Analysis, classification and construction of optimal cryptographic Boolean functions

Irene Villa

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

UNIVERSITY OF BERGEN

Analysis, classification and construction of optimal cryptographic Boolean functions

Irene Villa

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

Date of defense: 04.01.2021

Year: 2021

Title: Analysis, classification and construction of optimal cryptographic Boolean functions

Name: Irene Villa

Print: Skipnes Kommunikasjon / University of Bergen

Acknowledgements

First of all, I would like to thank my supervisor, Lilya Budaghyan. This experience has been challenging, sometimes stressful, but also fulfilling, interesting and stimulating. I am really grateful for all the help, support and appreciation she showed me. My gratitude goes also to Tor Helleseth and Marco Calderini, my co-supervisors. I want to thank Tor, a cornerstone of the Selmer center, for the care he always shows for the Selmer group. To Marco goes my appreciation for all the help he gave me throughout these years, not only research related. I want to express my gratitude to Claude Carlet and Robert Coulter for the research done together and for hosting me in Paris and in Delaware. I would also like to thank the administration staff at the Department of Informatics for always helping out.

I am very grateful to Prof. Kaisa Nyberg and Prof. Anne Canteaut for their helpful comments during the final stages of writing this thesis. My gratitude goes also to Chunlei Li.

Special thanks are due to all Selmer center (the list of previous and present members is now quite long) for the nice environment we built together. I consider myself very lucky to have found such a great work atmosphere. I share the same appreciation for all my flatmates, the old ones and the new ones. In particular I want to thank Isaac for all the time spent together, and for teaching me the right Spanish.

I want to thank all the friends that made these years in Bergen full of laughs, food, songs and sweat.

At last, I want to thank my friends from Italy and my big family. I am really glad to have all of you in my life. A special thought goes also to Francesco, Marco, Betti and Jack.

Buona strada

Abstract

Modern cryptography is deeply founded on mathematical theory and vectorial Boolean functions play an important role in it. In this context, some cryptographic properties of Boolean functions are defined. In simple terms, these properties evaluate the quality of the cryptographic algorithm in which the functions are implemented.

One cryptographic property is the *differential uniformity*, introduced by Nyberg in 1993. This property is related to the *differential attack*, introduced by Biham and Shamir in 1990. The corresponding optimal functions are called *Almost Perfect Nonlinear* functions, shortly APN. APN functions have been constructed, studied and classified up to equivalence relations. Very important is their classification in infinite families, i.e. constructing APN functions that are defined for infinitely many dimensions. In spite of an intensive study of these maps, many fundamental problems related to APN functions are still open and relatively few infinite families are known so far.

In this thesis we present some constructions of APN functions and study some of their properties. Specifically, we consider a known construction, $L_1(x^3) + L_2(x^9)$ with L_1 and L_2 linear maps, and we introduce two new constructions, the isotopic shift and the generalised isotopic shift. In particular, using the two isotopic shift constructing techniques, in dimensions 8 and 9 we obtain new APN functions and we cover many unclassified cases of APN maps. Here *new* stands for inequivalent (in respect to the so-called CCZ-equivalence) to already known ones.

Afterwards, we study two infinite families of APN functions and their generalisations. We show that all these families are equivalent to each other and they are included in another known family. For many years it was not known whether all the constructed infinite families of APN maps were pairwise inequivalent. With our work, we reduce the list to those inequivalent to each other.

Furthermore, we consider optimal functions with respect to the differential uniformity in fields of odd characteristic. These functions, called *planar*, have been valuable for the construction of new commutative semifields. Planar functions present often a close connection with APN maps. Indeed, the idea behind the isotopic shift construction comes from the study of isotopic equivalence, which is defined for quadratic planar functions. We completely characterise the mentioned equivalence by means of the isotopic shift and the extended affine equivalence. We show that the isotopic shift construction leads also to inequivalent planar functions and we analyse some particular cases of this construction.

Finally, we study another cryptographic property, the *boomerang uniformity*, introduced by Cid et al. in 2018. This property is related to the *boomerang attack*, presented by Wagner in 1999. Here, we study the boomerang uniformity for some known classes of permutation polynomials.

List of papers

The thesis is based on the following papers.

1. Irene Villa, *On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2*, Cryptography and Communications **11**, 1, pp. 3-20, 2019.
   Presented at ISPIT Seminar 2017 - Saint-Petersburg.

2. Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, and Irene Villa, *Constructing APN functions through isotopic shifts*, IEEE Transactions on Information Theory, vol. 66, no. 8, pp. 5299-5309, Aug. 2020.
   Presented at the conference SETA 2018 - Hong Kong.

3. Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, and Irene Villa, *Generalized isotopic shift construction for APN functions*, Cryptology ePrint Archive, Report 2020/295, 2020 (Accepted to Designs, Codes and Cryptography).
   Presented at the conference WCC 2019 - Saint-Jacut-de-la-Mer.

4. Lilya Budaghyan, Marco Calderini, and Irene Villa, *On equivalence between known families of quadratic APN functions*, Finite Fields and Their Applications, vol. 66, 2020.
   Presented at the conference WCC 2019 - Saint-Jacut-de-la-Mer.

5. Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S. Coulter, and Irene Villa, *On isotopic shift construction for planar functions*, 2019 IEEE International Symposium on Information Theory (ISIT), pp. 2962-2966, July 2019.

6. Marco Calderini, and Irene Villa, *On the boomerang uniformity of some permutation polynomials*, Cryptography and Communications **12**, 6, pp. 1161-1178, 2020.
   Presented at the conference BFA 2019 - Florence.

Contents

Acknowledgements i

Abstract iii

List of papers v

1 Introduction 1

2 Preliminaries 9

2.1 Cryptography and cryptographic primitives . . . 9

2.1.1 Stream ciphers . . . 11

2.1.2 Block ciphers . . . 12

2.1.3 On some attacks on block ciphers . . . 13

2.2 Functions over finite fields . . . 17

2.2.1 The differential uniformity . . . 20

2.2.2 Equivalence relations . . . 21

2.3 Vectorial Boolean functions . . . 22

2.3.1 Almost perfect nonlinear functions . . . 23

2.3.2 The boomerang uniformity . . . 31

2.3.3 The nonlinearity . . . 34

2.4 Semifields and presemifields . . . 35

2.4.1 Definitions . . . 35

2.4.2 Some known cases . . . 37

2.4.3 Connection with APN functions . . . 38

3 On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2 41

3.1 Some known results . . . 42

3.2 APN conditions . . . 43

3.2.1 Necessary and sufficient conditions . . . 43

3.2.2 On APN functions of the form $x^9 + L(x^3)$ . . . 48

3.2.3 On the components with constant derivative and the Walsh spectrum . . . 53

3.3 Comparison with some lists of known APN functions 58

4 Constructing APN functions through isotopic shifts 61
4.1 Isotopic equivalence for planar quadratic functions revisited . . . 62
4.2 Generic results on isotopic shifts 63
4.3 Isotopic shifts of APN functions 64
4.3.1 Isotopic shifts of quadratic APN functions 66
4.3.2 Isotopic shifts of Gold functions 67
4.4 Computational results 78

5 Generalised isotopic shift construction for APN functions 83
5.1 On generalisations of the form $xL_1(x)^{2^i} + x^{2^i}L_2(x)$ 84
5.1.1 The case $n = 8$ 86
5.1.2 A new EA-equivalence invariant 87
5.1.3 The case $n = 9$ 89
5.2 Isotopic shifts with nonlinear functions 90
5.2.1 Nonlinear shift for the Gold functions 91

6 On equivalence between known families of quadratic APN functions 95
6.1 On some known families 95
6.1.1 Correction of family C11* and family C3* 99
6.2 Equivalence between known families 101
6.2.1 C11 and C3 are equivalent 101
6.2.2 C11* is equivalent to C11 104
6.2.3 C3* is equivalent to C11 105
6.2.4 Equivalence with hexanomials (family C4) 106
6.3 The updated list 109

7 Isotopic shift construction for planar functions 111
7.1 On the linear shifts over fields of odd characteristic 111
7.1.1 The reciprocity of the isotopic shift 113
7.1.2 Comparison on linear shifts in odd and even characteristic 115
7.1.3 Shifting Albert-like functions by monomials 116
7.2 Generalised isotopic shift 117
7.2.1 For general Albert-like functions 117
7.2.2 The particular case of x^2 119
7.3 Computational results over $\mathbb{F}_{p^n}$ 122

8 On the boomerang uniformity of some permutation polynomials **125**
8.1 On the Bracken-Leander map 126
8.2 On the inverse function modified 138
9 Conclusions **143**
A Some computational results **145**
B Some proofs from Chapter 8 **153**

Chapter 1

Introduction

Vectorial Boolean functions are fundamental objects in mathematics and information theory. These functions take as an input a sequence of n bits and output a sequence of m bits. One of the important applications of Boolean functions is modern cryptography and, in this context, some cryptographic properties of Boolean functions have been defined. Interestingly, functions with optimal cryptographic properties define optimal objects in many domains of mathematics and information theory, such as coding theory [44], projective geometry [104] and the theory of commutative semifields [49]. Hence, solutions for problems of optimal cryptographic functions contribute to all these domains.

For a prime number p and positive integers n, m, an (n, m, p)-function F is a map from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, where $\mathbb{F}_p^n$ is identified with $\mathbb{F}_{p^n}$ when $m = n$. When p equals 2 we call F an (n, m)-function or a vectorial Boolean function. We focus on (n, n)-functions, which is the most interesting case for cryptographic applications. The *differential uniformity* is an important cryptographic property connected to the differential attack [12]: an (n, n)-function F is differentially δ-uniform if the equation $F(x + a) + F(x) = b$ admits at most δ solutions for every non-zero a and every b in $\mathbb{F}_{2^n}$. Optimal functions with respect to differential attacks have the smallest possible differential uniformity, that is $\delta = 2$, and they are called almost perfect nonlinear (APN).

Differential uniformity is invariant under linear, affine, extended affine and CCZ-equivalence. The equivalence relations are listed in increasing order of generality. Two (n, n)-functions are called affine (linear) equivalent if one is equal to the other one, composed on the left and on the right with affine (linear) permutations. They are called extended affine equivalent (EA-equivalent) if one is affine equivalent to the sum of the other one with an affine function. They are called Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent) if their

graphs are affine equivalent, where the graph of an (n,n)-function F is the set $\{(x,F(x)) : x \in \mathbb{F}_{2^n}\}$. Each of these equivalence relations has different applications, and much work has been done on the classification of functions with respect to these equivalences, see for instance [20, 21, 36, 53]. In spite of that, many important problems are still open.

The classification of APN functions over $\mathbb{F}_{2^n}$ with respect to EA and CCZ-equivalence is complete only for $n \leq 5$ [21]. Moreover, there are only a few classes of APN functions known. Up to now there are 6 known infinite families of APN power functions (see Table 2.1) with the last family being constructed in 2001 [61]. In 2008 some inequivalences between these families were shown [28] and only in 2016 it was proved that in general these families are all CCZ-inequivalent [54, 106]. It is conjectured that the list of APN power functions is complete up to CCZ-equivalence [59].

For many years it was believed that all APN functions were EA-equivalent to power functions. It was only in 2006 that the first classes of APN functions EA-inequivalent to power functions were constructed by applying CCZ-equivalence to power APN maps [32]. The first infinite families of APN polynomials CCZ-inequivalent to power mappings were constructed in 2008 as a sum of two quadratic power APN functions [29]. Since then, few infinite families of quadratic APN polynomials have been constructed, see Table 2.2. Several methods for constructing quadratic APN functions have also been proposed; they led to the discovery of many new instances of APN functions in fields of small dimension [66, 102, 109]. In particular, for $6 \leq n \leq 9$ there are large lists of CCZ-inequivalent quadratic APN functions that have not yet been classified into infinite families. Remarkably, all known APN functions are CCZ-equivalent to power or quadratic functions, with only a single exception in dimension six [21, 66]. Constructing an infinite family of such functions is still an open problem.

This work is primarily dedicated to the analysis, construction and classification of APN functions. In particular, it focuses on quadratic APN maps. Three of the known classes of quadratic APN polynomials, constructed in [30, 31],

$$\begin{aligned} F_1(x) &= x^3 + a^{-1}\mathrm{Tr}_n(a^3x^9), \\ F_2(x) &= x^3 + a^{-1}\mathrm{Tr}_n^3(a^3x^9 + a^6x^{18}), \\ F_3(x) &= x^3 + a^{-1}\mathrm{Tr}_n^3(a^6x^{18} + a^{12}x^{36}), \end{aligned}$$

were obtained by investigating functions of the form $L_1(x^3) + L_2(x^9)$, with L_1 and L_2 linear. The properties given in [30, 31] do not completely characterise APN functions of that type. In this thesis, we further investigate the APN property of maps of this form. For small dimensions, we computationally verify that all APN maps of the form $L_1(x^3) + x^9$ belong to the CCZ-class of an already known function. We show also that the extended Walsh spectrum of any APN map $L_1(x^3) + L_2(x^9)$ admits at most 5 values and that, for n odd and divisible by 3, L_1 must be a permutation. We analyse the lists of known APN functions presented in [66] and show that several of them are of the form $L_1(x^3) + L_2(x^9)$.

Another important question in the study of cryptographically significant vectorial Boolean functions is the existence of an equivalence notion that preserves the differential uniformity and is more general than CCZ-equivalence. Equivalence notions are important since they make the study of APN functions simpler, reducing the list of all APN functions to one representative function for each equivalence class. Moreover, equivalence notions are construction methods for optimal Boolean functions; by applying an equivalence transformation to an APN function we obtain a (different) APN function. When considering a special class of quadratic (n,n,p)-functions with p odd, such a notion does exist. It is called isotopic equivalence and is defined for quadratic planar functions, where a function F is planar if the equation $F(x+a) - F(x) = b$ has at most one solution for every non-zero a and every b in $\mathbb{F}_{p^n}$. Isotopic equivalence is known to be more general than CCZ-equivalence [33] and, for planar functions, CCZ-equivalence coincides with EA-equivalence [33]. Isotopic equivalence cannot be extended directly to APN functions in fields of even characteristic. We study this equivalence and try to find an analogue for (n,n)-functions. As a result we obtain a new construction method for APN functions, which we call *isotopic shift construction*. Whether it can lead to an equivalence relation, by finding more restrictions, is a matter of further investigations.

For two (n,n,p)-functions F and L, we define the isotopic shift of F by L as the map $F_L(x) = F(x + L(x)) - F(x) - F(L(x))$. In this work we show that isotopic equivalence can be simply described by means of the isotopic shift: given two isotopic equivalent quadratic planar functions F and G, there exists a linear permutation L such that G is EA-equivalent to F_L. There is a connection between quadratic planar functions in odd characteristic and quadratic APN functions in even characteristic. In the past years, families of quadratic planar

maps have been constructed by extension of known classes of quadratic APN families [33, 111]. The same has also been done in the opposite direction [112]. Motivated by the fact that for p odd the isotopic shift is a construction method for CCZ-inequivalent planar maps, in this work we investigate the isotopic shift construction for APN (n,n)-functions. We show that, for a quadratic map F and a linear map L, F_L is APN only if L is either a permutation or 2-to-1. We give some constructions of APN functions F_L when F is a Gold-like map, that is $F_L(x) = x^{2^i}L(x) + xL(x)^{2^i}$, in particular for $n = km$ and L a 2^m-linear map. This particular construction provides a new CCZ-inequivalent APN function for $n = 9$. We also show computationally that for any two quadratic APN functions F and G over $\mathbb{F}_{2^6}$, there exist a linear permutation L and a linear 2-to-1 map L' such that F_L and $F_{L'}$ are EA-equivalent to G.

Further, we generalise the concept of isotopic shift in two different ways. First, we consider an isotopic shift applied to Gold-like functions and we allow the construction to use two different linear maps L_1 and L_2, that is $x^{2^i}L_1(x) + xL_2(x)^{2^i}$. We study the APNness of these quadratic functions when L_1 and L_2 are 2^m-linear and we experimentally search for functions of this form in dimensions 8 and 9. For $n = 8$, we cover with this construction several APN functions given in [66, 102] which have not been previously identified as part of any APN family. For $n = 9$, we obtain 15 new CCZ-inequivalent APN functions and, in addition, cover the only known example in this dimension of an APN function which has not been previously identified as part of an APN family.

As a second generalisation, we consider the function F_L with L not necessarily linear. When n is even and L has coefficients in $\mathbb{F}_2$, we prove that F_L cannot be APN. We show that for odd n and any known APN power function F other than the Dobbertin function, there exist a monomial L and a Gold function x^{2^i+1} such that $x^{2^i}L(x) + xL(x)^{2^i}$ is EA-equivalent to F. Further investigation on the isotopic shift construction is a topic for future research.

In connection to the problem of determining whether two functions are equivalent, we introduce a new invariant for EA-equivalence. This invariant is particularly useful when studying quadratic APN functions since two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [105]. Hence, for quadratic APN maps, an EA-invariant is also a CCZ-invariant. For an (n,n)-function F we define $S(F)$ to be the set of all elements b such that the Walsh transform of F evaluated at (a,b) is zero for some

element a. We show that the number of $\mathbb{F}_2$-vector subspaces of certain dimension contained in $S(F)$ is EA-invariant.

As already mentioned, an important aspect in the study of APN functions is their classification. Few classes of quadratic APN multinomials are known. Unlike for the classes of APN power functions, there are not many theoretical proofs of their inequivalence. Indeed, proving CCZ-inequivalence is a rather difficult problem. Some inequivalences are shown computationally for small dimensions [35]. The problem of determining whether all the constructed families are pairwise inequivalent was left open despite such results. In this work, we consider two families introduced in [17, 26],

$$cx^{2^m+1} + x^{2^{2i}+2^i} + dx^{2^m(2^{2i}+2^i)}, \tag{C3}$$

$$cx^{2^m+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}. \tag{C11}$$

The computational work presented in [35] shows that in small dimensions the APN maps arising from family (C3) are CCZ-equivalent to the APN maps arising from family (C11). We show theoretically that, indeed, the two families are EA-equivalent. We consider also two generalisations of these families presented in [62]:

$$cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + x^{2^i+2^j} + dx^{2^m(2^i+2^j)}, \tag{C3*}$$

$$cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}). \tag{C11*}$$

The families (C3*) and (C11*) also coincide with the original families. Further, we prove that all the mentioned classes are contained in the family of APN hexanomials introduced in [26]:

$$dx^{2^i(2^m+1)} + x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + cx^{2^{m+i}+1} + c^{2^m} x^{2^i+2^m}. \tag{C4}$$

According to the table of CCZ-inequivalent functions which arise from known APN families (in dimensions up to 11) [35], the remaining families of APN functions are pairwise inequivalent in general. Thus, we are able to reduce the list of known families of quadratic APN multinomials to pairwise CCZ-inequivalent families.

