 (1995).

[42] P. Charpin and G. Gong, "Hyperbent functions, Kloosterman sums, and Dickson polynomials", *IEEE Transactions on Information Theory*, 54(9), pp. 4230–4238 (2008).

[43] P. Charpin, and G. Kyureghyan, "Cubic monomial bent functions: A subclass of MM", *SIAM Journal of Discrete Mathematics*, 22(2), pp. 650–665 (2008).

[44] W. Cherowitzo, "Hyperovals in Desarguesian planes of even order", *Annals of Discrete Mathematics*, 37, pp. 87–94 (1988).

[45] W. Cherowitzo, C. M. O'Keefe, T. Penttila, "A unified construction of finite geometries associated with q-clans in characteristic 2", *Advanced Geometry*, 3(1), pp. 1–21 (2003).

[46] W. Cherowitzo, T. Penttila, I. Pinneri, G.F. Royle, "Flocks and ovals", *Geom. Dedicata*, 60(1), pp. 17–37 (1996).

[47] J. Daemen, and V. Rijmen, *AES proposal: Rijndael*, http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf (1999).

[48] D. Davidova, and N. Kaleyski,"Generalization of a class of APN binomials to Gold-like function", *Lecture Notes in Computer Science*, 12542, pp. 195–206 (2021).

[49] D. Davidova, L. Budaghyan, C. Carlet, T. Helleseth, F. Ihringer, and T. Penttila, "Relation between o-equivalence and EA-equivalence for Niho bent function", *Finite Fields and Their Applications*, 72, pp. 1–42 (2021).

[50] J. F. Dillon, " APN Polynomials and Related Codes. Polynomials over Finite Fields and Applications", *Banff International Research Station*, Nov. 2006.

[51] J. F. Dillon, *Elementary Hadamard difference sets*, Ph.D.Thesis, Univeriy of Marylent, 1974.

[52] J.F. Dillon, and H. Dobbertin, "New cyclic difference sets with Singer parameters", *Finite Fields and Their Applications*, 10, pp. 342-389 (2004).

[53] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5", *Finite Fields and Applications*, Springer, Berlin, Heidelberg, pp. 113–121 (2001).

[54] H. Dobbertin. "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case", *Information and Computation*, 151(1-2), pp. 57-72 (1999).

[55] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case", *IEEE Transactions on Information Theory*, 45, pp. 1271–1275 (1999).

[56] H. Dobbertin, "Another Proof of Kasami's Theorem", *Designs, Codes and Cryptography*, 17, 177–180 (1999).

[57] H. Dobbertin, "One to one highly-nonlinear power functions on $GF(2^n)$", *Applicable Algebra in Engineering, Communication and Computing*, 9, pp. 139–152 (1998).

[58] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via Niho power functions," *Journal of Combinatorial Theory, Ser. A*, 113(5), pp. 779–798 (2006).

[59] Y. Edel, G. Kyureghyan, and A. Pott. "A new APN function which is not equivalent to a power fanction", *IEEE Transactions on Information Theory* 52(2), pp. 744–747 (2006).

[60] Y. Edel, and A. Pott, "A new almost perfect nonlinear function which is not quadratic", *Advances in Mathematics of Communications*, 3(1), pp. 59–81 (2009).

[61] D. Glynn, "Two new sequences of ovals in finite desarguesian planes of even order," *Combinatorial Mathematics, Lecture Notes in Mathematics*, 1036, pp. 217–229 (1983).

[62] D. Glynn, "A condition for the existence of ovals in $PG(2;q),q$ even", *Geometriae Dedicata*, 32, 247–252 (1980).

[63] R. Gold, "Maximal recursive sequences with 3-valued recursive correlation functions", *IEEE Transactions on Information Theory*, 14, pp. 154–156 (1968).

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

[65] F. Göloglu, " Gold-hybrid APN functions", Preprint (2020).

[66] T. Helleseth, A. Kholosha, and S. Mesnager, "Niho bent functions and Subiaco hyperovals", *Theory and Applications of Finite Fields, ser. Contemporary Mathematics, M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, Eds.*, 579. Providence, Rhode Island: American Mathematical Society pp. 91–101 (2012).

[67] 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).

[68] H. Janwa and R. M. Wilson, "Hyperplane sections of Fermat varieties in P 3 in char. 2 and some applications to cyclic codes", *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, Springer, Berlin, Heidelberg (1993).

[69] M. G. Karpovsky, and P. Nagvajara, "Optimal codes for minimax criterion on error detection", *IEEE Transaction on Information Theory*, 35(6), pp. 1299–1305 (1989).

[70] M. G. Karpovsky, and A. Taubin, "A new class of nonlinear symmetric error detecting codes", *IEEE Transaction on Information Theory*, 50(8), pp. 1818–1820 (2004).

[71] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes", *Information and Control*, 18(4), pp. 369-394 (1971).

[72] A. M. Kerdock, "A class of low-rate non linear codes", *Information and Control20*, pp. 182–187 (1972).

[73] A. Kholosha, and A. Pott, "Bent and related functions", in *Handbook of Finite Fields, ser. Discrete Mathematics and its Applications, G. L. Mullen and D. Panario, Eds. London: CRC Press*, 9.3, pp. 255–265 (2013).

[74] L. Knudsen, "Truncated and higher order differentials", *Proceedings of Fast Softwhere Encyption FSE 1995, Lecture Notes in Computer Science*, 1008, pp. 196–211 (1996).

[75] L. Kölsch, "On CCZ-equivalence of the inverse function", Arxiv 2020.

[76] G. Lachaud, and J. Wolfmann, "The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes". *IEEE Transaction on Information Theory* 36, pp. 686–692 (1990).

[77] P. Langevin, and G. Leander, "Counting all bent functions in dimension eight",*Designs, Codes and Cryptography*, 59(1-3), pp. 193–205 (2011).

[78] P. Langevin and G. Leander, "Monomial bent functions and Stickelberger's theorem", *Finite Fields and Their Applications*,14, pp. 727-742 (2008).

[79] N. G. Leander, "Monomial bent functions", *IEEE Transaction on Information Theory* , 52(2), pp. 738–743 (2006).

[80] G. Leander and A. Kholosha, "Bent functions with $2^r$ Niho exponents" *IEEE Transaction on Information Theory*, 52(12), pp. 5529–5532 (2006).

[81] N. Li, T. Helleseth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents", *IEEE Transaction on Information Theory*, 59(7), pp. 4662–4667 (2013).

[82] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, 20, Addison-Wesley, Reading, Massachussetts (1983).

[83] J. L. Massey, "Shift-register synthesis and BCH decoding", *IEEE Trasactions on Inform. Theory*, 15(1), pp. 122–127 (1969).

[84] M. Matsui, "Linear cryptanalysis methods for DES cipher, Advances in Cryptology", *Eurocrypt'93, In: Lecture Notes in Computer Science*, 765, pp. 386–397 (1993).

[85] R. L. McFarland, "A family of noncyclic difference sets", *Journal of Combinatorial Theory, Series A.*, 15, pp. 1–10 (1973).

[86] W. Meier, and O. Staffelbach, " Fast correlation attacks on stream ciphers". *EUROCRYPT'88, Lecture Notes in Computer Science*, 330, pp. 301–314 (1988).

[87] S. Mesnager. *Bent Functions: Fundamentals and Results*, Springer, Switzerland, 2016.

[88] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials", *Journal Designs, Codes and Cryptography*, 77(1), pp. 99–116,(2015).

[89] Y. Niho, *Multi-valued cross-correlation functions between two maxmal linear recursive sequences*, Ph.D. Thesis, University of Southern California, 1972.

[90] K. Nyberg, "Differentially uniform mappings for cryptography", *Eurocrypt'93, Lecture Notes in Computer Science*, 765, pp. 55–64 (1994).

[91] C. M.O'Keefe and T. Penttila, "Automorphism Groups of Generalized Quadrangles via an Unusual Action of $P\Gamma L(2,2^h)$," European Journal pf Combinatorics, 33, pp. 213-232 (2002).

[92] C. M. O'Keefe, and T. Penttila, "A new hyperoval in $PG(2,32)$", *Journal of Geometry*, 44, pp. 117–139, 1992.

[93] J. D. Olsen, R. A. Scholtz, and L.R. Welch, "Bent-functions sequences", *IEEE Transaction on Information Theory*, 28(6), pp. 858–864 (1982).

[94] S. E. Payne, "A new infinite family of generalized quadrangles", Congressus Numerantium, 49, pp. 115–128 (1985).

[95] S. E. Payne, *Multi-valued cross-correlation function between two maximal recursive sequences*, Ph.D Thesis, University of Southern California, 1972.

[96] O. S. Rothaus, " On bent functions", *Journal of Combinatorial Theory, Ser. A*, 20(3), pp. 300–305 (1976).

[97] D. Sarwate and M. Pursley, "Crosscorrelation properties of pseudorandom and related sequences", *Proceedings of IEEE*, 68, pp. 593–619 (1980).

[98] B. Serge, “Ovali e curve $\sigma$ nei piani di Galois di caratteristica due”, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.*, 8(32), pp. 785–790 (1962).

[99] V. Sidelnikov, “ On mutual correlation of sequences”, *Soviet Mathematics. Dokladi Akademii Nauk USSR*,12, pp. 19–201 (1971).

[100] H. Taniguchi, “ On some quadratic APN functions”, *Designs, Codes and Cryptography* 87, pp.1973–1983 (2019).

[101] Y. Yu, M. Wang, and Y. Li, “ A matrix approach for constructing quadratic APN functions”, *Designs, Codes and Cryptography*, 73(2), pp. 587–600, (2014).

[102] L. R. Welch, *Cross-Correlation and Quadratic Forms*, Department of Electrical Engineering, University of Southern California, Los Angeles, California, unpublished notes.

[103] S. Yoshiara, “Equivalences among plateauted APN functions”, *Design, Codes and Cryptography*, 85(2), pp. 205–217 (2017).

[104] S. Yoshiara, “ Equivalences of power APN functions with power or quadratic APN functions”, *Journal of Algebraic Combinatorics*, 44(3), pp. 561–485 (2016).

[105] S. Yoshiara, “ Equivalences of quadratic APN functions”, *Journal of Algebraic Combinatorics* 35, pp. 461–475 (2012).

[106] Y. Zhou, and A. Pott. “A New Family of Semifields with 2 Parameters”, *Advances in Mathematics*, 234, pp. 43–60 (2013).

# CHAPTER 2

PAPERS

# Paper I

## Relation between o-equivalence and EA-equivalence for Niho bent functions

Diana Davidova, Lilya Budaghyan, Claude Carlet, Tor Helleseth, Ferdinand Ihringer, and Tim Penttila
*Finite Fields and Their Applications*, 72, pp. 1–42 (2021)

# Relation between o-equivalence and EA-equivalence for Niho bent functions*

Diana Davidova,† Lilya Budaghyan,† Claude Carlet,‡†
Tor Helleseth,† Ferdinand Ihringer,§ Tim Penttila¶

**Abstract**

Boolean functions, and bent functions in particular, are considered up to so-called EA-equivalence, which is the most general known equivalence relation preserving bentness of functions. However, for a special type of bent functions, so-called Niho bent functions there is a more general equivalence relation called o-equivalence which is induced from the equivalence of o-polynomials. In the present work we study, for a given o-polynomial, a general construction which provides all possible o-equivalent Niho bent functions, and we considerably simplify it to a form which excludes EA-equivalent cases. That is, we identify all cases which can potentially lead to pairwise EA-inequivalent Niho bent functions derived from o-equivalence of any given Niho bent function. Furthermore, we determine all pairwise EA-inequivalent Niho bent functions arising from all known o-polynomials via o-equivalence.

**Keywords:** Bent function, Boolean function, EA-equivalence, maximum nonlinearity, Magic action, modified Magic action, Niho bent function, o-equivalence, o-polynomials, ovals, hyperovals, Walsh transform.

## 1 Introduction

Boolean functions of $n$ variables are binary functions over the vector space $\mathbb{F}_2^n$ of all binary vectors of length $n$, and can be viewed as functions over the Galois field $\mathbb{F}_{2^n}$, thanks to the choice of a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. In this paper, we shall always have this last viewpoint. Boolean functions are used in the pseudo-random generators of stream ciphers and play a central role in their security.

Bent functions, introduced by Rothaus [38] in 1976, are Boolean functions having an even number of variables $n$, that are maximally nonlinear in the sense that their nonlinearity, the minimum Hamming distance to all affine functions, is optimal (for more

*Some results of this paper were presented at Irsee 2014 conference, BFA 2018 and BFA 2019 workshops.

†Department of Informatics, University of Bergen, PB 7803, N-5020 Bergen, Norway, e-mail: {Diana.Davidova, Lilya.Budaghyan, Tor.Helleseth}@uib.no

‡Department of Mathematics, Universities of Paris 8 and Paris 13, 2 rue de la liberté, 93526 Saint-Denis Cedex, France, e-mail: claude.carlet@gmail.com

§Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Belgium, e-mail: ferdinand.ihringer@ugent.be

¶School of Mathematical Sciences, University of Adelaide, Adelaide SA 5005, Australia, e-mail: penttila86@msn.com

information on bent functions see, for instance, [13]). This corresponds to the fact that their Walsh transform takes the values $\pm 2^{n/2}$, only. Bent functions have attracted a lot of research interest in mathematics because of their relation to difference sets and to designs, and in the applications of mathematics to computer science because of their relations to coding theory and cryptography. Despite their simple and natural definition, bent functions admit a very complicated structure in general. An important focus of research is to find constructions of bent functions. Many methods are known and some of them allow explicit constructions. We distinguish between primary constructions giving bent functions from scratch and secondary constructions building new bent functions from one or several given bent functions (in the same number of variables or in different ones).

Boolean functions, and bent functions in particular, are considered up to so-called EA-equivalence, which is the most general known equivalence relation preserving bentness of functions [4, 5].

Bent functions are often better viewed in their bivariate representation, in the form $f(x,y)$, where $x$ and $y$ belong to $\mathbb{F}_2^m$ or to $\mathbb{F}_{2^m}$, where $m = n/2$. This representation has led to the general families of explicit bent functions which are the original Maiorana-McFarland class [32], the Partial Spreads ($PS_{ap}$) class and its generalizations to other spreads from finite geometry (see a survey in Subsection 6.1.15 of [10]); these latter classes are included in the more general but less explicit *PS* class, which is itself included in the *GPS* class. Bent functions can also be viewed in their univariate form, expressed by means of the trace function over $\mathbb{F}_{2^n}$. Finding explicit bent functions in this trace representation is usually more difficult than in the bivariate representation. References containing information on explicit primary constructions of bent functions in their bivariate and univariate forms are [10, 11, 27]. It is well known that some of these explicit constructions belong to the Maiorana-McFarland class and to the $PS_{ap}$ class. When, in the early 1970s, Dillon introduced in his thesis [19] the two above mentioned classes, he also introduced another one denoted by $H$, where bentness was proven under some conditions which were not obvious to achieve. This made class $H$ an example of a non-explicit construction: at that time, Dillon was able to exhibit only functions belonging, up to the affine equivalence (which is a particular case of EA-equivalence), to the Maiorana-McFarland class.

It was observed in [12] that the class of the, so called, Niho bent functions (introduced in [20] by Dobbertin *et al*) is, up to EA-equivalence, equal to the Dillon's class $H$. Note that functions in class $H$ are defined in their bivariate representation and Niho bent functions had originally a univariate form only. Three infinite families of Niho binomial bent functions were constructed in [20] and one of these constructions was later generalized by Leander and Kholosha [28] into a function with $2^r$ Niho exponents. Another class was also extended in [22]. In [7] it was proven that some of these infinite families of Niho bent functions are EA-inequivalent to any Maiorana-McFarland function which implied that classes $H$ and Maiorana-McFarland are different up to EA-equivalence.

In the same paper [12], the authors also showed that Niho bent functions define o-polynomials and, conversely, every o-polynomial defines a Niho bent function. They also discovered that a given o-polynomial $F$ can produce two different (up to EA-equivalence) Niho bent functions, namely, the ones derived from $F$ and its inverse $F^{-1}$. Since taking the inverse of an o-polynomial is a particular case of the equivalence of

o-polynomials, a natural question was to explore this equivalence for the construction of further EA-inequivalent cases of Niho bent functions. The first work in this direction was done in [8] where the group of transformations (introduced in [16]) of order 24 preserving the equivalence of o-polynomials was studied for relation to EA-equivalence. It was shown that these transformations can lead to up to four EA-inequivalent functions including those derived from an o-polynomial and its inverse. That is, two new transformations which can potentially provide EA-inequivalent functions from a given o-polynomial were discovered. Hence, application of the equivalence of o-polynomials can be considered as a construction method for new (up to EA-equivalence) Niho bent functions from the known ones.

Note that the group of transformations from [16] does not cover all possible transformations within equivalence of o-polynomials. A more general group of transformations, so-called the Magic action, was presented in [23], which is an action of a group of transformations acting on projective line on the set of o-permutations. In this paper we study the modified Magic action, a transformation of o-polynomials preserving projective equivalence. We show that o-polynomials are projectively equivalent if and only if they lie on the same orbit under the modified Magic action and the inverse map. Further we prove that, for a given o-polynomial, EA-inequivalent Niho bent functions can arise only from a specific formula involving particular compositions of transformations of the modified magic action and the inverse map. We show that each o-monomial can define up to four EA-inequivalent bent functions. We prove, for instance, that the Pyne hyperoval can give rise to EA-inequivalent Niho bent functions defined by o-polynomials which lie on 3 different orbits of the modified Magic action. For each of the known o-polynomials we provide an explicit number of pairwise EA-inequivalent Niho bent functions which can be derived via o-equivalence. Moreover, we give an explicit description (involving transformations of the modified magic action and the inverse map) of all o-polynomials providing pairwise EA-inequivalent Niho bent functions.

The paper is organized as follows. In Section 2 we recall necessary background, in Section 3 we define Niho bent functions via o-polynomials and vice versa. In Section 4 we prove that the affine equivalence of o-polynomials yields in some cases the EA-equivalence of the corresponding Niho bent functions. The known fact that every o-polynomial on $\mathbb{F}_{2^m}$ necessarily defines a vectorial Niho bent function from $\mathbb{F}_{2^{2m}}$ to $\mathbb{F}_{2^m}$ can be seen as a corollary. In Section 5 the modified magic action is introduced and it is proven that potentially EA-inequivalent Niho bent functions can arise from o-polynomials which lie on the same orbit under the modified Magic action and the inverse map. The main results of the paper are contained in Sections 6 and 7, where we obtain an exact form of the orbit on which o-polynomials should lie to produce potentially EA-inequivalent Niho bent functions. For each of the known o-polynomials we provide the explicit number and representations for all equivalent o-polynomials which provide pairwise EA-inequivalent Niho bent functions.

## 2 Notation and Preliminaries

## 2.1 Trace Representation, Boolean Functions in Univariate and Bivariate Forms

For any positive integer $k$ and any $r$ dividing $k$, the trace function $\mathrm{Tr}_r^k$ is the mapping from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$ defined by

$$\mathrm{Tr}_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \quad .$$

In particular, the *absolute trace* over $\mathbb{F}_{2^k}$ is the function $\mathrm{Tr}_1^k(x) = \sum_{i=0}^{k-1} x^{2^i}$ (in what follows, we just use $\mathrm{Tr}_k$ to denote the absolute trace). Recall that the trace function satisfies the transitivity property $\mathrm{Tr}_k = \mathrm{Tr}_r \circ \mathrm{Tr}_r^k$.

The univariate representation of a Boolean function is defined as follows: we identify $\mathbb{F}_2^n$ (the $n$-dimensional vector space over $\mathbb{F}_2$) with $\mathbb{F}_{2^n}$ and consider the arguments of $f$ as elements in $\mathbb{F}_{2^n}$. An inner product in $\mathbb{F}_{2^n}$ is $x \cdot y = \mathrm{Tr}_n(xy)$. There exists a unique univariate polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ over $\mathbb{F}_{2^n}$ that represents $f$ (this is true for any vectorial function from $\mathbb{F}_{2^n}$ to itself and therefore for any Boolean function since $\mathbb{F}_2$ is a subfield of $\mathbb{F}_{2^n}$). The algebraic degree of $f$ is equal to the maximum 2-weight of the exponents of those monomials with nonzero coefficients in the univariate representation, where the 2-weight $w_2(i)$ of an integer $i$ is the number of ones in its binary expansion. Moreover, $f$ being Boolean, its univariate representation can be written uniquely in the form of

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_{o(j)}(a_j x^j) + a_{2^n-1} x^{2^n-1} \quad ,$$

where $\Gamma_n$ is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $2^n - 1$ (with respect to 2), $o(j)$ is the size of the cyclotomic coset containing $j$, $a_j \in \mathbb{F}_{2^{o(j)}}$ and $a_{2^n-1} \in \mathbb{F}_2$. The function $f$ can also be written in a non-unique way as $\mathrm{Tr}_n(P(x))$ where $P(x)$ is a polynomial over $\mathbb{F}_{2^n}$.

The bivariate representation of a Boolean function is defined in this paper as follows: we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ (where $n = 2m$) and consider the argument of $f$ as an ordered pair $(x,y)$ of elements in $\mathbb{F}_{2^m}$. There exists a unique bivariate polynomial $\sum_{0 \le i,j \le 2^m-1} a_{i,j} x^i y^j$ over $\mathbb{F}_{2^m}$ that represents $f$. The algebraic degree of $f$ is equal to $\max_{(i,j)\,|\,a_{i,j} \neq 0}(w_2(i) + w_2(j))$. And $f$ being Boolean, its bivariate representation can be written in the form $f(x,y) = \mathrm{Tr}_m(P(x,y))$, where $P(x,y)$ is some polynomial of two variables over $\mathbb{F}_{2^m}$.

**Remark 1.** *Let $g(x,y)$ be a Boolean function over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then one can get a univariate representation of $g$ making the following substitutions:*

$$x = t + t^{2^m} \text{ and } y = \alpha t + (\alpha t)^{2^m},$$

*where $\alpha$ is a primitive element of $\mathbb{F}_{2^{2m}}$.*

## 2.2 Walsh Transform and Bent Functions

Let $f$ be an $n$-variable Boolean function. Its *"sign" function* is the integer-valued function $\chi_f := (-1)^f$. The *Walsh transform* of $f$ is the discrete Fourier transform of $\chi_f$

whose value at point $w \in \mathbb{F}_{2^n}$ is defined by

$$\widehat{\chi}_f(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_n(wx)} \quad .$$

For even $n$, a Boolean function $f$ in $n$ variables is said to be *bent* if for any $w \in \mathbb{F}_{2^n}$ we have $\widehat{\chi}_f(w) = \pm 2^{\frac{n}{2}}$.

It is well known (see, for instance, [11]) that the algebraic degree of a bent Boolean function in $n > 2$ variables is at most $\frac{n}{2}$.

Bentness and algebraic degree (when larger than 1) are preserved by extended-affine (EA-) equivalence. Two Boolean functions $f$ and $g$ in $n$ variables are called *EA-equivalent* if there exists an affine permutation $A$ of $\mathbb{F}_{2^n}$ and an affine Boolean function $\ell$ such that $f = g \circ A + \ell$. If $l = 0$ then $f$ and $g$ are called *affine equivalent*. In the case of vectorial functions there exists a more general notion of equivalence, called *CCZ-equivalence*, but for Boolean functions, it reduces to EA-equivalence, see [4] (as well as for bent vectorial functions [5]).

Two functions $F$ and $F'$ from $\mathbb{F}_{2^n}$ to itself are called EA-equivalent if $A_1 \circ F \circ A_2 + A$ for some affine permutations $A_1$ and $A_2$ and for some affine function $A$. If $A = 0$ then $F$ and $F'$ are called affine equivalent.

For positive integers $n$ and $t$, a vectorial Boolean function $F$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^t$ is called bent if for any $a \in \mathbb{F}_2^n \setminus \{0\}$ the Boolean function $a \cdot F(x)$ is bent. Bent functions exist if and only if $n$ is even and $t \leq n/2$ (see [33]).