Going back to the isotopic shift construction in fields of odd characteristic, we have already mentioned that it completely characterises the isotopic equivalence of quadratic planar functions (up to EA-equivalence). In particular, when

restricting to CCZ-equivalence (which coincides with EA-equivalence for planar maps), the characterisation is trivially verified. Indeed, for a quadratic planar function F, every function CCZ-equivalent to F is EA-equivalent to F_L where L is the identity map. Surprisingly, two functions connected by isotopic shift are not necessarily isotopic equivalent. Moreover, if F is planar, then F_L is not necessarily planar. We show that an isotopic shift with a linear map L is planar only if L is a permutation. A simple example of an isotopic shift leading to isotopic inequivalent functions is the following. Considering over $\mathbb{F}_{p^n}$ the planar function $F(x) = x^2$ and a linear permutation $L(x) = x^{p^j}$, the resulting function $F_L(x) = 2x^{p^j+1}$ is planar only if $n/\gcd(n,j)$ is odd and it is not isotopic equivalent to the original function F. This is encouraging, meaning that the isotopic shift is not only a useful tool for constructing new APN functions, but it may also lead to new planar functions. Some of the studies performed for APN functions in even characteristic are translated to the case of planar functions in odd characteristic. We study the generalised isotopic shift starting from an Albert-like map, that is $L_1(x)^{p^i}x + L_2(x)x^{p^i}$, and obtain similar constructions with p^m-linear polynomials. Some equivalence results are obtained when the starting function is x^2: for $n = 3m$ all planar functions of the form $x(x^{p^{2m}} + Ax^{p^m} + Bx)$ with A, B in $\mathbb{F}_{p^m}$ are affine equivalent to either x^2 or to x^{p^m+1}.

Finally, a chapter is dedicated to the *boomerang uniformity*. This cryptographic property was introduced in 2018 [16, 46] and is connected to the boomerang attack [101]. A permutation F has boomerang uniformity β if for any non-zero elements a, b the equation $F^{-1}(F(x) + b) + F^{-1}(F(x + a) + b) = a$ admits at most β solutions. The boomerang uniformity is invariant only under affine equivalence and inverse transformation. The value of β is always greater than or equal to the differential uniformity of F. Optimal functions with respect to boomerang uniformity are for $\beta = 2$ and they coincide with APN functions. Hence APN permutations are optimal with respect to both differential and boomerang uniformity. Unfortunately, APN permutations are difficult to discover: very few classes are known for n odd (these consist of all power APN functions and the APN binomials in [29]) and only a single function is known for n even (discovered in 2009 for $n = 6$ [23]). The search for and the construction of APN permutations is often referred to as the big APN problem. Another class of good functions are differentially 4-uniform permutations

with boomerang uniformity 4. The boomerang uniformity has been already studied for some primary constructions of differentially 4-uniform permutations (for n even). In particular, the Gold function, the inverse function and the Bracken-Tan-Tan function [16, 91] have boomerang uniformity 4 only when the dimension n is not a multiple of 4. The other primary constructions are the Kasami function and the Bracken-Leander function. The boomerang uniformity of these maps is more complicated to study. In this work, we investigate the Bracken-Leander permutation $x^{2^{2k}+2^k+1}$ [18]. We show that its boomerang uniformity is upper bounded by 24 and that, in small dimensions, the bound can be attained. Determining the boomerang uniformity of the Kasami function is still an open problem. Other differentially 4-uniform permutations have been obtained by modifying the inverse function [85, 108]. We study these functions and we show that when swapping two points in the inverse function the boomerang uniformity β is either 6, 8 or 10, and when swapping three points (all points in $\mathbb{F}_4$) β is either 6 or 8.

Structure of the thesis. In Chapter 2 we give preliminary notions on cryptography and on Boolean and discrete functions, providing the necessary background for the following chapters. In Chapter 3 we study quadratic APN functions of the particular form $L_1(x^3) + L_2(x^9)$ where L_1 and L_2 are linear maps. In Chapter 4 we introduce the notion of linear isotopic shift and we construct and study APN functions through it. Chapter 5 studies some possible generalisations of this construction. In Chapter 6 we analyse some known infinite families of quadratic APN maps and show that they are all equivalent to each other. In Chapter 7 we consider functions defined over fields of odd characteristic and we study the isotopic shift construction in relation to planar maps. In Chapter 8 we analyse the boomerang uniformity of some permutation polynomials: the Bracken-Leander map and some cases of the modified inverse function.

Chapter 2

Preliminaries

Boolean functions and vectorial Boolean functions are basic mathematical objects: functions that take as an input a sequence of n bits and give as an output a sequence of m bits. Regardless of their simplicity, they have a fundamental role in many research areas and they are one of the most studied objects in pure and applied mathematics and in computer science. One of such areas is modern cryptography.

2.1 Cryptography and cryptographic primitives

In this section we give a brief introduction to cryptography. We focus in particular on block ciphers and on two attacks on block ciphers: the differential attack and the boomerang attack. This section is based on the following references [77, 97, 100].

Cryptography is a tool that can be used to achieve different security goals when communicating and exchanging information; its strength relies on the hardness of solving some mathematical problems. The need of secure communication has been present since the ancient times. One of the first examples of employment of cryptography is by Julius Caesar who used the now-called "Caesar cipher" to secretly communicate information. More recently, during World War II, the Enigma machine was used to securely establish communication within the German army. In nowadays society, the need of secure communication is not related to military and government communications only, but it impacts our everyday life. Cryptography has drastically evolved due to the technological advancement of the last century. All old ciphers cannot be securely used anymore. They are vulnerable since the difficult mathematical

problems upon which they rely can be easily solved with a powerful enough computer; sometimes even a personal computer is enough. Hence, modern cryptography combines mathematical knowledge and computer science expertise to design new hard problems.

One of the basic elements in cryptography is a cipher, which can be thought of as an algorithm to encrypt and decrypt information using two keys, i.e. to respectively make intelligible information into non-intelligible and vice-versa. Assume that two persons want to exchange a secret message. Then, the sender will encrypt the message, also called *plaintext*, using the encryption key and send it through an insecure channel. The receiver will take the encrypted message, also called *ciphertext*, and decrypt it with the decryption key. It is con-

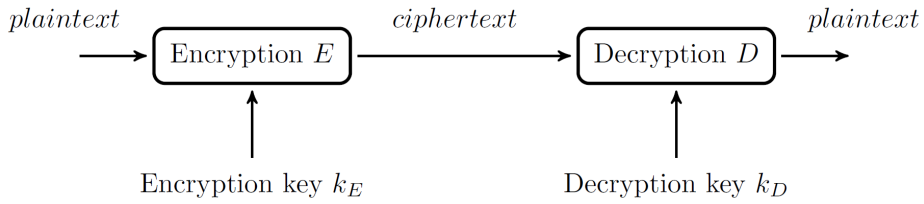


Figure 2.1: A cipher's operating principle

sidered a good practice that the operations involved in the encryption and decryption algorithms are public. The decryption key involved is the only secret information. This assumption is also known as Kerckhoffs's principle [79]. A cryptosystem is characterised by the following:

- $\mathcal{P}$ is the set of possible plaintexts,
- $\mathcal{C}$ is the set of possible ciphertexts,
- $\mathcal{K}$ is the set of possible encryption and decryption keys,
- for any $(k_E, k_D) \in \mathcal{K}$ the encryption and decryption functions are respectively

$$E_{k_E} : \mathcal{P} \to \mathcal{C} \text{ and } D_{k_D} : \mathcal{C} \to \mathcal{P} \text{ such that } D_{k_D} \circ E_{k_E} = Id_{\mathcal{P}}.$$

Cryptography can be classified into symmetric cryptography and asymmetric cryptography. In *symmetric cryptography* the encryption and decryption keys are the same, $k = k_E = k_D$. The key is supposed to be known only by the sender

and the receiver. One of the drawbacks of these cryptosystems is that the two parties need to agree on the shared secret key in a secure way before exchanging information. Symmetric-key ciphers are implemented as either stream ciphers or block ciphers.

In *asymmetric cryptography* or *public-key cryptography* there are two different keys, one that is public and one that is private. The public key can be freely distributed without affecting the security. The private key has to be known only by the owner. In these cryptosystems, the public key is used for encryption and the private key is used for decryption. Anybody can then encrypt a message but only the receiver, who owns the private key, is able to decrypt it. Asymmetric cryptography does not require previously shared keys to establish secure communication. Hence, it can be also used to securely agree on the secret key for a symmetric cryptosystem. However, it has some drawbacks. For instance, it requires larger keys and the efficiency of encryption/decryption is lower compared to the symmetric counterpart. Symmetric cryptography is then preferred for encrypting large amounts of information.

In this thesis we will focus on studying objects that can be applied in symmetric cryptography. In the following we give a brief introduction to stream ciphers, block ciphers and on some attacks on block ciphers.

2.1.1 Stream ciphers

Stream ciphers are based on the so-called *Vernam cipher*. The Vernam cipher is a simple cipher in which the plaintext is seen as a stream of elements and it is combined element-wise with the secret key k, which is another stream of elements. Assume for example that plaintexts, ciphertexts and keys are sequences of n bits. Then the encryption function operates as follows:

$$c = E_k(m) = m \oplus k,$$

where $\oplus$ is the bitwise addition. The decryption acts in the same way, $m = D_k(c) = c \oplus k$. For the Vernam cipher, the secret key has the same length as the secret message. This cipher offers unconditional security[1], assuming that the key is selected at random and renewed at every different encryption. However,

[1]The concept of unconditional security, or perfect secrecy, was formalised by Shannon in [96]. It is assumed that the attacker has an infinite computational power and still no information on the plaintext can be obtained, given the corresponding ciphertext. The following relation is satisfied: for every $p \in \mathcal{P}$ and $c \in \mathcal{C}$, $Pr(X = p|Y = c) = Pr(X = p)$.

this is not feasible in practical applications. To overcome this problem, pseudo-random generators are used to generate a *key stream*, which is a sequence that is used instead of the random key. The pseudo-random generator uses a secret key to generate the key stream. This secret key is of a fixed length and corresponds to the key k in the definition of cryptosystem above.

2.1.2 Block ciphers

Block ciphers are among the most extensively used cryptographic primitives. They combine simple operations to construct a complex encryption transformation. This concept has its roots in Shannon's paper [96] connecting cryptography with information theory. Shannon's idea was to apply simple components iteratively in a number of rounds to substantiate the so-called confusion and diffusion of data. Feistel, Notz and Smith were the first to implement Shannon's concepts in a practical architecture [67, 68] .

Block ciphers encrypt and decrypt blocks of data of fixed length. The message $m \in \mathcal{P}$ is split into blocks as $m = m_1, m_2, \ldots, m_r$, where each m_i is a sequence of n bits. Each block is encrypted using the secret key k, $c_i = E_k(m_i)$, and the encrypted message c is obtained as $c = c_1, c_2, \ldots, c_r$, see Figure 2.2. The cipher-

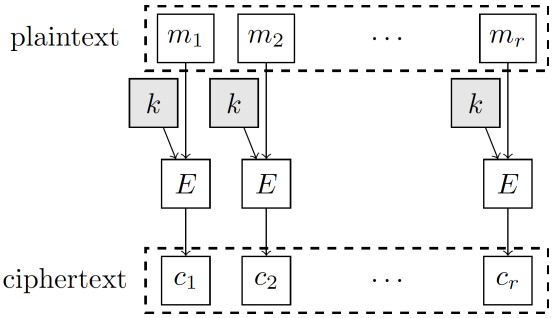


Figure 2.2: Block cipher's model

text is then decrypted by inverting the process. Most modern block ciphers are iterative ciphers: they are designed as the composition of a finite number N of rounds,

$$E_k = \tau_{k_N}^N \circ \ldots \circ \tau_{k_2}^2 \circ \tau_{k_1}^1.$$

The mappings involved in the rounds are vectorial Boolean functions. The j-th round takes as input the output of the previous round $(j-1)$ and a key k_j,

called round key. In general, the operation involving the round key is a bit-wise sum. The round keys are generated from the original secret key k by a key scheduling algorithm. Usually, every round consists of a non-linear substitution operation, called *S-box*, and a permutation. The S-box acts on disjoint parts of the input, whereas the permutation is generally a linear transformation and acts on the entire input. The goal of the S-box is to provide "confusion" inside the algorithm, i.e. to make the relationship between plaintext, ciphertext and key very complicated. The "diffusion" property is instead achieved by the permutation whose goal is to spread out the influence of any minor modifications of the input (plaintext or key) over all outputs.

As an example, Figure 2.3 describes an intermediate round of the *Advanced Encryption Standard (AES)* [52], a widely used block cipher. The figure depicts AES in its 128-bit version. The input block is a string of 128 bits that is divided into 16 sub-strings of 8 bits. The S-box is the concatenation of 16 sub-S-boxes that operate on 8 bits. In this block cipher, the S-boxes have to be bijective (so the output of each S-box is an 8-bit string). This allows to invert the process and make the decryption possible.

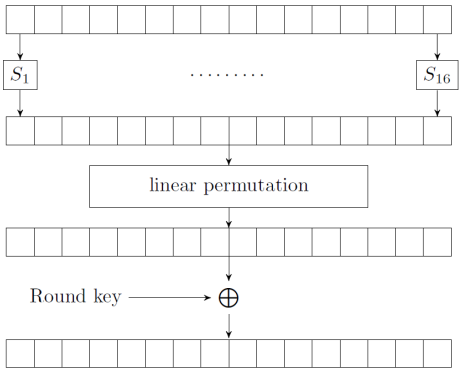


Figure 2.3: An AES round

2.1.3 On some attacks on block ciphers

Attacks on block ciphers can be classified according to the goal of the attacker. For example, in a *key recovery attack* the objective is to get the secret key. In a *distinguishing attack*, the goal is to distinguish whether the output is a random sequence or the result of the encryption process.

Attacks can also be classified based on the amount of information that the adversary has access to. In this case, three different models are defined.

- The *black-box attacker model*. In this scenario we assume that the attacker has complete knowledge of the algorithm used for encrypting (and decrypting) but it has no knowledge of the key used. We assume that the attacker can observe some pairs of inputs and/or corresponding outputs but he has no further knowledge beyond it. In some scenarios we assume furthermore that the attacker can choose the value of some inputs or outputs. Until recently, this model was the only one considered by cryptographers.

- The *gray-box attacker model*. An attack belonging to this model is also called a *side-channel attack*. In this scenario, the adversary has physical access to the device which performs the cryptographic operations. Therefore all the side channel information leaked during the execution of the algorithm can be collected and analysed. The leakages can correspond to power consumption, temperature change, running-time, electromagnetic emanation, etc. Usually, the attacker tries to perform an attack on the first or the last round of the block cipher.

- The *white-box attacker model*. In this scenario the attacker has knowledge of every information except the secret key. This includes all the intermediate values of the algorithms. The set of the intermediate values of a block cipher consists of the outputs of each function involved in every round of the block cipher.

Different techniques are required to make a block cipher robust against attacks from different models. In general, the security of a block cipher strongly depends on the S-boxes implemented in the algorithms. Many scientists and researchers have focused their work on these functions with particular interest on good cryptographic properties. They defined mathematical properties of the S-box that measure its resistance, and therefore that of the entire cipher, to some of these attacks. In the following we give a brief idea of two attacks from the black-box model, which have a connection with the work presented in the next chapters.

The *differential attack*, introduced by Biham and Shamir [12] in 1990, is among the most efficient attacks on block ciphers. The attack is based on the study of how differences between two inputs can affect the resulting differences at the output. To be effective, it assumes that there exists an ordered pair (a,b), $a \neq 0$, of sequences of bits satisfying the following property: for m a random block of the plaintext, $c = E_k(m)$ and $c' = E_k(m \oplus a)$, the sequence $c \oplus c'$ has a larger probability to equal b than if c and c' are sequences of bits randomly chosen. In [92] Nyberg introduced the notion of *differential uniformity*, which measures the resistance of an S-box to this attack. The smaller the differential uniformity, the better resistance the S-box has. Such property is obtained by studying the behaviour of the S-box S in the situation described in Figure 2.4. Boolean functions that achieve the best resistance are called *al-*

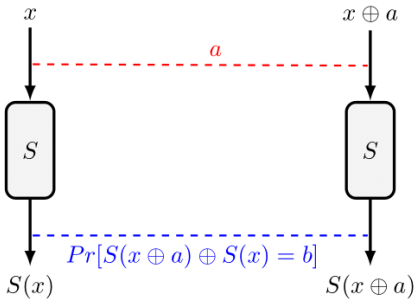


Figure 2.4: The differential attack at the S-box level

most perfect nonlinear, shortly APN. The role of APN functions is not restricted only to cryptography. For example, in coding theory such optimal functions define optimal, in a certain sense, binary error correcting codes [44]. In projective geometry, quadratic APN functions define dual hyperovals [104] and they also have connections with the theory of commutative semifields [49]. For functions defined over fields of odd characteristic, optimal differential uniformity is achieved by *perfect nonlinear* (PN) functions, also called *planar* functions.

In 1999 Wagner [101] introduced the *boomerang attack*, an important cryptanalysis technique against block ciphers. This attack can be seen as an extension of the differential attack. In fact, it combines two differentials for the upper part and the lower part of the cipher. More precisely, the cipher E is considered as the composition of two sub-ciphers E_1 and E_2. For E_1 the attacker considers

a differential (a,d) with probability p, for E_2 a differential (c,b) with probability q, see Figure 2.5. Then the attack is based on the following estimation of probability:

$$Pr[E^{-1}(E(x) \oplus b) \oplus E^{-1}(E(x \oplus a) \oplus b)) = a] \approx p^2 q^2. \tag{2.1}$$

Since Wagner's seminal paper, many improvements and variations of boomerang attacks have been proposed (see for instance [11, 13, 78]). One of them is the *sandwich attack*, proposed in [63]. In this attack the cipher is further decomposed as $E = E_2 \circ E_m \circ E_1$, where E_m is typically one round (or one S-box layer) of the cipher, see Figure 2.6. Then the sandwich attack is based on the estima-

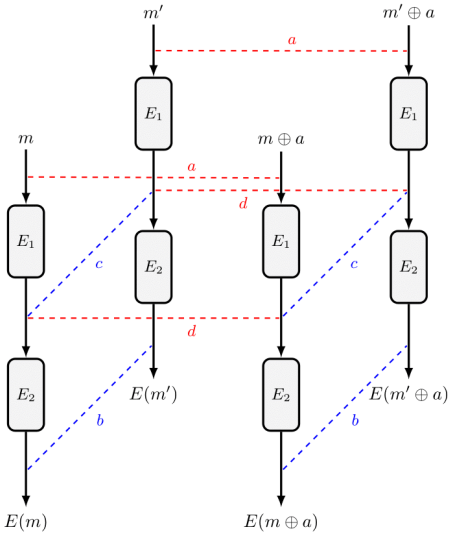


Figure 2.5: The boomerang attack

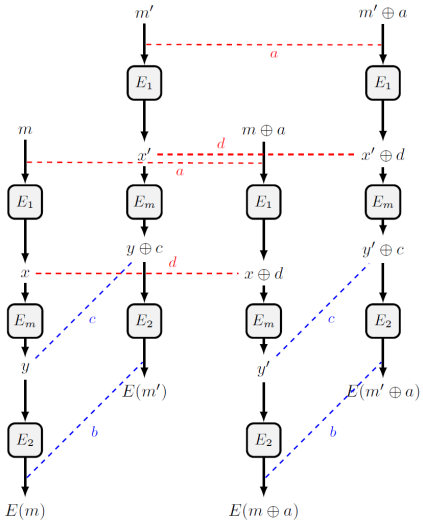


Figure 2.6: The sandwich attack

tion of probability in (2.1) multiplied by

$$Pr[E_m^{-1}(E_m(x) \oplus c) \oplus E_m^{-1}(E_m(x \oplus d) \oplus c) = d]. \tag{2.2}$$

In order to evaluate the feasibility of boomerang-style attacks, Cid et al. introduced in EUROCRYPT 2018 [46] a new cryptanalysis tool: the Boomerang Connectivity Table (BCT). Later in 2018, Boura and Canteaut [16] introduced a parameter for cryptographic S-boxes called *boomerang uniformity*. It is defined as the maximum value in the BCT and it measures the resistance of the S-box against the boomerang attack. Figure 2.7 shows how the BCT at entry (a,b) is obtained for an invertible S-box S. Notice that it corresponds to the proba-

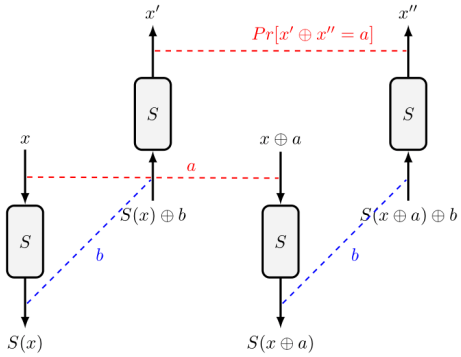


Figure 2.7: Computation of the BCT at point (a, b) for an S-box S

bility studied in (2.2) when E_m is an S-box. There is a strong relation between boomerang and differential uniformity. The former is always bigger than or equal to the latter and functions with optimal differential uniformity also have optimal boomerang uniformity.

Another rather powerful attack on symmetric cryptosystems is the linear attack, see [88]. This attack is effective when it is possible to find good linear approximations to the cipher up to a certain number of rounds. The nonlinearity property evaluates the resistance of the S-box to such attack.

As already mentioned, optimal cryptographic functions, are often optimal for other mathematical fields as well. Hence studying and getting a better understanding of such functions can lead to important results in other research areas. The work of this thesis is focused on the differential uniformity property and on the boomerang uniformity property. In particular it focuses on the study of optimal vectorial Boolean functions with respect to these properties.

2.2 Functions over finite fields

We present here necessary mathematical notions for understanding the content of the next chapters. Even though most of the results presented in this work concern finite fields of even characteristic, we prefer to introduce many mathematical objects in their general definition. This is done in particular for definitions that will be used also for the case of finite fields of odd characteris-

tic in Chapter 7.

For p a prime number and n a positive integer, we define $\mathbb{F}_{p^n}$ the finite field with p^n elements, and $\mathbb{F}_p^n$ the n-dimensional vector space over $\mathbb{F}_p$, where an element $\lambda \in \mathbb{F}_p^n$ is of the form $\lambda = (\lambda_1, \ldots, \lambda_n)$. The p-weight of $\lambda \in \mathbb{F}_p^n$ is the integer $w_p(\lambda) = \sum_{i=1}^{n} \lambda_i$. Instead, the p-weight of a positive integer $k \leq p^n - 1$ is the p-weight of the p-ary expansion $\sum_{i=0}^{n-1} p^i k_i$ of k, that is $w_p(k_0, \ldots, k_{n-1})$. With $\mathbb{F}_{p^n}^\star = \langle \zeta \rangle$ we denote the multiplicative subgroup of $\mathbb{F}_{p^n}$, where ζ is a primitive element. In general, for any set E, $E^\star$ denotes its subset $E \setminus \{0\}$.

Definition 2.1. *An* (n,m,p)-function*, or a* vectorial function*, is a map F from the vector space $\mathbb{F}_p^n$ to the vector space $\mathbb{F}_p^m$. When $p = 2$, such function is simply called an* (n,m)-function *or a* vectorial Boolean function*.*

Remark 2.1. *We assume here and in the next chapters that, when referring to an (n,m,p)-function, we have $m \leq n$.*

When $m = 1$, the function is usually denoted by a lower case f and it is called a *Boolean function* when $p = 2$. In this last case we call f also an *n-variable Boolean function*.

An (n,m,p)-function F can be seen as a vector of $(n,1,p)$-functions:

$$F = (f_1, \ldots, f_m),$$

where $f_1, \ldots, f_m$ are $(n,1,p)$-functions called the coordinates of F. Given an element $\lambda \in \mathbb{F}_p^m$, $\lambda \neq 0$, the λ-component of F is the $(n,1,p)$-function

$$f_\lambda = \lambda \cdot F = \sum_{i=1}^{m} \lambda_i f_i.$$

A vectorial function admits different representations. The *algebraic normal form*, shortly ANF, of an (n,m,p)-function F is its representation as a polynomial with coefficients in $\mathbb{F}_p^m$. Hence the ANF representation of $F \in \mathbb{F}_p^m[x_1, \ldots, x_n]$ is of the form

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

The *algebraic degree* of F, denoted as $\deg(F)$, is the maximum value in the set $\{w_p(u) : u \in \mathbb{F}_p^n \ s.t. \ a_u \neq (0, \ldots, 0)\}$ and it corresponds to the maximum algebraic degree of the coordinate functions of F.

The value set or image set of F is denoted by $\mathrm{Im}(F)$, i.e. $\mathrm{Im}(F) = \{F(c) : c \in \mathbb{F}_p^n\}$, and the set of roots of F over $\mathbb{F}_p^n$ is denoted by $\mathrm{Ker}(F)$. When $m = n$ the polynomial F is a *permutation polynomial* (PP) over $\mathbb{F}_p^n$ if $\mathrm{Im}(F) = \mathbb{F}_p^n$, and it is a *complete mapping* over $\mathbb{F}_p^n$ if both F and $F + Id$ are PPs. With Id we indicate the identity map, i.e. $Id(u) = u$ for every $u \in \mathbb{F}_p^n$.

An (n, m, p)-function is called *balanced* if it takes every value of $\mathbb{F}_p^m$ the same number p^{n-m} of times. It is equivalent to have all the non-zero components balanced. Obviously, for $m = n$, balanced functions are the permutations of $\mathbb{F}_p^n$.

When $m = n$ the *univariate polynomial representation* is often used. Indeed, the vector space $\mathbb{F}_p^n$ is identified with the finite field $\mathbb{F}_{p^n}$, and a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ admits a unique representation as a polynomial over $\mathbb{F}_{p^n}$ of degree at most $p^n - 1$,

$$F(x) = \sum_{i=0}^{p^n-1} a_i x^i, \text{ with } a_i \in \mathbb{F}_{p^n}.$$

In this case the algebraic degree can be expressed using the p-weight of the exponents. It corresponds to the maximal p-weight of i such that $a_i \neq 0$, see [42, p. 404] for the case $p = 2$.

Given an (n, n, p)-function F, we call F

- p^m*-linear* or a p^m*-polynomial*, for m a positive divisor of n, if it is of the form $F(x) = \sum_{i=0}^{n/m-1} a_i x^{p^{mi}}$, with $a_i \in \mathbb{F}_{p^n}$;
- *linear* if it is of the form $F(x) = \sum_{i=0}^{n-1} a_i x^{p^i}$, with $a_i \in \mathbb{F}_{p^n}$;
- *affine* if it is the sum of a linear function and a constant;
- *DO polynomial* (Dembowski-Ostrom polynomial) if it is of the form $F(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j}$, with $a_{ij} \in \mathbb{F}_{p^n}$ (if $p = 2$ then $i < j$);
- *quadratic* if it is the sum of a DO polynomial and an affine function.[2]

A well-known example of linear function is the *trace* function that maps $\mathbb{F}_{p^n}$ into $\mathbb{F}_p$:

$$\mathrm{Tr}_n(x) = \mathrm{Tr}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}} = \sum_{k=0}^{n-1} x^{p^k}.$$

For m a positive divisor of n, the map Tr_n^m denotes the trace function from $\mathbb{F}_{p^n}$ into $\mathbb{F}_{p^m}$:

$$\mathrm{Tr}_n^m(x) = \mathrm{Tr}^m(x) = x + x^{p^m} + x^{p^{2m}} + \ldots + x^{p^{(n/m-1)m}}.$$

[2] Affine functions and quadratic functions have algebraic degree at most one and two respectively.

For the univariate representation, the λ-component of F is the map $f_\lambda = \mathrm{Tr}(\lambda F)$.

Remark 2.2. *If m is a positive divisor of n, then a map $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ admits a univariate polynomial representation since it can be viewed as a function from $\mathbb{F}_{p^n}$ to itself.*

2.2.1 The differential uniformity

Definition 2.2. *For an (n,m,p)-function F and $(a,b) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$, let $\delta_F(a,b)$ be the number of solutions of the equation $F(x+a) - F(x) = b$. Then the value*

$$\delta_F = \max_{a \in \mathbb{F}_p^n \setminus \{0\}, b \in \mathbb{F}_p^m} \delta_F(a,b) \tag{2.3}$$

is called the differential uniformity *of F and F is said to be* differentially δ_F-uniform. *The function*

$$\Delta_F(x,y) = F(x+y) - F(x) - F(y) \in \mathbb{F}_p^m[x,y]$$

is called the difference operator of F *and the map*

$$D_a F(x) = F(x+a) - F(x) = \Delta_F(x,a) + F(a)$$

is the derivative of F in the direction of a.

When the map F, considered in its univariate polynomial representation, is a power function, then the differential uniformity can be computed by fixing $a = 1$. Indeed, for $F(x) = x^d$, $D_a F(x) = (x+a)^d - x^d = a^d\left[\left(\frac{x}{a}+1\right)^d - \left(\frac{x}{a}\right)^d\right]$. The number of solutions of $D_a F(x) = b$ equals the number of solutions of $D_1 F(x) = \frac{b}{a^d}$.

Differential uniformity measures the resistance of F, used as an S-box inside a cryptosystem, to the differential attack. To achieve a good resistance, the value of δ_F has to be small. Hence the best resistance is achieved when $\delta_F = p^{n-m}$ and in this case the function F is called *perfect nonlinear* (PN). A function F is perfect nonlinear if and only if all its derivatives, except the one in the zero direction, are balanced, see Proposition 9.3 in [42] for the case $p = 2$. For $m = n$ such functions, with $\delta_F = 1$, that is, with all non-zero derivatives being permutations, are also called *planar*.

Clearly, for $p = 2$, the smallest value achievable for (n,n)-functions is 2. Indeed if x' is a solution of $D_a F(x) = b$, also $x' + a$ satisfies the equation. In even characteristic, functions that achieve the best resistance are called *almost perfect nonlinear* (APN).

2.2.2 Equivalence relations

In order to study vectorial functions, it is important to use equivalence relations. This is especially true since the number of functions is so huge that it is not feasible to analyse each function. In this situation, it is easier to divide the set of all functions into equivalence classes and, for each class, study the properties of one representative function. For example, the total number of (n,n)-functions is $(2^n)^{2^n}$ but, when considering an equivalence relation, the number of classes may be considerably smaller. Even for small dimensions the equivalence relations give us a big advantage. Indeed for $n = 4$ there are in total 2^{64} (4,4)-functions but, for the case of EA-equivalence, it has been computed that there are only 4713 different classes, see [20]. Since we are mainly interested in studying the differential property of vectorial functions, we introduce equivalence relations that preserve the differential uniformity.

Given F, F' two functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, they are called

- *linear equivalent* if $F' = A_1 \circ F \circ A_2$, for A_1, A_2 linear permutations of $\mathbb{F}_p^m$ and $\mathbb{F}_p^n$ respectively;
- *affine equivalent* if $F' = A_1 \circ F \circ A_2$, for A_1, A_2 affine permutations of $\mathbb{F}_p^m$ and $\mathbb{F}_p^n$ respectively;
- *extended affine equivalent* (EA-equivalent) if $F' = F'' + A$, for A (n,m,p)-affine map and F'' (n,m,p)-function affine equivalent to F;
- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent [44]) if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_p^n \times \mathbb{F}_p^m$ that maps the graph of F into the graph of F' ($\mathcal{L}(\Gamma_F) = \Gamma_{F'}$), where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_p^n\}$ and $\Gamma_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_p^n\}$.

These relations are connected to each other: linear equivalence is a particular case of affine equivalence, affine equivalence is contained in EA-equivalence and EA-equivalence is contained in CCZ-equivalence. Moreover, every permutation is CCZ-equivalent to its inverse, while, in general, a permutation and its inverse are not EA-equivalent. When a function is not affine, its algebraic degree is preserved via EA-equivalence but not via CCZ-equivalence. CCZ-equivalence is so far the most general notion of equivalence for which the differential uniformity is an invariant. Indeed, it has been proved to be more general than EA-equivalence together with taking the inverse of a permutation, see

[32]. However there are some specific cases for which these two equivalences coincide:

- for planar functions, in the case of DO planar functions they coincide also with linear equivalence, [33];
- for Boolean functions, [27];
- two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent, as conjectured by Edel and proved by Yoshiara in [105].

Another notion of equivalence is known for planar quadratic functions which preserve differential uniformity and which is more general than CCZ-equivalence. This equivalence is called isotopic equivalence and it will be explained in Section 2.4.

2.3 Vectorial Boolean functions

We assume now that F is an (n,n)-function

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

As mentioned in the previous section, a well known linear map with image set $\mathbb{F}_2$ is the *trace* function

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

For m a positive divisor of n, the map

$$\mathrm{Tr}_n^m(x) = \mathrm{Tr}^m(x) = \sum_{j=0}^{n/m-1} x^{2^{jm}},$$

has $\mathbb{F}_{2^m}$ as image set.

Definition 2.3. *For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, the* Walsh transform *of f is the map*

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(ux)},$$

with $u \in \mathbb{F}_{2^n}$. We indicate with the symbol $\mathcal{F}(f)$ the Walsh transform value in 0,

$$\mathcal{F}(f) = \mathcal{W}_f(0) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)}.$$

A Boolean function f is then balanced *if and only if $\mathcal{F}(f) = 0$.*

The Walsh transform *of F, for $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, is the function that maps $(u, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ into the Walsh transform of the component function $\mathrm{Tr}(vF)$ evaluated in u, i.e.*

$$\mathcal{W}_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ux + vF(x))}.$$

The Walsh spectrum *of F is the multiset of all values of the Walsh transform of F. With* extended Walsh spectrum *we indicate the multiset of their absolute values.*

The extended Walsh spectrum is invariant under CCZ-equivalence, see [66].

2.3.1 Almost perfect nonlinear functions

Several works have been focused on finding and constructing new families of APN functions. Table 2.1 shows all known values, up to CCZ-equivalence, for exponents d such that the (n, n)-function x^d is APN. Since EA-equivalence pre-

Table 2.1: Known APN power functions x^d over $\mathbb{F}_{2^n}$

Name	Exponent d	Conditions	Degree	Proven
Gold	$2^i + 1$	$\gcd(i, n)$=1	2	[73, 92]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n)$=1	i+1	[75, 76]
Welch	$2^t + 3$	$n = 2t + 1$	3	[60]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ t+1	[59]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[7, 82, 92]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[61]

serves the algebraic degree of a function and, in general, the functions listed in Table 2.1 have different algebraic degrees, it is easy to verify that these APN functions are EA-inequivalent. Instead the algebraic degree is not an invariant for CCZ-equivalence. But also for this case it was possible to prove the inequalities. In both [106] and [54] Yoshiara and Dempwolff show that two APN power functions are CCZ-equivalent if and only if they are *cyclotomic-equivalent*, i.e. they are EA-equivalent or one is EA-equivalent to the inverse of the second one. To be more precise if we consider x^k and x^l defined over $\mathbb{F}_{2^n}$, these functions are cyclotomic-equivalent if there exists an integer $0 \leq a < n$ such that $l \equiv k2^a \mod (2^n - 1)$ or $kl \equiv 2^a \mod (2^n - 1)$, when k is coprime with $2^n - 1$. Before these works, some inequivalences between families of APN

power functions were proved in [28]. The list in Table 2.1 was conjectured to be complete in [59] and this was confirmed computationally up to $n = 25$, see [61].

Before [32] the only known APN functions were EA-equivalent to power functions and it was assumed that all APN functions were EA-equivalent to power functions. In [32] Budaghyan, Carlet and Pott showed the existence of classes of APN mappings EA-inequivalent to power functions. Such functions were constructed by applying CCZ-equivalence to the Gold APN mappings. In [65] Edel, Kyureghyan and Pott gave the first examples of APN functions CCZ-inequivalent to power functions. The first infinite families of such APN polynomials were constructed in [29]. In Table 2.2 one representative for each of these families is listed, considering also the other families discovered through the years. All these CCZ-equivalence classes contain quadratic maps. Besides quadratic and power APN functions, very little is known. Indeed, up to CCZ-equivalence, only one example of APN function CCZ-inequivalent to power and to quadratic mappings has been constructed. This function is defined over $\mathbb{F}_{2^6}$.