## 2.3 Projective plane, Ovals, Hyperovals

In the following we give a short introduction to the projective plane. We refer to [18] for a detailed introduction to projective geometry. A projective plane consists of a set of *points P*, a set of *lines L*, and an incidence relation $I$ between $P$ and $L$. The classical *projective plane* $PG(2,q)$ over $\mathbb{F}_q^3$ has the 1-spaces of $\mathbb{F}_q^3$ as points and the 2-spaces of $\mathbb{F}_q^3$ as lines. A point $p$ is contained in a line $\ell$ if $p \subseteq \ell$ in $\mathbb{F}_q^3$. A set of points is called *collinear* if they all lie on the same line. Note that $PG(2,q)$ has $q^2+q+1$ points, $q^2+q+1$ lines, each line contains $q+1$ points, and each point lies in $q+1$ lines. The group $P\Gamma L(3,q)$ acts naturally on $PG(2,q)$. In particular, it preserves incidence.

Let $\mathscr{O}$ be a set of points in $PG(2,q)$ such that no three points are collinear. It is well-known that $|\mathscr{O}| \leq q+1$ if $q$ is odd and $|\mathscr{O}| \leq q+2$ is $q$ is even. One can see this as follows: Consider a point $P \in \mathscr{O}$. Each of the $q+1$ lines on $P$ contains at most one more points, so $|\mathscr{O}| \leq q+2$. Suppose that equality holds. Then each line contains either 0 or 2 points. Consider a point $R \in \mathscr{O}$. Then there are $s$ lines through $R$ with 2 points and $q+1-s$ lines through $R$ with 0 points. Hence, $q+2 = 2s$, so $q$ is even.

Call a line $\ell$ *passant*, *tangent*, respectively, *secant* if $|\ell \cap \mathscr{O}| = 0$, $|\ell \cap \mathscr{O}| = 1$, respectively, $|\ell \cap \mathscr{O}| = 2$. If $|\mathscr{O}| = q+1$, then $\mathscr{O}$ is called an *oval*. From the argument above it follows that in this case each point of $\mathscr{O}$ lies on exactly one tangent and $q$ secants. For $q$ even these secants all meet in one point $N$, the *nucleus* of $\mathscr{O}$. If $|\mathscr{O}| = q+2$, then $\mathscr{O}$ is called a *hyperoval* and we usually write $\mathscr{H}$ instead of $\mathscr{O}$. If $|\mathscr{O}| = q+1$ and $q$ even, then $\mathscr{O} \cup \{N\}$ is a hyperoval.

In the following we limit ourselves to $q = 2^m$ even.

A *frame* of $PG(2,q)$ is a set of four points $\mathscr{P} = \{P_1, P_2, P_3, P_4\}$ such that any 3-subset of $\mathscr{P}$ spans $\mathbb{F}_q^3$. The fundamental theorem of projective geometry (for projective planes) states that $P\Gamma L(3,q)$ acts transitive on frames. As any four points of a hyperoval $\mathscr{H}$ are a frame, we can assume that an oval $\mathscr{O}$ contains $\langle(1,0,0)\rangle, \langle(0,0,1)\rangle, \langle(1,1,1)\rangle \in \mathscr{O}$ and has $\langle(0,1,0)\rangle$ as its nucleus. In the following we usually leave out the brackets $\langle\cdot\rangle$ for the sake of readibility. Hence, we can write $\mathscr{O}$ as

$$\mathscr{O} = \{(x, F(x), 1) : x \in \mathbb{F}_{2^m}\} \cup \{(1,0,0)\},$$

where the polynomial $F$ satisfies the following:

(a) $F$ is a permutation polynomial over $\mathbb{F}_{2^m}$ of degree at most $q-2$ satisfying $F(0) = 0$ and $F(1) = 1$.

(b) For any $s \in \mathbb{F}_{2^m}^*$ the function

$$F_s(x) := \begin{cases} \frac{F(x+s)+F(x)}{x} & \text{if } x \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

is a permutation polynomial. Here and further int he paper we denote $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$.

Such a polynomial $F$ is called an *o-polynomial* and, conversely, each o-polynomial defines an oval. If we do not require $F(1) = 1$, then $F$ is called an *o-permutation*. We write $\mathscr{O}(F)$ for the oval defined by the o-polynomial $F$, and we write $\mathscr{H}(F)$ for the hyperoval defined by $F$.

Note that throughout this paper $\mathscr{O}$ consists of points of the form $(x, F(x), 1)$, while in the hyperplane literature, usually the form $(1, x, f(x))$ is used.

For a hyperoval $\mathscr{H}$ we have $2^m + 2$ choices for the nucleus $N \in \mathscr{H}$ to obtain an oval $\mathscr{H} \setminus \{N\}$. Hence, each hyperoval $\mathscr{H}$ defines $2^m + 2$ o-polynomials. Two o-polynomials are called *(projectively) equivalent*, if they define equivalent hyperovals (under the natural action of $P\Gamma L(3,q)$).

## 2.4 Niho Bent Functions

A positive integer $d$ (always understood modulo $2^n - 1$ with $n = 2m$) is a *Niho exponent* and $t \to t^d$ is a *Niho power function* if the restriction of $t^d$ to $\mathbb{F}_{2^m}$ is linear or, equivalently, if $d \equiv 2^j \pmod{2^m - 1}$ for some $j < n$. As we consider $\mathrm{Tr}_n(at^d)$ with $a \in \mathbb{F}_{2^n}$, without loss of generality, we can assume that $d$ is in the normalized form, i.e., with $j = 0$. Then we have a unique representation $d = (2^m - 1)s + 1$ with $2 \leq s \leq 2^m$. If some $s$ is written as a fraction, this has to be interpreted modulo $2^m + 1$ (e.g., $1/2 = 2^{m-1} + 1$). Following are examples of bent functions consisting of one or more Niho exponents:

1. Quadratic function $\mathrm{Tr}_m(at^{2^m+1})$ with $a \in \mathbb{F}_{2^m}^*$ (here $s = 2^{m-1} + 1$).

2. Binomials of the form $f(t) = \mathrm{Tr}_n(\alpha_1 t^{d_1} + \alpha_2 t^{d_2})$, where $2d_1 \equiv 2^m + 1 \pmod{2^n - 1}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}^*$ are such that $(\alpha_1 + \alpha_1^{2^m})^2 = \alpha_2^{2^m+1}$. Equivalently, denoting $a = (\alpha_1 + \alpha_1^{2^m})^2$ and $b = \alpha_2$ we have $a = b^{2^m+1} \in \mathbb{F}_{2^m}^*$ and

$$f(t) = \mathrm{Tr}_m(at^{2^m+1}) + \mathrm{Tr}_n(bt^{d_2}).$$

We note that if $b = 0$ and $a \neq 0$ then $f$ is a bent function listed under number 1. The possible values of $d_2$ are [20, 22]:

$$d_2 = (2^m - 1)3 + 1,$$
$$6d_2 = (2^m - 1) + 6 \text{ (taking } m \text{ even)}.$$

These functions have algebraic degree $m$ and do not belong to the completed Maiorana-McFarland class [7].

3. Take $1 < r < m$ with $\gcd(r,m) = 1$ and define

$$f(t) = \mathrm{Tr}_n\left(a^2 t^{2^m+1} + (a + a^{2^m}) \sum_{i=1}^{2^{r-1}-1} t^{d_i}\right), \tag{1}$$

where $2^r d_i = (2^m - 1)i + 2^r$ and $a \in \mathbb{F}_{2^n}$ is such that $a + a^{2^m} \neq 0$ [28, 29]. This function has algebraic degree $r+1$ (see [6]) and belongs to the completed Maiorana-McFarland class [14].

4. Bent functions in a bivariate representation obtained from the known o-polynomials.

Consider the listed above two binomial bent functions. If $\gcd(d_2, 2^n - 1) = d$ and $b = \beta^d$ for some $\beta \in \mathbb{F}_{2^n}$ then $b$ can be "absorbed" in the power term $t^{d_2}$ by a linear substitution of variable $t$. In this case, up to EA-equivalence, $b = a = 1$. In particular, this applies to any $b$ when $\gcd(d_2, 2^n - 1) = 1$ that holds in both cases except when $d_2 = (2^m - 1)3 + 1$ with $m \equiv 2 \pmod 4$ where $d = 5$. In this exceptional case, we can get up to 5 different classes but the exact situation has to be further investigated.

## 3 Class $\mathscr{H}$ of Bent Functions and o-polynomials

Here we restrict ourselves with fields $\mathbb{F}_{2^n}$ with $n$ even, $n = 2m$.

In his thesis [19], Dillon introduced the class of bent functions denoted by $H$. The functions in this class are defined in their bivariate form as

$$f(x,y) = Tr_m(y + xF(yx^{2^m-2})),$$

where $x, y \in \mathbb{F}_{2^m}$, and

- $F$ is a permutation of $\mathbb{F}_{2^m}$ s.t. $F(x) + x$ doesn't vanish,
- for any $\beta \in \mathbb{F}_{2^m}^*$ the function $F(x) + \beta x$ is 2-to-1.

Dillon was able to exhibit bent functions in $H$ that also belong to the completed Maiorana-McFarland class. Dillon's class $H$ was modified in [12] into a class $\mathscr{H}$ of the functions:

$$g(x,y) = \begin{cases} Tr_m\left(xG\left(\frac{y}{x}\right)\right), \text{ if } x \neq 0 \\ Tr_m(\mu y), \text{ otherwise} \end{cases} \tag{2}$$

where $\mu \in \mathbb{F}_{2^m}, G : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ satisfying the following conditions:

$$F : z \mapsto G(z) + \mu z \text{ is a permutation over } \mathbb{F}_{2^m}, \tag{3}$$

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \tag{4}$$

Here condition (4) implies condition (3) and it is necessary and sufficient for $g$ being bent. Functions in $\mathscr{H}$ and the Dillon class are the same up to addition of a linear term $Tr_m((\mu+1)y)$ to (2). Niho bent functions are functions in $\mathscr{H}$ in their univariant representation.

**Theorem 1** ([12]). *A polynomial $F$ on $\mathbb{F}_{2^m}$ satisfying $F(0) = 0$ and $F(1) = 1$ is an o-polynomial if and only if*

$$z \mapsto F(z) + \beta z \text{ is 2-to-1 on } \mathbb{F}_{2^m} \text{ for any } \beta \in \mathbb{F}_{2^m}^*. \tag{5}$$

Hence, obviously every o-polynomial defines a Niho bent function. And vice versa, every Niho bent function defines an o-polynomial since it defines a polynomial $F$ satisfying condition (5) of Theorem 1, and we can derive an o-polynomial $F'(x) = \frac{F(x)+F(0)}{F(1)+F(0)}$ which fixes the requirements $F'(0) = 0$ and $F'(1) = 1$. Note that to get a Niho bent function from a polynomial $F$ it is sufficient that $F$ satisfies only condition (5) while the conditions $F(0) = 0$ and $F(1) = 1$ are not necessary.

In Section 2.3 we saw that each o-polynomial corresponds to a hyperoval and vice versa, each hyperoval corresponds to an o-polynomial. We say that Niho bent functions are *o-equivalent* if they define projectively equivalent hyperovals. As shown in [8, 12], o-equivalent Niho bent functions may be EA-inequivalent. For example, Niho bent functions defined by o-polynomials $F$ and $F^{-1}$ are o-equivalent but they are, in general, EA-inequivalent.

Here is the list of all known o-polynomials (we also give names of the corresponding hyperovals):

1. $F(x) = x^2$, *regular hyperoval*;
2. $F(x) = x^{2^i}$, $i$ and $m$ are coprime, $i > 1$, *irregular translation hyperoval*;
3. $F(x) = x^6$, $m$ is odd, *Segre hyperoval*;
4. $F(x) = x^{3\cdot 2^k+4}$, $m = 2k-1$, *Glynn I*;
5. $F(x) = x^{2^k+2^{2k}}$, $m = 4k-1$, *Glynn II*;
6. $F(x) = x^{2^{2k+1}+2^{3k+1}}$, $m = 4k+1$, *Glynn II*;
7. $F(x) = x^{2^k} + x^{2^k+2} + x^{3\cdot 2^k+4}$, $m = 2k-1$, *Cherowitzo hyperoval*;
8. $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$, $m$ is odd, *Payne hyperoval*;
9. $F(x) = \dfrac{\delta^2(x^4+x) + \delta^2(1+\delta+\delta^2)(x^3+x^2)}{x^4+\delta^2x^2+1} + x^{\frac{1}{2}}$,

   where $Tr_m(\frac{1}{\delta}) = 1$ (if $m \equiv 2 \pmod 4$, then $\delta \notin \mathbb{F}_4$), *Subiaco hyperoval* (for $m = 4$ also known as *Lunelli-Sce hyperoval*);

10. $F(x) = \frac{1}{Tr_m^n}(v)\Big(Tr_m^n(v^r)(x+1) + (x + Tr_m^n(v)x^{\frac{1}{2}} + 1)^{1-r} Tr_m^n(vx + v^{2^m})^r\Big) + x^{\frac{1}{2}}$, where $m$ is even, $r = \pm\frac{2^m-1}{3}$, $v \in \mathbb{F}_{2^{2m}}, v^{2^m+1} \neq 1, v \neq 1$, *Adelaide hyperoval*.
11. $F(x) = x^4 + x^{16} + x^{28} + \omega^{11}(x^6 + x^{10} + x^{14} + x^{18} + x^{22} + x^{26}) + \omega^{20}(x^8 + x^{20}) + \omega^6(x^{12} + x^{24})$ with $\omega^5 = \omega^2 + 1$ and $m = 5$, *O'Keefe-Penttila hyperoval*.

Note that an o-polynomial $F$ defined on $\mathbb{F}_{2^m}$ has the following form [18]:

$$F(x) = \sum_{k=1}^{\frac{2^m-2}{2}} b_{2k} x^{2k}.$$

A comprehensive survey on the class $\mathscr{H}$, bent functions and o-polynomias can be found in [31], Chapter 8.

# 4 Vectorial Niho bent functions from o-polynomials

It is known since 2011 that every o-polynomial defines a Boolean Niho bent function [12]. In this section, we revisit the fact that, actually, every o-polynomial on $\mathbb{F}_{2^m}$ defines a vectorial Niho bent function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. This connection has been originally observed in [30]. In the present paper, we derive this result by studying some simple transformations of o-polynomials.

Below we show that in some cases, affine equivalence of o-polynomials yields EA-equivalence of the corresponding Niho bent functions. Note that in general if a function $F'$ is affine equivalent to an o-polynomial $F$ then $F'$ is not necessarily an o-polynomial.

**Lemma 1.** *Let $F$ be an o-polynomial defined on $\mathbb{F}_{2^m}$ and $a, b \in \mathbb{F}_{2^m}^*$. Then $G(x) = aF(bx)$ is an o-polynomial on $\mathbb{F}_{2^m}$ if and only if $a = \frac{1}{F(b)}$ (or, what is the same, $b = F^{-1}(a^{-1})$). The Niho bent functions defined by the o-polynomials $F$ and $G = \frac{1}{F(b)}F(bx)$ are affine equivalent.*

*Proof.* Suppose $G(x) = aF(bx)$ is an o-polynomial, then $G(0) = aF(0) = 0$ for any $a, b \in \mathbb{F}_{2^m}$ and $1 = G(1) = aF(b)$, hence $G$ is an o-polynomial if and only if $a = \frac{1}{F(b)}$.
The Niho bent function corresponding to the o-polynomial $F$ is $f(x,y) = Tr_m(xF(\frac{y}{x}))$, and the one corresponding to $G$ is
$g(x,y) = Tr_m(xG(\frac{y}{x})) = Tr_m(xaF(b\frac{y}{x})) = Tr_m(xaF(\frac{aby}{ax})) = Tr_m(vF(\frac{u}{v}))$,
where $v = ax$ , $u = aby$. Hence, $g = f \circ A$ with $A(x,y) = (ax, aby)$, and, therefore, $f$ and $g$ are affine equivalent. □

**Corollary 1.** *For every o-polynomial $F$ defined on $\mathbb{F}_{2^m}$ the function $xF(\frac{y}{x})$ from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is bent. That is, every o-polynomial on $\mathbb{F}_{2^m}$ defines a vectorial Niho bent function $xF(\frac{y}{x})$ from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.*

*Proof.* From Lemma 1 we have that for a given o-polynomial $F$ and any $a \in \mathbb{F}_{2^m}^*$ the function $g(x,y) = Tr_m(axF(\frac{by}{x}))$ is Niho bent where $b = F^{-1}(a^{-1})$. Then the function

$\bar{g}(x,y) = Tr_m(axF(\frac{y}{x}))$ is also bent since $g$ and $\bar{g}$ are affine equivalent, that is, $g = \bar{g} \circ A$ with $A(x,y) = (x, by)$, and clearly, such a transformation $A$ keeps $\bar{g}$ as a Niho function. □

**Lemma 2.** *Let $F$ be an o-polynomial on $\mathbb{F}_{2^m}$ and $A(x) = x^{2^j}$ be an automorphism over $\mathbb{F}_{2^m}$. Then the Niho bent functions defined by o-polynomials $F$ and $G = A \circ F \circ A^{-1}$ are affine equivalent.*

*Proof.* Obviously if $F$ is an o-polynomial, then $G(x) = (F(x^{2^{-j}}))^{2^j}$ is also an o-polynomial. Consider the Niho bent function defined by $G$:

$$g(x,y) = Tr_m\Big(xG\Big(\frac{y}{x}\Big)\Big) = Tr_m\Big(xA \circ F \circ A^{-1}\Big(\frac{y}{x}\Big)\Big) =$$
$$Tr_m\Big(x\Big(F\Big(\Big(\frac{y}{x}\Big)^{2^{-j}}\Big)\Big)^{2^j}\Big) = Tr_m\Big(x^{2^{-j}}F\Big(\Big(\frac{y}{x}\Big)^{2^{-j}}\Big)\Big) = Tr_m\Big(uF\Big(\frac{v}{u}\Big)\Big),$$

where $u = x^{2^{-j}}$ and $v = y^{2^{-j}}$. Thus, $f$ and $g$ are affine equivalent ($g = f \circ A$ with $A(x,y) = (x,y)^{2^{-j}}$). □

**Lemma 3.** *Let $F$ be an o-polynomial on $\mathbb{F}_{2^m}$ and $A_1(x) = x + a$ and $A_2(x) = x + b$ for $a, b \in \mathbb{F}_{2^m}$. Then $G = A_1 \circ F \circ A_2$ is an o-polynomial on $\mathbb{F}_{2^m}$ if and only if $b = F(a)$ and $F(a+1) + F(a) = 1$. Furthermore, the Niho bent functions defined by o-polynomials $F$ and $G$ are EA-equivalent.*

*Proof.* Suppose $G(x) = A_1 \circ F \circ A_2(x) = F(x+a) + b$ is an o-polynomial. Then $0 = G(0) = F(a) + b$ and, therefore, $F(a) = b$ and $1 = G(1) = F(1+a) + b = F(1+a) + F(a)$.
Further we have
$g(x,y) = Tr_m\Big(xA_1 \circ F \circ A_2\Big(\frac{y}{x}\Big)\Big) = Tr_m\Big(x\Big(F\Big(\frac{y}{x} + a\Big) + b\Big)\Big) =$
$Tr_m\Big(xF\Big(\frac{y+ax}{x}\Big)\Big) + Tr_m(bx) = Tr_m\Big(xF\Big(\frac{u}{x}\Big)\Big) + Tr_m(bx),$

where $u = y + ax$. Thus, $g$ and $f$ are EA-equivalent ($g = f \circ A + l$ with $A(x,y) = (x, y+ax)$ and $l(x,y) = Tr_m(bx)$). □

# 5 The modified Magic action

Let $\mathscr{F}$ be the collection of all functions $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ such that $F(0) = 0$.

The following set

$$P\Gamma L(2,2^m) = \{x \mapsto Ax^{2^j} | A \in GL(2,\mathbb{F}_{2^m}), 0 \le j \le m-1\}$$

is a group of transformations acting on the projective lines, i.e. on the set with the elements of the form: $\{(a \cdot x, a \cdot y) | (x,y) \neq (0,0), x, y \in \mathbb{F}_{2^m}, a \neq 0\}$.

An action of the group $P\Gamma L(2,2^m)$ on $\mathscr{F}$ was introduced and described in [23]. Define the image of $F \in \mathscr{F}$ under the transformation $\psi \in P\Gamma L(2,2^m)$, $\psi : x \mapsto Ax^{2^j}$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,2^m)$, $0 \le j \le m-1$, as a function $\psi F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ such that

$$\psi F(x) = |A|^{-\frac{1}{2}}\Big[(bx+d)F^{2^j}\Big(\frac{ax+c}{bx+d}\Big) + bxF^{2^j}\Big(\frac{a}{b}\Big) + dF^{2^j}\Big(\frac{c}{d}\Big)\Big].$$

This yields an action of $P\Gamma L(2,2^m)$ on $\mathscr{F}$, which is called *the magic action*. The magic action takes o-permutations to o-permutations and it is a semi-linear transformation, i.e.
$\psi(F+G)=\psi F+\psi G$, for any $F,G\in\mathscr{F}$,
$\psi aF=a^{2^j}\psi F$, for any $a\in\mathbb{F}_{2^m}$, $F\in\mathscr{F}$, $0\le j\le m-1$.

Let us recall two theorems (Theorem 4 and Theorem 6) from [23]. For a given o-polynomial $F$ denote $\mathscr{O}(F)$ the oval defined by $F$.

**Theorem 2.** *[23] Let $F$ be an o-permutation on $\mathbb{F}_{2^m}$ and let $\psi\in P\Gamma L(2,2^m)$ be $\psi: x\mapsto Ax^{2^j}$ for $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL(2,\mathbb{F}_{2^m})$ and $0\le j\le m-1$. Then $G=\psi F$ is also an o-permutation on $\mathbb{F}_{2^m}$. In fact, $\mathscr{O}(G)=\bar{\psi}(\mathscr{O}(F))$, where $\bar{\psi}\in P\Gamma L(3,2^m)$ is defined by $\bar{\psi}: x\mapsto \bar{A}x^{2^j}$, where $\bar{A}=\begin{pmatrix} d & 0 & c\\ b\psi F(\frac{d}{b}) & |A|^{\frac{1}{2}} & a\psi F(\frac{c}{a})\\ b & 0 & a\end{pmatrix}$.*

Note that the formulation of the theorem above differs from the one in [23] because in the current paper (following notations of [8]) the points of the oval (or the hyperoval) defined by an o-polynomial $F$ are considered as $(x,F(x),1)$, meanwhile in [23] the form $(1,x,F(x))$ is used.

**Theorem 3.** *[23] Let $F$ and $G$ be o-permutations on $\mathbb{F}_{2^m}$, and suppose further that the ovals defined by $F$ and $G$, i.e. $\mathscr{O}(F)$ and $\mathscr{O}(G)$ are equivalent under $P\Gamma L(3,2^m)$. Then there exists $\psi\in P\Gamma L(2,2^m)$ such that $G=\psi F$.*

The magic action can be also described by a collection of generators of $P\Gamma L(2,2^m)$ [23]:

$$\begin{aligned}
&\sigma_a: x\mapsto \begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}x,\ \sigma_aF(x)=a^{-\frac{1}{2}}F(ax),\ a\in\mathbb{F}_{2^m}^*;\\
&\tau_c: x\mapsto \begin{pmatrix}1 & 0\\ c & 1\end{pmatrix}x,\ \tau_cF(x)=F(x+c)+F(c),\ c\in\mathbb{F}_{2^m};\\
&\varphi: x\mapsto \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}x,\ \varphi F(x)=xF(x^{-1});\\
&\rho_{2^j}: x\mapsto x^{2^j},\ \rho_{2^j}F(x)=(F(x^{-2^j}))^{2^j},\ 0\le j\le m-1.
\end{aligned}\tag{6}$$

We slightly modify the magic action generators $\sigma_a$ and $\tau_c$ multiplying them by appropriate constants to preserve the image of 1 at 1:

$$\begin{aligned}
&\tilde{\sigma}_aF(x)=\frac{a^{\frac{1}{2}}}{F(a)}\sigma_aF(x)=\frac{1}{F(a)}F(ax),\ a\in\mathbb{F}_{2^m}^*;\\
&\tilde{\tau}_cF(x)=\frac{1}{F(1+c)+F(c)}\tau_cF(x)=\frac{1}{F(1+c)+F(c)}(F(x+c)+F(c)),\ c\in\mathbb{F}_{2^m}.
\end{aligned}\tag{7}$$

The new set of generators

$$H=\{\tilde{\sigma}_a,\tilde{\tau}_c,\varphi,\rho_{2^j}|0\le j\le m-1,c\in\mathbb{F}_{2^m},a\in\mathbb{F}_{2^m}^*$$

preserves the property $F(1) = 1$ of the function $F$.