APN permutations

As mentioned in Section 2.1, block ciphers need to be invertible for decrypting a ciphertext. For some constructions of block cipher (for example AES, PRESENT and SERPENT [10, 15, 52]) this implies that all the vectorial boolean functions implemented in the algorithm must be invertible, hence must be permutations. APN permutations are therefore of particular interest. Moreover, because of implementation reasons, it is often required to operate over fields of even degree extension. Therefore APN permutations over $\mathbb{F}_{2^{2k}}$ are of great importance.

In odd dimension, few examples of APN permutations are available. In 1998, H. Dobbertin showed the following, see Proposition 9.19 in [42] for a proof.

Proposition 2.1. *APN power functions over $\mathbb{F}_{2^n}$ are permutations if n is odd, and are 3-to-1 if n is even.*

Among the known families of APN functions presented in Table 2.2, the only permutations are the binomials introduced in [29] with $p = 3$ and k odd.

Table 2.2: Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

Function	Conditions	In
$x^{2^s+1}+\alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,3)=\gcd(s,3k)=1$, $p\in\{3,4\}$, $i=sk \mod p$, $m=p-i$, $n\geq 12$, α primitive in $\mathbb{F}_{2^n}^*$	[29]
$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q(2^{2i}+2^i)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $gcd(2^i+1,q+1)\neq 1$, $cb^q+b\neq 0$, $c\notin\{\lambda^{(2^i+1)(q-1)},\lambda\in\mathbb{F}_{2^n}\}$, $c^{q+1}=1$	[26]
$x(x^{2^i}+x^q+cx^{2^iq})+$ $x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ is irreducible over $\mathbb{F}_{2^n}$	[26]
$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$	[30]
$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[31]
$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n$, $a\neq 0$	[31]
$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\|(k+s)$, $\mathbb{F}_{2^n}^\star=\langle u\rangle$	[17]
$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_sx^{2^s(q+1)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, i,m odd, $c\notin\mathbb{F}_{2^m}$, $\gamma_s\in\mathbb{F}_{2^m}$, d not a cube	[17]
$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$	$q=2^m$, $n=2m$, $m\geq 2$ even, $\gcd(i,m)=1$ and j even $\mathbb{F}_{2^n}^\star=\langle u\rangle$, $u'\in\mathbb{F}_{2^m}$ not a cube	[112]
$ut(x)(x^q+x)+t(x)^{2^{2i}+2^{3i}}+$ $at(x)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$ $a,b\in\mathbb{F}_{2^m}$, $u\notin\mathbb{F}_{2^m}$, $t(x)=u^qx+x^qu$ and $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$	[99]
$x^3+ax^{2^k(2^i+1)}$ $+bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$	$n=2m=10$, $(a,b,c)=(\beta,1,0)$, $i=3$, $k=2$, $\mathbb{F}_4^*=\langle\beta\rangle$	[34]
	$n=2m$, m odd, $3\not\|\, m$, $(a,b,c)=(\beta,\beta^2,1)$, $\mathbb{F}_4^*=\langle\beta\rangle$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \mod n\}$	

Up to CCZ-equivalence, the binomials together with power APN functions are the only known cases of APN permutations in odd dimension.

The problem of the existence of APN permutations in even dimension has been first asked (at least in a printed form) in 1994 in [93]. Only in 2009, Dillon and his team discovered the first example of APN permutation over $\mathbb{F}_{2^6}$, see [23]. The map is obtained by applying a CCZ-equivalence transformation over the so-called Kim function $x^3+x^{10}+\zeta x^{24}$ (given in [22]). So far, this is the only example, up to CCZ-equivalence, of APN permutation in even dimension. The problem of finding an APN permutation in dimension $n\geq 8$, or better, an infinite class of APN permutations in even dimensions, has often been referred

to as the *big APN problem*.

Some partial non-existence results have been discovered during the years. In [74], Hou showed computationally that there are no APN permutations in dimension 4 (the first theoretical proof appeared later on in [37]). Given F a permutation over $\mathbb{F}_{2^{2k}}$, the following conditions are satisfied:

- if k is even and $F \in \mathbb{F}_{2^4}[x]$ then F is not APN, see [74];
- if $F \in \mathbb{F}_{2^k}[x]$ then F is not APN, see [74];
- if F is a power function then F is not APN, see Proposition 2.1;
- if F is plateaued[3] then F is not APN, see [6];
- if F has a partially-bent[4] component then F is not APN, see [37].

As we explained before, the only example of APN permutation in even dimension was obtained by applying a CCZ-equivalent transformation to a quadratic APN function. Therefore many studies have been focused on APN maps of degree 2. These functions are relatively easy to construct and to study and, even though a low algebraic degree is usually a bad quality for cryptographic purposes[5], there might lay an APN permutation of high degree in their CCZ-equivalence classes. This possibility has been checked for many known quadratic APN functions in small dimensions, but, so far, in even dimensions the Kim function is the only one that is CCZ-equivalent to a permutation. In particular, in [109] the test has been performed over the list of 470 quadratic APN functions in dimension 7 and 8157 in dimension 8. Also some results on CCZ-inequivalence to permutations have been recently discovered for some of the known infinite families of APN functions. The Gold functions over $\mathbb{F}_{2^n}$ for n even and the Kasami functions over $\mathbb{F}_{2^n}$ for $n = 4m$ are not CCZ-equivalent to permutations, see [71]. The map $x^3 + \mathrm{Tr}(x^9)$ over $\mathbb{F}_{2^{4m}}$ is not CCZ-equivalent to a permutation, see [72].

[3] A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *plateaued* if for every $v \in \mathbb{F}_{2^n}^\star$ there exists a positive integer λ_v such that $\mathcal{W}(u,v) \in \{0, \pm\lambda_v\}$ for every $u \in \mathbb{F}_{2^n}$. Quadratic functions are plateaued.

[4] A Boolean function f is called *partially-bent* if all its derivatives are either balanced or constant. Quadratic functions are partially-bent.

[5] The *higher order differential attack* [80, 83] is efficient when the algebraic degree of the S-box is low.

On equivalences and invariants

To determine whether two functions are CCZ-equivalent is usually mathematically and computationally difficult. In the following we report some properties of the CCZ-equivalence that can facilitate this problem.

The CCZ-equivalence between functions is often determined through the equivalence between the corresponding codes. Given an (n,n)-function F, consider the $(2n+1) \times 2^n$ matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \zeta & \zeta^2 & \dots & \zeta^{2^n-2} \\ F(0) & F(1) & F(\zeta) & F(\zeta^2) & \dots & F(\zeta^{2^n-2}) \end{bmatrix},$$

where $\zeta \in \mathbb{F}_{2^n}^\star$ is a primitive element and each symbol from the last two rows is in its vector representation (element of $\mathbb{F}_2^n$). Let $\widetilde{C}_F$ be the linear code admitting H as parity-check matrix[6]. It is shown in [22] that two (n,n)-functions F and G are CCZ-equivalent if and only if the codes $\widetilde{C}_F$ and $\widetilde{C}_G$ are equivalent. However, to check whether two codes are equivalent can also be difficult. In these situations, invariants can help to determine whether two functions are equivalent. An invariant is a property, or a statistic, which is preserved under a specific equivalence relation. For example, as we mentioned before, the algebraic degree is invariant under EA-equivalence. Therefore if two functions have different algebraic degrees, we know that they are not EA-equivalent. However, functions belonging to different equivalence classes may have the same invariant property. So, the more invariants are discovered, the better we can study the equivalences. Constructing and analysing invariants for CCZ-equivalence and EA-equivalence is therefore important. We remind that, when considering quadratic maps, these two equivalences coincide. So, in this case, EA-invariants are also CCZ-invariants.

We recall here some notions of CCZ-invariants for APN functions that will be used in the next chapters: the Γ-rank, the Δ-rank and $|\mathcal{M}(G_F)|$. For more details on the construction of these invariants, we refer the reader to [66].

Consider a function F as a map from $\mathbb{F}_2^n$ to itself. We associate with F a

[6]Note that the APN property can be expressed in terms of properties of the related code. Indeed, F is APN if and only if the code $\widetilde{C}_F$ has parameters $[2^n, 2^n-1-2n, 6]$ [42, p. 424].

group algebra element $G_F \in \mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$,

$$G_F = \sum_{v \in \mathbb{F}_2^n} (v, F(v)).$$

Recalling that the multiplication for group algebras over $\mathbb{F}[G]$ is as follow

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

from [66] we have the following lemma.

Lemma 2.1. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if*

$$G_F \cdot G_F = 2^n \cdot (0,0) + 2 \cdot D_F \text{ in } \mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$$

for some subset $D_F \in (\mathbb{F}_2^n \times \mathbb{F}_2^n) \setminus \{(0,0)\}$.

Definition 2.4. *For an APN function F, the Γ-rank of F is the dimension of the ideal generated by G_F in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$. Similarly, the Δ-rank of F is the dimension of the ideal generated by D_F in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$.*

Γ-rank and Δ-rank are invariant under CCZ-equivalence, see [66].

Definition 2.5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. We call the development of G_F, denoted by dev(G_F), the design over the point set $\mathbb{F}_2^n \times \mathbb{F}_2^n$ with blocks*

$$G_F \cdot (a,b) = \{(x + a, F(x) + b) : x \in \mathbb{F}_2^n\}$$

for $a, b \in \mathbb{F}_2^n$.

For two CCZ-equivalent APN functions F and H, the designs dev(G_F) and dev(G_H) are isomorphic, shown in [66]. Defined the multiplier group $\mathcal{M}(G_F)$ of dev(G_F) as the group of automorphisms φ of $\mathbb{F}_2^{2n}$ such that $\varphi(G_F) = G_F \cdot (u,v)$ for some $u, v \in \mathbb{F}_2^n$, then also $|\mathcal{M}(G_F)|$ is invariant under CCZ-equivalence.

On known examples of APN functions

The construction of infinite families of APN functions is an important problem in the field of vectorial Boolean functions. Related to it, the computational search for examples of APN maps in different dimensions is of fundamental importance. Indeed, from the observation of computational results, it might be possible to notice a pattern and this could lead to the construction of an infinite

family of APN functions. Moreover, as mentioned before, constructing new APN functions might also lead to the discovery of an APN permutation.

Over small dimensions such computational search has been done exhaustively. Indeed the classification of APN functions over $\mathbb{F}_{2^n}$ is complete for $n \leq 5$ [21]: in these dimensions, up to CCZ-equivalence, the only APN maps are power functions. For $n = 6$ the classification is complete for quadratic and cubic APN functions: up to CCZ-equivalence there exist 13 quadratic APN maps and 1 cubic APN map, see [22, 64]. In Table 2.3 we report these 14 CCZ-inequivalent APN polynomials over $\mathbb{F}_{2^6}$ (as listed in [66, Table 5]). We include the values of Γ-rank, Δ-rank and $|\mathcal{M}(G_F)|$ from [66, Table 6]. Function no. 2.11

Table 2.3: APN functions over $\mathbb{F}_{2^6}$ presented in [66]

no.	$F(x)$	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
1.1	x^3	1102	94	$2^7 \cdot 3^3 \cdot 7$
1.2	(no. 1.1)$+\zeta(\mathrm{Tr}(\zeta^{56}x^3) + \mathrm{Tr}_3(\zeta^{18}x^9))$	1146	94	$2^6 \cdot 3^2 \cdot 7$
2.1	$x^3 + \zeta x^{24} + x^{10}$	1166	96	$2^7 \cdot 7$
2.2	(no. 2.1)$+\zeta^3(\mathrm{Tr}(\zeta^{10}x^3 + \zeta^{53}x^5) + \mathrm{Tr}_3(\zeta^{36}x^9))$	1168	96	2^6
2.3	(no. 2.1)$+(\mathrm{Tr}(\zeta^{34}x^3 + \zeta^{48}x^5) + \mathrm{Tr}_3(\zeta^9x^9))$	1170	96	2^6
2.4	(no. 2.1)$+\zeta^2(\mathrm{Tr}(\zeta^{24}x^3 + \zeta^{28}x^5) + \mathrm{Tr}_3(x^9))$	1172	96	2^6
2.5	(no. 2.3)$+\zeta^{42}(\mathrm{Tr}(\zeta^{10}x^3 + \zeta^{51}x^5) + \mathrm{Tr}_3(\zeta^9x^9))$	1158	96	$2^6 \cdot 5$
2.6	(no. 2.3)$+\zeta^{23}(\mathrm{Tr}(\zeta^{31}x^3 + \zeta^{49}x^5) + \mathrm{Tr}_3(\zeta^9x^9))$	1170	96	$2^6 \cdot 5$
2.7	(no. 2.3)$+\zeta^{12}(\mathrm{Tr}(\zeta^{42}x^3 + \zeta^{13}x^5) + \mathrm{Tr}_3(\zeta^{54}x^9))$	1170	96	2^6
2.8	(no. 2.3)$+\zeta(\mathrm{Tr}(\zeta^{51}x^3 + \zeta^{60}x^5) + \mathrm{Tr}_3(\zeta^{18}x^9))$	1170	96	2^6
2.9	(no. 2.3)$+\zeta^{14}(\mathrm{Tr}(\zeta^{18}x^3 + \zeta^{61}x^5) + \mathrm{Tr}_3(\zeta^{18}x^9))$	1172	96	2^6
2.10	(no. 2.3)$+\zeta^{17}(\mathrm{Tr}(\zeta^{50}x^3 + \zeta^{56}x^5))$	1174	96	2^6
2.11	(no. 2.3)$+\zeta^{19}(\mathrm{Tr}(\zeta^{11}x^3 + \zeta^7x^5 + \zeta^{38}x^7 + \zeta^{61}x^{11} + \zeta^{23}x^{13})$ $+\mathrm{Tr}_3(\zeta^{54}x^9) + \mathrm{Tr}_2(\zeta^{42}x^{21}))$	1300	152	2^3
2.12	(no. 2.4)$+\zeta(\mathrm{Tr}(\zeta^{54}x^3 + \zeta^{47}x^5) + \mathrm{Tr}_3(\zeta^9x^9))$	1166	94	$2^6 \cdot 7$

in Table 2.3 is the only known example of APN function not CCZ-equivalent to power and to quadratic maps, [21, 66].

In bigger dimensions, $n = 7,8,9$, the classification is complete for quadratic APN functions with coefficients over $\mathbb{F}_2$, see [107]. Moreover, partial lists of CCZ-inequivalent APN functions were presented in [22] and in [66] for the same dimensions. In the last mentioned paper the authors listed 19 APN maps for $n = 7$, 23 APN maps for $n = 8$ and 11 APN maps for $n = 9$. In Tables 2.4, 2.5, 2.6 we report Tables 7, 9, 11 from [66] respectively. We include the values of Γ-rank, Δ-rank and $|\mathcal{M}(G_F)|$ from [66, Tables 8,10,12].

Table 2.4: APN functions over $\mathbb{F}_{2^7}$ presented in [66]

no.	$F(x)$	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
1.1	x^3	3610	198	$2^7 \cdot 7 \cdot 127$
1.2	$x^3 + \mathrm{Tr}(x^9)$	4026	212	$2^7 \cdot 7$
2.1	$x^{34} + x^{18} + x^5$	4034	210	$2^7 \cdot 7$
2.2	(no. 2.1)+$\mathrm{Tr}(x^3 + \zeta^{103}x^5 + \zeta^5 x^9)$	4040	212	$2^7 \cdot 7$
3.1	x^5	3708	198	$2^7 \cdot 7 \cdot 127$
4.1	x^9	3610	198	$2^7 \cdot 7 \cdot 127$
5.1	x^{13}	4270	338	$7 \cdot 127$
6.1	x^{57}	4704	436	$7 \cdot 127$
7.1	x^{-1}	8128	4928	$2 \cdot 7 \cdot 127$
8.1	$x^{65} + x^{10} + x^3$	4038	212	$2^7 \cdot 7$
9.1	$x^{66} + x^{18} + x^9 + x^3$	4044	212	$2^7 \cdot 7$
10.1	$x^{33} + x^{17} + x^{12} + x^3$	4048	210	$2^7 \cdot 7$
10.2	(no. 10.1)+$\mathrm{Tr}(\zeta^{41}x^3 + \zeta^{17}x^5 + \zeta^{34}x^9)$	4040	210	$2^7 \cdot 7$
11.1	$x^{66} + x^{34} + x^{20} + x^3$	4048	210	$2^7 \cdot 7$
12.1	$x^{72} + x^{40} + x^{12} + x^3$	4048	210	$2^7 \cdot 7$
13.1	$x^{34} + x^{33} + x^{10} + x^5 + x^3$	4040	212	$2^7 \cdot 7$
14.1	$x^{72} + x^{40} + x^{34} + x^6 + x^3$	4048	212	$2^7 \cdot 7$
14.2	(no. 14.1)+$\mathrm{Tr}(\zeta^{105}x^3 + \zeta^{84}x^5 + \zeta^{123}x^9)$	4050	210	$2^7 \cdot 7$
14.3	(no. 14.1)+$\zeta^{27}\mathrm{Tr}(\zeta^{20}x^3 + \zeta^{94}x^5 + \zeta^{66}x^9)$	4046	212	2^7

In a more recent work presented at WCC 2013, Yu et al. [109] introduced a new approach for constructing quadratic APN maps. With their method the authors extended the lists of CCZ-inequivalent APN functions for dimensions 7 and 8, adding 471 maps for $n = 7$ and 8157 for $n = 8$. At the same conference, Weng et al. [102] presented a similar approach to construct quadratic APN functions. With their construction they obtained many quadratic APN functions in dimensions 7 and 8 and listed, for each dimension, 10 functions CCZ-inequivalent to those listed in [66]. Each function in the list for $n = 7$ is EA-equivalent to a function presented in [109]. For $n = 8$ the first nine functions in [102, Table 5] are EA-inequivalent to any of the functions listed in [66, 109] and the last one, no. 10, is EA-equivalent to a map from the family introduced by Zhou and Pott in [112]. Notice that Table 6 in [102], which presents some invariants for the 10 newly constructed APN maps in dimension 8, has some misprints. In the following we report the same table with the values corrected, see Table 2.7. Excluding the power functions, all the aforementioned APN functions listed for n =7, 8 and 9 are quadratic.

Table 2.5: APN functions over $\mathbb{F}_{2^8}$ presented in [66]

no.	$F(x)$		Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
1.1	x^3		11818	420	$2^{11}\cdot 255$
1.2	(no. 1.1)+$\mathrm{Tr}(\zeta^{48}x^3+x^9)$	(EA-eq. to $x^3+\mathrm{Tr}(x^9)$)	13800	432	$2^{11}\cdot 255$
1.3	(no. 1.1)+$\zeta\mathrm{Tr}(\zeta^{63}x^3+\zeta^{252}x^9)$		13842	436	$2^{10}\cdot 3$
1.4	(no. 1.2)+$\zeta^{38}\mathrm{Tr}(\zeta^{84}x^3+\zeta^{213}x^9)$		14034	438	$2^8\cdot 3$
1.5	(no. 1.2)+$\zeta^{51}\mathrm{Tr}(\zeta^{253}x^3+\zeta^{102}x^9)$		14032	438	$2^{10}\cdot 3$
1.6	(no. 1.3)+$\zeta^{154}\mathrm{Tr}(\zeta^{68}x^3+\zeta^{235}x^9)$		14036	438	$2^{10}\cdot 3$
1.7	(no. 1.4)+$\zeta^{69}\mathrm{Tr}(\zeta^{147}x^3+\zeta^{20}x^9)$		14036	438	$2^9\cdot 3$
1.8	(no. 1.5)+$\zeta^{68}\mathrm{Tr}(\zeta^{153}x^3+\zeta^{51}x^9)$		14032	438	$2^{10}\cdot 3$
1.9	(no. 1.6)+$\zeta^{35}\mathrm{Tr}(\zeta^{216}x^3+\zeta^{116}x^9)$		14034	438	$2^{10}\cdot 3$
1.10	(no. 1.7)+$\zeta^{22}\mathrm{Tr}(\zeta^{232}x^3+\zeta^{195}x^9)$		14030	438	$2^9\cdot 3$
1.11	(no. 1.8)+$\zeta^{85}\mathrm{Tr}(\zeta^{243}x^3+\zeta^{170}x^9)$	(EA-eq. to $x^9+\mathrm{Tr}(x^3)$)	13804	434	$2^{11}\cdot 3$
1.12	(no. 1.9)+$\zeta^{103}\mathrm{Tr}(\zeta^{172}x^3+\zeta^{31}x^9)$		13848	438	$2^{10}\cdot 3$
1.13	(no. 1.10)+$\zeta^{90}(\mathrm{Tr}(\zeta^{87}x^3+\zeta^{141}x^5+\zeta^{20}x^9)+\mathrm{Tr}_4(\zeta^{51}x^{17}+\zeta^{102}x^{34}))$		14046	454	2^9
1.14	(no. 1.11)+$\zeta^5\mathrm{Tr}(\zeta^{160}x^3+\zeta^{250}x^9)$		14036	438	$2^8\cdot 3$
1.15	(no. 1.11)+$\zeta^{102}\mathrm{Tr}(\zeta^6x^3+\zeta^{119}x^9)$	(EA-eq. to x^9)	12370	420	$2^{11}\cdot 255$
1.16	(no. 1.14)+$\zeta^{64}\mathrm{Tr}(\zeta^{133}x^3+\zeta^{30}x^9)$		14032	438	$2^9\cdot 3$
1.17	(no. 1.16)+$\zeta^{78}\mathrm{Tr}(\zeta^{235}x^3+\zeta^{146}x^9)$		14028	438	$2^9\cdot 3$
2.1	$x^3+x^{17}+\zeta^{16}(x^{18}+x^{33})+\zeta^{15}x^{48}$		13200	414	$2^{10}\cdot 3^2\cdot 5$
3.1	$x^3+\zeta^{24}x^6+\zeta^{182}x^{132}+\zeta^{67}x^{192}$		14024	438	$2^{10}\cdot 3$
4.1	$x^3+x^6+x^{68}+x^{80}+x^{132}+x^{160}$		14040	454	2^{11}
5.1	$x^3+x^5+x^{18}+x^{40}+x^{66}$		14044	446	2^{11}
6.1	$x^3+x^{12}+x^{40}+x^{66}+x^{130}$		14046	438	2^{11}
7.1	x^{57}		15358	960	$2^3\cdot 255$

2.3.2 The boomerang uniformity

In [46], Cid et al. introduced the concept of Boomerang Connectivity Table for a permutation F over $\mathbb{F}_{2^n}$. Next, in [16] the authors presented the notion of boomerang uniformity.

Definition 2.6. *Let F be a permutation over $\mathbb{F}_{2^n}$, and a,b in $\mathbb{F}_{2^n}$.*

The Boomerang Connectivity Table *(BCT) of F is a $2^n\times 2^n$ table T_F, also denoted by T when there is no ambiguity on the function F, in which the entry for the position (a,b) is given by*

$$T_F(a,b)=T(a,b)=|\{x\in\mathbb{F}_{2^n}\ s.t\ F^{-1}(F(x)+b)+F^{-1}(F(x+a)+b)=a\}|.$$

Moreover, the maximum value reached in the BCT, $T(a,b)$ for $a,b\in\mathbb{F}_{2^n}^\star$, i.e. the value

$$\beta_F=\max_{a,b\in\mathbb{F}_{2^n}^\star}|\{x\in\mathbb{F}_{2^n}\ s.t.\ F^{-1}(F(x)+b)+F^{-1}(F(x+a)+b)=a\}|,$$

is called the boomerang uniformity *of F, or we call F a* boomerang β_F-uniform *function.*

Table 2.6: APN functions over $\mathbb{F}_{2^9}$ presented in [66]

no.	$F(x)$	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
1.1	x^3	38470	872	$9 \cdot 2^9 \cdot 511$
1.2	(no. 1.1)+$\mathrm{Tr}(x^9)$	47890	920	$9 \cdot 2^9$
1.3	(no. 1.2)+$\zeta^{73}\mathrm{Tr}(\zeta^{426}x^3 + \zeta^{292}x^9)$	48428	930	$9 \cdot 2^9$
1.4	(no. 1.2)+$\zeta^{219}\mathrm{Tr}(\zeta^{303}x^3 + \zeta^{365}x^9)$	48460	944	$9 \cdot 2^9$
2.1	x^5	41494	872	$9 \cdot 2^9 \cdot 511$
3.1	x^{17}	38470	872	$9 \cdot 2^9 \cdot 511$
4.1	x^{13}	58676	3086	$9 \cdot 511$
5.1	x^{19}	60894	3956	$9 \cdot 511$
6.1	x^{241}	61726	3482	$9 \cdot 511$
7.1	x^{-1}	130816	93024	$2 \cdot 9 \cdot 511$
8.1	$x^3 + x^{10} + \zeta^{438}x^{136}$	48608	938	$3 \cdot 7 \cdot 2^9$

Table 2.7: Invariants of the new APN functions of $\mathbb{F}_{2^8}$ presented in [102]

No.	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F)\rvert$
1	14042	438	$2^8 \cdot 3$
2	14040	438	$2^8 \cdot 3$
3	14040	438	$2^8 \cdot 3$
4	14040	438	$2^8 \cdot 3$
5	14040	438	$2^8 \cdot 3$
6	14048	438	$2^8 \cdot 3$
7	14036	438	$2^8 \cdot 3$
8	14044	438	$2^8 \cdot 3$
9	14034	438	$2^{10} \cdot 3$
10	13642	436	$2^{10} \cdot 3^2 \cdot 5$

The differential uniformity is invariant under all the previously mentioned equivalence relations, while the boomerang uniformity is invariant under affine equivalence and inverse transformation but, in general, not under EA and CCZ-equivalence (see [16]). Indeed let F and G be two affine-equivalent permutations of $\mathbb{F}_{2^n}$, $G = A_2 \circ F \circ A_1$ for A_1, A_2 affine permutations of $\mathbb{F}_{2^n}$. Then $T_G(a,b) = T_F(L_1(a), L_2^{-1}(b))$, where L_i denotes the linear part of A_i, $i = 1,2$, while $T_F(a,b) = T_{F^{-1}}(b,a)$.

As it was noted in [84], the entry $T_F(a,b)$ of the BCT can be given by the number of solutions of the system

$$\begin{cases} F^{-1}(x+a) + F^{-1}(y+a) = b \\ F^{-1}(x) + F^{-1}(y) = b. \end{cases}$$

Since the BCT of F and the BCT of F^{-1} are such that $T_F(a,b) = T_{F^{-1}}(b,a)$, the boomerang uniformity of F is given by the maximum number of solutions of the system

$$\begin{cases} F(x+a) + F(y+a) = b \\ F(x) + F(y) = b \end{cases} \tag{2.4}$$

or equivalently

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

Letting $y = x + \alpha$, it is equivalent to

$$\begin{cases} D_a D_\alpha F(x) = 0 \\ D_\alpha F(x) = b. \end{cases} \tag{2.5}$$

Thus, the boomerang uniformity of F is given by

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}^\star} |\{(x,\alpha) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \; s.t. \; (x,\alpha) \text{ is a solution of (2.5)}\}|.$$

We denote by $S_{a,b}$ the number of solutions of the system (2.5) for any $a, b \in \mathbb{F}_{2^n}$.

When F is a power function, as for the differential uniformity, the boomerang uniformity can be computed fixing $a = 1$.

Proposition 2.2 ([84]). *Let $F(x) = x^d$ be defined over $\mathbb{F}_{2^n}$. Then the boomerang uniformity of F is given by $\max_{b \in \mathbb{F}_{2^n}^\star} S_{1,b}$.*

It has been proved in [46] that $\delta_F \leq \beta_F$ for any permutation F. Moreover, $\delta_F = 2$ if and only if $\beta_F = 2$. So, APN permutations offer an optimal resistance to both differential and boomerang attacks.

As mentioned in Subsection 2.3.1, for odd values of n there are few known families of APN permutations while, for n even, up to CCZ-equivalence there is only one example of APN permutation (over $\mathbb{F}_{2^6}$). So, it is interesting to study the boomerang uniformity of non-APN permutations, and in particular of the differentially 4-uniform permutations. For an even integer n there are five primary constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^n}$, which are listed in Table 2.8.

The boomerang uniformity of Gold and Inverse functions have been determined in [16]. For the Bracken-Tan-Tan function the boomerang uniformity

Table 2.8: Primary constructions of differentially 4-uniform permutations over $\mathbb{F}_{2^n}$ (n even)

Name	Function	deg	Conditions	In
Gold	x^{2^i+1}	2	$n=2k$, k odd $\gcd(i,n)=2$	[73]
Kasami	$x^{2^{2i}-2^i+1}$	$i+1$	$n=2k$, k odd $\gcd(i,n)=2$	[76]
Inverse	x^{2^n-2}	$n-1$	$n=2k$, $k\geq 1$	[92]
Bracken-Leander	$x^{2^{2k}+2^k+1}$	3	$n=4k$, k odd	[18]
Bracken-Tan-Tan	$\zeta x^{2^i+1}+\zeta^{2^m}x^{2^{-m}+2^{m+i}}$	2	$n=3m$, m even, $m/2$ odd, $\gcd(n,i)=2$, $3\|m+i$, $\mathbb{F}_{2^n}^\star=\langle\zeta\rangle$	[19]

was obtained from the results in [91]. In particular

$$\beta_{F_1}=4,\ \beta_{F_2}=\begin{cases}4 \text{ if } n\equiv 2 \mod 4\\ 6 \text{ if } n\equiv 0 \mod 4\end{cases} \text{ and } \beta_{F_3}=4,$$

where F_1, F_2 and F_3 are the Gold function, the inverse function and the Bracken-Tan-Tan function respectively.

2.3.3 The nonlinearity

As mentioned in Section 2.1, another important cryptographic property is the nonlinearity. To achieve a good resistance to the linear attack [88], a high value of nonlinearity is required. Here we briefly introduce this property and its relation with the differential uniformity.

Consider f an n-variable Boolean function. The *nonlinearity* of f, $\mathcal{NL}(f)$, is its distance to the set of affine functions, where the distance between two functions f and g is the size of the set $\{x\in\mathbb{F}_{2^n} \ s.t.\ f(x)\neq g(x)\}$.

Definition 2.7. *For an (n,m)-function F, the nonlinearity of F is defined as*

$$\mathcal{NL}(F)=\min_{\lambda\in\mathbb{F}_{2^n}^\star}\mathcal{NL}(f_\lambda).$$

Functions achieving the maximal value, that is $2^{n-1}-2^{n/2-1}$, are called *bent*. All bent functions are also PN, and vice versa, see [42, p. 410]. When $m=n$ these functions do not exist and in this case the nonlinearity is upper bounded by $2^{n-1}-2^{\frac{n-1}{2}}$. The functions that achieve this bound are called *almost bent* (AB) and exist only for odd values of n. All AB functions are APN, see [45], but the converse is not true in general. In odd dimension, if an APN function

is plateaued then it is AB [42, p. 426]. For n even, the maximum for the nonlinearity of APN functions is still to be determined. In general, it is conjectured that for n even the nonlinearity of an arbitrary function is upper bounded by $2^{n-1} - 2^{\frac{n}{2}}$. All the maps listed in Table 2.8 have this nonlinearity. Similar to the differential uniformity, the nonlinearity is invariant under affine, EA and CCZ-equivalence [44]. The extended Walsh spectrum is strictly related to the notion of nonlinearity, indeed we have

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^\star} |\mathcal{W}_F(a,b)|.$$

2.4 Semifields and presemifields

Commutative presemifields are objects closely connected with planar functions. In this section we introduce them and show their connection with planar maps.

2.4.1 Definitions

Definition 2.8. *Given a set $\mathbb{F}$ endowed with two binary operations, an addition $+$ and a multiplication $*$, $\mathbb{S} = (\mathbb{F}, +, *)$ is a* semifield *if the following axioms are satisfied:*

- $(\mathbb{F}, +)$ *is a group with identity 0;*
- $(\mathbb{F}, *)$ *is a quasigroup;*
- $0 * x = x * 0 = 0$ *for all* $x \in \mathbb{F}$*;*
- *the left and right distributivity laws hold;*
- *there is an element* $e \in \mathbb{F}$ *such that* $e * x = x * e = x$ *for all* $x \in \mathbb{F}$.

If the last axiom is not required to be satisfied, then $\mathbb{S}$ is called a presemifield. *Moreover, $\mathbb{S}$ is commutative if the multiplication $*$ is commutative.*

Given a presemifield $\mathbb{S} = (\mathbb{F}, +, *)$, it is always possible to define a semifield $\mathbb{S}' = (\mathbb{F}, +, \star)$ with

$$(x * a) \star (y * a) = x * y,$$

for a fixed $a \in \mathbb{F}^\star$. The unit of $\mathbb{S}'$ is the element $a * a$.

Any finite presemifield must have order a prime power p^n, and can be represented by $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$. A finite field is a trivial example of a commutative semifield. The first non-trivial examples of commutative semifields were constructed by Dickson in [55]. Since then commutative semifields have been intensively studied. They have applications in many different areas of mathematics, such as difference sets, coding theory, group theory and finite geometry.

The concept of *isotopic equivalence* was originally defined by Albert [2] in the study of presemifields and semifields. Given two finite presemifields with same order, $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, *)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$, they are *isotopic* if there exist $M, N, T \in \mathbb{F}_{p^n}[x]$ linear permutations such that, for any $x, y \in \mathbb{F}_{p^n}$,

$$T(x * y) = M(x) \star N(y).$$

The triplet (M, N, T) is referred to as the *isotopism* between $\mathbb{S}_1$ and $\mathbb{S}_2$. If $M = N$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are called *strongly isotopic*.

Clearly, a presemifield and its corresponding semifield are strongly isotopic with isotopism (L_a, L_a, Id), where $L_a(x) = x * a$.

As mentioned above, there is a close connection between planar functions and presemifields. Indeed it was shown by Coulter and Henderson in [49] that there is a 1-to-1 correspondence between commutative presemifields of odd order and planar DO polynomials. Given a commutative presemifield $\mathbb{S} = (\mathbb{F}_{p^n}, +, *)$ of odd order, the function

$$F_{\mathbb{S}}(x) = \frac{1}{2}(x * x)$$

is a planar DO polynomial. Conversely, given $F \in \mathbb{F}_{p^n}[x]$ a quadratic planar function, then $\mathbb{S}_F = (\mathbb{F}_{p^n}, +, *)$ with

$$x * y = F(x + y) - F(x) - F(y)$$

is a commutative presemifield.

It is natural to extend the notion of isotopic equivalence to planar quadratic functions.

Definition 2.9. *Given $F, F' \in \mathbb{F}_{p^n}[x]$ quadratic planar functions, they are called* isotopic equivalent *if their corresponding presemifields $\mathbb{S}_F$ and $\mathbb{S}_{F'}$ are isotopic equivalent.*

The notion of isotopic equivalence is connected with the notion of CCZ-equivalence. Indeed we have the following:

- F, F' planar functions are CCZ-equivalent if and only if they are EA-equivalent [33];
- F, F' planar DO functions are CCZ-equivalent if and only if they are linear equivalent [33];
- F, F' planar DO functions are CCZ-equivalent if and only if $\mathbb{S}_F$ and $\mathbb{S}_{F'}$ are strongly isotopic [33];
- if n is odd then isotopic equivalence coincides with strongly isotopic equivalence, and so with CCZ-equivalence [49];
- any commutative presemifields of odd order can generate at most two CCZ-equivalence classes of planar DO polynomials [49].

Moreover, an example of isotopism that is not strong is given in [94]. Therefore, for the case of planar DO polynomials, the isotopic equivalence is more general than the CCZ-equivalence.

2.4.2 Some known cases

Among the known examples of planar functions, the only ones that are not quadratic belong to the family

$$x^{\frac{3^t+1}{2}}$$

defined over $\mathbb{F}_{3^n}$, with t odd such that $\gcd(t,n) = 1$, [51]. The other known planar functions are DO polynomials, so they can either be identified with the polynomial representations or with the associated commutative semifields. Very few cases of commutative semifields of odd order are known so far. Further we list some of the known families.