The action of the group with the new set of generators $H$ on the set of all functions $F$ defined on $\mathbb{F}_{2^m}$ with the properties $F(0) = 0$ and $F(1) = 1$ will be called *the modified magic action*.

**Proposition 1.** *Two o-polynomials arise from equivalent hyperovals if and only if they lie on the same orbit of the group generated by H and the inverse map.*

*Proof.* According to the first part of Theorem 2, the magic action takes o-permutations to o-permutations. Since the generators of the modified magic action differ from the original magic action generators only by constant coefficient (what allows as to preserve the property of $F(1) = 1$ for any o-polynomial $F$), then the modified magic action takes o-polynomials to o-polynomials.

According to the second part of Theorem 2, if two o-permutations lie on the same orbit under the magic action, then the corresponding ovals are equivalent and have fixed nucleus $(0,1,0)$.
Now suppose that two o-polynomials lie on the same orbit under the modified magic action and the inverse map. Since each o-polynomial is an o-permutation, then the corresponding ovals defined by o-polynomials are equivalent and have nucleus $(0,1,0)$. As we know, each oval is contained in a unique hyperoval, which is obtained by adding nucleus to the points of oval. So, hyperovals defined by the o-polynomials on the same orbit under the modified magic action are equivalent. Also it is well known that o-polynomials $F$ and $F^{-1}$ define equivalent hyperovals. Thus, we conclude that hyperovals defined by the o-polynomials on the same orbit under the modified magic action and the inverse map are equivalent.

Let's show the converse statement. Suppose that hyperovals $\mathscr{H}(F)$ and $\mathscr{H}(G)$ defined by o-polynomials $F$ and $G$ are equivalent. It means that there is a collineation which maps $\mathscr{H}(F)$ to $\mathscr{H}(G)$. Consider the preimage of $(0,1,0)$ under this collineation, there are 3 possible cases:

1. The preimage of $(0,1,0)$ is $(0,1,0)$. It means that this collineation fixes point $(0,1,0)$. So deleting this point from hyperovals $\mathscr{H}(F)$ and $\mathscr{H}(G)$, we will get equivalent ovals with fixed nucleus, hence by Theorem 3, their generator o-polynomials are on the same orbit under the magic action, hence under the modified magic action.

2. The preimage of $(0,1,0)$ is $(1,0,0)$. Since hyperovals defined by o-polynomial and its inverse o-polynomial are equivalent, then hyperoval $\mathscr{H}(F)$ is equivalent to a hyperoval $\mathscr{H}(F^{-1})$ and by the corresponding collineation the point $(1,0,0)$ has preimage $(0,1,0)$. So, at the end we have that hyperovals $\mathscr{H}(F^{-1})$ and $\mathscr{H}(G)$ are equivalent and the preimage of $(0,1,0)$ is $(0,1,0)$. Hence by the previous case 1 (and the fact that an o-polynomial and its inverse belong to the same orbit under modified action and the inverse) o-polynomials $F$ and $G$ are on the same orbit under modified magic action and the inverse map.

The following diagram illustrates the previous decisions.

$$\begin{array}{ccccc} \mathscr{H}(F^{-1}) & \cong & \mathscr{H}(F) & \cong & \mathscr{H}(G) \\ \cup & & \cup & & \cup \\ (0,1,0) & \mapsto & (1,0,0) & \mapsto & (0,1,0) \end{array}$$

3. The preimage of $(0,1,0)$ is $(t,f(t),1)$. Choose an element $\varphi$ of $P\Gamma L(2,2^m)$ taking $(1,t)$ to $(0,1)$ (such authomorphism always exist, for example it can be defined by matrix $A=\begin{pmatrix}0&0\\1&0\end{pmatrix}$). Applying $\varphi$ to $F$ we will get a hyperoval $\mathscr{H}(\varphi F)$ equivalent to $\mathscr{H}(G)$ where the preimage of $(0,1,0)$ is $(1,0,0)$. Because of the case 2, we get that $\varphi F$ and $G$ belong to the same orbit under the modified magic action and the inverse map and so do $F$ and $G$. □

We formulate the next theorem without proof. First this result was announced in September 2014 at the Forth Isree Conference "Finite Geometries" [9] by the authors of this paper, the complete proof can be found in [1].

**Theorem 4.** *Two Niho bent functions are EA-equivalent if and only if the corresponding ovals are equivalent. Hence, the number of EA-equivalence classes of Niho bent functions arising from a hyperoval of $PG(2,2^m)$ is the number of orbits of the collineation stabiliser of the hyperoval on the points of the hyperoval.*

# 6 Niho bent functions and the modified magic action

A group of transformations of order 24 with 3 generators preserving o-polynomials was considered in [8]. This group of transformations is a subgroup of the group with the (modified) magic action generators and the inverse map. Precisely, they are the transformations generated by $\varphi$, $\tilde{\tau}_1=\tau_1$ and the inverse map. Only 4 of these transformations can lead to *EA*-inequivalent Niho bent functions [8].

As a continuation of the work of [8], let's consider the modified magic action generators, and the inverse map and see which of them give rise to EA-inequivalent Niho bent functions. From Proposition 1 it is clear that o-polynomials on the same orbit under the modified magic action and the inverse map and only they are projectively equivalent. Since we are interested in EA-inequivalent Niho bent functions arising from projectively equivalent o-polynomials, we focus on the orbits of the modified magic action together with the inverse map. We prove below that to get EA-inequivalent Niho bent functions from a given o-polynomial it is sufficient to use only $\tilde{\tau}$ and $\varphi$ generators together with inverse map while $\rho$ and $\tilde{\sigma}$ do not play any role in it. Moreover, we show that all EA-inequivalent Niho bent functions can be obtained from a special formula.

## 6.1 Preliminary results

Following notations of [8] the generator $\varphi$ will be denoted by $\prime$ when needed. Let's recall the set of generators

$$H=\{\tilde{\tau}_c,\tilde{\sigma}_a,\prime,\rho_{2^j}|c\in\mathbb{F}_{2^m},a\in\mathbb{F}_{2^m}^*,0\le j\le m-1\},$$

where

$$\tilde{\sigma}_a F(x) = \frac{1}{F(a)} F(ax),\ a \in \mathbb{F}_{2^m}^*;$$
$$\tilde{\tau}_c F(x) = \alpha_F^c \tau_c F(x) = \alpha_F^c (F(x+c)+F(c)),\ c \in \mathbb{F}_{2^m}, \text{where } \alpha_F^c = \frac{1}{\tau_c F(1)};$$
$$F'(x) = \varphi F(x) = xF(x^{-1});$$
$$\rho_{2^j} F(x) = (F(x^{-2^j}))^{2^j},\ 0 \le j \le m-1;$$

and prove a few statements about the generators of magic action and the inverse map.

**Lemma 4.** *Let $F$ be an o-polynomial on $\mathbb{F}_{2^m}$. Then the following identities hold:*

$$\tilde{\tau}_c \circ \tilde{\tau}_d F = \tilde{\tau}_{c+d} F, \tag{8}$$
$$\tilde{\sigma}_a \circ \tilde{\sigma}_b F = \tilde{\sigma}_{ab} F, \tag{9}$$
$$\rho_{2^j} \circ \rho_{2^i} F = \rho_{2^{j+i}} F, \tag{10}$$

*where $a,b \in \mathbb{F}_{2^m}^*$, $c,d \in \mathbb{F}_{2^m}$, $0 \le i,j \le m-1$.*

*Proof.* To prove the first equality note that

$$\tau_c \circ \tau_d F(x) = \tau_d F(x+c) + \tau_d F(c) = F(x+c+d)+F(d)+F(c+d)+F(d) = F(x+c+d)+F(c+d) = \tau_{c+d} F.$$

Since magic action is a semilinear transformation we get:

$$\tilde{\tau}_c \circ \tilde{\tau}_d F(x) = \frac{1}{F(1+d)+F(d)} \frac{1}{\tilde{\tau}_d F(1+c)+\tilde{\tau}_d(c)} \tau_c(\tau_d(F(x))) = \frac{1}{F(1+d)+F(d)} \frac{F(1+d)+F(d)}{F(1+d+c)+F(d+c)} \tau_{c+d} F(x) = \frac{1}{F(1+d+c)+F(d+c)} \tau_{c+d} F(x) = \tilde{\tau}_{c+d} F(x).$$

The other two equalities are straightforward to prove:

$$\tilde{\sigma}_a \circ \tilde{\sigma}_b F = \frac{1}{\tilde{\sigma}_b F(a)} \tilde{\sigma}_b F(ax) = \frac{1}{\frac{1}{F(b)} F(ab)} \frac{1}{F(b)} F(abx) = \frac{1}{F(ab)} F(abx) = \tilde{\sigma}_{ab} F(x),$$
$$\rho_{2^i} \circ \rho_{2^j} F(x) = \rho_{2^i}(F(x^{\frac{1}{2^j}}))^{2^j} = F(x^{\frac{1}{2^{j+i}}})^{2^{j+i}} = \rho_{2^{i+j}} F(x).$$

□

**Corollary 2.** *Let $F$ be an o-polynomial on $\mathbb{F}_{2^m}$ and $k$ a positive integer. Then*

$$(\tilde{\sigma}_{a_1} \circ \tilde{\sigma}_{a_2} \circ \ldots \circ \tilde{\sigma}_{a_k}) F = \tilde{\sigma}_{a_1 \cdot a_2 \cdot \ldots \cdot a_k} F,$$
$$(\tilde{\tau}_{c_1} \circ \tilde{\tau}_{c_2} \circ \ldots \circ \tilde{\tau}_{c_k}) F = \tilde{\tau}_{c_1+c_2+\ldots c_k} F,$$
$$(\rho_{2^{i_1}} \circ \rho_{2^{i_2}} \circ \ldots \circ \rho_{2^{i_k}}) F = \rho_{2^{i_1+i_2+\ldots+i_k}} F,$$

*where $a_1,\ldots,a_k \in \mathbb{F}_{2^m}^*, c_1,\ldots,c_k \in \mathbb{F}_{2^m}$, $0 \le i_j \le m-1$ for all $j \in \{1,\ldots,k\}$.*

*Proof.* The proof follows by induction using Lemma 4. □

**Lemma 5.** *Let $F$ be an o-polynomial on $\mathbb{F}_2^m$. Then the following identities hold:*

$$(\tilde{\tau}_c F)^{-1}(x) = \tilde{\tau}_{F(c)} F^{-1}\Big(\frac{1}{\alpha_F^c} x\Big), \tag{11}$$

$$(\tilde{\sigma}_a F)^{-1}(x) = \tilde{\sigma}_{F(a)} F^{-1}(x), \tag{12}$$

$$(\rho_{2^j} F)^{-1}(x) = \rho_{2^j} F^{-1}(x), \tag{13}$$

*where $a \in \mathbb{F}_{2^m}^*$, $c \in \mathbb{F}_{2^m}$ and $0 \le j \le m-1$.*

*Proof.* It is easy to see that $\tilde{\tau}_{F(c)} F^{-1}\Big(\frac{1}{\alpha_F^c}\Big) = 1$, therefore

$$(\tilde{\tau}_c F)^{-1}(x) = (\alpha_F^c (F(x+c)+F(c)))^{-1} = F^{-1}\Big(\frac{1}{\alpha_F^c} x + F(c)\Big) + c =$$
$$F^{-1}\Big(\frac{1}{\alpha_F^c} x + F(c)\Big) + F^{-1}(F(c)) = \tilde{\tau}_{F(c)} F^{-1}\Big(\frac{1}{\alpha_F^c} x\Big).$$

Equalities (12) and (13) are straightforward to prove:

$$(\tilde{\sigma}_a F)^{-1}(x) = \Big(\frac{1}{F(a)} F(ax)\Big)^{-1} = \frac{1}{a} F^{-1}(F(a)x) = \tilde{\sigma}_{F(a)} F^{-1}(x),$$
$$(\rho_{2^j} F)^{-1}(x) = ((F(x^{2^{-j}}))^{2^j})^{-1} = (F(x^{2^{-j}})^{-1})^{2^j} = \rho_{2^j} F^{-1}(x).$$

□

**Lemma 6.** *Let $F$ be an o-polynomial on $\mathbb{F}_{2^m}$. Then the following identities hold:*

$$\tilde{\tau}_c \circ \rho_{2^j} F = \rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}} F, \tag{14}$$

$$\tilde{\tau}_c \circ \tilde{\sigma}_a F = \tilde{\sigma}_a \circ \tilde{\tau}_{ac} F, \tag{15}$$

$$(\rho_{2^j} F)' = \rho_{2^j} F' \tag{16}$$

$$(\tilde{\sigma}_a F)' = \tilde{\sigma}_{\frac{1}{a}} F', \tag{17}$$

*where $a \in \mathbb{F}_{2^m}^*$, $c \in \mathbb{F}_{2^m}$, $0 \le j \le m-1$.*

*Proof.* To prove the first equality, transform its left and right sides.

$$\tilde{\tau}_c \circ \rho_{2^j} F(x) = \alpha^c_{\rho_{2^j} F}(\rho_{2^j} F(x+c) + \rho_{2^j} F(c)) =$$
$$\alpha^c_{\rho_{2^j} F}((F((x+c)^{2^{-j}}))^{2^j} + (F(c^{2^{-j}}))^{2^j}) = \alpha^c_{\rho_{2^j} F}((F(x^{2^{-j}} + c^{2^{-j}}))^{2^j} + (F(c^{2^{-j}}))^{2^j}) =$$
$$\alpha^c_{\rho_{2^j} F}(F(x^{2^{-j}} + c^{2^{-j}}) + F(c^{2^{-j}}))^{2^j}$$

On the other hand,

$$\rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}} F(x) = (\tilde{\tau}_{c^{2^{-j}}} F(x^{2^{-j}}))^{2^j} = (\alpha_F^{c^{2^{-j}}}(F(x^{2^{-j}} + c^{2^{-j}}) + F(c^{2^{-j}}))^{2^j}.$$

So, it is left to check that $(\alpha_F^{c^{2^{-j}}})^{2^j} = \alpha^c_{\rho_{2^j}F}$. Indeed,

$$\alpha^c_{\rho_{2^j}F} = \frac{1}{\rho_{2^j}F(1+c)+\rho_{2^j}F(c)} = \frac{1}{(F((1+c)^{2^{-j}}))^{2^j}+(F(c^{2^{-j}}))^{2^j}} = \Big(\frac{1}{F(1+c^{2^{-j}})+F(c^{2^{-j}})}\Big)^{2^j} = (\alpha_F^{c^{2^{-j}}})^{2^j}.$$

Thus we proved that $\tilde{\tau}_c \circ \rho_{2^j}F = \rho_{2^j} \circ \tilde{\tau}_{c^{2^{-j}}}F$.

Computing the left and the right sides of equality (15) we get

$$\tilde{\tau}_c \circ \tilde{\sigma}_a F(x) = \alpha^c_{\tilde{\sigma}_a F}(\tilde{\sigma}_a F(x+c)+\tilde{\sigma}_a F(c)) = \alpha^c_{\tilde{\sigma}_a F}(\frac{1}{F(a)}F(a(x+c))+\frac{1}{F(a)}F(ac)),$$

$$\tilde{\sigma}_a \circ \tilde{\tau}_{ac}F(x) = \frac{1}{\tilde{\tau}_{ac}F(a)}\alpha^{ac}_F(F(ax+ac)+F(ac)).$$

Note that the coefficients $\frac{1}{F(a)}\alpha^c_{\tilde{\sigma}_a F}$ and $\frac{1}{\tilde{\tau}_{ac}F(a)}\alpha^{ac}_F$ are equal which means that $\tilde{\tau}_c \circ \tilde{\sigma}_a F = \tilde{\sigma}_a \circ \tilde{\tau}_{ac}F$. Indeed,

$$\frac{1}{F(a)}\alpha^c_{\tilde{\sigma}_a F} = \frac{1}{F(a)}\frac{1}{\tilde{\sigma}_a F(1+c)+\tilde{\sigma}_a F(c)} = \frac{1}{F(a)}\frac{F(a)}{F(a(1+c))+F(ac)} = \frac{1}{F(a+ac)+F(ac)},$$

$$\frac{1}{\tilde{\tau}_{ac}F(a)}\alpha^{ac}_F = \frac{F(1+ac)+F(ac)}{F(a+ac)+F(ac)}\frac{1}{F(1+ac)+F(ac)} = \frac{1}{F(a+ac)+F(ac)}.$$

The remaining two equalities are proved similarly. For (16) we get

$$\rho_{2^j}F'(x) = (F'(x^{2^{-j}}))^{2^j} = (x^{2^{-j}}F(\frac{1}{x^{2^{-j}}}))^{2^j} = x(F(\frac{1}{x^{2^{-j}}}))^{2^j} = x\rho_{2^j}F(\frac{1}{x}) = (\rho_{2^j}F)'(x).$$

Transforming both sides of Equality (17) we get

$$(\tilde{\sigma}_a F)'(x) = x\tilde{\sigma}_a F\Big(\frac{1}{x}\Big) = \frac{x}{F(a)}F\Big(\frac{a}{x}\Big).$$

$$\tilde{\sigma}_{\frac{1}{a}}F'(x) = \frac{1}{F'(\frac{1}{a})}F'\Big(\frac{x}{a}\Big) = \frac{a}{F(a)}\frac{x}{a}F\Big(\frac{a}{x}\Big) = \frac{x}{F(a)}F\Big(\frac{a}{x}\Big).$$

□

## 6.2 EA-inequivalent Niho bent functions and orbits

Further we need the following equality from [8]

$$((F')^{-1})' = ((F^{-1})')^{-1} \tag{18}$$

Let's introduce a few notations. Denote by $g_F$ the Niho bent function defined by an o-polynomial $F$. When Niho bent functions $g_F$ and $g_{\bar{F}}$ are EA-equivalent (respectively, EA-inequivalent), we will write $g_F \sim_{EA} g_{\bar{F}}$ (respectively, $g_F \nsim_{EA} g_{\bar{F}}$). We will use notation "$A \overset{(\mathrm{p})}{=} B$", when the expression $B$ is obtained from the expression $A$ using equality number p.

**Theorem 5.** *Let $F$ be an o-polynomial. Then an o-polynomial $\bar{F}$ obtained from $F$ using one generator of the modified magic action and the inverse map can produce a Niho bent function EA-inequivalent to those defined by $F$ and $F^{-1}$ only if $\bar{F} = (F')^{-1}$.*

*Proof.* Assume $\bar{F}$ is an o-polynomial which is obtained from o-polynomial $F$ using one generator of the modified magic action and the inverse map, i.e. $\bar{F}$ has one of the following forms: $hF, hF^{-1}, (hF)^{-1}, (hF^{-1})^{-1}$, where $h \in H$.

As we show below, when $h$ is $\tilde{\sigma}_a$, $\tilde{\tau}_c$ or $\rho_{2^j}$, $\bar{F}$ defines a Niho bent function EA-equivalent to those defined by $F$ or $F^{-1}$.

a) Let $h$ be $\tilde{\sigma}_a, a \in \mathbb{F}_{2^m}^*$. Then $hF(x) = \tilde{\sigma}_a F(x) = \frac{1}{F(a)} F(ax)$ and by Lemma 1, the corresponding Niho bent function is EA-equivalent to those defined by $F$. By the same reason $hF^{-1} = \tilde{\sigma}_a F^{-1}$ and $F^{-1}$ define EA-equivalent Niho bent functions. Further note that

$$(hF)^{-1}(x) = (\tilde{\sigma}_a F)^{-1}(x) \overset{(12)}{=} \tilde{\sigma}_{F(a)} F^{-1}(x).$$

Hence, $g_{(\tilde{\sigma}_a F)^{-1}} \sim_{EA} g_{F^{-1}}$ and

$$(hF^{-1})^{-1}(x) = (\tilde{\sigma}_a F^{-1})^{-1}(x) \overset{(12)}{=} \tilde{\sigma}_{F^{-1}(a)} (F^{-1})^{-1}(x) = \tilde{\sigma}_{F^{-1}(a)} F(x),$$

and therefore $g_{(\tilde{\sigma}_a F^{-1})^{-1}} \sim_{EA} g_F$.

b) Suppose $h$ is $\tilde{\tau}_c$ with $c \in \mathbb{F}_{2^m}$. Then $hF(x) = \tilde{\tau}_c F(x) = \alpha_F^c (F(x+c) + F(c))$ and $hF^{-1}(x) = \tilde{\tau}_c F^{-1}$ define Niho bent functions EA-equivalent to those defined by $F$ and $F^{-1}$ respectively (by Lemma 3). Hence,

$$(hF)^{-1}(x) = (\tilde{\tau}_c F(x))^{-1}(x) \overset{(11)}{=} \tau_{F(c)} F^{-1}((\alpha_F^c)^{-1} x)$$

yields that $g_{(hF)^{-1}} \sim_{EA} g_F$ and from

$$(hF^{-1})^{-1}(x) = (\tilde{\tau}_c F^{-1})^{-1}(x) \overset{(11)}{=} \tau_{F^{-1}(c)} (F^{-1})^{-1}\Big(\frac{1}{\alpha_{F^{-1}}^c} x\Big) = \tau_{F^{-1}(c)} F\Big(\frac{1}{\alpha_{F^{-1}}^c} x\Big)$$

follows $g_{(hF^{-1})^{-1}} \sim_{EA} g_F$.

c) Take now $h = \rho_{2^j}$ with $0 \le j \le m-1$. Then $hF(x) = \rho_{2^j} F(x) = (F(x^{2^{-i}}))^{2^i}$ and $hF^{-1}(x) = \rho_{2^j} F^{-1} = (F^{-1}(x^{2^{-i}}))^{2^i}$, and by Lemma 2 we get that $g_{\rho_{2^j} F}$ and $g_{\rho_{2^j} F^{-1}}$ are EA-equivalent to $g_F$ and $g_{F^{-1}}$, respectively. Therefore, from $(hF)^{-1}(x) = (\rho_{2^j} F)^{-1}(x) \overset{(13)}{=} \rho_{2^j} F^{-1}$ and
$(hF^{-1})^{-1}(x) = (\rho_{2^j} F^{-1})^{-1} \overset{(13)}{=} \rho_{2^j} F$ it follows that $g_{(\rho_{2^j} F)^{-1}} \sim_{EA} g_{F^{-1}}$ and $g_{(\rho_{2^j} F^{-1})^{-1}} \sim_{EA} g_F$.

d) Consider $h = \prime$. The Niho bent function defined by an o-polynomial $hF(x) = F'(x) = xF(x^{-1})$ is

$$g_{F'}(x,y) = Tr_m(x(F'(\frac{y}{x}))) = Tr_m(x\frac{y}{x} F((\frac{y}{x})^{-1})) = Tr_m(yF(\frac{x}{y})) = g_F(y,x),$$

i.e. $g_{F'} \sim_{EA} g_F$. Similarly, $g_{(F^{-1})'} \sim_{EA} g_{F^{-1}}$.

The function $(hF)^{-1}(x) = (F')^{-1}(x) = (xF(x^{-1}))^{-1}$ can define a Niho bent function EA-inequivalent to those defined by $F$ and $F^{-1}$. For example, an o-monomial $x^{2^i}$ defines three surely EA-inequivalent Niho bent functions corresponding to o-polynomials

$F, F^{-1}$ and $(F')^{-1}$ [8].
Using equality (18), we immediately get that a Niho bent function defined by the o-polynomial $(hF^{-1})^{-1}(x) = ((F^{-1})')^{-1}(x)$ is EA-equivalent to one defined by $(F')^{-1}$. □

We rewrite the equalities of Lemmas 4, 5 and 6 in a more compact way. Equalities (8) - (10) as

$$h_{b_1} \circ h_{b_2} F = h_{b_3} F, \tag{19}$$

where $h_{b_1}, h_{b_2}, h_{b_3}$ are the same generators from the set $H \setminus \{\prime\}$ with different parameters $b_1, b_2, b_3 \in \mathbb{F}_{2^m}$.
Equalities (11) - (13) as

$$(h_{b_1} F)^{-1} = h_{b_2} F^{-1}, \tag{20}$$

where $h_{b_1}, h_{b_2}$ are the same generators from the set $H \setminus \{\prime\}$ with different parameters $b_1, b_2 \in \mathbb{F}_{2^m}$. Note that right and left parts of the equality (11) have different arguments, but it does not play any role in our study of EA-equivalence of resulting Niho bent functions.
Equalities (14) - (15) as

$$\tilde{\tau}_{c_1} \circ h_b F = h_b \circ \tilde{\tau}_{c_2} F, \tag{21}$$

where $h_b \in \{\tilde{\sigma}_a, \rho_{2^j}\}$. And equalities (16) - (17) as

$$(h_{b_1} F)' = h_{b_2} F', \tag{22}$$

where $h_{b_1}, h_{b_2}$ are the same generators from the set $\{\tilde{\sigma}_a, \rho_{2^j}\}$ with different parameters $b_1, b_2 \in \mathbb{F}_{2^m}$.

To make the formulation of the next theorem more visual instead of using the notation $\prime$ we will use the initial one, i.e. $\varphi$. We will also refer to the original notation $\varphi$ in some parts of the proof when convenient. Further, by *"reduce o-polynomial"* we mean that the original o-polynomial and the new one (reduced) define EA-equivalent Niho bent functions. When we are saying *"delete generator"* we mean that if we skip this generator the new o-polynomial will define a Niho bent function EA-equivalent to one generated by the original o-polynomial.

Let $i$ be a positive integer and $k_i \geq 0$. By $H_i$ we denote a composition of length $k_i$ of generators $\varphi$ and $\tilde{\tau}_c$ following each other as follows:

$$H_i = \underbrace{\varphi \circ \tilde{\tau}_{c_{i_1}} \circ \varphi \circ \tilde{\tau}_{c_{i_2}} \circ \dots}_{k_i} \tag{23}$$

That is, if $F$ is an o-polynomial and we denote $T_j = \varphi \circ \tilde{\tau}_{c_{i_j}}$, $0 \leq j < (k_i+1)/2$ then

$$H_i F = \begin{cases} F & \text{if } k_i = 0, \\ \varphi F & \text{if } k_i = 1, \\ T_1 \circ \dots \circ T_{s_i} F & \text{if } k_i = 2s_i, \\ T_1 \circ \dots \circ T_{s_i} \circ \varphi F & \text{if } k_i = 2s_i + 1. \end{cases}$$

In the theorem below we prove that for a given o-polynomial we can derive all EA-inequivalent Niho bent functions only using transformations $\varphi$, $\tilde{\tau}_c$ and the inverse map in a special sequence.

**Theorem 6.** *Let $F$ be an o-polynomial, $g_F$ the corresponding Niho bent function and $G_F$ the class of all functions o-equivalent to $g_F$. Then o-polynomials of the form*

$$(H_1(H_2(H_3(\dots(H_qF)^{-1}\dots)^{-1})^{-1})^{-1}, \tag{24}$$

*where $H_i$ is defined by (23), for all $i \in \{1\dots q\}$, $q \geq 1$, and $k_i \geq 1$ for $i \geq 3$, $k_i \geq 0$ for $i \leq 2$, provide representatives for all EA-equivalence classes within $G_F$. That is, up to EA-equivalence, all Niho bent functions o-equivalent to $g_F$ arise from (24).*

*Proof.* Note first that we can get $F$ itself in the form (24) if we take $q = 2$, $k_1 = k_2 = 0$. if $q = 1$ and $k_1 = 0$ then we get $F^{-1}$. Further we have a restriction $k_i \geq 1$ for $i \geq 3$ to avoid repetitions.

According to Proposition 1 any function o-equivalent to $g_F$ corresponds to an o-polynomial of the form

$$h_1 \circ h_2 \circ \dots \circ h_kF, \tag{25}$$

where $h_1, h_2, \dots, h_k$ (for some $k \geq 0$) are generators of the modified magic action and the inverse map. Our aim is to simplify this expression to exclude as many cases leading to EA-equivalent functions as possible. That is, we exclude certain sequences of generators which surely lead to EA-equivalent Niho bent functions. By $h_{i_j}$ we denote a generator of the same type as $h_i$ but with a different parameter.

From Theorem 5 it follows

a) If $h_1 \in H$, then $g_{h_1 \circ h_2 \circ \dots \circ h_kF} \sim_{EA} g_{h_2 \circ \dots \circ h_kF}$ and we can consider reduced o-polynomial $h_2 \circ \dots \circ h_kF$;

b) If $h_1$ is the inverse map and $h_2 \in H \setminus \{\prime\}$ then $g_{h_1 \circ h_2 \circ \dots \circ h_kF} \sim_{EA} g_{h_1 \circ h_3 \circ \dots \circ h_kF}$, so we can consider the reduced o-polynomial $h_1 \circ h_3 \circ \dots \circ h_kF$.

Hence, if $k = 1$ in (25) then we can get an EA-inequivalent case only if $h_1$ is the inverse map, and it corresponds to (24) with $q = 1$ and $k_1 = 0$. If $k = 2$ in (25) (and it cannot be reduced to the case $k = 1$) then we can get EA-inequivalent cases only if $h_1$ is the inverse map and $h_2 = \prime$, and it corresponds to (24) with $q = 1$ and $k_1 = 1$. If $k \geq 3$ we can reduce (25) until at some moment we will get an o-polynomial $h_i \circ h_{i+1} \circ \dots \circ h_kF$, where $h_i$ is the inverse map and $h_{i+1} = \prime$, that is, we have

$$((h_{i+2} \circ \dots \circ h_kF)')^{-1}. \tag{26}$$

Note that here and further we assume that $k$ is large enough to allow such a redaction while otherwise, it is easy to see that the process would stop and provide a formula (24) for some parameters.

If $h_{i+2} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ or $h_{i+2}$ is the inverse map then we can delete the generator $h_{i+2}$ and consider the reduced o-polynomial $h_i \circ h_{i+1} \circ h_{i+3} \circ \dots \circ h_kF$. Indeed, suppose $h_{i+2} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then

$h_i \circ h_{i+1} \circ h_{i+2} \circ \dots \circ h_kF = ((h_{i+2} \circ \dots \circ h_kF)')^{-1} \overset{(22)}{=}$

$(h_{(i+2)_1} \circ (h_{i+3} \circ \ldots \circ h_k F)')^{-1} \overset{(20)}{=} h_{(i+2)_2} \circ ((h_{i+3} \circ \ldots \circ h_k F)')^{-1}$
and, according to (a), $g_{h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F} \sim_{EA} g_{h_i \circ h_{i+1} \circ h_{i+3} \circ \ldots \circ h_k F}$. In the case when $h_{i+2}$ is the inverse map, using (18) we get the same result that the o-polynomials $(((h_{i+3} \circ \ldots \circ h_k F)^{-1})')^{-1} = ((h_{i+3} \circ \ldots \circ h_k F)')^{-1})'$ and $((h_{i+3} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{i+3} \circ \ldots \circ h_k F$ define EA-equivalent Niho bent functions.
If $h_{i+2}$ is $\prime$, then $h_{i+1}$ and $h_{i+2}$ eliminate each other: $h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F = h_i \circ h_{i+3} \circ \ldots \circ h_k F$. If $h_{i+2} = \tilde{\tau}_c$, then we cannot eliminate it from the o-polynomial $h_i \circ h_{i+1} \circ h_{i+2} \ldots \circ h_k F$.

Further consider an o-polynomial $h_i \circ h_{i+1} \circ h_{i+2} \circ \ldots \circ h_k F$ where $h_i$ is the inverse map, $h_{i+1} = \prime$, $h_{i+2} = \tilde{\tau}_c$, i.e. an o-polynomial

$$((\tilde{\tau}_c \circ h_{i+3} \circ \ldots \circ h_k F)')^{-1}. \tag{27}$$

When $k = i+2$ then we get $((\tilde{\tau}_c F)')^{-1}$ which has the form (24) with $q = 1$ and $k_1 = 2$. Hence, in (27) we can assume that $k \geq i+3$. Further we can reduce $h_{i+3}$ from (27) unless $h_{i+3}$ is $\prime$. Indeed, consider first $h_{i+3} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then
$((\tilde{\tau}_c \circ h_{i+3} \circ \ldots \circ h_k F)')^{-1} \overset{(21)}{=} ((h_{i+3} \circ \tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} \overset{(22)}{=}$
$(h_{(i+3)_1} \circ (\tilde{\tau}_{c_1} \circ \ldots \circ h_k F)')^{-1} \overset{(20)}{=} h_{(i+3)_2} \circ ((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1}$.
The last o-polynomial defines a Niho bent function EA-equivalent to one defined by the o-polynomial $((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$.
If $h_{i+3} = \tilde{\tau}_{c_1}$, then using (8) we immediately get $h_i \circ h_{i+1} \circ h_{i+2} \circ h_{i+3} \circ \ldots \circ h_k F = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$, where $h_{(i+2)_1} = \tilde{\tau}_{c+c_1}$.
If $h_{i+3}$ is the inverse map then

$h_i \circ h_{i+1} \circ h_{i+2} \circ h_{i+3} \circ \ldots \circ h_k F = ((\tilde{\tau}_c((h_{i+4} \circ \ldots \circ h_k F)^{-1}))')^{-1} \overset{(20)}{=}$
$(((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)^{-1})')^{-1} = (((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1})'$, defines a Niho bent function EA-equivalent to the one defined by $((\tilde{\tau}_{c_1} \circ h_{i+4} \circ \ldots \circ h_k F)')^{-1} = h_i \circ h_{i+1} \circ h_{(i+2)_1} \circ h_{i+4} \circ \ldots \circ h_k F$.
Note that we could eliminate $h_{i+3}$ as the inverse here because it is followed by $h_{i+2} = \tilde{\tau}_c$, $h_{i+1} = \prime$ and $h_i$ as the inverse map.

Hence, if (25) produces a Niho bent function $g$ EA-inequivalent to those corresponding to $F$, $F^{-1}$, $(F')^{-1}$ and $((\tilde{\tau}_c F)')^{-1}$ then $g$ is EA-equivalent to the function corresponding to an o-polynomial

$$(\varphi \circ \tilde{\tau}_{c'} \circ \varphi \circ h_{l'} \circ \ldots \circ h_k F)^{-1}. \tag{28}$$

Now consider an o-polynomial of the form:

$$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ h_l \circ \ldots \circ h_k F)^{-1}. \tag{29}$$

Case 1. First we restrict to the case $h_l, \ldots, h_k \in H$ when considering (29). Note that if $l$ is an even number in (29), then the generator $\varphi$ acts on $h_l$; if $l$ is odd, then the generator $\tilde{\tau}_c$ acts on $h_l$ (for some $c \in \mathbb{F}_{2^m}$). We consider $l$ odd case, i.e. $l = 2t+1$ while for $l$ even case the proof is similar and we skip it.
If $h_{2t+1} \in \{\tilde{\sigma}_a, \rho_{2^j}\}$ then
$(\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \circ \tilde{\tau}_{c_t} \circ h_{2t+1} \circ \ldots \circ h_k F)^{-1} \overset{(21)}{=}$

$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\ldots\circ\varphi\circ h_{2t+1}\circ\tilde{\tau}_{c_{t_1}}(h_{2t+2}\circ\ldots\circ h_kF))^{-1}\overset{(22)}{=}$
$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\ldots\circ h_{(2t+1)_1}\circ\varphi(\tilde{\tau}_{c_{t_1}}(h_{2t+2}\circ\ldots\circ h_kF)))^{-1}\overset{(21)}{=}$
$\ldots$
$(h_{(2t+1)_t}(\varphi(\tilde{\tau}_{c_{1_1}}(\varphi(\ldots(\tilde{\tau}_{c_{t_1}}(h_{2t+2}\circ\ldots\circ h_kF))\ldots))))^{-1}\overset{(20)}{=}$
$h_{(2t+1)_{t+1}}(\varphi(\tilde{\tau}_{c_{1_1}}(\varphi(\ldots(\tilde{\tau}_{c_{t_1}}(h_{2t+2}\circ\ldots\circ h_kF))\ldots))))^{-1}$,
hence we can reduce the o-polynomial $(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ\tilde{\tau}_{c_t}\circ h_{2t+1}\circ\ldots\circ h_kF)^{-1}$, and consider $(\varphi\circ\tilde{\tau}_{c_{1_1}}\circ\varphi\circ\tilde{\tau}_{c_{2_1}}\circ\varphi\circ\ldots\circ\tilde{\tau}_{c_{t_1}}\circ h_{2t+2}\circ\ldots\circ h_kF)^{-1}$.
If $h_{2t+1}=\tilde{\tau}_{c_{t+1}}$ then obviously we can consider o-polynomial
$((\tilde{\tau}_{c_1}(\tilde{\tau}_{c_2}(\ldots(\tilde{\tau}_{c_t+c_{t+1}}(h_{2t+2}\circ\ldots\circ h_kF))'\ldots)')')')^{-1}$.
If $h_{2t+1}=\prime$ then we cannot eliminate it.
Continuing this process we get for this case that the o-polynomial (25) can be reduced to $(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ F)^{-1}$ as in (23). This corresponds to the case $q=1$ in (24).

Case 2. Now we consider (29) and allow $h_l,\ldots,h_k$ to be inverses too. We still assume $l$ be odd and (as we saw earlier in the proof) w.l.o.g. $h_l,\ldots,h_k\in\{\prime,\tilde{\tau}_c,\text{the inverse}|c\in\mathbb{F}_{2^m}\}$. Take $h_l$ the inverse (the other possibilities for $h_l$ were discussed earlier in the proof), i.e. consider the following o-polynomial:

$$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots(h_{l+1}\circ\ldots\circ h_kF)^{-1})^{-1}. \tag{30}$$

If $h_{l+1}$ is the inverse, then it cancels with $h_l$. If $h_{l+1}$ is $\tilde{\tau}_{c_{t+1}}$, then
$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ(\tilde{\tau}_{c_{t+1}}\circ h_{l+2}\circ\ldots\circ h_kF)^{-1})^{-1}\overset{(20)}{=}$
$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ\tilde{\tau}_{c_{(t+1)_1}}(h_{l+2}\circ\ldots\circ h_kF)^{-1})^{-1}$,
which is of the form (30) with fewer transformations in the inner brackets.

If $h_{l+1}$ is $\varphi$ then we get $(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ(\varphi\circ h_{l+2}\circ\ldots\circ h_kF)^{-1})^{-1}$.

If further $h_{l+2}$ is $\tilde{\tau}_{c_{t+1}}$, then $(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ(\varphi\circ\tilde{\tau}_{c_{t+1}}\circ h_{l+3}\circ\ldots\circ h_kF)^{-1})^{-1})^{-1}$. If $h_{l+2}$ is the inverse or $h_{l+2}=\varphi$ then we get (30). Indeed, if $h_{l+2}=\varphi$ then it cancels with $h_{l+1}$, and if $h_{l+2}$ is the inverse then we get:
$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ(\varphi(h_{l+3}\circ\ldots\circ h_kF)^{-1})^{-1})^{-1}\overset{(18)}{=}$
$(\varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}\circ\varphi\circ\ldots\circ\varphi(\varphi\circ h_{l+3}\circ\ldots\circ h_kF)^{-1})^{-1}$.

Continuing these process we will clearly transform (30) to (24) in a way that these o-polynomials produce EA-equivalent Niho bent functions. □

In this paper, when we say that two o-polynomials $F$ and $F'$ define potentially EA-inequivalent Niho bent functions $g_F$ and $g_{F'}$, it means that either in some cases $g_F$ and $g_{F'}$ are EA-inequivalent, or it is not possible to deduce EA-equivalence with the developed technique which leaves a possibility that $g_F$ and $g_{F'}$ may be EA-inequivalent.

Below we consider some particular cases of formula (24).

**Corollary 3.** *Let $F$ be an o-polynomial defined on $\mathbb{F}_{2^m}$. Then o-polynomials*

$$F_c^\circ(x)=\left(\alpha_F^c x\left(F\left(\frac{1}{x}+c\right)+F(c)\right)\right)^{-1},\quad c\in\mathbb{F}_{2^m} \tag{31}$$

*define a sequence of Niho bent functions $g_{F_c^\circ}$ potentially EA-inequivalent to each other for different $c$, and EA-inequivalent to Niho bent functions defined by $F$, $F^{-1}$.*

*Proof.* o-polynomial (31) is the explicit form of o-polynomial (24) for $q = 1, k_1 = 2$. Indeed,
$((\tilde{\tau}_c F)')^{-1}(x) = \left(x\tilde{\tau}_c F\left(\frac{1}{x}\right)\right)^{-1} = \left(\alpha_F^c x\left(F\left(\frac{1}{x}+c\right)+F(c)\right)\right)^{-1}$.

Note that $F_c^\circ = (F')^{-1}$ for $c = 0$. Hence, the o-polynomial $(F')^{-1}$ is included in the class of o-polynomials $F_c^\circ$.

For $c = 1$ we get the function $F^\circ = \left(x\left(F\left(\frac{1}{x}+1\right)+1\right)\right)^{-1}$ studied in [8] and which can define a Niho bent function EA-inequivalent to those defined by $F$, $F^{-1}$ and $(F')^{-1}$. For instance, when $F(x) = x^{2^i}$, $g_{F^\circ}$ is EA-inequivalent to $g_F$, $g_{F^{-1}}$ and $g_{(F')^{-1}}$[8].

Using the equality (8) for every $c \in \mathbb{F}_{2^m}$ we can write:

$$F_c^\circ = ((\tilde{\tau}_c F)')^{-1} = ((\tilde{\tau}_1 \circ \tilde{\tau}_{c+1} F)')^{-1} = (\tilde{\tau}_{c+1} F)^\circ.$$

Since $F^\circ$, $F$, $F^{-1}$ and $(F')^{-1}$ can define four potentially EA-inequivalent Niho bent functions, we obtain that $F_c^\circ$ can define Niho bent functions potentially EA-inequivalent to those defined by $\tilde{\tau}_{c+1}F$, $(\tilde{\tau}_{c+1}F)^{-1}$, $((\tilde{\tau}_{c+1}F)')^{-1}$. It means that, for any $c \in \mathbb{F}_{2^m}$ a Niho bent function $g_{F_c^\circ}$ can be potentially EA-inequivalent to $g_F$, $g_{F^{-1}}$ and $g_{F_{c+1}^\circ}$. □

**Corollary 4.** *Let $F$ be an o-polynomial defined on $\mathbb{F}_{2^m}$. Then o-polynomials*

$$(F_c^*)^{-1} = \left(\alpha_{F'}^c\left((1+cx)F\left(\frac{x}{1+cx}\right)+cxF\left(\frac{1}{c}\right)\right)\right)^{-1}, \quad c \in \mathbb{F}_{2^m} \tag{32}$$

*define Niho bent functions $g_{(F_c^*)^{-1}}$ which can potentially be EA-inequivalent to each other for different $c$ and EA-inequivalent to Niho bent functions defined by $F$, $(F')^{-1}$.*

*Proof.* o-polynomial (32) is the explicit form of o-polynomial (24) for $q = 1$ and $k_1 = 3$. Indeed,

$$((\tilde{\tau}_c F')')^{-1}(x) = \left(\alpha_{F'}^c x\left(\left(F'\left(\frac{1}{x}+c\right)+F'(c)\right)\right)^{-1} = \right.$$
$$\left(\alpha_{F'}^c x\left(\frac{1+cx}{x}F\left(\frac{x}{1+cx}\right)+cF\left(\frac{1}{c}\right)\right)\right)^{-1} =$$
$$\left.\left(\alpha_{F'}^c\left((1+cx)F\left(\frac{x}{1+cx}\right)+cxF\left(\frac{1}{c}\right)\right)\right)^{-1}.\right.$$

Note that $(F_0^*)^{-1} = F^{-1}$. So the o-polynomial $F^{-1}$ is included in the class of o-polynomials $(F_c^*)^{-1}$ with $c = 0$.

For $c = 1$ we get the function $(F_1^*)^{-1} = ((x+1)F(\frac{x}{x+1})+x)^{-1}$ also studied in[8], and the Niho bent function associated with it is EA-equivalent to the one defined by $F^\circ$ [8]. But in the general case, for arbitrary $c \in \mathbb{F}_{2^m}$ we can't say that $(F_c^*)^{-1}$ defines an o-polynomial EA-equivalent to those defined by $F$ and $F_c^\circ$.

Using equalities (8) and (31) note that $(F_c^*)^{-1} = (F')_c^\circ = (\tilde{\tau}_{c+1}F')^\circ$.

Hence, we can say that $(F_c^*)^{-1} = (F')_c^\circ$ defines a Niho bent function potentially EA-inequivalent to Niho bent functions defined by $F'$, $(F')^{-1}$ and $(F')_{c+1}^\circ = (F_{c+1}^*)^{-1}$. □

## 6.3 The case of o-monomials and the known o-polynomials

Further we study the consequences of the obtained results for the particular cases of o-monomials and the known o-polynomials.

**Lemma 7.** *For an o-monomial $F(x) = x^d$, the Niho bent functions defined by $F_c^\circ$ and $F^\circ$ are EA-equivalent, for any $c \in \mathbb{F}_{2^m}^*$.*

*Proof.* We have for $c \neq 0$

$$F_c^\circ(x) = (\varphi \circ \tilde{\tau}_c F)^{-1} = \Big(\alpha_F^c x\Big(\Big(F\Big(\frac{1}{x}+c\Big)+F(c)\Big)\Big)^{-1} =$$
$$\Big(\alpha_F^c x\Big(\Big(\frac{1}{x}+c\Big)^d + c^d\Big)\Big)^{-1} = \Big(\alpha_F^c x\Big(\Big(\frac{1+cx}{x}\Big)^d + c^d\Big)\Big)^{-1} =$$
$$\Big(\alpha_F^c c^d x\Big(\Big(\frac{1+cx}{cx}\Big)^d + 1\Big)\Big)^{-1} = \Big(\alpha_F^c c^{d-1} cx\Big(\Big(\frac{1+cx}{cx}\Big)^d + 1\Big)\Big)^{-1} = \frac{1}{c} F^\circ\Big(\frac{1}{\alpha_F^c c^{d-1}} x\Big).$$

From Lemma 1 it follows that Niho bent functions defined by $F_c^\circ$ and $F^\circ$ are EA-equivalent for any $c \neq 0$. □

From the proof of the previous lemma it is easy to see that for any o-monomial $F$

$$\varphi \circ \tilde{\tau}_c F(x) = \beta_c \, \varphi \circ \tau_1 F(cx), \tag{33}$$

where $\beta_c = \alpha_F^c c^{d-1}, c \in F_{2^m}^*$.

**Lemma 8.** *For an o-monomial $F(x) = x^d$, the Niho bent functions defined by $(F_c^*)^{-1}$, $(F^*)^{-1}$ and $F^\circ$ are EA-equivalent, for $c \in \mathbb{F}_{2^m}^*$.*

*Proof.* $F^*(x) = (x+1)F(\frac{x}{x+1}) + x = (x+1)(\frac{x}{x+1})^d + x$.
For $c \neq 0$ we have

$$(F_c^*)^{-1}(x) = (\varphi \circ \tau_c \circ \varphi F)^{-1} = \Big(\alpha_{F'}^c \Big((1+cx)F\Big(\frac{x}{1+cx}\Big) + cxF\Big(\frac{1}{c}\Big)\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c \Big((1+cx)\Big(\frac{x}{1+cx}\Big)^d + cx\Big(\frac{1}{c}\Big)^d\Big)\Big)^{-1} =$$
$$\Big(\alpha_{F'}^c \Big(\frac{1}{c}\Big)^d \Big((1+cx)\Big(\frac{cx}{1+cx}\Big)^d + cx\Big)\Big)^{-1} = \frac{1}{c}(F^*)^{-1}\Big(\frac{c^d}{\alpha_{F'}^c} x\Big).$$

Using Lemma 1, we conclude that the Niho bent functions defined by $(F^*)^{-1}$ and $(F_c^*)^{-1}$ are EA-equivalent for $c \neq 0$. According to [8], the Niho bent function defined by $(F^*)^{-1}$ and $F^\circ$ are EA-equivalent, and taking into account Lemma 7, we get that Niho bent functions defined by $(F_c^*)^{-1}$, $(F^*)^{-1}$ and $F^\circ$ are EA-equivalent to each other for any $c \neq 0$. □

From the proof of above lemma it is easy to see that for any o-monomial $F$

$$\varphi \circ \tilde{\tau}_c \circ \varphi F(x) = \gamma_c \, \varphi \circ \tau_1 \circ \varphi F(cx). \tag{34}$$

where $\gamma_c = \alpha_{F'}^c c^{d-1}, c \in \mathbb{F}_{2^m}^*, F' = \varphi F$.