For any p odd we have the following planar functions:

(i) x^2, defined over $\mathbb{F}_{p^n}$, it corresponds to the finite field $\mathbb{F}_{p^n}$;

(ii) x^{p^t+1}, defined over $\mathbb{F}_{p^n}$, with $n/\gcd(n,t)$ odd, it corresponds to Albert's commutative twisted field [1];

(iii) $L(t^2(x)) + \frac{1}{2}x^2$, defined over $\mathbb{F}_{p^{2k}}$ for $k = er$, with $t(x) = x^{p^k} - x$ and $L(x) = 8^{-1}(x^{p^r} - x)$, it corresponds to the Dickson semifield [55];

(iv) $c(bx^{p^s+1} + (bx^{p^s+1})^{p^k}) + x^{p^k+1}$, defined over $\mathbb{F}_{p^{2k}}$, with $b \in \mathbb{F}^{\star}_{p^{2k}}$ not a square, $c \in \mathbb{F}_{p^{2k}} \setminus \mathbb{F}_{p^k}$, $\gcd(k+s,2k) = \gcd(k+s,k)$ (for any such b different choices of c lead to equivalent planar functions), it corresponds to Budaghyan-Helleseth (BH) semifield [9, 33];

(v) $\big((a^{p^k}x + x^{p^k}a) + \alpha(b^{p^k}y + y^{p^k}b)^{\sigma}, ay + bx\big)$, defined over $\mathbb{F}^2_{p^m}$, with $a,b \in \mathbb{F}_{p^m}$, $\alpha \in \mathbb{F}_{p^m}$ non-square, $\frac{n}{\gcd(n,k)}$ odd and $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^m})$, it corresponds to the Zhou-Pott (ZP) semifield [112];

(vi) $x^{p^s+1} - a^{p^t+1}x^{p^t+p^{2t+s}}$, defined over $\mathbb{F}_{p^{3t}}$, with a primitive element in $\mathbb{F}_{p^{3t}}$, $\gcd(t,3) = 1$, $t - s \equiv 0 \mod 3$ and $3t/\gcd(s,3t)$ odd, it corresponds to Zha-Kyureghyan-Wang (ZKW) semifield [111];

(vii) $x^{p^s+1} - a^{p^t-1}x^{p^{3t}+p^{t+s}}$, defined over $\mathbb{F}_{p^{4t}}$, with a primitive element in $\mathbb{F}_{p^{4t}}$, $p^s \equiv p^t \equiv 1 \mod 4$, $2t/\gcd(2t,s)$ odd, it corresponds to Bierbrauer semifield [8];

For $p = 3$, there are:

(viii) $L(t^2(x)) + D(t(x)) + \frac{1}{2}x^2$, defined over $\mathbb{F}_{3^{2k}}$ for $k = er$ odd, with $t(x) = x^{3^k} - x$, $\alpha = t(\beta)$ for $\beta \in \mathbb{F}_{3^{2k}} \setminus \mathbb{F}_{3^k}$, $L(x) = \alpha^{-5}x^3 + x$ and $D(x) = -\alpha^{-10}x^{10}$, it corresponds to the Ganley semifield [69];

(ix) $L(t^2(x)) + \frac{1}{2}x^2$, defined over $\mathbb{F}_{3^{2k}}$ for $k = er$, with $t(x) = x^{3^k} - x$, $\alpha = t(\beta)$ for $\beta \in \mathbb{F}_{3^{2k}} \setminus \mathbb{F}_{3^k}$ and $L(x) = -x^9 - \alpha x^3 + (1 - \alpha^4)x$, it corresponds to the Cohen-Ganley (CG) semifield [48];

(x) $x^{10} \pm x^6 - x^2$, defined over $\mathbb{F}_{3^n}$, with n odd, it corresponds to the Coulter-Matthews and Ding-Yuan semifield [51, 58].

Note that another family of planar functions is presented in [86], which corresponds to Lunardon-Marino-Polverino-Trombetti (LMPT) semifield. In [87] it is shown that the semifield is isotopic equivalent to a BH semifield and the isotopism is strong if and only if $p \equiv 1 \mod 4$.

2.4.3 Connection with APN functions

Observing the known planar DO polynomials listed above and the known families of APN maps presented in Table 2.2, we can notice some similarities in the univariate representation of some functions. For example, the BH semifield

$c(bx^{p^s+1} + (bx^{p^s+1})^{p^k}) + x^{p^k+1}$ over $\mathbb{F}_{p^{2k}}$ and the second function in the table $x^{2^{2i}+2^i} + bx^{2^m+1} + cx^{2^m(2^{2i}+2^i)}$ over $\mathbb{F}_{2^{2m}}$[7] have a similar structure.

In the last decades, families of planar maps have been constructed by extension of known classes of quadratic APN families. This was firstly done with the BH semifield in 2008 [33]. This approach has been very useful since, after the work of Dickson in 1906 [55] and Albert in 1952 [1], these were the firstly found infinite families of commutative semifields defined for all odd primes p. Hence, new classes of APN functions over fields of even characteristic can serve as a source for further constructions of planar mappings (and semifields) over fields of odd characteristic.

The same has been done in the other direction. Zhou and Pott in [112] constructed a new family of semifields, and thus planar functions, then they extended the construction over fields of even characteristic, obtaining a new APN family. Therefore, new classes of planar functions over fields of odd characteristic may serve as a source for further construction of APN mappings over fields of even characteristic.

[7] Note furthermore that this function is EA-equivalent to a function of the form $dx^{2^i+1} + (dx^{2^i+1})^{2^m} + cx^{2^m+1}$, verified in Chapter 6.

Chapter 3

On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2

In this chapter we consider quadratic APN functions $F \in \mathbb{F}_{2^n}[x]$ of the form

$$F(x) = L_1(x^3) + L_2(x^9), \tag{3.1}$$

with L_1 and L_2 linear maps. These functions were introduced and studied by Budaghyan, Carlet and Leander in [30, 31], where they derived several infinite families of APN functions of this particular form. However, this study was not complete. In particular, these infinite families did not cover all possible APN maps defined by (3.1). Below we present further investigations of such functions.

In Section 3.1 we recall the results of [30, 31]. In Section 3.2 we present new necessary and sufficient conditions for these functions to be APN. We focus on functions of the form $x^9 + L_1(x^3)$ and, using the software MAGMA, we analyse some specific cases in small dimensions. Then we compare the obtained functions with the already known ones. Thanks to the conditions derived, it was possible for example to check computationally that the (n,n)-function $x^9 + \mathrm{Tr}(x^3)$, for $3 \leq n \leq 200$, is APN only if $n = 4, 5, 8$. In addition, we give some specific constructions for APN maps. In Subsection 3.2.3 we give some observations on the nonlinearity of the components for quadratic APN functions of the type (3.1). In particular, we show that their extended Walsh spectrum contains at most 5 values. In Section 3.3 we verify that, among the known APN functions, many have the form (3.1).

3.1 Some known results

Some results on the APN properties of F, defined by (3.1), have already been given in different papers by Budaghyan, Carlet and Leander. In [30] the function $x^3 + \mathrm{Tr}(x^9)$ is proved to be APN for any dimension n. Moreover, for $n \geq 7$ it is proved to be CCZ-inequivalent to the Gold functions, to the inverse and Dobbertin functions and EA-inequivalent to power functions. For a quadratic APN function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and a quadratic Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, under some conditions it is proved that the function[1] $F + f$ is APN [30, Theorem 1]. A similar theorem (Theorem 2 in [30]) is proved when $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, where m is a divisor of n. Due to this result the following functions, defined over $\mathbb{F}_{2^{2m}}$ where m is an even positive integer, are APN[2]

- $x^3 + \mathrm{Tr}^m(x^{2^m+2}) = x^3 + x^{2^m+2} + x^{2^{m+1}+1}$,
- $x^3 + (\mathrm{Tr}^m(x))^3$.

These functions resulted to be EA-equivalent to $x^{2^{m-1}+1}$. When F is a Gold function, all possible APN mappings $F + f$, where f is a Boolean function, are computed until dimension 15. The only possibilities, different from $x^3 + \mathrm{Tr}(x^9)$, are for $n = 5$ the function $x^5 + \mathrm{Tr}(x^3)$ (CCZ-equivalent to Gold functions) and for $n = 8$ the function $x^9 + \mathrm{Tr}(x^3)$ (CCZ-inequivalent to power functions and to $x^3 + \mathrm{Tr}(x^9)$).

Later, in [31] functions of a more general form (3.1) were studied. It was proven that for n even a sufficient condition for F as in (3.1) to be APN is $L_1(x) + L_2(x^3)$ being a permutation over $\mathbb{F}_{2^n}$ (see Proposition 2 in [31]). In odd dimensions, a similar but more complicated condition was obtained, see [31, Proposition 3]. In [31, Corollary 2] it is stated that for n even, L a linear function over $\mathbb{F}_{2^n}$, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ if $x + L(x^3)$ is a permutation over $\mathbb{F}_{2^n}$, then the function $ax^3 + L(a^3x^9 + a^2bx^6 + ab^2x^3)$ is APN over $\mathbb{F}_{2^n}$. This result gives new examples of APN functions in even dimensions. The following infinite families of functions are proved to be APN also in odd dimensions [31, Corollary 4]:

1. $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$, with $a \in \mathbb{F}_{2^n}^*$ and any positive n;

[1] From Remark 2.2 we know that f admits a univariate representation as a polynomial over $\mathbb{F}_{2^n}$.

[2] Since $\mathbb{F}_{2^m} \subseteq \mathbb{F}_{2^n}$, for m a positive divisor of n, then every element $u \in \mathbb{F}_{2^m}$ can be seen as an element in $\mathbb{F}_{2^n}$ and the sum $v + u$ is well defined for every $v \in \mathbb{F}_{2^n}$.

2. $x^3 + a^{-1}\mathrm{Tr}^3(a^6x^{18} + a^{12}x^{36})$, with $a \in \mathbb{F}_{2^n}^*$ and n divisible by 3;

3. $x^3 + a^{-1}\mathrm{Tr}^3(a^3x^9 + a^6x^{18})$, with $a \in \mathbb{F}_{2^n}^*$ and n divisible by 3.

The above mentioned function $F(x) = x^9 + \mathrm{Tr}(x^3)$ over $\mathbb{F}_{2^8}$, for which the map $x^3 + \mathrm{Tr}(x)$ is not a permutation, leads us to the acknowledgement that Proposition 2 in [31] does not describe completely the APN functions of the form (3.1). This motivated us for further study of the APN property for functions of this form.

3.2 APN conditions

Let us recall the function defined by (3.1),

$$F(x) = F'(x^3) = L_1(x^3) + L_2(x^9).$$

We refer to L_1 and L_2 as to the linear functions

$$L_1(x) = \sum_{i=0}^{n-1} b_i x^{2^i} \text{ and } L_2(x) = \sum_{i=0}^{n-1} c_i x^{2^i}, \tag{3.2}$$

with $b_i, c_i \in \mathbb{F}_{2^n}$. We want to study conditions on L_1 and L_2 such that F is APN.

3.2.1 Necessary and sufficient conditions

We introduce here some conditions for the APN property of F as in (3.1). These conditions are rather helpful for checking more efficiently that some functions of this form are not APN.

By analysing the APN property for a quadratic function we can state the following theorem.

Theorem 3.1. *For any positive integer n and any linear functions L_1 and L_2 over $\mathbb{F}_{2^n}$, a function F defined by (3.1) is APN if and only if for every $a \in \mathbb{F}_{2^n}^*$ one of the following equivalent conditions is satisfied:*

1. *for all $x \neq 0, 1$*
$$L_1(a^3(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0; \tag{3.3}$$

2. *for all $y \neq 0$ such that $\mathrm{Tr}(y) = 0$*
$$L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \neq 0. \tag{3.4}$$

Proof. Since F is a quadratic function satisfying $F(0)=0$, the APN condition can be reformulated as the following:
for any $a \in \mathbb{F}_{2^n}^*$

$$F(ax+a)+F(ax)+F(a)=0 \text{ if and only if } x \in \{0,1\}.$$

The equation above is equivalent to $L_1(a^3(x^2+x))+L_2(a^9(x^8+x))=0$, therefore we have that

$$L_1(a^3(x^2+x))+L_2(a^9(x^8+x)) \neq 0 \text{ if and only if } x \neq 0,1.$$

Let us denote now $y=x^2+x$. Since $x \neq 0,1$ we have that $y \neq 0$ and $\mathrm{Tr}(y)=0$. The second condition follows easily. □

The following propositions are necessary conditions, for the APN property, derived from the previous theorem.

Proposition 3.1. *Let F, defined as in (3.1), be APN and, referring to (3.2), construct the linear function $L_3(x)=\sum_{i=0}^{n-1} d_i x^{2^i}$ with coefficients*

$$\begin{aligned} d_0 &= b_0+b_{n-1}+c_0+c_{n-3},\\ d_1 &= b_1+b_0+c_1+c_{n-2},\\ d_2 &= b_2+b_1+c_2+c_{n-1},\\ d_i &= b_i+b_{i-1}+c_i+c_{i-3}, \quad \text{for } 3 \leq i \leq n-1. \end{aligned}$$

Then L_3 is a 2-to-1 map satisfying $L_3(x)=0$ if and only if $x=0,1$.

Proof. Using equation (3.3) with $a=1$, consider the following map: $L_1(x^2+x)+L_2(x^8+x)$. Analysing the two linear functions we have:

$$\begin{aligned} L_1(x^2+x) =& (b_0+b_{n-1})x+\sum_{i=1}^{n-1}(b_i+b_{i-1})x^{2^i},\\ L_2(x^8+x) =& (c_0+c_{n-3})x+(c_1+c_{n-2})x^2+(c_2+c_{n-1})x^{2^2}+\sum_{i=3}^{n-1}(c_i+c_{i-3})x^{2^i}. \end{aligned}$$

Therefore $L_1(x^2+x)+L_2(x^8+x)$ corresponds to the linear function $L_3(x)$ described above. From Lemma 3.1 we have that $L_3(x)=0$ if and only if $x=0,1$. □

Proposition 3.2. *For n even assume that F, defined by (3.1), is APN. Let $\zeta \in \mathbb{F}_{2^n}^*$ be a primitive element and $k=\frac{2^n-1}{3}$. Then $F(a) \neq 0$ for any $a \neq 0$ or equivalently $F'(\zeta^{3j})=F(\zeta^j) \neq 0$ for $0 \leq j \leq k-1$.*

Proof. For n even we have $\mathrm{Tr}(1) = 0$. Therefore using equation (3.4) with $y = 1$ we get for any $a \neq 0$

$$L_1(a^3) + L_2(a^9) = F'(a^3) = F(a) \neq 0.$$

For $a \neq 0$ we have that $a = \zeta^j$ with $0 \leq j \leq 2^n - 2$. Since we consider just cubic power of a, we can restrict the possibilities to $0 \leq j \leq k - 1$. This concludes the proof. □

Remark 3.1. *If we consider $j = 0$ in Proposition 3.2 then*

$$L_1(1) + L_2(1) = \sum_{i=0}^{n-1} b_i + \sum_{i=0}^{n-1} c_i = \sum_{i=0}^{n-1} (b_i + c_i) \neq 0.$$

Moreover, if we just consider linear functions with coefficients in $\mathbb{F}_2$ ($b_i, c_i \in \mathbb{F}_2$) then a fast way to check if F is not APN is by verifying that L_1 and L_2 have the same parity number of monomials.

Proposition 3.3. *Let n be an even number multiple of 3 and F defined by (3.1) be APN. Then for any $a \neq 0$ $L_1(a^3\beta) \neq 0$, with $\beta \in \mathbb{F}_{2^3}^*$ such that $\mathrm{Tr}_3(\beta) = 0$.*

Proof. Consider such an element β and call m the integer $\frac{n}{3}$. We have that $\mathrm{Tr}_n(\beta)$ is equal to $\sum_{j=1}^{m} \sum_{i=0}^{2} \beta^{2^i} = \sum_{j=1}^{m} \mathrm{Tr}_3(\beta) = 0$. Therefore we can apply (3.4) with $y = \beta$ and obtain

$$L_1(a^3\beta) + L_2(a^9(\beta^4 + \beta^2 + \beta)) = L_1(a^3\beta) \neq 0 \text{ for any } a \neq 0.$$

□

The following theorem gives another necessary and sufficient condition for the APN property of a function of the type $L_1(x^3) + L_2(x^9)$.

Theorem 3.2. *Consider a function F from $\mathbb{F}_{2^n}$ to itself defined as in (3.1). F is APN if and only if it satisfies the following condition:*

for every a, y, t with $a, y \neq 0$, $\mathrm{Tr}(y) = \mathrm{Tr}(t) = 0$ and such that $L_1(a^3y) = L_2(a^9y^3t)$ then $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$.

Proof. By Theorem 3.1 we have that the APN property for F is equivalent to

$$\forall a, y \in \mathbb{F}_{2^n}^* \text{ with } \mathrm{Tr}(y) = 0 \Rightarrow L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \neq 0.$$

First, let us assume that F is APN and consider $a, y, t \in \mathbb{F}_{2^n}$ such that $a, y \neq 0$, $\mathrm{Tr}(y) = \mathrm{Tr}(t) = 0$ and $L_1(a^3y) = L_2(a^9y^3t)$. Then we obtain $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$ since

$$\begin{aligned} 0 \neq & L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) = \\ & L_2(a^9y^3t) + L_2(a^9(y^4 + y^2 + y)) = L_2(a^9(y^4 + ty^3 + y^2 + y)). \end{aligned}$$

Assume now that the second condition of the statement is satisfied, so for every a, y, t with $a, y \neq 0$, $\mathrm{Tr}(y) = \mathrm{Tr}(t) = 0$ and such that $L_1(a^3y) = L_2(a^9y^3t)$ then $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$. Assume that F is not APN. So, there exist $a, y \neq 0$ with $\mathrm{Tr}(y) = 0$ such that $L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) = 0$. For $t = y + 1/y + 1/y^2$ we have

$$\begin{aligned} 0 &= L_1(a^3y) + L_2(a^9(y^4 + y^2 + y)) \\ &= L_1(a^3y) + L_2(a^9y^3(y + 1/y + 1/y^2)) = L_1(a^3y) + L_2(a^9y^3t). \end{aligned}$$

Hence $\mathrm{Tr}(t) = 0$ and $L_1(a^3y) = L_2(a^9y^3t)$, which leads to a contradiction:

$$0 \neq L_2(a^9(y^4 + ty^3 + y^2 + y)) = L_2(0) = 0.$$

So F is APN and this concludes the proof. □

Remark 3.2. *Note that Theorem 3.2 is also valid without the condition* $\mathrm{Tr}(t) = 0$. *However, this condition allows to restrict the set of elements t to consider.*

Lemma 3.1. *Given $n \neq 2$, every element in $\mathbb{F}_{2^n}^\star$ is the product of a cube and an element of null trace.*

Proof. Consider a general element $u \in \mathbb{F}_{2^n}^\star$. We want to show that $u = a^3y$, for some $a, y \in \mathbb{F}_{2^n}^\star$ with $\mathrm{Tr}(y) = 0$. If n is odd, then for any $y \neq 0$ with $\mathrm{Tr}(y) = 0$ there exists an element a such that $a^3 = uy^{-1}$. If n is even, consider $u = \zeta^j$ for ζ a primitive element of $\mathbb{F}_{2^n}^\star$ such that $\mathrm{Tr}(\zeta) = 0$ (from [47] we know that such primitive element always exists for $n \neq 2$). If $j \equiv 0 \mod 3$ then $a = \zeta^{j/3}$ and $y = 1$. If $j \equiv 1 \mod 3$ then $a = \zeta^{(j-1)/3}$ and $y = \zeta$. If $j \equiv 2 \mod 3$ then $a = \zeta^{(j-2)/3}$ and $y = \zeta^2$. This concludes the proof. □

Given this result, it is possible to derive a corollary from Theorem 3.2.