Further we will need the following equality, which holds for any o-polynomial $F$

$$\varphi \circ \tau_1 \circ \varphi F = \tau_1 \circ \varphi \circ \tau_1 F. \tag{35}$$

Indeed,
$\tau_1 \circ \varphi \circ \tau_1 F(x) = (1+x)\Big(F\Big(\frac{1}{1+x}+1\Big)+1\Big)+1 = (1+x)F\Big(\frac{x}{1+x}\Big)+x =$
$\varphi \circ \tau_1 \circ \varphi F(x)$.

To keep notations as simple as possible, since we are interested in EA-equivalence of Niho bent functions and coefficients of arguments of o-polynomial do not affect on EA-equivalence of Niho bent functions as well as coefficient of o-polynomial, then instead of $aF(bx) = G(x)$ we will write $F \approx G$ for $a,b \in \mathbb{F}_{2^m}^*$.

**Lemma 9.** *Let $F$ be an o-monomial defined on $\mathbb{F}_{2^m}$. Then*

$$\underbrace{\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots}_{k} F \approx \begin{cases} \begin{cases} \tau_1 F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1 F, & \text{if } t \equiv 1 \mod 4; \\ \tau_1 \circ \varphi F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 3 \mod 4; \end{cases} & \text{if } k = 2t \\ \begin{cases} \tau_1 \circ \varphi F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 1 \mod 4; \\ \tau_1 F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 F, & \text{if } t \equiv 3 \mod 4; \end{cases} & \text{if } k = 2t+1, \end{cases}$$

*where $t \geq 1$.*

*Proof.* Assume that $k = 2t$, i.e. the orbit in the statment of this lemma has the form $\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \varphi \circ \tilde{\tau}_{c_t} F$. Then
1) For $t = 1$ we have $\varphi \circ \tilde{\tau}_{c_1} F \overset{(33)}{\approx} \varphi \circ \tilde{\tau}_1 F$.
2) For $t = 2$,
$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} F \overset{(33)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_1 F \overset{(34)}{\approx} \varphi \circ \tau_1 \circ \varphi \circ \tilde{\tau}_{c_1} F \overset{(33)}{\approx} \varphi \circ \tau_1 \circ \varphi \circ \tau_1 F \overset{(35)}{\approx} \varphi \circ \varphi \circ \tilde{\tau}_1 \circ \varphi F \approx \tau_1 \circ \varphi F$.
3) For $t = 3$,
$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} F \overset{2)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \tau_1 \circ \varphi F \approx \varphi \circ \tilde{\tau}_{c_1+1} \circ \varphi F \overset{(34)}{\approx} \varphi \circ \tau_1 \circ \varphi F$
4) For $t = 4$
$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} \circ \varphi \circ \tilde{\tau}_{c_4} F \overset{3)}{\approx} \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_1 \circ \varphi F \overset{2)}{\approx} \tau_1 \circ \varphi(\varphi F) \approx \tau_1 F$.

Thus for even $k$ ,
$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-3}} \circ \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t} F \overset{4)}{\approx}$
$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-4}} \circ \tau_1 F \approx \varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-4}+1} F \overset{4)}{\approx}$
$\ldots$

$$\begin{cases} \tau_1 F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \tau_1 F \overset{1)}{\approx} \varphi \circ \tau_1 F, & \text{if } t \equiv 1 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \tau_1 F \overset{2)}{\approx} \tau_1 \circ \varphi F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tilde{\tau}_{c_3} \circ \tau_1 F \overset{3)}{\approx} \varphi \circ \tau_1 \circ \varphi F, & \text{if } t \equiv 3 \mod 4; \end{cases}$$

Note that $\varphi F$ is an o-monomial, therefore we can apply the previous formula to the case of odd $k$. Indeed,
$\varphi \circ \tilde{\tau}_{c_1} \circ \ldots \circ \varphi \circ \tilde{\tau}_{c_{t-3}} \circ \varphi \circ \tilde{\tau}_{c_{t-2}} \circ \varphi \circ \tilde{\tau}_{c_{t-1}} \circ \varphi \circ \tilde{\tau}_{c_t}(\varphi F) \approx$

$$\begin{cases} \tau_1 \circ \varphi F, & \text{if } t \equiv 0 \mod 4; \\ \varphi \circ \tau_1(\varphi F), & \text{if } t \equiv 1 \mod 4; \\ \tau_1 \circ \varphi(\varphi F) \approx \tau_1 F, & \text{if } t \equiv 2 \mod 4; \\ \varphi \circ \tau_1 \circ \varphi(\varphi F) \approx \varphi \circ \tau_1\, F, & \text{if } t \equiv 3 \mod 4; \end{cases}$$

□

**Lemma 10.** *Let $F$ be an o-monomial defined on $\mathbb{F}_{2^m}$. Then*

$$\underbrace{\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots}_{k} (\varphi \circ \tau_1 F)^{-1} \approx$$

$$\begin{cases} \begin{cases} (\varphi \circ \tau_1 F)^{-1}, & \text{if } t \equiv 0 \mod 3; \\ (\varphi \circ \tau_1(\varphi F)^{-1})^{-1}, & \text{if } t \equiv 1 \mod 3; \\ (\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}, & \text{if } t \equiv 2 \mod 3, \end{cases} & \text{if } k = 2t \\ \begin{cases} (\varphi \circ \tau_1 F^{-1})^{-1}, & \text{if } t \equiv 0 \mod 3; \\ (\varphi \circ \tau_1(\varphi F^{-1})^{-1})^{-1}, & \text{if } t \equiv 1 \mod 3; \\ (\varphi \circ \tau_1 \circ \varphi F)^{-1}, & \text{if } t \equiv 2 \mod 3, \end{cases} & \text{if } k = 2t+1, \end{cases} \tag{36}$$

*where $t \geq 1$.*

*Proof.* Assume that $k = 2t$, i.e. the orbit in the statement of this lemma has the form $\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \ldots \varphi \circ \tilde{\tau}_{c_t}(\varphi \circ \tau_1 F)^{-1}$. Then

1) For $t = 1$ we get:

$\varphi \circ \tilde{\tau}_{c_1}(\varphi \circ \tau_1 F)^{-1} \overset{(20)}{\approx} \varphi(\tilde{\tau}_{c_{1_1}} \circ \varphi \circ \tau_1 F)^{-1} \overset{(18)}{\approx} (\varphi(\varphi \circ \tilde{\tau}_{c_{1_1}} \circ \varphi \circ \tau_1 F)^{-1})^{-1} \overset{(??)}{\approx}$
$(\varphi(\varphi \circ \tau_1 \circ \varphi \circ \tilde{\tau}_{c_{1_1}} F)^{-1})^{-1} \overset{(33)}{\approx} (\varphi(\varphi \circ \tau_1 \circ \varphi \circ \tau_1 F)^{-1})^{-1} \overset{(35)}{\approx} (\varphi(\tau_1 \circ \varphi F)^{-1})^{-1} \overset{(20)}{\approx}$
$(\varphi \circ \tau_1(\varphi F)^{-1})^{-1}$.

2) For $t = 2$

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tau_{c_2}(\varphi \circ \tau_1 F)^{-1} \overset{1)}{\approx} \varphi \circ \tilde{\tau}_{c_1}(\varphi \circ \tau_1(\varphi F)^{-1})^{-1} \overset{1)}{\approx} (\varphi \circ \tau_1(\varphi(\varphi F)^{-1})^{-1})^{-1} \overset{(18)}{\approx}$
$(\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1}$.

3) For $t = 3$,

$\varphi \circ \tilde{\tau}_{c_1} \circ \varphi \circ \tilde{\tau}_{c_2} \circ \varphi \circ \tau_{c_3}(\varphi \circ \tau_1 F)^{-1} \overset{2)}{\approx} \varphi \circ \tilde{\tau}_{c_1}(\varphi \circ \tau_1 \circ \varphi F^{-1})^{-1} \overset{1)}{\approx} (\varphi \circ \tau_1 F)^{-1}$.

Thus,

$$\varphi\circ\tilde{\tau}_{c_1}\circ\ldots\varphi\circ\tilde{\tau}_{c_{t-2}}\circ\varphi\circ\tilde{\tau}_{c_{t-1}}\circ\varphi\circ\tilde{\tau}_{c_t}(\varphi\circ\tau_1F)^{-1}\overset{3)}{\approx}$$

$$\varphi\circ\tilde{\tau}_{c_1}\circ\ldots\varphi\circ\tilde{\tau}_{c_{t-3}}(\varphi\circ\tau_1F)^{-1}\overset{3)}{\approx}$$

$\ldots$

$$\begin{cases}(\varphi\circ\tau_1F)^{-1}, \text{ if } t\equiv 0 \mod 3;\\ \varphi\circ\tilde{\tau}_{c_1}(\varphi\circ\tau_1F)^{-1}\overset{1)}{\approx}(\varphi\circ\tau_1(\varphi F)^{-1})^{-1}, \text{ if } t\equiv 1 \mod 3;\\ \varphi\circ\tilde{\tau}_{c_1}\circ\varphi\circ\tilde{\tau}_{c_2}(\varphi\circ\tau_1F)^{-1}\overset{2)}{\approx}(\varphi\circ\tau_1\circ\varphi F^{-1})^{-1}, \text{ if } t\equiv 2 \mod 3.\end{cases}$$

Note that from (18) follows that $\varphi(\varphi\circ\tau_1F)^{-1}=(\varphi(\tau_1F)^{-1})^{-1}=$
$(\varphi\circ\tau_1F^{-1})^{-1}$. Therefor the case of odd $k$ comes down to the previous case. Indeed,

$$\varphi\circ\tilde{\tau}_{c_1}\circ\ldots\varphi\circ\tilde{\tau}_{c_{t-2}}\circ\varphi\circ\tilde{\tau}_{c_{t-1}}\circ\varphi\circ\tilde{\tau}_{c_t}\circ\varphi(\varphi\circ\tau_1F)^{-1}\overset{3)}{\approx}$$
$$\varphi\circ\tilde{\tau}_{c_1}\circ\ldots\varphi\circ\tilde{\tau}_{c_{t-2}}\circ\varphi\circ\tilde{\tau}_{c_{t-1}}\circ\varphi\circ\tilde{\tau}_{c_t}(\varphi\circ\tau_1F^{-1})^{-1}\approx$$
$$\begin{cases}(\varphi\circ\tau_1F^{-1})^{-1}, \text{ if } t\equiv 0 \mod 3;\\ (\varphi\circ\tau_1(\varphi F^{-1})^{-1})^{-1}, \text{ if } t\equiv 1 \mod 3;\\ (\varphi\circ\tau_1\circ\varphi F)^{-1}, \text{ if } \equiv 2 \mod 3.\end{cases}$$ □

**Lemma 11.** *Let $F$ be an o-monomial. Then for $q\geq 3$*

$$(H_1(H_2(\ldots(H_qF)^{-1}\ldots)^{-1})^{-1}\approx\begin{cases}\tau_1G^{-1};\\ (\varphi\circ\tau_1G)^{-1};\\ \varphi\circ\tau_1G,\end{cases}$$

*where $G\in\{F,(\varphi F)^{-1},\varphi F^{-1},F^{-1},(\varphi F^{-1})^{-1},\varphi F\}$ and $H_i$ are defined by (23) for all $1\leq i\leq q$.*

*Proof.* First consider the following cases:

1. $q=1$. It is easy to see that from Lemma 9 follows

$$(H_1F)^{-1}\approx\begin{cases}(\tau_1F)^{-1}\approx\tau_1F^{-1};\\ (\varphi\circ\tau_1F)^{-1};\\ (\tau_1\circ\varphi F)^{-1}\approx\tau_1(\varphi F)^{-1};\\ (\varphi\circ\tau_1\circ\varphi F)^{-1};\end{cases}=\begin{cases}\tau_1G^{-1};\\ (\varphi\circ\tau_1G)^{-1},\end{cases}\tag{37}$$

where $G\in\{F,\varphi F\}$

2. $q=2$. Obviously from Lemma 10 we have

$$(H_1(\varphi\circ\tau_1F)^{-1})^{-1}=\varphi\circ\tau_1\overline{G},\tag{38}$$

where $\overline{G}\in\{F,(\varphi F)^{-1},\varphi F^{-1},F^{-1},(\varphi F^{-1})^{-1},\varphi F\}$.

Using (37) and (38) we get

$$(H_1(H_2F)^{-1})^{-1}\overset{37}{\approx}\begin{cases}(H_1\circ\tau_1G_1^{-1})^{-1}\overset{37}{\approx}\begin{cases}\tau_1G_2^{-1};\\ (\varphi\circ\tau_1G_2)^{-1};\end{cases}\\ (H_1(\varphi\circ\tau_1G_1)^{-1})^{-1}\overset{38}{\approx}\varphi\circ\tau_1\overline{G}_2,\end{cases}\tag{39}$$

where
$G_1 \in \{F, \varphi F\}$,
$G_2 \in \{G_1^{-1}, \varphi G_1^{-1}\} = A_1$,
$\overline{G}_2 \in \{G_1, (\varphi G_1)^{-1}, \varphi G_1^{-1}, G_1^{-1}, (\varphi G_1^{-1})^{-1}, \varphi G_1\} = A_2$.
It is easy to see that

$$A_1 = \{F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}\},$$

$$A_2 = \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}.$$

Indeed,
if we take $G_1 = F$ in $A_2$, then we get $\{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$, if we take $G_1 = \varphi F$, then we get the same set of o-polynomials, since
$(\varphi(\varphi F)^{-1})^{-1} \overset{(18)}{=} ((\varphi F^{-1})^{-1})^{-1} = \varphi F^{-1}$.

Note that all functions in the sets $A_1$ and $A_2$ are o-monomials.

3. $q = 3$,

$$(H_1(H_2(H_3F)^{-1})^{-1})^{-1} \overset{(39)}{\approx} \begin{cases} (H_1 \circ \tau_1 G_2^{-1})^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 G_3^{-1}; \\ (\varphi \circ \tau_1 G_3)^{-1}, \end{cases} \\ (H_1(\varphi \circ \tau_1 G_2)^{-1})^{-1} \overset{(38)}{\approx} \varphi \circ \tau_1 \overline{G}_3 \\ (H_1 \circ \varphi \circ \tau_1 \overline{G}_2)^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 \tilde{G}_3^{-1}; \\ (\varphi \circ \tau_1 \tilde{G}_3)^{-1}, \end{cases} \end{cases}$$

where $G_3 \in \{G_2^{-1}, \varphi G_2^{-1}\}$, $\overline{G}_3 \in \{G_2, \varphi G_2^{-1}, (\varphi G_2)^{-1}, G_2^{-1}, (\varphi G_2^{-1})^{-1}, \varphi G_2\}$,
$\tilde{G}_3 \in \{\overline{G}_2, \varphi \overline{G}_2\}$, $G_2 \in A_1$, $\overline{G}_2 \in A_2$.
Substituting in the corresponding sets o-monomials from $A_1$ and $A_2$, using (18), we get that $G_3, \overline{G}_3, \tilde{G}_3$ belong to $A_2$, therefore

$$(H_1(H_2(H_3F)^{-1})^{-1})^{-1} \approx \begin{cases} \tau_1 G_3^{-1}; \\ \varphi \circ \tau_1 G_3; \\ (\varphi \circ \tau_1 G_3)^{-1}, \end{cases}$$

where $G_3 \in A_2 = \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

We are going to prove this lemma by induction on the length of orbit $q$. For $q = 3$ the statement of the lemma is true as we saw above. Suppose that it is true for any $l \leq q-1$ and $l \geq 3$. By our assumption:

$$(H_1(H_2(\ldots(H_qF)^{-1}\ldots)^{-1})^{-1} \approx \begin{cases} (H_1 \circ \tau_1 G^{-1})^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 G_1^{-1}; \\ (\varphi \circ \tau_1 G_1)^{-1}, \end{cases} \\ (H_1(\varphi \circ \tau_1 G)^{-1})^{-1} \overset{(38)}{\approx} \varphi \circ \tau_1 \overline{G}_1, \\ (H_1 \circ \varphi \circ \tau_1 G)^{-1} \overset{(37)}{\approx} \begin{cases} \tau_1 \tilde{G}_1^{-1}; \\ (\varphi \circ \tau_1 \tilde{G}_1)^{-1}, \end{cases} \end{cases}$$

where $G \in A_2$, $G_1 \in \{G^{-1}, \varphi G^{-1}\}$, $\overline{G}_1 \in \{G, (\varphi G)^{-1}, \varphi G^{-1}, G^{-1}, (\varphi G^{-1})^{-1}, \varphi G\}$, $\tilde{G}_1 \in \{G, \varphi G\}$. By straightforward computations it is easy to see that all of the sets are equal to $A_2$, thus

$$(H_1(H_2(\dots(H_qF)^{-1}\dots)^{-1})^{-1} \approx \begin{cases} \tau_1 G^{-1}; \\ (\varphi\circ\tau_1 G)^{-1}; \\ \varphi\circ\tau_1 G, \end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$, which proves our statement. □

**Proposition 2.** *The modified magic action and the inverse map applied to o-monomials give at most 4 EA-inequivalent functions. For an o-monomial $F$ the 4 potentially EA-inequivalent bent functions are defined by $F, F^{-1}, (F')^{-1}$ and $F^\circ$.*

*Proof.* We use Lemma 11 and discuss the cases $q = 1, 2$ and $q \geq 3$ separately.

1. $q = 1$. According to (37) $(H_1F)^{-1}$ has the following two forms $\tau_1 G^{-1}$ and $(\varphi\circ\tau_1 G)^{-1}$, where $G \in \{F, \varphi F\}$. The first function obviously defines Niho bent functions EA-equivalent to one defined by $G^{-1}$ and therefore to those defined by $F^{-1}$ and $(\varphi F)^{-1}$ . The second function defines Niho bent functions EA-equivalent to one defined by $F^\circ$ ( by Lemma 8 ).

2. $q = 2$ . From (39) we have:

$$(H_1(H_2F)^{-1})^{-1} \approx \begin{cases} \tau_1 G_2^{-1}; \\ (\varphi\circ\tau_1 G_2)^{-1}; \\ \varphi\circ\tau_1 \overline{G}_2, \end{cases}$$

where
$G_2 \in \{F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}\}$,
$\overline{G}_2 \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

Obviously, $\tau_1 G_2^{-1}$ and $\varphi\circ\tau_1\overline{G}_2$ define Niho bent function EA-equivalent to those defined by $G_2^{-1}$ and $\overline{G}_2$ respectively, which in their turn define Niho bent functions EA-equivalent to $F, F^{-1}$ and $(F')^{-1}$. $(\varphi\circ\tau_1 G_2)^{-1}$ defines functions EA-equivalent to one defined by $F^\circ$. Indeed, $(\varphi\circ\tau_1 G_2)^{-1}$ has one of the following forms:

• $(\varphi\circ\tau_1 F^{-1})^{-1} \overset{(20)}{=} (\varphi(\tau_1 F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi\circ\tau_1 F)^{-1}$ defines Niho bent function EA-equivalent to $(\varphi\circ\tau_1 F)^{-1} = F^\circ$

• $(\varphi\circ\tau_1\circ\varphi F^{-1})^{-1}$, by Lemma 8 defines Niho bent functions EA-equivalent to $(\varphi\circ\tau_1 F^{-1})^{-1} = (\varphi(\tau_1 F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi\circ\tau_1 F)^{-1}$, which defines functions EA-equivalent to one defined by $(\varphi\circ\tau_1 F)^{-1} = F^\circ$ ;

• $(\varphi\circ\tau_1(\varphi F)^{-1})^{-1} \overset{(20)}{=} (\varphi(\tau_1\circ\varphi F)^{-1})^{-1} \overset{(18)}{=} \varphi(\varphi\circ\tau_1\circ\varphi F)^{-1}$ defines Niho bent function EA-equivalent to $F^\circ$(by Lemma 8);

• $(\varphi\circ\tau_1(\varphi F^{-1})^{-1})^{-1} = (\varphi\circ\tau_1\circ\varphi(\varphi F)^{-1})^{-1} \overset{(35)}{=} (\tau_1\circ\varphi\circ\tau_1(\varphi F)^{-1})^{-1} \overset{(20)}{=} \tau_1(\varphi\circ\tau_1(\varphi F)^{-1})^{-1}$ defines Niho bent function EA-equivalent to $(\varphi\circ\tau_1(\varphi F)^{-1})^{-1}$, which by the previous case defines Niho bent function EA-equivalent to $F^\circ$.

3. For $q \geq 3$ by Lemma 11,

$$(H_1(H_2(\dots(H_qF)^{-1}\dots)^{-1})^{-1} \approx \begin{cases} \tau_1 G^{-1}; \\ (\varphi\circ\tau_1 G)^{-1}; \\ \varphi\circ\tau_1 G, \end{cases}$$

where $G \in \{F, (\varphi F)^{-1}, \varphi F^{-1}, F^{-1}, (\varphi F^{-1})^{-1}, \varphi F\}$.

$\tau_1 G^{-1}$ and $\varphi \circ \tau_1 G$ define Niho bent function EA-equivalent to $G^{-1}$ and $G$ correspondingly, which in their turn define Niho bent functions EA-equivalent to $F, F^{-1}$ and $(\varphi F)^{-1}$.
$(\varphi \circ \tau_1 G)^{-1}$ defines Niho bent functions EA-equivalent to $F^\circ$. Indeed, for $G$ equals to $F^{-1}, (\varphi F)^{-1}, \varphi F^{-1}, (\varphi F^{-1})^{-1}$, we already prove it in the case $q = 2$. If $G = \varphi F$, then $(\varphi \circ \tau_1 G)^{-1} = (\varphi \circ \tau_1 \circ \varphi F)^{-1}$ which defines Niho bent function EA-equivalent to one defined by $F^\circ$ (by Lemma 8). If $G = F$, then $(\varphi \circ \tau_1 F)^{-1} = F^\circ$.

□

**Proposition 3.** *The modified magic action and the inverse map applied to the Frobenius map, give exactly 3 EA-inequivalent functions corresponding to $F$, $F^{-1}$, $(F')^{-1}$.*

*Proof.* For the Frobenius map $F(x) = x^{2^i}$ we have: $F^\circ = (F')^{-1} = x^{\frac{1}{1-2^i}}$. Hence by Proposition 2, $F$ can potentially define 3 EA-inequivalent Niho bent functions corresponding to $F$, $F'$ and $(F')^{-1}$. This 3 o-polynomials define 3 surly EA-inequivalent Niho bent functions [8]. □

The Payne o-polynomial can be represented via Dickson polynomials. Let us recall **Dickson Polynomials.** For every non-negative integer $d$ Dickson polynomials $D_d(x)$ over $\mathbb{F}_{2^m}$ can be defined by a recursion relation in the following way:
$D_0(x) = 0, D_1(x) = x$, $D_{d+2}(x) = xD_{d+1} + D_d(x)$, for all integers $d \geq 0$.
It satisfies the following properties:
1. $D_d \circ D_{d'} = D_{dd'}$.
2. If $d$ is co-prime with $2^m - 1$, then $D_d$ is a permutational polynomial.

Using Dickson polynomials we can prove the following results for the Payne o-polynomials.

**Lemma 12.** *Let $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$. Then $F_c^\circ = (F_c^*)^{-1}$ for any $c \in \mathbb{F}_{2^m}$.*

*Proof.* Note first, that $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}} = D_5(x^{\frac{1}{6}})$. Also it is easy to see that $F' = F$. Indeed,

$$F'(x) = xF(x^{-1}) = xD_5(x^{-\frac{1}{6}}) = x(x^{-\frac{1}{6}} + x^{-\frac{1}{2}} + x^{-\frac{5}{6}}) =$$
$$x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}} = D_5(x^{\frac{1}{6}}) = F(x).$$

Therefore $(F')^{-1} = F^{-1}$, and hence,

$$(F_c^*)^{-1} = ((\tau_c F')')^{-1} = ((\tau_c F)')^{-1} = F_c^\circ, \text{for any } c \in \mathbb{F}_{2^m}.$$

□

**Proposition 4.** *The modified magic action and the inverse map applied to o-polynomial $F(x) = x^{\frac{1}{6}} + x^{\frac{1}{2}} + x^{\frac{5}{6}}$ can potentially give EA-inequivalent Niho bent functions corresponding to o-polynomials $F$ and $F_c^\circ$, $c \in \mathbb{F}_{2^m}^*$.*

*Proof.* Immediately follows from Lemma 12. □

*Example* For $m = 5$ we checked computationally that the o-polynomial $F(x) = D_5(x^{\frac{1}{6}})$ over $\mathbb{F}_{2^m}$ defines 6 EA-inequivalent Niho bent functions corresponding to o-polynomials

$F$, $F^{-1}$ and $F_w^\circ, F_{w^3}^\circ, F_{w^5}^\circ$, where $w$ is a primitive element of $\mathbb{F}_{2^m}$.

*Remark* The modified magic action and the inverse map applied to Subiaco, Adelaide and $x^{2^k}+x^{2^k+2}+x^{3\cdot 2^k+4}$ o-polinomials $F$ can give a sequence of EA-inequivalent functions defined by o-polynomials on the orbits $F$, $F^{-1}$, $F_c^\circ$, $(\tilde{\tau}_c F)_c^\circ$, $(\tilde{\tau}_c(F'))_c^\circ$ and so on.

# 7 The Known Hyperovals[1]

Over two decades, finite geometers determined the stabilizers of all known hyperovals. In this section we provide an explicit list of all o-polynomials which provide EA-inequivalent Niho bent functions for each of the known hyperovals. We start by giving an overview over the number of EA-inequivalent Niho bent functions for each known hyperoval.

| Name | Hyperoval | Condition | Number | Ref. |
|---|---|---|---|---|
| Regular | $x^2$ | $m=1$ | 1 | [25, Th. 4.1] |
| | | $m=2$ | 1 | [25, Th. 4.1] |
| | | $m\geq 3$ | 2 | [25, Th. 4.2] |
| Irregular Translation | $x^{2^i}$ | $m=5$ or $m\geq 7$ | 3 | [25, Th. 4.3] |
| Segre | $x^6$ | $m=5$ | 2 | [25, Th. 4.4] |
| | | $m>5$ odd | 4 | [25, Th. 4.4] |
| Glynn I | $x^{3\sigma+4}$ | $m\geq 7$ odd<br>$\sigma=2^{(m+1)/2}$ | 4 | Th. 7 |
| Glynn II | $x^{\sigma+\lambda}$ | $m=7$<br>$\sigma=4=\lambda$ | 2 | Th. 7 |
| | | $m>7$ odd<br>$\sigma=2^{(m+1)/2}$<br>$\lambda=2^k$ for<br>$m=4k-1$;<br>$\lambda=2^{3k+1}$ for<br>$m=4k+1$ | 4 | Th. 7 |
| Cherowitzo | $x^\sigma+x^{\sigma+2}+x^{3\sigma+4}$ | $m=5$ | 10 | [25, Th. 4.6] |
| | | $m>5$ prime | $\frac{4m+2^m-2}{m}$ | Th. 9 |
| | | $m>5$ odd | $n_C(m)$ | [25] |
| Payne | $x^{1/6}+x^{3/6}+x^{5/6}$ | $m\geq 5$<br>is prime | $\frac{3m+2^{m-1}-1}{m}$ | Th. 8 |

[1] Some of the results will repeat Section 6.2 results. We decided to keep both of them, since we use a mix of algebraic and geometric approach.

| | | | |
|---|---|---|---|
| | $m \geq 5$<br>is odd | $n_P(m)$ | Th. 8 |
| Lunelli-Sce<br>(Subiaco) | $m = 4$<br>$\nu$ prim. root<br>$\nu^4 = \nu + 1$ | 1 | [25, Th. 4.1] |
| Subiaco | $m = 6$<br>$\lvert\mathrm{Aut}\rvert = 60$ | 3 | [35, p. 98] |
| | $m = 6$<br>$\lvert\mathrm{Aut}\rvert = 15$ | 6 | [35, p. 98] |
| | $m$ odd<br>$m = 7$ | 12 | [37] |
| | $m$ odd<br>$m > 7$ | $n_S(m)$ | Th. 11 |
| | $m \equiv 0 \pmod 4$<br>$m > 6$ | $n_S(m)$ | Th. 11 |
| | $m \equiv 2 \pmod 4$<br>$m > 6$<br>$\lvert\mathrm{Aut}\rvert = 10e$ | | Th. 12 |
| | $m \equiv 2 \pmod 4$<br>$m > 6$<br>$\lvert\mathrm{Aut}\rvert = 5e/2$<br>$5 \nmid m$ | | Th. 12 |
| Adelaide | $m = 6$ | 8 | [37] |
| | $m > 6$<br>$m$ even | $n_A(m)$ | Th. 10 |
| O'Keefe-<br>Penttila | $m = 5$ | 12 | [24, Case 2][2] |

Below, for given o-polynomials $F_1$ and $F_2$, we denote $F_1 \cong F_2$ if $F_1$ and $F_2$ define EA-equivalent Niho bent functions $g_{F_1}$ and $g_{F_2}$.

Note that a matrix corresponding to the transformation $\varphi \circ \tau_c$ is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} c & 1 \\ 1 & 0 \end{pmatrix},$$

and that $\varphi \circ \tilde{\tau}_c = \alpha_F^c \cdot (\varphi \circ \tau_c)$. Hence, by Theorem 3 the hyperoval defined by the o-polynomial $F_c^\circ$ is obtained from the hyperoval defined by $F$ using the following transformation matrix (the first matrix in the product corresponds to the inverse transforma-

[2]Notice that the reference claims $1 + 110$ instead of $1 + 11$ orbits due to a typo.

tion):

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 0 & 0 & 1 \\ 1 & 0 & c \end{pmatrix}.$$

That is,

$$F_c^\circ(x) = \left( \alpha_F^c x \Big( F\Big(\frac{1}{x} + c\Big) + F(c) \Big) \right)^{-1}$$

corresponds to the map

$$A_F^c := \begin{pmatrix} 0 & \alpha_F^c & \alpha_F^c F(c)/c \\ 0 & 0 & 1 \\ 1 & 0 & c \end{pmatrix}.$$

Also recall that the choice of an o-polynomial for a given hyperoval $\mathscr{H}$ only depends on which point of $\mathscr{H}$ is chosen as nucleus, so the o-polynomial is determined by the preimage of $(0,1,0)$. We have

$$A_F^c(c,F(c),1)^T = (\alpha_F^c F(c) + \alpha_F^c F(c)/c, 1, c+c)^T = (0,1,0).$$

Hence, $F_c^\circ \cong F_d^\circ$ if and only if $\langle (c,F(c),1) \rangle$ and $\langle (d,F(d),1) \rangle$ lie in the same point orbit of the stabilizer of $\mathscr{H}$. To summarize, we have the following:

(a) $F_c^\circ \cong F_d^\circ$ if and only if $\langle (c,F(c),1) \rangle$ and $\langle (d,F(d),1) \rangle$ lie in the same point orbit;

(b) $F \cong F_c^\circ$ if and only if $\langle (0,1,0) \rangle$ and $\langle (c,F(c),1) \rangle$ lie in the same point orbit;

(c) $F^{-1} \cong F_c^\circ$ if and only if $\langle (1,0,0) \rangle$ and $\langle (c,F(c),1) \rangle$ lie in the same point orbit;

(d) $F \cong F^{-1}$ if and only if $\langle (0,1,0) \rangle$ and $\langle (1,0,0) \rangle$ lie in the same point orbit.

As guidelined in [9] we use the known results on the orbits of the known hyperovals to get the explicit numbers and representations for o-polynomials which provide o-equivalent but EA-inequivalent Niho bent functions for each of the known hyperovals.

**Lemma 13.** *Let $m \geq 3$. The two o-polynomials obtained from the regular hyperoval $\mathscr{H}$, that is $F(x) = x^2$, are (up to EA-equivalence for the corresponding Niho bent functions) $F$ and $F^{-1}$.*

*Proof.* By [25, Th. 4.2], one point orbit is the nucleus $N$ and the other point orbit is $\mathscr{H} \setminus \{N\}$. Hence, $F^{-1}$ is a representative of the second orbit. □

**Lemma 14.** *Let $m = 5$ or $m \geq 7$. The three o-polynomials obtained from the irregular translation hyperoval $\mathscr{H}$, that is $F(x) = x^{2^i}$ with $1 < i < m-1$ co-prime to $m$, are (up to EA-equivalence for the corresponding Niho bent functions) $F$, $F^{-1}$ and $F_0^\circ$.*

*Proof.* By [25, Th. 4.3], one point orbit is the nucleus $N = (0,1,0)$, another point orbit is $N' := (1,0,0)$, and the last point orbit is $\mathscr{H} \setminus \{N, N'\}$. Hence, $F$, $F^{-1}$, and $F_0^\circ$ are representatives of the three orbits. □

**Lemma 15.** *Let $m = 3$ be odd. Consider the Segre hyperoval $\mathscr{H}$, that is $F(x) = x^6$.*

(a) *If $m = 5$, then the two o-polynomials obtained from $\mathscr{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) $F$ and $F_1^\circ$.*

(b) *If $m > 5$, then the two o-polynomials obtained from $\mathscr{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) $F$, $F^{-1}$, $F_0^\circ$, and $F_1^\circ$.*

*Proof.* By [25, Th. 4.4], for $m = 5$ the point orbits of $\mathscr{H}$ are $\{(1,0,0),(0,1,0),(0,0,1)\}$ and all the remaining points. Hence, $(0,1,0)$ and $(1,1,1)$ are representatives, so we can choose $F$ and $F_1^\circ$ as representatives. For $m > 5$ the first orbit splits into three orbits, so we have to add $F^{-1}$ and $F_0^\circ$ to the previous list. □

**Theorem 7.** *The collineation stabilizer of a Glynn hyperoval has* 4 *orbits unless it is of type II and $m = 7$.*

*Proof.* First consider the case Glynn I. By [25, Th. 4.4] we have 4 orbits unless $(3\sigma + 4)^2 - (3\sigma + 4) + 1 \equiv 0 \pmod{2^m - 1}$. This simplifies to

$$9 \cdot 2^{m+1} + 21 \cdot 2^{(m+1)/2} + 13 \equiv 31 + 21 \cdot 2^{(m+1)/2} \equiv 0 \pmod{2^m - 1}.$$

One can easily check that this is never satisfied.

Now consider the case Glynn II. By [25, Th. 4.4] we have 4 orbits unless $(\sigma + \lambda)^2 - (\sigma + \lambda) + 1 \equiv 0 \pmod{2^m - 1}$. For $m = 4k - 1$, this is

$$2^{(3m+7)/4} - 2^{(m+1)/4} + 3 \equiv 0 \pmod{2^m - 1}.$$

Equality holds only for $m = 7$ as for $m > 7$ the left hand side is smaller than $2^m - 1$. The calculation for $m = 4k + 1$ is similar. □

Similar to Lemma 15, we obtain the following.

**Lemma 16.** *Let $m \geq 7$ be odd. Consider a hyperoval $\mathscr{H}$ of type Glynn I or Glynn II.*

(a) *If $m = 7$ , then the two o-polynomials obtained from $\mathscr{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) $F$ and $F_1^\circ$.*

(b) *Otherwise, the four o-polynomials obtained from $\mathscr{H}$ are (up to EA-equivalence for the corresponding Niho bent functions) $F$, $F^{-1}$, $F_0^\circ$, and $F_1^\circ$.*

**Theorem 8.** *The number of orbits of the collineation stabilizer of the Payne hyperoval $\mathscr{H}$ is given by $3 + \frac{2^{m-1}}{m}$ if $m$ is a prime. More generally, the number of orbits are given by*

$$n_P(m) := 3 + \sum_{\ell \mid m, \ell > 1} \left| \mathbb{F}_{2^\ell}^* \setminus \bigcup_{h \mid \ell,\, h < \ell} \mathbb{F}_{2^h}^* \right| / (2\ell).$$

*For $w$ a primitive element of $\mathbb{F}_q$ and $c = w^{2n}$, we get $F_c^\circ \cong F_d^\circ$ if and only if $d = w^{2^i n}$ or $d = w^{-2^i n}$ for some $i \in \{1, \ldots, m\}$. The o-polynomials $F$ and $F^{-1}$ define Niho bent functions EA-inequivalent to those defined by all other o-polynomials from $\mathscr{H}$.*

*Proof.* By [25, Th. 4.5], the orbits are $\{(0,1,0)\}$, $\{(1,0,0),(0,0,1)\}$, and sets

$$\mathscr{H}_n := \{(w^{n2^i}, f(w^{n2^i}),1) : i = 1,\ldots,m\} \cup \{(1, f(w^{n2^i}), w^{n2^i}) : i = 1,\ldots,m\},$$

where $w$ is a primitive element of $\mathbb{F}_q$. Notice that $\mathscr{H}_0$ is $\{(1,1,1)\}$. For $m$ prime it is easy to see that each orbit $\mathscr{H}_n$ has length $m$ for $n > 1$, hence the total number of orbits is $3 + \frac{2^{m-1}-1}{m}$. In general, if $w^n \in \mathbb{F}_\ell$ with $\ell \mid m$, then $\{(w^n)^{2^i}\} \in \mathbb{F}_\ell$. This yields the general formula.

The description of the equivalence of $F_c^\circ$ and $F_d^\circ$ follows directly from the explicit description of the orbits. □

For example for $m = 5$, the previous result gives the following representatives for all 6 o-polynomials which can be obtained from the Payne hyperoval:

$$F,\ F^{-1},\ F_1^\circ,\ F_w^\circ,\ F_{w^3}^\circ,\ F_{w^5}^\circ.$$

**Theorem 9.** *The number of orbits of the collineation stabilizer of the Cherowitzo hyperoval is given by* $4 + 2\frac{2^{m-1}-1}{m}$ *if m is a prime. More generally, the number of orbits are given by*

$$n_C(m) := 3 + \sum_{\ell \mid m} \left| F^*(2^\ell) \setminus \bigcup_{h \mid \ell,\, h<\ell} \mathbb{F}_{2^h}^* \right| / \ell.$$

*For w a primitive element of* $\mathbb{F}_q$ *and* $c = w^{2n}$*, we get* $F_c^\circ \cong F_d^\circ$ *if and only if* $d = w^{2^i n}$ *for some* $i \in \{1,\ldots,m\}$*. The Niho bent functions* $g_F$ *and* $g_{F^{-1}}$ *are both EA-inequivalent to Niho bent functions defined by all other o-polynomials from* $\mathscr{H}$*.*

*Proof.* Corollary 4.5 in [3] describes the stabilizer as

$$\{(x,y,z) \mapsto (x^\alpha, y^\alpha, z^\alpha) : \alpha \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

The rest of the calculation is similar to the Payne hyperoval, just that this time the first and second coordinate cannot be interchanged. □

**Theorem 10.** *Let* $[1] := \delta + \delta^{-1}$*. For* $c \in \mathbb{F}_q$*, let*

$$O_c := \{c^{2^h} + \sum_{i=1}^{h-1} [1]^{2^i} : i = 0,\ldots,2m-1\}.$$

*The number of EA-inequivalent Niho bent functions obtained from the Adelaide hyperoval is* $n_A(m) := 2 + |\{O_c : c \in F_q\}|$*. In particular, for fixed* $c \in F_q$*, the Niho bent functions defined by the o-polynomials* $F$*,* $F^{-1}$*,* $F_c^\circ$ *are pairwise EA-inequivalent. Furthermore,* $g_{F_c^\circ}$ *and* $g_{F_d^\circ}$ *are EA-equivalent if and only if* $d \in O_c$*.*

*Proof.* In [34, Eq. (9)] (in a slightly different representation) the stabilizer of the Adelaide polynomial was determined as the cyclic group generated by the map

$$\theta : x \mapsto \begin{pmatrix} 1 & 0 & [1] \\ 0 & 1 & [1] \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ F(x) \\ 1 \end{pmatrix}^2.$$

From this it is easily verified that $\theta$ fixes $(0,1,0)$ and $(1,0,0)$, so $g_F$ and $g_{F^{-1}}$ are not EA-equivalent to those functions defined by any of the other o-polynomials. Furthermore, it is easily checked that the orbit of $(c,F(c),1)$ is

$$\{(x,F(x),1) : x \in O_c\}. \qquad \square$$

**Theorem 11.** *Let $m \geq 7$ with $m \not\equiv 2 \pmod 4$, let*

$$O_c := \{x^{(-1)^{i+1}2^i} : i = 0,\ldots,2m-1\}.$$

*The number of EA-inequivalent Niho bent functions obtained from the Subiaco hyperoval is $n_S(m) := 2+|\{O_c : c \in F_q\}|$. In particular, for fixed $c \neq 0,1$, the o-polynomials $F$, $F^{-1}$, $F_0^\circ$, $F_c^\circ$ provide pairwise EA-inequivalent Niho bent functions. Furthermore, $g_{F_c^\circ}$ and $g_{F_d^\circ}$ are EA-equivalent if and only if $d \in O_c$.*

*Proof.* By [26, Th. 13, Th. 16] (see also [17]), the stabilizer of the Subiaco hyperoval $\mathscr{H}$ is generated by the map

$$\theta : x \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ F(x) \\ 1 \end{pmatrix}^2.$$

From this it is easily verified that $\theta$ fixes $(0,1,0)$, $\{(1,0,0),(0,0,1)\}$, $(1,1,1)$, so Niho bent functions defined by $F$, $F^{-1} \cong F_0^\circ$, and $F_1^\circ$ are not EA-equivalent to those defined by any other o-polynomial obtained from $\mathscr{H}$. Furthermore, it is easily checked that the orbit of $(c,F(c),1)$ is

$$\{(x,F(x),1) : x \in O_c\}. \qquad \square$$

For $m \equiv 2 \pmod 4$ there are two types of non-equivalent hyperovals, see [36]. In particular, from Theorem 6.6 and Theorem 6.7 in [36] we obtain the following. We are not aware of any nice description of the orbits of the given groups, but the information is sufficient to calculate all o-polynomials efficiently.

**Theorem 12.** *Let $m \geq 6$ with $m \equiv 2 \pmod 4$.*

*(a) If $F(x) = \frac{\delta^2(x^4+x)}{x^4+\delta^2x^2+1} + x^{1/2}$, then $g_F$ is EA-inequivalent to all $g_{F_c^\circ}$ and we have $F^{-1} \cong F_0^\circ$. Furthermore, $F_c^\circ \cong F_d^\circ$ if and only if $(c,F(c),1)^h = (d,F(d),1)$ for an element $h$ of the group (of size $10m$) generated by*

- *(i)* $(x,y,z) \mapsto (z,y,x)$,
- *(ii)* $(x,y,z) \mapsto (x+\delta z, y+\delta^2 z, z)$,
- *(iii)* $(x,y,z) \mapsto (z^2+\delta^2x^2, z^2+\delta y^2, z^2)$.

*(b) If $F(x) = \frac{x^3+x^2+\delta^2x}{x^4+\delta^2x^2+1} + \delta x^{1/2}$, then $g_F$, $g_{F^{-1}}$, and $g_{F_0^\circ}$ are pairwise EA-inequivalent. Furthermore, $F_c^\circ \cong F_d^\circ$ if and only if $(c,F(c),1)^h = (d,F(d),1)^h$ for an element $h$ of the group (of size $5m/2$) generated by*

- *(i)* $(x,y,z) \mapsto (x^\sigma, y^\sigma, z^\sigma)$ *for* $\sigma \in Aut(F)$ *with* $\delta^\sigma = \delta$,

*(ii)* $(x,y,z) \mapsto (z, y+\delta z, x+\delta z)$.

The O'Keefe-Penttila hyperoval for $m = 5$, which is not known to belong to any infinite family, is stabilized by the group generated by

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Hence, most orbits have the form $\{(c, F(c), 1), (1+c^{-1}, 1+c^{-1}F(c), 1), ((1+c)^{-1}, c^{-1}(1+F(c), 1)\}$. Then, representatives for the 14 o-polynomials obtained from the hyperoval and defining EA-inequivalent Niho bent functions are

$$F,\ F^{-1},\ F_w^\circ,\ F_{w^2}^\circ,\ F_{w^4}^\circ,\ F_{w^5}^\circ,\ F_{w^7}^\circ,\ F_{w^8}^\circ,\ F_{w^{10}}^\circ,\ F_{w^{14}}^\circ,\ F_{w^{16}}^\circ,\ F_{w^{19}}^\circ.$$

Here $w$ is a primitive element of $\mathbb{F}_{2^5}$.

Note that one can find similar results in [2]. We use a different approach for finding representatives of o-polynomials on the different orbits. Also, we use their different representation (via generators of the Magic action and the inverse map) than in [2]. Therefore, we consider our representation sufficiently different. Furthermore, our results are slightly more detailed, for instance in [2] the author only estimates the number of EA-inequivalent Niho bent functions from Cherowitzo and Payne hyperovals, while we provide explicit formulas.

## Acknowledgment

The authors would like to thank Alexander Kholosha for useful discussions. This research was supported by Trond Mohn Stiftelse (TMS). The work of Ferdinand Ihringer is supported by a postdoctoral fellowship of the Research Foundation – Flanders (FWO).

## References

[1] K. Abdukhalikov, "Bent functions and line oval", *Finite Fields Appl.*, 47, pp. 97–124, 2017.

[2] K. Abdukhalikov, "Equivalence classes of Niho bent functions", 2019. https://arxiv.org/abs/1903.04450

[3] L. Bayens, W. Cherowitzo and T. Penttila. "Groups of hyperovals in Desarguesian planes", *Inn. Inc. Geom.*, pp. 6–7, 2007.

[4] L. Budaghyan and C. Carlet, "CCZ-equivalence of single and multi output Boolean functions", AMS Contemporary Math. 518, *Post-proceedings of the conference Fq9*, pp. 43–54, 2010.

[5] L. Budaghyan and C. Carlet, "On CCZ-equivalence and its use in secondary constructions of bent functions", *Preproceedings of International Workshop on Coding and Cryptography WCC 2009*, pp. 19–36, 2009.

[6] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, “Niho bent functions from quadratic o-monomials”, *Proceedings of the 2014 IEEE International Symposium on Information Theory*, pp. 1827–1831, 2014.

[7] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, “Further results on Niho bent functions”, *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 6979–6985, 2012.

[8] L. Budaghyan, C. Carlet, T. Helleseth and A. Kholosha, ”On o-equivalence of Niho Bent functions”, *WAIFI 2014*, Lecture Notes in Comp. Sci. 9061, pp. 155–168, 2015.

[9] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, T. Penttila. ”Projective equivalence of ovals and EA-equivalence of Niho bent functions”, Book of Abstracts of ”Finite geometries fourth Irsee conference”, Sept. 2014; the slides from the presentation can be found at https://people.uib.no/lbu061/irsee.pdf

[10] C. Carlet, ”Boolean Functions for Cryptography and Coding Theory”, Monograph in *Cambridge University Press*, 562 pages, 2020 .

[11] C. Carlet, “Boolean functions for cryptography and error-correcting codes”, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ser. Encyclopedia of Mathematics and its Applications, Y. Crama and P. L. Hammer, Eds. Cambridge: Cambridge University Press, 2010, vol. 134, ch. 8, pp. 257–397.

[12] C. Carlet and S. Mesnager, “On Dillon’s class $H$ of bent functions, Niho bent functions and o-polynomials”, *J. Combin. Theory Ser. A*, vol. 118, no. 8, pp. 2392–2410, Nov. 2011.

[13] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography* 78(1), pp. 5–50, 2016.

[14] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, “On the dual of bent functions with $2^r$ Niho exponents”, *Proceedings of the 2011 IEEE International Symposium on Information Theory*. IEEE, Jul./Aug. 2011, pp. 657–661.

[15] W. E. Cherowitzo and L. Storme, “$\alpha$-Flocks with oval herds and monomial hyperovals”, *Finite Fields Appl.*, vol. 4, no. 2, pp. 185–199, Apr. 1998.

[16] W. Cherowitzo, “Hyperovals in Desarguesian planes of even order”, *Ann. Discrete Math.*, 37, pp. 87–94, 1988.

[17] W. Cherowitzo, T. Penttila, I. Pinneri, and G. Royle. ”Flocks and Ovals”, *Geom. Dedicata*, 60, pp. 17–37, 1996.

[18] P. Dembowski, Finite Geometries, Springer, 1968.