Corollary 3.1. *If for every $u \in \mathbb{F}_{2^n}^\star$ the equation $L_1(u) = L_2(u^3t)$ is satisfied only for t with $\mathrm{Tr}(t) = 1$, then the function $L_1(x^3) + L_2(x^9)$ is APN.*

Notice that, using Corollary 3.1, we can show in few lines that the map $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$, with $a \in \mathbb{F}_{2^n}^\star$, is APN. Indeed, for $L_1(x) = x$ and $L_2(x) = a^{-1}\mathrm{Tr}(a^3x)$, the equation $L_1(u) = L_2(u^3t)$ corresponds to $u = a^{-1}\mathrm{Tr}(a^3u^3t)$. This implies $u \in \{0, a^{-1}\}$ and, since we need to consider $u \neq 0$, for $u = a^{-1}$ we have $\mathrm{Tr}(a^3u^3t) = 1$. Therefore $\mathrm{Tr}(t) = 1$ and the map is APN.

When L_1 and L_2 are permutations

We consider now a further assumption: we assume that the linear functions L_1 and L_2, used to construct F defined by (3.1), are both permutations. As it will be shown in Section 3.3, APN functions of this form exist. Hence we want to further characterise the APN property for these maps.

Consider therefore the case $L_1(x^3) + L_2(x^9)$ with L_1 and L_2 permutations. By applying the inverse of one of the two linear L_i, F is linearly equivalent to a function of the form $x^9 + L(x^3)$ with L a linear permutation (or equivalently $x^3 + L(x^9)$).

The theorem below gives a necessary and sufficient condition on L such that $x^9 + L(x^3)$ is APN (an equivalent formulation can be given also for $x^3 + L(x^9)$).

Theorem 3.3. *Let n be an even integer and a function $F'(x) = x^3 + L(x)$ be defined over $\mathbb{F}_{2^n}$ where L is a linear permutation. The function $F'(x^3)$ is APN if and only if for any $u, x \in \mathbb{F}_{2^n}$ with $u \neq 0$, the equality $F'(ux + u) = F'(ux)$ implies that $x + x^2 \neq \frac{(y+1)^3}{y^2}$ where y is any non-zero element of null trace such that uy^{-1} is a cube.*

Proof. From Theorem 3.1 we know that APN property for $F'(x^3)$ is equivalent to:
for any $a, y \neq 0$ with $\mathrm{Tr}(y) = 0$

$$a^9(y^4 + y^2 + y) + L(a^3y) = (a^3y)^3(y + 1/y + 1/y^2) + L(a^3y) \neq 0. \tag{3.5}$$

Let assume that the second condition in the theorem is satisfied, we want to show that (3.5) holds.

Let $u = a^3y \neq 0$. As proved in Proposition 1 in [31], if for any element x, $F'(ux + u) \neq F'(ux)$ then condition (3.5) is always satisfied. Indeed $F'(ux + u) \neq F'(ux)$ implies that $L(u) \neq u^3(x^2 + x + 1)$, so $L(u) \notin \{u^3z \ s.t. \ \mathrm{Tr}(z) = 0\}$. Relation (3.5) can be written as $L(u) + u^3(y + 1/y + 1/y^2) \neq 0$ and it is satisfied since $\mathrm{Tr}(y + 1/y + 1/y^2) = 0$.
Assume therefore that there exists an element x such that $F'(ux) = F'(ux + u)$.

Hence we have that

$$\begin{aligned} 0 &= F'(ux+u)+F'(ux) \\ &= u^3(x^2+x+1)+L(u) \\ &= (a^3y)^3(x^2+x+1)+L(a^3y). \end{aligned} \tag{3.6}$$

Moreover the element x is unique (up to adding 1). Indeed, assume there is another element z such that $F'(uz)=F'(uz+u)$, then we have $u^3(z^2+z+1)+L(u)=0$. So, considering both equations, $u^3(x+z+x^2+z^2)=0$ and therefore $(x+z)=(x+z)^2$, that has solutions $z=x$ and $z=x+1$.
If we now consider (3.5) and (3.6) we want $(a^3y)(y+1/y+1/y^2+x^2+x+1)\neq 0$. Hence

$$\begin{aligned} 0 &\neq y+1/y+1/y^2+x^2+x+1 \\ &\neq \frac{y^3+y+1+y^2}{y^2}+x+x^2 \\ &\neq \frac{(y+1)^3}{y^2}+x+x^2 \end{aligned}$$

Since $uy^{-1}=a^3$ the APN condition is satisfied.

On the other side, assume $F'(x^3)$ APN and contradict the statement. Hence let assume that there exist $u,x,y\in\mathbb{F}_{2^n}$ with $u\neq 0$, $y\neq 0$, $\mathrm{Tr}(y)=0$, uy^{-1} a cube, $F'(ux+u)=F'(ux)$ and $x+x^2=\frac{(y+1)^3}{y^2}$. With $a^3=uy^{-1}$ and considering (3.5) and (3.6) we obtain a contradiction. □

3.2.2 On APN functions of the form $x^9+L(x^3)$

Consider a linear map $L(x)=\sum_{i=0}^{n-1}b_ix^{2^i}$ and a quadratic map $F(x)=x^9+L(x^3)$ defined over $\mathbb{F}_{2^n}[x]$. Then

$$\begin{aligned} F(x) &= x^9+\sum_{i=0}^{n-1}b_ix^{2^i\cdot 3}, \\ F(x^{2^{n-1}})^2 &= x^9+\sum_{i=0}^{n-1}b_i^2x^{2^i\cdot 3}=x^9+M(x^3), \end{aligned}$$

with $M(x)=\sum_{i=0}^{n-1}b_i^2x^{2^i}$. Moreover, for a primitive element $\zeta\in\mathbb{F}_{2^n}^\star$ and $N(x)=\sum_{i=0}^{n-1}b_i\zeta^{3\cdot 2^i-9}x^{2^i}$, we have

$$\zeta^{-9}F(\zeta x)=\zeta^{-9}(\zeta^9x^9+L(\zeta^3x^3))=x^9+\sum_{i=0}^{n-1}b_i\zeta^{3\cdot 2^i-9}x^{3\cdot 2^i}=x^9+N(x^3).$$

By applying these two linear equivalence transformations iteratively, we obtain the following proposition.

Proposition 3.4. *For a linear function* $L(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$ *over* $\mathbb{F}_{2^n}$*, the map* $x^9 + L(x^3)$ *is linear equivalent to* $x^9 + M(x^3)$ *where* $M(x) = \sum_{i=0}^{n-1} (b_i \zeta^{k(3\cdot 2^i - 9)})^{2^t} x^{2^i}$ *for any* k, t *integers.*

This result allows us to perform a restriction over one coefficient of the linear function L. Consider therefore an integer j with $0 \leq j \leq n-1$, without loss of generality, up to linear equivalence, we can consider a linear function L with coefficient $b_j = 0$ or $b_j = \zeta^k$, with $0 \leq k < |3 \cdot 2^j - 9|$ and k either 0 or odd[3]. Note that a similar result can be obtained when considering the quadratic function $x^3 + L(x^9)$.

From [30] we know that in $\mathbb{F}_{2^8}$ the function $F(x) = x^9 + \mathrm{Tr}(x^3)$ is APN. Below we give a nonexistence result for APN functions of this type for n divisible by 3.

Proposition 3.5. *If* $3|n$ *then the function* $x^9 + \mathrm{Tr}(x^3)$ *is not APN over* $\mathbb{F}_{2^n}$*.*

Proof. From Theorem 3.1 we have that $x^9 + \mathrm{Tr}(x^3)$ is APN if and only if for any $a \neq 0$ and any $x \neq 0, 1$

$$\mathrm{Tr}(a^3(x^2 + x)) + a^9(x^8 + x) \neq 0.$$

If we now consider n multiple of 3, $x \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$ and $a = 1$ we obtain

$$\mathrm{Tr}(a^3(x^2 + x)) + a^9(x^8 + x) = 0.$$

□

Using Theorem 3.2 we implemented, using the software MAGMA, an algorithm that checks a necessary condition for the APN property of $x^9 + \mathrm{Tr}(x^3)$ over $\mathbb{F}_{2^n}$. Specifically, Theorem 3.2 states that $x^9 + \mathrm{Tr}(x^3)$ is APN if and only if for any $a, y \neq 0$, with $\mathrm{Tr}(y) = 0$ and such that $\mathrm{Tr}(t) = 0$, for $t = \frac{\mathrm{Tr}(a^3 y)}{a^9 y^3}$, then $y^4 + y^2 + y + \frac{\mathrm{Tr}(a^3 y)}{a^9} \neq 0$. The algorithm considers the cases $\mathrm{Tr}(a^3 y) = 1$, so with $t = \frac{1}{a^9 y^3}$. It verifies that the hypothesis is satisfied, that is $\mathrm{Tr}(y) = 0$ and $\mathrm{Tr}(t) = 0$, and that the thesis is not, hence $y^4 + ty^3 + y^2 + y = 0$. See in the following the pseudo-code for the algorithm[4].

[3] If we take $j = 1$ then we need to consider only the cases $b_1 = 0$, $b_1 = 1$ and $b_1 = \zeta$.

[4] Note that the function f, for which we need to obtain the roots, is a linear map.

for $a \in \mathbb{F}_{2^n}^\star$ **do**
  $f := y^4 + y^2 + y + a^{-9} \in \mathbb{F}_{2^n}[y]$;
  for $\bar{y} \in Roots(f)$ **do**
    if $\mathrm{Tr}(\bar{y}) = \mathrm{Tr}(a^{-9}\bar{y}^{-3}) = 0$ *and* $\mathrm{Tr}(a^3\bar{y}) = 1$ **then**
      return: f not APN;
    end
  end
end
return: f might be APN;

Algorithm 1: Pseudo-code for checking if $x^9 + \mathrm{Tr}(x^3)$ cannot be APN over $\mathbb{F}_{2^n}$

Running the algorithm for n up to 200 the only dimensions for which the necessary APN condition is satisfied are $n = 4,5,8$. In these dimensions the map $x^9 + \mathrm{Tr}(x^3)$ is APN. For $n = 4$ the map is CCZ-equivalent to the Gold function x^3 (equivalent to x^9). For $n = 5$ the map is CCZ-equivalent to the Gold function x^3. For $n = 8$ the map is not CCZ-equivalent to any function belonging to a known family of APN functions.

Let us consider now a more general form for F, $F(x) = x^9 + L(x^3)$ with L a linear function over $\mathbb{F}_{2^n}$. With some computational work, done with MAGMA, we search for more APN functions of this form in other dimensions.

Over $\mathbb{F}_{2^n}$, for $n = 4,\ldots,10$, we consider all functions of the form $x^9 + L(x^3)$, with one of the coefficients of L restricted using Proposition 3.4. We select those which are APN and divide them into CCZ-equivalence classes. A representative function for each class is shown in Table 3.1. Obviously for every n not multiple of 3, the Gold function x^9 (corresponding to the case $L = 0$) is APN.

For $n = 6$ we get:

- for $L(x) = \zeta^{44}x + \zeta x^2$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \zeta^{-1}\mathrm{Tr}(\zeta^3 x^9)$;
- for $L(x) = \zeta^{23}x + x^{2^2}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to x^3.

Both of these functions belong to the class of APN functions studied in [31], since in $\mathbb{F}_{2^6}$ $\mathrm{Tr}(x^9) = 0$, hence $x^3 = x^3 + \mathrm{Tr}(x^9)$.
For $n = 8$ we compare the found APN mappings with the list of APN functions in dimension 8 in Table 2.5. We get the following:

- for $L(x) = x^2 + x^{2^4}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to $x^3 + \mathrm{Tr}(x^9)$;

Table 3.1: APN functions (up to CCZ-equivalence) of the form $x^9 + L(x^3)$ over $\mathbb{F}_{2^n}$

n	CCZ-eq	Representatives
4	1	$L(x) = 0$
5	2	$L(x) = 0$, $L(x) = \mathrm{Tr}(x)$
6	2	$L(x) = \zeta^{44}x + \zeta x^2$, $L(x) = \zeta^{23}x + x^{2^2}$
7	1	$L(x) = 0$
8	8	$L(x) = 0$, $L(x) = x^2 + x^{2^4}$, $L(x) = x^{2^3} + x^{2^7}$, $L(x) = \mathrm{Tr}(x)$, $L(x) = x^{2^2} + \zeta^{85}x^{2^3} + x^{2^4}$, $L(x) = \zeta^{60}x + \zeta^{200}x^2 + \zeta^{242}x^{2^2} + \zeta^{190}x^{2^3} + \zeta x^{2^4}$, $L(x) = \zeta^{189}x + \zeta^{137}x^2 + \zeta^{80}x^{2^3} + \zeta^{107}x^{2^5} + \zeta^{228}x^{2^6}$, $L(x) = \zeta^{146}x^2 + \zeta^{194}x^{2^2} + \zeta^{25}x^{2^7}$
9	0	-
10	2	$L(x) = 0$, $L(x) = \zeta^{1021}x + \zeta^{1022}x^2 + \zeta x^{2^2}$

- for $L(x) = x^{2^3} + x^{2^7}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to x^3;
- for $L(x) = x^{2^2} + \zeta^{85}x^{2^3} + x^{2^4}$ the function $x^9 + L(x^3)$ is not CCZ-equivalent to any function of the form $x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ but it is CCZ-equivalent to function 1.12 in Table 2.5;
- for $L(x) = \zeta^{60}x + \zeta^{200}x^2 + \zeta^{242}x^4 + \zeta^{190}x^8 + \zeta x^{16}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to function 1.6 in Table 2.5;
- for $L(x) = \zeta^{189}x + \zeta^{137}x^2 + \zeta^{80}x^8 + \zeta^{107}x^{32} + \zeta^{228}x^{64}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to function no. 1.3 in Table 2.5;
- for $L(x) = \zeta^{146}x^2 + \zeta^{194}x^4 + \zeta^{25}x^{128}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to function no. 3.1 in Table 2.5.

For $n = 10$, with $L(x) = \zeta^{1021}x + \zeta^{1022}x^2 + \zeta x^{2^2}$ the function $x^9 + L(x^3)$ is CCZ-equivalent to x^3.

Remark 3.3. *The obtained computational results show us that, for $4 \leq n \leq 10$, all APN functions of the form $x^9 + L(x^3)$, with $L \in \mathbb{F}_{2^n}[x]$ linear, are CCZ-equivalent to some already known APN functions.*

For higher dimensions, we restrict the linear functions L to having coefficients in $\mathbb{F}_2$. So, for $11 \leq n \leq 16$, we consider all functions of the form $x^9 + L(x^3)$ with $L \in \mathbb{F}_2[x]$ linear. Among these, the only APN maps are the ones constructed with $L(x) = 0$ over $\mathbb{F}_{2^n}$ with n not multiple of 3.

Analysing the obtained results we are able to construct a family of APN functions defined for any n even:

$$\text{the function } F(x) = x^9 + L(x^3) \text{ with } L(x) = \zeta x^4 + \zeta^{-1}x^2 + \zeta^{-2}x,$$

where $\zeta \in \mathbb{F}_{2^n}^*$ is a primitive element, is APN over $\mathbb{F}_{2^n}$ for every n even.

It is possible to generalise this family as follows.

Proposition 3.6. *In $\mathbb{F}_{2^n}$ for n even the function*

$$x^9 + L(x^3) \text{ with } L(x) = \gamma x^4 + \gamma^{-1}x^2 + \gamma^{-2}x$$

is APN for any $\gamma \in \mathbb{F}_{2^n}^*$ not a cube. Moreover the obtained function is linearly equivalent to the Gold function x^3.

In order to prove it we need the following remark.

Remark 3.4. *If n is even and γ is a non-cube element in $\mathbb{F}_{2^n}$, then for every non-zero element b of the finite field we have $b^3\gamma \neq 1$. It trivially follows from the fact that $3|(2^n - 1)$ when n is even.*

Proof of Proposition 3.6. The obtained function $F(x) = x^9 + L(x^3)$ is

$$\begin{aligned} F(x) &= x^9 + \gamma x^{12} + \gamma^{-1}x^6 + \gamma^{-2}x^3 \\ &= \gamma^{-2}x^3[\gamma^3x^9 + \gamma^2x^6 + \gamma x^3 + 1] = \gamma^{-2}x^3[\gamma x^3 + 1]^3 \\ &= \gamma^{-2}[x(\gamma x^3 + 1)]^3 = \gamma^{-2}(\gamma x^4 + x)^3. \end{aligned}$$

If γ is not a cube then $\gamma x^4 + x$ is a linear permutation, since $\gamma x^3 \neq 1$. Hence the function F is equivalent to x^3 and so it is APN. □

Consider now the more general case $F(x) = x^{2^{3i}+1} + L(x^{2^i+1})$ with

$$L(x) = \gamma x^{2^{2i}} + \gamma^{1-2^i}x^{2^i} + \gamma^{-2^i}x \text{ and } \gamma \neq 0.$$

We have

$$\begin{aligned} F(x) =& x^{2^{3i}+1} + \gamma x^{2^{3i}+2^{2i}} + \gamma^{1-2^i}x^{2^{2i}+2^i} + \gamma^{-2^i}x^{2^i+1} = \\ =& \gamma^{-2^i}(x + \gamma x^{2^{2i}})(x^{2^i} + \gamma^{2^i}x^{2^{3i}}) = \gamma^{-2^i}(x + \gamma x^{2^{2i}})^{2^i+1}. \end{aligned}$$

Now, the linear function $x + \gamma x^{2^{2i}}$ is a permutation if $\gamma x^{2^{2i}-1} \neq 1$. Since $3 \mid (2^{2i} - 1)$ the condition that γ is not a cube is a sufficient condition for n even. Therefore the obtained function is linear equivalent to x^{2^i+1} that is APN if $\gcd(i,n) = 1$ (corresponding to a Gold function).
Therefore we can state the following:

Proposition 3.7. *Over $\mathbb{F}_{2^n}$, with n even, consider the function*

$$F(x) = x^{2^{3i}+1} + L(x^{2^i+1}) \text{ with}$$

$$L(x) = \gamma x^{2^{2i}} + \gamma^{1-2^i} x^{2^i} + \gamma^{-2^i} x \text{ and } \gamma \neq 0.$$

Then the function F is APN for every γ not a cube and every i coprime with n. In these cases the function is linearly equivalent to the Gold function x^{2^i+1}.