[19] J. F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, Univ. Maryland, College Park. MD, USA, 1974.

[20] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, “Construction of bent functions via Niho power functions”, *J. Combin. Theory Ser. A*, vol. 113, no. 5, pp. 779–798, Jul. 2006.

[21] D. Glynn, "Two new sequences of ovals in finite desarguesian planes of even order", *Combinatorial Mathematics*, Lecture Notes in Mathematics, vol. 1036, pp. 217–229, 1983.

[22] T. Helleseth, A. Kholosha, and S. Mesnager, "Niho bent functions and Subiaco hyperovals", *Theory and Applications of Finite Fields*, ser. Contemporary Mathematics, M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, Eds., vol. 579. Providence, Rhode Island: American Mathematical Society, pp. 91–101, 2012.

[23] C. M. O'Keefe and T. Penttila, "Automorphism Groups of Generalized Quadrangles via an Unusual Action of $P\Gamma L(2,2^h)$", *Europ J. Combinatorics*, 33, pp. 213–232, 2002.

[24] C. M. O'Keefe and T. Penttila. "A new hyperoval in $PG(2,32)$", *J. Geom.*, 44, pp. 117–139, 1992.

[25] C. M. O'Keefe and T. Penttila. "Symmetries of Arcs", *J. Combin. Theory Ser. A*, 66, pp. 53–67, 1994.

[26] C. M. O'Keefe and J. Thas. "Collineations of Subiaco and Cherowitzo hyperovals", *Bull. Belg. Math. Soc.*, 3, pp. 177–192, 1996.

[27] A. Kholosha and A. Pott, "Bent and related functions" in *Handbook of Finite Fields*, ser. Discrete Mathematics and its Applications, G. L. Mullen and D. Panario, Eds. London: CRC Press, 2013, ch. 9.3, pp. 255–265.

[28] G. Leander and A. Kholosha, "Bent functions with $2^r$ Niho exponents", *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5529–5532, Dec. 2006.

[29] N. Li, T. Helleseth, A. Kholosha, and X. Tang, "On the Walsh transform of a class of functions from Niho exponents", *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4662–4667, Jul. 2013.

[30] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials", *Journal Designs, Codes and Cryptography*. 77(1), pp. 99–116, 2015.

[31] S. Mesnager, "Bent Functions: Fundamentals and Results", Springer, Switzerland S2016, ISBN 978-3-319-32593-4.

[32] R. L. McFarland, "A family of difference sets in non-cyclic groups", *J. Combin. Theory Ser. A*, vol. 15, no. 1, pp. 1–10, Jul. 1973.

[33] K. Nyberg, " S-boxes and Round Functions with Controllable Linearity and Differential Uniformity", *Proceedings of Fast Software Encryption*, LNCS 1008, 1994, pp. 111-130, 1995.

[34] S. Payne and J. A. Thas. "The stabilizer of the Adelaide oval", *Discrete Math.*, 294, pp. 161–173, 2005.

[35] T. Penttila and I. Pinneri. "Irregular Hyperovals in $PG(64,2)$", *J. Geom.*, 51, pp. 89–100, 1994.

[36] S. E. Payne, T. Penttila and I. Pinneri. "Isomorphisms Between Subiaco and $q$-Clan Geometries", *Bull. Belg. Math. Soc.*, 2, pp. 197–222, 1995.

[37] T. Penttila and G. Royle. ”On Hyperovals in Small Projective Planes”, *J. Geom.*, 54, pp. 91–104, 1995.

[38] O. S. Rothaus, “On “bent” functions,” *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, May 1976.

[39] T. L. Vis, “Monomial hyperovals in Desarguesian planes,” Ph.D. dissertation, University of Colorado Denver, 2010.

# Paper II

## On two fundamental problems on APN power functions

Lilya Budaghyan, Marco Calderini, Claude Carlet, Diana Davidova, and Nikolay S. Kaleyski
*Cryptology ePrint Archive: Report 2020/1359*
Submitted to *IEEE Transactions on Information Theory* in 2020

# Paper III

## Generalization of a class of APN binomials to Gold-like functions

Diana Davidova and Nikolay S. Kaleyski
*Lecture Notes in Computer Science*, 12542, pp. 195–206 (2021)

# Generalization of a class of APN binomials to Gold-like functions

Diana Davidova and Nikolay Kaleyski
Department of Informatics, University of Bergen, Norway

**Abstract**

In 2008 Budaghyan, Carlet and Leander generalized a known instance of an APN function over the finite field $\mathbb{F}_{2^{12}}$ and constructed two new infinite families of APN binomials over the finite field $\mathbb{F}_{2^n}$, one for $n$ divisible by 3, and one for $n$ divisible by 4. By relaxing conditions, the family of APN binomials for $n$ divisible by 3 was generalized to a family of differentially $2^t$-uniform functions in 2012 by Bracken, Tan and Tan; in this sense, the binomials behave in the same way as the Gold functions. In this paper, we show that when relaxing conditions on the APN binomials for $n$ divisible by 4, they also behave in the same way as the Gold function $x^{2^s+1}$ (with $s$ and $n$ not necessarily coprime). As a counterexample, we also show that a family of APN quadrinomials obtained as a generalization of a known APN instance over $\mathbb{F}_{2^{10}}$ cannot be generalized to functions with $2^t$-to-1 derivatives by relaxing conditions in a similar way.

**Keywords.** Almost perfect nonlinear, Boolean functions Differential uniformity Walsh transform Walsh spectrum.

## 1 Introduction

Let $n,m$ be natural numbers. A *vectorial Boolean* $(n,m)$*-function*, or simply an $(n,m)$*-function*, or vectorial Boolean function, is a mapping from the $n$-dimensional vector space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2 = \{0,1\}$ to the $m$-dimensional vector space $\mathbb{F}_2^m$. Since the extension field $\mathbb{F}_{2^n}$ can be identified with an $n$-dimensional vector space over $\mathbb{F}_2$, $(n,m)$-functions can be seen as functions between the Galois fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$. Vectorial Boolean functions have many applications in mathematics and computer science. In cryptography, they are the basic building blocks of block ciphers, and the choice of functions directly influences the security of the cipher. In order to construct cryptographically secure ciphers, it is necessary to understand what properties such functions need to possess in order to resist various types of cryptanalytic attacks, and to find methods for constructing functions having these desirable properties. In our work, we mostly concentrate on the case when $n = m$, i.e. when the numbers of input and output bits are the same. A comprehensive survey on $(n,m)$-functions can be found in [4, 8].

One of the most powerful attacks against block ciphers is differential cryptanalysis, introduced by Biham and Shamir [1]. The attack is based on studying how the difference in two inputs to a function affects the difference in the corresponding outputs. The resistance to differential attacks of an $(n,m)$-function is measured by a property called its differential uniformity. The lower the differential uniformity, the more resistant the cryptosystem is to differential attacks. The class of almost perfect nonlinear (APN) functions is defined as the class of $(n,n)$-functions having the best possible differential uniformity, and thus provides optimal security against differential cryptanalysis.

Another powerful attack against block ciphers is linear cryptanalysis, introduced by Matsui [12]. The property of a function which measures the resistance to this kind of attack is called nonlinearity. The nonlinearity $\mathscr{NL}(F)$ of an $(n,m)$-function $F$ is defined to be the minimum Hamming distance between any component of $F$ and any affine $(n,1)$-function. An upper bound on the nonlinearity of any $(n,n)$-function can be derived, and the class of almost bent (AB) functions is defined as the class of those functions that meet this bound with equality and therefore provide the best possible resistance to linear attacks.

Recall that the Gold functions are APN power functions over $\mathbb{F}_{2^n}$ of the form $x^{2^s+1}$ for some natural number $s$ satisfying $\gcd(s,n)=1$. Relaxing the condition to $\gcd(s,n)=t$ for some positive integer $t$, the functions of the form $F(x)=x^{2^s+1}$ become differentially $2^t$-uniform, with all their derivatives $D_aF(x)=F(x)+F(a+x)$ for $a\neq 0$ being $2^t$-to-1 functions. These functions are permutations if and only if $n/\gcd(s,n)=n/t$ is odd [13], and are $(2^t+1)$–to–1 functions otherwise. Their nonlinearity is $2^{n-1}-2^{(n+t)/2}$ when $n/t$ is odd, and $2^{n-1}-2^{(n+2t)/2}$ otherwise.

In 2008, two infinite families of (n, n)-APN binomials inequivalent to power functions were introduced in [5] for values of n divisible by 3 or by 4 as generalizations of a known sporadic APN instance over $\mathbb{F}_{2^{12}}$ [11]. These were the first known infinite families of APN functions that are inequivalent to power functions. It was later shown in 2012 that the family of APN binomials for $n$ divisible by 3 can be generalized to functions with $2^t$-to-1 derivatives (for some positive integer $t$) with nonlinearity equal to $2^{n-1}-2^{(n+t)/2}$ for $n+t$ even, and $2^{n-1}-2^{(n+t-1)/2}$ for $n+t$ odd by relaxing conditions [3]. Thus, the APN binomials for $n$ divisible by 3 behave in the same way as the Gold functions from the point of view of differential uniformity, nonlinearity and properties of the image set.

In this paper we show that the second class of APN binomials from [5] (for $n$ divisible by 4) also behaves in the same way as the Gold functions in this respect. We note that all the constructed functions (much like the APN binomials) are quadratic, and are therefore not directly suitable for cryptographic use in practice. Nonetheless, the vast majority of known APN functions are given by a quadratic representation, but contain representatives of higher algebraic degrees in their CCZ-equivalence class. We also consider the family of APN quadrinomials constructed by generalizing a known APN instance over $\mathbb{F}_{2^{10}}$ [7] and computationally verify that they provide a counterexample to this approach, in the sense that they cannot be generalized to functions with $2^t$-to-1 derivatives by relaxing conditions in a similar way for any even dimension $n$ in the range $6\leq n\leq 14$.

The paper is structured as follows. In Section 2, we recall the basic definitions and results that we use throughout our work. In Section 3, we compute the differential uniformity of the generalized families of binomials; an upper bound on their nonlinearity is then derived in Section 4. Section 5, in which we computationally show that the APN quadrinomials constructed in [7] cannot be generalized to $2^t$-uniform functions over $\mathbb{F}_{2^n}$ with $6\leq n\leq 14$, concludes the paper.

# 2 Preliminaries

Let $n$ be a positive integer. Then $\mathbb{F}_{2^n}$ denotes the finite field with $2^n$ elements, and $\mathbb{F}_{2^n}^*$ denotes its multiplicative group. For any positive integer $k$ dividing $n$, the trace function $\mathrm{Tr}_k^n$ is the mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ defined by $\mathrm{Tr}_k^n(x)=\sum_{i=0}^{\mathbb{F}racnk-1}x^{2^{ik}}$. For $k=1$, the function $\mathrm{Tr}_1^n:\mathbb{F}_{2^n}\to\mathbb{F}_2$ is called the *absolute trace* over $\mathbb{F}_{2^n}$ and is denoted simply by $\mathrm{Tr}_n(x)$, or by $\mathrm{Tr}(x)$ if the dimension $n$ is clear from context.

Let $n$ and $m$ be positive integers. An $(n,m)$-*function* is any function $F$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$. For any $(n,m)$-function $F$ and for any $a \in \mathbb{F}_{2^n}$, the function $D_aF(x) = F(x+a) + F(x)$ is called the *derivative of $F$ in the direction $a$*. Let $\delta_F(a,b)$ denote the number of solutions of the equation $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$. The multiset $\{\delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^m}\}$ is called the *differential spectrum* of $F$. The *differential uniformity* of $F$ is the largest value in its differential spectrum. We say that $F$ is *differentially $\delta$-uniform* if its differential uniformity is at most $\delta$. The differential uniformity of any $(n,m)$-function is clearly always even, since if $x \in \mathbb{F}_{2^n}$ is a solution to $D_aF(x) = b$ for some $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^m}$, then so is $x+a$. The lowest possible differential uniformity of any function is thus 2. A function with differential uniformity equal to 2 is called *almost perfect nonlinear (APN)*. Since a low differential uniformity corresponds to a strong resistance to differential cryptanalysis, APN functions provide optimal security against this type of attack.

A *component function* of an $(n,m)$-function $F$ is any function of the form $x \mapsto \mathrm{Tr}_m(cF(x))$ for $c \in \mathbb{F}_{2^m}^*$. The component functions are clearly $(n,1)$-functions. The nonlinearity $\mathscr{NL}(F)$ of $F$ is the minimum Hamming distance between any component function of $F$ and any affine $(n,1)$-function, i.e. any function $a : \mathbb{F}_{2^n} \to \mathbb{F}_2$ satisfying $a(x) + a(y) + a(z) = a(x+y+z)$ for all $x,y,z \in \mathbb{F}_{2^n}$. Recall that the Hamming distance between two $(n,1)$-functions $f$ and $g$ is the number of inputs $x \in \mathbb{F}_{2^n}$ for which $f(x) \neq g(x)$.

An important tool for analyzing any $(n,m)$-function $F$ is the so-called Walsh transform. The *Walsh transform of $F$* is the function $W_F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^n} \to \mathbb{Z}$ defined as $W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_m(aF(x)) + Tr_n(bx)}$.

The nonlinearity of an $(n,m)$-function $F$ can be expressed as $\mathscr{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^n}} |W_F(a,b)|$. The nonlinearity of any $(n,n)$-function is bounded from above by $2^{n-1} - 2^{(n-1)/2}$[10]. Functions attaining this bound are called *almost bent (AB)*. Clearly, AB functions exist only for odd values of $n$; when $n$ is even, functions with nonlinearity $2^{n-1} - 2^{n/2}$ are known, and it is conjectured that this value is optimal in the even case. Nonlinearity measures the resistance to linear cryptanalysis; the higher the nonlinearity, the better. Thus, AB functions provide optimal security against linear cryptanalysis when $n$ is odd. Furthermore, all AB functions are necessarily APN [10], so that AB functions are optimal with respect to differential cryptanalysis as well.

Due to the huge number of $(n,m)$-functions for non-trivial values of $n$ and $m$, they are typically classified up to some notion of equivalence. The most general known equivalence relation which preserves differential uniformity (and hence APN-ness) is Carlet-Charpin-Zinoviev (or CCZ) equivalence [6, 9]. We say that two $(n,m)$-functions $F$ and $F'$ are *CCZ-equivalent* if there is an affine permutation $\mathscr{A}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ that maps the graph $\mathscr{G}(F) = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of $F$ to the graph $\mathscr{G}(F')$ of $F'$. A special case of CCZ-equivalence is extended affine (or EA) equivalence. We say that $F$ and $F'$ are *EA-equivalent* if there are affine permutations $A_1$ and $A_2$ of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively, and an affine $(n,m)$-function $A$ such that $F' = A_1 \circ F \circ A_2 + A$.

In [5], Budaghyan, Carlet and Leander introduced the following two infinite families of APN binomials:

1. For $n = 3k$:

$$F_3(x) = x^{2^s+1} + w^{2^k-1} x^{2^{ik}+2^{mk+s}}, \tag{1}$$

where $s$ and $k$ are positive integers such that $s \leq 4k-1$, $\gcd(k,3) = \gcd(s,3k) = 1$, $i = sk \bmod 3$, $m = 3-i$ and $w$ is a primitive element of the field $\mathbb{F}_{2^n}$.

2. For $n = 4k$:

$$F_4(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}}, \tag{2}$$

where $s$ and $k$ are positive integers such that $s \leq 4k-1$, $\gcd(k,2) = \gcd(s,2k) = 1$, $i = sk \mod 4$, $m = 4-i$ and $w$ is a primitive element of the field $\mathbb{F}_{2^n}$.

The first class of APN binomials (for $n$ divisible by 3) are permutations if and only if $k$ is odd.

As we show below, if the condition of $k$ being odd is omitted, the binomials for $n$ divisible by 4 are EA-equivalent to the Gold functions. Indeed, let $k$ be even. Then $i = sk \mod 4$ is also even. If $i = 2$, then

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1}x^{2^{2k}+2^{2k+s}} = x^{2^s+1} + w^{2^k-1}x^{2^{2k}(1+2^s)} = x^{2^s+1} + w^{2^k-1}(x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to $x^{2^s+1}$ since $x \mapsto x + w^{2^k-1}x^{2^{2k}}$ is a linear permutation. Indeed, if $x + w^{2^k-1}x^{2^{2k}} = y + w^{2^k-1}y^{2^{2k}}$ and $x \neq y$, then we must have $w^{1-2^k} = (x+y)^{2^{2k}-1}$ which is impossible since $2^{2k}-1$ is a multiple of 5 under the hypothesis, whereas $2^k-1$ is not.

In the same manner, if $i = 0$, we get

$$F(x) = x^{2^s+1} + w^{2^k-1}x^{2^{ik}+2^{mk+s}} = x^{2^s+1} + w^{2^k-1}x^{1+2^s} = x^{2^s+1}(1 + w^{2^k-1}).$$

The complete Walsh spectra of the functions $F_3$ and $F_4$ were determined in [2].

As previously mentioned, relaxing the conditions allows the functions $F_3$ to be generalized to a family of $2^t$-differentially uniform functions in the same way as the Gold functions [3]. In this paper, we show how the family $F_4$ can be generalized to functions with $2^t$-to-1 derivatives in a similar way. Further, we provide a counterexample to the question of whether this construction can be used to generalize any family of quadratic APN functions to a family of $2^t$-uniform functions: for the family of quadrinomials from [7], we computationally verify that relaxing conditions does not lead to functions with $2^t$-to-1 derivatives for $t > 1$ over $\mathbb{F}_{2^n}$ for any $6 \leq n \leq 14$.

For background on APN functions and cryptographic Boolean functions, we refer the reader to [4] or [8].

# 3 Differential uniformity

In the following theorem, we show that by relaxing the condition $\gcd(s,2k) = 1$ in (2) to $\gcd(s,2k) = t$ for some positive integer $t$, we obtain functions over $\mathbb{F}_{2^{4k}}$ all of whose derivatives are $2^t$-to-1 functions.

**Theorem 1.** *Let $s,k,t$ be positive integers and let $n = 4k$. Let $\gcd(s,2k) = t$, $2 \nmid k$, $i = sk \mod 4$, $m = 4-i$, and $w$ be a primitive element of $\mathbb{F}_{2^n}$. Then all derivatives $D_aF$ for $a \in \mathbb{F}_{2^n}^*$ of the function*

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^{ik}+2^{mk+s}} \tag{3}$$

*are $2^t$-to-1 functions. In particular, $F$ is differentially $2^t$-uniform.*

*Proof.* We first show that for $i$ even, $F$ is EA-equivalent to $x^{2^s+1}$. To see this, consider two cases depending on the value of $i$. First, suppose $i = 2$. Then

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^{2k}+2^{2k+s}} = wx^{2^s+1} + w^{2^k}(x^{2^s+1})^{2^{2k}}$$

which is EA-equivalent to $x^{2^s+1}$ since $x \mapsto wx + w^{2^k}x^{2^{2k}}$ is a linear permutation. Indeed, suppose that $wx + w^{2^k}x^{2^{2k}} = wy + w^{2^k}y^{2^{2k}}$ for some two distinct elements $x, y \in \mathbb{F}_{2^n}$; then $(x+y)^{2^{2k}-1} = w^{1-2^k}$ which is a contradiction since the exponent on the left-hand side is a multiple of three, while the one on the right-hand side is not. Finally, note that the derivatives of $x^{2^s+1}$ are all $2^t$-to-1 functions since $\gcd(s, 4k) = \gcd(s, 2k) = t$.

If $i = 0$, then

$$F(x) = wx^{2^s+1} + w^{2^k}x^{1+2^{4k+s}} = wx^{2^s+1} + w^{2^k}x^{1+2^s} = x^{2^s+1}(w + w^{2^k}),$$

which is EA-equivalent to $x^{2^s+1}$ (as $w$ is a primitive element, we have $w + w^{2^k} \neq 0$), and hence all of its derivatives are $2^t$-to-1 under the conditions on $s, t$ and $k$.

We now consider the case of $i$ odd. Both possibilities for $i$ produce functions in the same EA-equivalence class. For $i = 1$, the function (3) takes the form

$$F(x) = wx^{2^s+1} + w^{2^k}x^{2^k+2^{3k+s}}. \tag{4}$$

Consider the function $F'$ defined by

$$F'(x) = F(x)^{2^{3k}} = (wx^{2^s+1} + w^{2^k}x^{2^k+2^{3k+s}})^{2^{3k}} = wx^{2^{2k+s}+1} + w^{2^{3k}}x^{2^{3k}(2^s+1)}.$$

Clearly, $F'$ is EA-equivalent to $F$. From the condition $ks = 1 \mod 4$ we get $k \mod 4 = s \mod 4$, i.e. $2k + s = 3s \mod 4$, hence $(2k+s)k = 3sk = 3 \mod 4$. Thus, denoting $2k+s$ by $s'$, we get $F'(x) = wx^{2^{s'}+1} + w^{2^{-k}}x^{2^{3k}+2^{k+s'}}$, which is precisely the function from (3) for $i = 3$.

It is thus enough to prove the theorem for $i = 3$, i.e. for the function $F(x) = wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}}$.

The derivatives of $F$ are $2^t$-to-1 functions if and only if the equation $F(x) + F(x+v) = u$ has either 0 or $2^t$ solutions for any $u, v \in \mathbb{F}_2^n, v \neq 0$. The left-hand side of this equality takes the form

$$\begin{aligned}
&F(x) + F(x+v) = \\
&wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}} + w(x+v)^{2^s+1} + w^{2^k}(x+v)^{2^{3k}+2^{k+s}} = \\
&wx^{2^s+1} + w^{2^k}x^{2^{3k}+2^{k+s}} + wx^{2^s+1} + wv^{2^s+1} + wx^{2^s}v + wxv^{2^s} + w^{2^k}x^{2^{3k}+2^{k+s}} + \\
&w^{2^k}v^{2^{3k}+2^{k+s}} + w^{2^k}x^{2^{3k}}v^{2^{k+s}} + w^{2^k}v^{2^{3k}}x^{2^{k+s}} = \\
&wv^{2^s+1} + wx^{2^s}v + wxv^{2^s} + w^{2^k}v^{2^{3k}+2^{k+s}} + w^{2^k}x^{2^{3k}}v^{2^{k+s}} + w^{2^k}v^{2^{3k}}x^{2^{k+s}} = \\
&w^{2^k}v^{2^{3k}+2^{k+s}}\left(\left(\frac{x}{v}\right)^{2^{3k}} + \left(\frac{x}{v}\right)^{2^{k+s}}\right) + wv^{2^s+1}\left(\left(\frac{x}{v}\right)^{2^s} + \left(\frac{x}{v}\right)\right) + wv^{2^s+1} + \\
&w^{2^k}v^{2^{3k}+2^{k+s}}.
\end{aligned}$$

Dividing the last expression by $wv^{2^s+1}$ and substituting $vx$ for $x$, we get a linear expression in $x$:

$$a(x^{2^{3k}} + x^{2^{k+s}}) + (x^{2^s} + x) + 1 + a,$$

where $a = w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)}$. So, $F(x)+F(x+v)=u$ has 0 or $2^t$ solutions if and only if the kernel of the linear map

$$\Delta_a(x) = a(x^{2^{3k}}+x^{2^{k+s}})+(x^{2^s}+x)$$

has $2^t$ elements. Consider the equation $\Delta_a(x)=0$. We use Dobbertin's multivariate method and follow the computations from Theorem 2 of [5]. Let $b=a^{2^k}$ and $c=b^{2^k}$. We get that

$$\Delta_a(x)=0 \text{ if and only if } ab(bc+1)^{2^s+1}(x^{2^{2s}}+x^{2^s})=0,$$

assuming that $P(a)=c(ab+1)^{2^s+1}+a^{2^s}(bc+1)^{2^s+1}\neq 0$.

We now show that $bc+1\neq 0$. Clearly, $bc+1=0$ if and only if $ab+1=0$. Suppose $ab=1$, i.e. $a^{2^k+1}=1$. From

$$(2^{3k}+2^{k+s}-(2^s+1))(2^k+1) = (2^{2k}-1)(2^k+2^s) \mod (2^{4k}-1)$$

we get

$$1=a^{2^k+1}=(w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)})^{2^k+1}=w^{2^{2k}-1}v^{(2^{2k}-1)(2^k+2^s)}=$$
$$(wv^{2^k+2^s})^{2^{2k}-1},$$

hence $wv^{2^k+2^s}$ is a $(2^{2k}+1)$-st power of an element from $\mathbb{F}_{2^n}$. On the other hand, from $ks=3 \mod 4$ and $2\nmid k$ we have that $k$ and $s$ are odd, and $k\neq s \mod 4$, which means that $k-s=2p$ for some odd $p$. Thus, $2^k+2^s=2^s(2^{k-s}+1)=2^s(2^{2p}+1)$. Since $p$ is odd, we have $5\mid 2^{2p}+1$, and therefore $u^{2^k+2^s}$ is the fifth power of an element of the field, while $wu^{2^k+2^s}$ is not. Thus $wu^{2^k+2^s}$ is also not a $(2^{2k}+1)$-st power. Hence, we get a contradiction, and so we must have $ab+1\neq 0$ and hence $bc+1\neq 0$. Therefore, we have

$$\Delta_a(x)=0 \text{ if and only if } x^{2^{2s}}+x^{2^s}=0$$

when $P(a)\neq 0$.

By the statement of Theorem 1, $k$ is odd and $sk=3 \mod 4$, so that $s$ is also odd, and from $\gcd(s,2k)=t$ it follows that $\gcd(s,4k)=t$. Therefore the equation $x^{2^{2s}}+x^{2^s}=0$, which is equivalent to $x^{2^s}=1$, has exactly $2^{\gcd(s,4k)}=2^t$ solutions.

So we only have to show that $P(a)=c(ab+1)^{2^s+1}+a^{2^s}(bc+1)^{2^s+1}$ does not vanish.

Assume $P(a)=0$, i.e.

$$\frac{c}{a^{2^s}}=\left(\frac{bc+1}{ab+1}\right)^{2^s+1}.$$

We have that $\frac{c}{a^{2^s}}$ is the third power of an element of the field since $3\mid 2^s+1, 2^n-1$ (since $s$ is odd and $n$ is even). On the other hand,

$$\frac{c}{a^{2^s}}=a^{2^{2k}-2^s}=a^{2^s(2^{2k-s}-1)}=(w^{2^k-1}v^{2^{3k}+2^{k+s}-(2^s+1)})^{2^s(2^{2k-s}-1)}=$$
$$w^{(2^k-1)2^s(2^{2k-s}-1)}v^{(2^{3k}+2^{k+s}-(2^s+1))2^s(2^{2k-s}-1)}$$

and $2^{3k}+2^{k+s}-(2^s+1)=2^s(2^{3k-s}-1)+(2^{k+s}-1)$ is divisible by 3 because $3\mid 2^{3k-s}-1$ and $3\mid 2^{k+s}-1$ due to $k$ and $s$ being odd. But since $k$ and $2k-s$ are odd, we have $3\nmid 2^k-1$ and $3\nmid 2^{2k-s}-1$, which means that $w^{(2^k-1)2^s(2^{2k-s}-1)}$ is not a third power, therefore $\frac{c}{a^{2^s}}$ is not a third power either, and we get a contradiction. □

As the following proposition illustrates, the binomials from (3) also behave in the same way as the Gold functions from the point of view of bijectivity.

**Proposition 1.** *A function of the form* (3) *is a permutation if and only if it is EA-equivalent to a $2^t$-differentially uniform permutation of the form $x^{2^s+1}$ for some positive integer $s$.*

*Proof.* Recall that the power function $x^{2^s+1}$ over $\mathbb{F}_{2^n}$ is $2^t$-uniform for some positive integer $t$ if and only if $\gcd(s,n)=t$, and it is a permutation if and only if $n/t$ is odd.

Let $F(x)=wx^{2^s+1}+w^{2^k}x^{2^{ik}+2^{mk+s}}$ be a function satisfying the conditions of Theorem 1. If $F$ is a permutation, then $4k/\gcd(s,4k)$ is odd. Indeed, assume that $F$ is a permutation and $4k/\gcd(s,4k)$ is even. Since $k$ is odd, we have that $\gcd(s,4k)$ should be odd or $\gcd(s,4k)=2 \mod 4$. If $\gcd(s,4k)$ is odd, then so is $s$, and therefore $3 \mid 2^s+1$. Since $i=(sk \mod 4)$ and $s,k$ are odd, then $i$ is an odd number, and hence $(m-i)k+s$ is also odd; hence $3 \mid 2^{ik}(1+2^{(m-i)k+s})=2^{ik}+2^{mk+s}$. Thus, for any $\gamma \in \mathbb{F}_{2^2}$, we have $F(\gamma x)=F(x)$. On the other hand, if $\gcd(s,4k)=2 \mod 4$, then $s$ is even, and therefore $i$ is also even due to $i=sk \mod 4$. Hence, as we discussed in the proof of Theorem 1, $F$ is EA-equivalent to $x^{2^s+1}$ which is not a permutation since $4k/\gcd(s,4k)$ is even. Therefore $4k/\gcd(s,4k)$ is necessarily odd if $F$ is a permutation. However, when $4k/\gcd(4k,s)$ is odd, $\gcd(4k,s)$ is divisible by 4, and therefore $s$ is also divisible by 4 since $k$ is odd. This means that $F$ is EA-equivalent to a $2^t$-differentially uniform permutation of the form $x^{2^l+1}$ for some positive integer $l$. □

# 4 Magnitude of the Walsh coefficients

In following theorem, we compute an upper bound on the absolute values of the Walsh coefficients of the functions from (3). In the proof we make use of the following result.

**Lemma 2** ([14])**.** *Let $n,l,d$ be positive integers such that $\gcd(n,s)=1$ and let $G(x)=\sum_{i=0}^{d} a_i x^{li} \in \mathbb{F}_{2^n}[x]$. Then the equation $G(x)=0$ has at most $2^d$ solutions.*

We are now ready to present the main result of this section.

**Theorem 2.** *Let $s,k,t$ be positive integers and let $n=4k$. Let $\gcd(s,2k)=t$, $2 \nmid k$, $i=sk \mod 4$, $m=4-i$ and let $w$ be a primitive element of $\mathbb{F}_{2^n}$. Then the Walsh coefficients of the function $F$ from* (3) *satisfy*

$$|W_F(a,b)| \leq 2^{2k+t}$$

*for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.*

*Proof.* For simplicity, instead of $F(x)=wx^{2^s+1}+w^{2^k}x^{2^{ik}+2^{mk+s}}$, we consider the *EA*-equivalent function $F'(x)=x^{2^s+1}+\alpha x^{2^{ik}+2^{mk+s}}$, where $\alpha=w^{2^k-1}$.

We are going to prove the theorem for $i=3$ since as we already observed in the proof of Theorem 1, if $i$ is even, the function $F(x)$ is EA-equivalent to a Gold-like differentially $2^t$-uniform function; and if $i$ is odd, the functions that we obtain for $i=1$ and for $i=3$ are EA-equivalent.

We have

$$W_{F'}^2(a,b)=\sum_x \sum_y (-1)^{\mathrm{Tr}(ax+ay+bF'(x)+bF'(y))}.$$

Substituting $x+y$ for $y$, we get

$$W_{F'}^2(a,b)=\sum_x \sum_y (-1)^{\mathrm{Tr}(ax+a(x+y)+bF'(x)+bF'(x+y))}.$$

The exponent from the previous expression by straightforward calculations becomes

$$\begin{aligned}
&\mathrm{Tr}(ax+a(x+y)+bF'(x)+bF'(x+y))=\\
&\mathrm{Tr}(ay+b(x^{2^s+1}+\alpha x^{2^{3k}+2^{k+s}}+(x+y)^{2^s+1}+\alpha(x+y)^{2^{3k}+2^{k+s}}))=\\
&\mathrm{Tr}(ay+by^{2^s+1}+b\alpha y^{2^{k+s}+2^{3k}})+\mathrm{Tr}(bx^{2^s}y+bxy^{2^s}+b\alpha x^{2^{3k}}y^{2^{k+s}}+b\alpha y^{2^{3k}}x^{2^{k+s}})=\\
&\mathrm{Tr}(ay+by^{2^s+1}+b\alpha y^{2^{k+s}+2^{3k}})+\mathrm{Tr}(x\mathscr{L}(y)),
\end{aligned}$$

where $\mathscr{L}(y)=(by)^{2^{-s}}+by^{2^s}+(b\alpha)^{2^{-3k}}y^{2^{s-2k}}+(b\alpha)^{2^{3k-s}}y^{2^{2k-s}}=(by)^{2^{-s}}+by^{2^s}+(b\alpha)^{2^{2k}}y^{2^{s+2k}}+(b\alpha)^{2^{3k-s}}y^{2^{2k-s}}$ is a linear function.

Thus

$$W_{F'}^2(a,b)=2^n\sum_{\{y|\mathscr{L}(y)=0\}}(-1)^{\mathrm{Tr}(ay+by^{2^s+1}+b\alpha y^{2^{k+s}+2^{3k}})}.$$

The next step is to show that the cardinality of the kernel of $\mathscr{L}(y)$ is at most $2^{2t}$, where $t=\gcd(2k,s)$. Following the computations of [2], we have

$$b^{2^{-s+2k}}\mathscr{L}(y)+(b\alpha)^{2^{3k-s}}\mathscr{L}^{2^{2k}}(y)=0 \text{ and } b^{2^{2k}}\mathscr{L}(y)+(b\alpha)^{2^k}\mathscr{L}^{2^{2k}}(y)=0,$$

from where we get

$$Ay^{2^s}+By^{2^{-s}}+Cy^{2^{s+2k}}=0, \tag{5}$$
$$B^{2^s}y^{2^s}+A^{2^{2k}}y^{2^{-s}}+Cy^{2^{-s+2k}}=0, \tag{6}$$

where

$$\begin{aligned}
A&=b^{2^{-s+2k}+1}+(b\alpha)^{2^{-k}+2^{3k-s}}\neq 0,\\
B&=b^{2^{-s}+2^{-s+2k}}+(b\alpha)^{2^{k-s}+2^{3k-s}}, \text{ and}\\
C&=b^{2^{-s+2k}+2^k}\alpha^{2^k}+b^{2^{2k}+2^{3k-s}}\alpha^{2^{3k-s}}\neq 0,
\end{aligned}$$

with $B=0$ if and only if $B^{2^s-1}$ is a cube.

Assume that $B\neq 0$, i.e. $B^{2^s-1}$ is not a cube. Then from (5) and (6) we get

$$B^{2^{2s}}C^{2^{-s}}y^{2^{2s}}+C^{2^{-s}}A^{2^{2k+s}}y+B^{2^{-s}}C^{2^s}y^{2^{-2s}}+A^{2^{-s}}C^{2^s}y=0.$$

Denote the last expression by $G(y)$. For some $v\neq 0$ in the kernel of $G(y)$, consider the expression $G_v(y)=yG(y)+vG(v)+(y+v)G(y+v)$ , i.e.

$$C^{2^s}B^{2^{-s}}(y^{2^{-2s}}v+v^{2^{-2s}}y)+C^{2^{-s}}B^{2^{2s}}(y^{2^{2s}}v+v^{2^{2s}}y).$$

Note that the kernel of $\mathscr{L}(y)$ is contained in that of $G_v(y)$. Then from $G_v(y)=0$ we get

$$C^{2^{-s}-2^s}B^{2^{2s-1}}(y^{2^{-2s}}v+v^{2^{-2s}}y)^{2^{2s}-1}=B^{2^s-1}.$$

If $y^{2^{-2s}}v+v^{2^{-2s}}y=0$, i.e. $yv^{-1}=(yv^{-1})^{2^{2s}}$, then $yv^{-1}\in\mathbb{F}_{\gcd(2s,4k)}=\mathbb{F}_{2^{2t}}$ and therefore $\mathscr{L}(y)=0$ has exactly $2^{2t}$ solutions. Otherwise, if $y^{2^{-2s}}v+v^{2^{-2s}}y$ does not vanish, then the right-hand side of the previous equation is not a cube by our assumption, while the left-hand side is. Hence, $\mathscr{L}(y)=0$ has exactly $2^{2t}$ solutions, where $t=\gcd(2k,s)$.

Suppose now that $B = 0$. Following the computations of [2], the equation $\mathscr{L}(y) = 0$ becomes

$$(b + (bw)^{2^k} v^{2^{2k+s}-2^s}) y^{2^s} + (b^{2^{-s}} + (bw)^{2^{3k-s}} v^{2^{2k-s}-2^{-s}}) y^{2^{-s}} = 0.$$

If both coefficients (in front of $y^{2^s}$ and in front of $y^{2^{-s}}$) in the above equation are nonzero, then raising both sides to the power $2^s$, we get

$$(b + (bw)^{2^k} v^{2^{2k+s}-2^s})^{2^s} y^{2^{2s}} + (b^{2^{-s}} + (bw)^{2^{3k-s}} v^{2^{2k-s}-2^{-s}})^{2^s} y = 0.$$

Note that $2s = 2t\frac{s}{t}$ and $\gcd(\frac{s}{t}, 4k) = 1$. Then, applying Lemma 2, we get that $\mathscr{L}(y) = 0$ has at most $2^{2t}$ solutions. If exactly one of the coefficients is not zero, then the equation will have exactly one solution, namely $y = 0$. If both coefficients are equal to zero, then raising them to the power of $2^s$ and of $2^{-s}$, and adding these powers together, we get $v^{2^{2k}-1} = b^{2^{3k}-2^{k-s}} w^{-2^{k-s}} = b^{1-2^{3k}} w^{-2^{3k}}$ which implies $C = 0$, a contradiction.

Thus, the kernel of $\mathscr{L}(y)$ consists of at most $2^{2t}$ elements, where $t = \gcd(2k, s)$ and therefore $|W_F^2(a,b)| \leq 2^n 2^{2t}$ and $|W_F(a,b)| \leq 2^{2k+t}$ . □

The next corollary immediately follows from Theorem 2.

**Corollary 1.** *Let $s,k,t$ be positive integers and let $n = 4k$. Let* $\gcd(s,2k) = t$, $2 \nmid k$, $i = sk \bmod 4$, *$m = 4 - i$ and let $w$ be a primitive element of $\mathbb{F}_{2^n}$. Then the nonlinearity of the function $F$ from* (3) *satisfies*

$$\mathscr{NL}(F) \geq 2^{n-1} - 2^{2k+t-1}.$$

# 5 A counterexample: generalizing a family of APN quadrinomials to $2^t$-uniform functions

As discussed above, both families of APN binomials from [5] can be generalized to functions all of whose derivatives are $2^t$-to-1 by relaxing conditions; furthermore, the two families are obtained as generalizations of a previously unclassified sporadic APN instance over $\mathbb{F}_{2^{12}}$. Another sporadic APN instance, this time over $\mathbb{F}_{2^{10}}$, was recently also generalized into an infinite family [7]. This immediately raises the question of whether the same approach, i.e. relaxing conditions in order to obtain functions with $2^t$-to-1 derivatives, could be applied to the latter family. In this section, we summarize our experimental results, which suggest that this is impossible.

The functions in the infinite family from [7] are defined over $\mathbb{F}_{2^n}$ with $n = 2m$ with $m$ odd such that $3 \nmid m$, and have the form

$$F(x) = x^3 + \beta (x^{2^i+1})^{2^k} + \beta^2 (x^3)^{2^m} + (x^{2^i+1})^{2^{m+k}}, \tag{7}$$

where $k$ is a non-negative integer, and $\beta$ is a primitive element of $\mathbb{F}_{2^2}$. It is shown that the function in (7) is APN for $i = m-2$ and $i = (m-2)^{-1} \mod n$, as well as for $i = m$ and $i = m-1$ (however, the last two values yield functions that are trivially EA-equivalent to known ones).

We computationally go through all functions of the form

$$F(x) = x^{2^j+1} + \beta (x^{2^i+1})^{2^k} + \beta^2 (x^{2^j+1})^{2^m} + (x^{2^i+1})^{2^{m+k}} \tag{8}$$

with $0 \leq i, j \leq n-1$ for all values of $n = 2m$ with $6 \leq n \leq 14$, disregarding the conditions of $3 \nmid m$ and of $m$ being odd. For each such function, we test whether all of its derivatives are $2^t$-to-1 functions for some positive integer $t$. We restrict ourselves to the cases $k = 0$ and $k = 1$, as the APN functions constructed for $k \in \{0, 1\}$ appear to exhaust all CCZ-equivalence classes [7].

Besides the already known APN functions, for $k = 0$, we only encounter functions with $2^t$-to-1 derivatives when $j = i$, i.e. when all exponents are in the same cyclotomic coset. In the case of $k = 1$, the only exceptions are for $n = 12$ where each pair $(j, i)$ with $2 \leq j, i \leq 12$ and $i, j$ even yields a $2^2$-to-1, i.e. 4-to-1 function. However, since we do not observe other such non-trivial functions for other dimensions $n$, this does not suggest that (7) can be generalized to $2^t$-functions in general.

These computational results constitute convincing evidence that the quadrinomials of the form (7) cannot be generalized to $2^t$-to-1 functions in the same way as the binomials from [5].

# 6 Conclusion

The APN binomial $x^3 + \alpha x^{258}$ over $\mathbb{F}_{2^{12}}$ was generalized in 2008 to two infinite APN families over $\mathbb{F}_{2^n}$, one for $3 \mid n$, and one for $4 \mid n$. The family for $3 \mid n$ was generalized to a family of functions with $2^t$-to-1 derivatives in 2012 [3] by relaxing conditions. We have shown that the same approach can be applied to the family for $4 \mid n$, and have computed the differential uniformity of the resulting functions. We have also given a lower bound on their nonlinearity, and have shown that this construction cannot be applied to any infinite family of quadratic APN functions by computationally verifying that the quadrinomial family from [7] constitutes a counterexample.

# Acknowledgment

This research was supported by the Trond Mohn foundation (TMS).

# References

[1] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems”, J. Cryptol., vol. 4, no. 1, 1991, pp. 3–72.

[2] C. Bracken, C. Byrne, N. Markin, and G. Mcguire, “Fourier spectra of binomial APN functions”, SIAM J, Discrete Math., vol. 23, no. 2, 2009, pp. 596–608.

[3] C. Bracken, C. Tan, and Y. Tan, “Binomial differentially 4 uniform permutations with hight nonlinearity”, Finite Fields and Their Applications, 18, 2012, pp. 537–546.

[4] L. Budaghyan. “Construction and Analysis of Cryptographic Functions”. Springer Verlag, 2015.

[5] L. Budaghyan, C. Carlet, and G. Leander, “Two classes of quadratic APN binomials inequivalent to power functions”, IEEE Transactions on Information Theory, vol. 54, 9, 2008, pp. 4218-4229.

[6] L. Budaghyan, C. Carlet, and A. Pott,"New classes of almost bent and almost perfect nonlinear functions", IEEE Trans. Inform. Theory, vol.52, no.3, 2006, pp.1141–1152.

[7] L. Budaghyan, T. Helleseth, and N. Kaleyski, "A new family of APN quadrinomials", IEEE Trans. Inform. Theory, 2020, early access article.

[8] C. Carlet. "Vectorial (multi-output) Boolean Functions for Cryptography". Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[9] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptography", Design, Codes and Cryptography, vol.15, no.2, 1998, pp.125–156.

[10] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis", Advances in Cryptology, Eurocrypt'94, Lecture Notes in Comput.Sci., vol, 950, 1995, pp. 356–365.

[11] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping", IEEE Trans. Inf. Theory, vol. 52, no.2, 2006, pp. 744–747.

[12] M.Matsui, "Linear cryptanalysis methods for DES cipher", Advances in Cryptology, Eurocrypt'93, Lecture Notes in Comput.Sci., vol, 765, 1993,pp. 386–397.

[13] K. Nyberg, "Differentially uniform mappings for cryptography", Eurocrypt'93, Lecture Notes in Comput.Sci., vol, 765, 1994, pp. 55-64.

[14] H. M. Trachtenberg, "On the Cross–Correlation Functions of Maximal Linear Sequences" , Ph.D. dissertation, University of Southern California, Los Angeles, 1970.

# CHAPTER 3

# CONCLUSIONS

The research of the present thesis is dedicated to the following four problems related to bent and almost perfect nonlinear (APN) functions: *construction of new Niho bent functions via o-equivalence (Paper I); the Walsh spectrum of the Dobbertin APN power function (Paper II); the Dobbertin conjecture on non-existence of APN power functions inequivalent to the known ones (Paper II) and possible generalization of known families of APN functions into Gold-like functions (Paper III).*

Regarding *the first problem*, we studied the relation of o-equivalence (for Niho bent functions, it is a more general equivalence relation than EA-equivalence, and is induced from the equivalence of o- polynomials) as a method for secondary construction of Niho bent functions. We studied a group of transformations, which preserves the o-equivalence of Niho bent functions, but does not preserve their EA-equivalence, and identified the exact transformations which always lead to EA-inequivalent Niho bent functions within one o-equivalence class, in the case of o-monomials. For o-polynomials, which are not monomials we identified the form of transformations which can potentially lead to EA-inequivalent Niho bent functions within one o-equivalence class. Our results lead, in particular, to the following interesting questions that can be studied in the future:

- Find transformations always leading to a set of pairwise EA-inequivalent Niho bent functions within one o-equivalence class;
- Identify in the set of pairwise EA-inequivalent Niho bent functions within one of the o-equivalence classes known, those which are not EA-equivalent to other known cases of Niho bent functions;
- Using o-equivalence, find a more general equivalence relation than CCZ-equivalence for vectorial functions preserving differential uniformity and nonlinearity. If such equivalence relation can be found, it will lead to numerous new problems.

For *the second problem*, which has been open without any progress for 20 years, we introduced a conjecture giving a full description of the Walsh spectrum of the Dob-

bertin functions. We obtained (optimal in certain sense) alternative representations of the exponents for some of the known APN power functions, in particular, for the exponent of the Dobbertin function. These alternative representations may be useful in future, for instance, for studying our conjecture about the Walsh spectrum of the Dobbertin functions, and may possibly lead to simpler proofs of the APN property of the corresponding power functions. Thus, we leave the following problems for the future study:

- Study the conjecture about the Walsh spectrum of the Dobbertin functions. In particular,
  - Collect and analyze data about the multiplicity of the Walsh coefficients of the Dobbertin functions;
  - Study alternative representations of the Dobbertin functions obtained in Paper II for proving the conjecture;
- Simplify the proofs of the APN property of the Dobbertin and Niho APN power functions, using their alternative representations obtained in Paper II.

For *the third problem* which has been also open since 2000, we considered a composition of the form $x^i \circ L \circ x^{1/j}$ , where $L$ is a linear polynomial and a power function $x^d$ over $\mathbb{F}_{2^{mk}}$, where $d = \sum_{i=0}^{k-1} 2^{mi} - 1$. We showed that some of the known APN power functions can be obtained from each other via $x^i \circ L \circ x^{1/j}$. This construction is yet not well studied and admits many possible developments such as

- Examine functions of the form $x^i \circ L \circ x^{1/j}$, for L with non-binary coefficients (the case of binary coefficients is covered in Paper II);
- Investigate constructions of the form $x^i \circ L \circ x^{1/j}$, where $L$ is a linear function and $x^i \circ x^{1/j}$ is an alternative representation of the Niho and Dobberin functions obtained in Paper II;
- Study constructions $F_2 \circ L \circ F_1^{-1}$, where $F_2 \circ F_1^{-1}$ is CCZ-equivalent to $F$.

Moreover, power functions $x^d$ over $\mathbb{F}_{2^{mk}}$ , where $d = \sum_{i=0}^{k-1} 2^{mi} - 1$ studied in Paper II could be a useful tool for approaching the conjecture about non-existence of APN power functions inequivalent to known ones. Thus, further investigation of these power functions can be done. In particular, an interesting problem is

- Investigation of the compositions of the power functions $x^d$ over $\mathbb{F}_{2^{mk}}$ , where $d = \sum_{i=0}^{k-1} 2^{mi} - 1$ with known APN power functions and a linear map in between.

For *the fourth problem* we considered the family of APN binomials, for n divisible by 4 and showed that they behave exactly as the Gold functions (can be generalized to a family of functions with all derivatives on non-zero directions being $2^t$-to-1 mappings, for some positive integer t). As well as we showed that not all APN families behave in this way. In the future, the following problem can be studied:

- Whether recently constructed APN families behave as Gold functions.

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS


uib.no

ISBN: 9788230861721 (print)
9788230846612 (PDF)