3.2.3 On the components with constant derivative and the Walsh spectrum

From [6] we get the following theorem.

Theorem 3.4. *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Then for any non-zero $a \in \mathbb{F}_{2^n}$*

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) \geq 2^{2n+1}.$$

Moreover, F is APN if and only if for every non-zero $a \in \mathbb{F}_{2^n}$

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n+1}.$$

For an (n,n)-function F and $a, \lambda \in \mathbb{F}_{2^n}$, consider the sets

$$\Lambda_a = \{\lambda \in \mathbb{F}_{2^n} \; s.t. \; D_a f_\lambda \text{ is constant}\}, \tag{3.7}$$

$$\mathcal{LS}(f_\lambda) = \{a \in \mathbb{F}_{2^n} \; s.t. \; D_a f_\lambda \text{ is constant}\}. \tag{3.8}$$

The set $\mathcal{LS}(f_\lambda)$ is often called the *linear space* of f_λ. Consider now a quadratic function $F \in \mathbb{F}_{2^n}[x]$. Every component of F has at most algebraic degree 2 and, consequently, the Boolean function $D_a f_\lambda$ can be either affine or constant. If $D_a f_\lambda$ is affine then $\mathcal{F}(D_a f_\lambda) = 0$. In the other case we have $\mathcal{F}(D_a f_\lambda) = \pm 2^n$ and $\mathcal{F}^2(D_a f_\lambda) = 2^{2n}$. Therefore

$$\sum_{\lambda \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\lambda) = 2^{2n} \cdot |\Lambda_a|.$$

From the previous theorem we have that F is APN if and only if the sum is equal to 2^{2n+1}, hence if and only if $|\Lambda_a| = 2$ for any non-zero a. Clearly we have always $0 \in \Lambda_a$, so $|\Lambda_a^\star| = 1$.

Equivalently, we have that F is APN if and only if for any two distinct elements λ_1, λ_2 in $\mathbb{F}_{2^n}^\star$,

$$\mathcal{LS}(f_{\lambda_1})^\star \cap \mathcal{LS}(f_{\lambda_2})^\star = \emptyset \text{ and } \sum_{\lambda \neq 0} |\mathcal{LS}(f_\lambda)^\star| = 2^n - 1.$$

According to Proposition 1 in [38] we have that the dimension of the kernel K of f_λ and n have the same parity, where the *kernel of a quadratic form* f is the subspace of $\mathbb{F}_{2^n}$ $\{u \in \mathbb{F}_{2^n} \; s.t. \; f(u+v) + f(u) + f(v) = 0 \text{ for any } v \in \mathbb{F}_{2^n}\}$. From Lemma 1 in [38] we know also that K corresponds to the subspace $\mathcal{LS}(f_\lambda)$. Therefore we have $\dim_{\mathbb{F}_2}(\mathcal{LS}(f_\lambda)) \equiv n \bmod 2$.

Consider now, for $0 \leq i \leq n$, the set

$$\Omega_i = \{\lambda \neq 0 \; s.t. \; \dim(\mathcal{LS}(f_\lambda)) = i\}.$$

If Ω_i is not empty then i has the same parity as n. It can be easily proved by considering a non-zero element λ in the set, i.e. such that $\dim(\mathcal{LS}(f_\lambda)) = i$. Since the dimension of $\mathcal{LS}(f_\lambda)$ has the same parity as n, the same can be stated on i.

The set Ω_0 corresponds to the set of all bent components. It is well known that, for n even, a quadratic APN function has at least $\frac{2(2^n-1)}{3}$ bent components, see for example [93].

Hence, for a quadratic APN function F defined over even dimension, the following relations are satisfied.

$$2^n - 1 = \sum_{j=0}^{n/2} |\Omega_{2j}|,$$

$$2^n - 1 = \sum_{\lambda \neq 0} |\mathcal{LS}(f_\lambda)^\star| = \sum_{j=0}^{n/2} (2^{2j} - 1)|\Omega_{2j}| = \sum_{j=1}^{n/2} (2^{2j} - 1)|\Omega_{2j}|.$$

Hence

$$|\Omega_2| = \frac{2^n - 1}{3} - \sum_{j=2}^{n/2} \frac{(2^{2j} - 1)}{3} |\Omega_{2j}|,$$

$$|\Omega_0| = 2\frac{2^n - 1}{3} + \sum_{j=2}^{n/2} \frac{(2^{2j} - 4)}{3} |\Omega_{2j}|.$$

Therefore F has exactly $\frac{2(2^n-1)}{3}$ bent components if and only if for any $\lambda \in \mathbb{F}_{2^n}^\star$ $\dim(\mathcal{LS}(f_\lambda)) \leq 2$. The result just stated is a particular case of Corollary 3 in [6].

Let us apply now what we have obtained so far to functions of the form $F(x) = L_1(x^3) + L_2(x^9)$, with L_1 and L_2 as in (3.2).

Proposition 3.8. *$F(x) = L_1(x^3) + L_2(x^9)$ is an APN function if and only if for any $a \in \mathbb{F}_{2^n}^*$ there exists one and only one $\lambda \in \mathbb{F}_{2^n}^*$ such that*

$$\mathrm{Tr}(\lambda L_1(ax^2 + a^2x) + \lambda L_2(ax^8 + a^8x)) \equiv 0 \tag{3.9}$$

Proof. Considering a component of the derivative function, we have the following formulation

$$\begin{aligned} D_a f_\lambda(x) &= \mathrm{Tr}(\lambda[F(x) + F(x+a)]) \\ &= \mathrm{Tr}(\lambda[L_1(ax^2 + a^2x + a^3) + L_2(ax^8 + a^8x + a^9)]) \\ &= \mathrm{Tr}(\lambda[L_1(ax^2 + a^2x) + L_2(ax^8 + a^8x)]) + \mathrm{Tr}(\lambda[L_1(a^3) + L_2(a^9)]). \end{aligned}$$

In order to determine whether it is constant, it is sufficient to study the function $g(x) = \mathrm{Tr}(\lambda[L_1(ax^2 + a^2x) + L_2(ax^8 + a^8x)])$. Since $g(0) = 0$, we have that if g is constant then it is the constant zero function and this concludes the proof. □

Remark 3.5. *Equivalently, we can study the conditions for $\mathrm{Tr}(\lambda L_1(a^3[x^2 + x]) + \lambda L_2(a^9[x^8 + x]))$ to be the constant zero function. Due to the property of the trace function we can study the conditions for $\lambda L_1(a^3[x^2 + x]) + \lambda L_2(a^9[x^8 + x])$ to be equal to $\eta + \eta^2$, with $\eta = \eta(a, \lambda, x)$.*

From Proposition 3.8, we can obtain some observations on the possible dimensions of $\mathcal{LS}(f_\lambda)$. We recall that the dimension of $\mathcal{LS}(f_\lambda)$ is linked to the nonlinearity of f_λ. Indeed, since f_λ is a quadratic map, $\mathcal{NL}(f_\lambda) = 2^{n-1} - 2^{\frac{n+k}{2}-1}$ where $k = \dim(\mathcal{LS}(f_\lambda))$[5]. Recall also that, in odd dimensions, all quadratic APN functions are AB. This implies that for a quadratic APN map F in odd dimension $\dim(\mathcal{LS}(f_\lambda)) = 1$ for every $\lambda \neq 0$.

Let L_1^* and L_2^* be the adjoint operators[6] of L_1 and L_2 respectively. Set

$$\beta_\lambda = L_1^*(\lambda) \text{ and } \gamma_\lambda = L_2^*(\lambda), \tag{3.10}$$

[5]For every Boolean function f, $\mathcal{F}(f)^2 = \sum_{b \in \mathbb{F}_{2^n}} \mathcal{F}(D_b f)$ (see [40]) and, when f is plateaued, $\mathcal{W}_f(u) \in \{0, \pm\nu\}$ for any $u \in \mathbb{F}_{2^n}$. So, $\mathcal{W}_{f_\lambda}(0) = \mathcal{F}(f_\lambda) = 2^{\frac{n+k}{2}}$ and $\max_{u \in \mathbb{F}_{2^n}} |\mathcal{W}_{f_\lambda}(u)| = 2^{\frac{n+k}{2}}$.

[6]Given a linear map L over $\mathbb{F}_{2^n}$, the *adjoint operator* of L is the linear map $L^\star$ satisfying $\mathrm{Tr}(xL(y)) = \mathrm{Tr}(L^\star(x)y)$ for every $x, y \in \mathbb{F}_{2^n}$.

and expand Equation (3.9), recalling that $\mathrm{Tr}(x)=\mathrm{Tr}(x^2)$.

$$\begin{aligned}0\equiv&\mathrm{Tr}(\lambda L_1(ax^2+a^2x)+\lambda L_2(ax^8+a^8x))\\ \equiv&\mathrm{Tr}(L_1^*(\lambda)(ax^2+a^2x)+L_2^*(\lambda)(ax^8+a^8x))\\ \equiv&\mathrm{Tr}(\beta_\lambda^{2^{n-1}}a^{2^{n-1}}x+\beta_\lambda a^2x+\gamma_\lambda^{2^{n-3}}a^{2^{n-3}}x+\gamma_\lambda a^8x)\\ \equiv&\mathrm{Tr}(x\cdot[\beta_\lambda^{2^{n-1}}a^{2^{n-1}}+\beta_\lambda a^2+\gamma_\lambda^{2^{n-3}}a^{2^{n-3}}+\gamma_\lambda a^8]).\end{aligned}$$

This implies that

$$P'_\lambda(a)=\beta_\lambda a^2+\beta_\lambda^{2^{n-1}}a^{2^{n-1}}+\gamma_\lambda a^8+\gamma_\lambda^{2^{n-3}}a^{2^{n-3}}=0.$$

Let $P_\lambda=(P'_\lambda)^8$, then D_af_λ is constant if and only if a is a root of the polynomial

$$P_\lambda(x)=\gamma_\lambda^8x^{64}+\beta_\lambda^8x^{16}+\beta_\lambda^4x^4+\gamma_\lambda x=x\cdot(\gamma_\lambda^8x^{63}+\beta_\lambda^8x^{15}+\beta_\lambda^4x^3+\gamma_\lambda).$$

Therefore we have the following proposition.

Proposition 3.9. *Consider $F(x)=L_1(x^3)+L_2(x^9)$, with L_1 and L_2 as in (3.2), an APN map defined over $\mathbb{F}_{2^n}$ with n even. F has exactly $\frac{2(2^n-1)}{3}$ bent components if and only if for any $\lambda\in\mathbb{F}_{2^n}^\star$ the polynomial*

$$x\cdot(\gamma_\lambda^8x^{63}+\beta_\lambda^8x^{15}+\beta_\lambda^4x^3+\gamma_\lambda)$$

admits at most 4 roots, with β_λ and γ_λ defined by (3.10).

Assume now that there exists an element $\lambda\neq0$ s.t. $\dim(\mathcal{LS}(f_\lambda))>6$ then the polynomial P_λ has to be the zero polynomial (hence f_λ is linear). This is not possible for an APN map (see Proposition 9.15 in [42]).

Proposition 3.10. *If F as in (3.1) is APN then for any $\lambda\neq0$ $\dim(\mathcal{LS}(f_\lambda))\leq6$. In particular, for n even, we need only to consider the sets Ω_0, Ω_2, Ω_4 and Ω_6.*

Corollary 3.2. *Let n be an even integer. If F as in (3.1) is APN then its Walsh spectrum is a subset of $\{0,\pm2^{\frac{n}{2}},\pm2^{\frac{n+2}{2}},\pm2^{\frac{n+4}{2}},\pm2^{\frac{n+6}{2}}\}$.*

Notice that $\beta_\lambda=0$ implies that $\mathrm{Tr}(\lambda L_1(x))=\mathrm{Tr}(\beta_\lambda x)\equiv0$, hence the λ-component of L_1 is the null function and L_1 is not a permutation. The same applies for γ_λ and L_2. Moreover $L_1(x^3)+L_2(x^9)$ being APN implies that the two linear functions cannot have common zero components (indeed if $\beta_\lambda=\gamma_\lambda=0$ then $\mathcal{LS}(f_\lambda)=\mathbb{F}_{2^n}$). We consider now some particular cases.

- If $\gamma_\lambda=0$ ($\beta_\lambda\neq0$) then $P_\lambda(x)=x^4\beta_\lambda^4\cdot(\beta_\lambda^4x^{12}+1)=x^4\beta_\lambda^4\cdot(\beta_\lambda x^3+1)^4=0$.

  - If n is odd then $\dim(\mathcal{LS}(f_\lambda)) = 1$.
  - If n is even then $\dim(\mathcal{LS}(f_\lambda)) = 2$ if β_λ is a 3-rd power and $\dim(\mathcal{LS}(f_\lambda)) = 0$ otherwise.

- If $\beta_\lambda = 0$ ($\gamma_\lambda \neq 0$) then $P_\lambda(x) = x\gamma_\lambda \cdot (\gamma_\lambda^7 x^{63} + 1) = x\gamma_\lambda \cdot ((\gamma_\lambda x^9)^7 + 1) = 0$.
  - If $3 \nmid n$ then $7 \nmid (2^n - 1)$, implying $x\gamma_\lambda \cdot (\gamma_\lambda x^9 + 1) = 0$.
    If n is odd then $\dim(\mathcal{LS}(f_\lambda)) = 1$.
    If n is even then $\dim(\mathcal{LS}(f_\lambda)) = 2$ if γ_λ is a 3-rd power and $\dim(\mathcal{LS}(f_\lambda)) = 0$ otherwise.
  - If $3 \mid n$ then $7 \mid (2^n - 1)$.
    If n is odd then $\dim(\mathcal{LS}(f_\lambda)) = 3$ (F is not APN).
    If n is even then $9 \mid (2^n - 1)$, hence $\dim(\mathcal{LS}(f_\lambda)) = 6$ if γ_λ is a 9-th power and $\dim(\mathcal{LS}(f_\lambda)) = 0$ otherwise.

From the previous analysis, the following proposition is obtained.

Proposition 3.11. *Consider $F(x) = L_1(x^3) + L_2(x^9)$ as in (3.1) defined over $\mathbb{F}_{2^{3m}}$, with m an odd integer. If L_1 is not a permutation then F is not APN.*

Remark 3.6. *Analysing P_λ for $n = 4$ we obtain that it has at most 4 roots, hence $\dim(\mathcal{LS}(f_\lambda)) \leq 2$. This implies that all APN functions defined by (3.1) have exactly $\frac{2(2^n-1)}{3}$ bent components. This fact is already known since in dimension 4 all APN functions are EA-equivalent to the Gold function, hence with $\frac{2(2^n-1)}{3}$ bent components.*

Computational Results

Using the software MAGMA we studied, for functions F of form (3.1) defined over small dimensions, the relation between the APN property and the number of bent components. From the results obtained taking random linear functions L_1, L_2 and constructing F for $n \in \{6, 8\}$ the relation seems the following one:

Conjecture 3.1. *For an even n, a function F over $\mathbb{F}_{2^n}$ of the form (3.1) is APN if and only if it has exactly $\frac{2}{3}(2^n - 1)$ bent components.*

We know that this is not true for general quadratic functions. Indeed consider the quadratic APN function presented by Dillon in 2006 [57]

$$F(x) = x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{33} + x^{48}$$

defined over $\mathbb{F}_{2^6}$ where u is a primitive element, root of the polynomial $x^6 + x^4 + x^3 + x + 1$. This function has 46 bent components and $46 > \frac{2}{3}(2^6 - 1) = 42$. Moreover it has the following characterisation: $|\Omega_0| = 46$, $|\Omega_2| = 16$ and $|\Omega_4| = 1$.

3.3 Comparison with some lists of known APN functions

An interesting question is how often in the CCZ-classes of APN maps, there is a function of the form (3.1). To partially attack the problem, we consider the work done by Edel and Pott in [66], where the authors gave for $n = 6,7,8$ a list of some known CCZ-inequivalent APN functions, reported in Tables 2.3, 2.4 and 2.5. Hence, in the following, we check if the construction $L_1(x^3) + L_2(x^9)$ appears often in these lists.

In Table 2.3 for $\mathbb{F}_{2^6}$ there are 14 functions, 13 of which are quadratic, and the only ones in the form $L_1(x^3) + L_2(x^9)$ are:

- x^3,
- $x^3 + \zeta^{11}x^6 + \zeta x^9$, where $L_1(x) = x + \zeta^{11}x^2$ and $L_2(x) = \zeta x$.

In Table 2.4 for $\mathbb{F}_{2^7}$ there are 19 functions and the only ones in the form $L_1(x^3) + L_2(x^9)$ are:

- x^3,
- x^9,
- $x^3 + \mathrm{Tr}(x^9)$.

Analysing Table 2.5 of the 23 APN functions in $\mathbb{F}_{2^8}$, we noticed the following:

- Exactly 17 of them are of the form $L_1(x^3) + L_2(x^9)$, their corresponding positions in the list are $1.1 - 1.12, 1.14 - 1.17, 3.1$.
- Moreover, 11 of them are such that the linear function L_1 is a permutation. Their corresponding positions in the studied list are $1.1 - 1.6, 1.8 - 1.12$. Therefore there exists an affine equivalent function of the form $x^3 + L(x^9)$ where $L = L_1^{-1} \circ L_2$.

- Further, 2 of them are such that L_2 is a permutation. Therefore they are affine equivalent to functions of the form $x^9 + L(x^3)$ where $L = L_2^{-1} \circ L_1$. They are the ones in positions 1.15 and 3.1.

The linear parts of the 11 obtained functions of the form $x^3 + L(x^9)$ are listed in Table 3.2. The linear parts L_1, L_2 for the other functions $L_1(x^3) + L_2(x^9)$ are

Table 3.2: List of linear function L such that $x^3 + L(x^9)$ is APN in $\mathbb{F}_{2^8}$, from Table 2.5.

No. in Table 2.5	$L(x)$
1.1	0
1.2	$x^{128} + x^{64} + x^{32} + x^{16} + x^8 + x^4 + x^2 + x$
1.3	$\zeta^{127}x^{128} + \zeta^{64}x^{64} + \zeta^{160}x^{32} + \zeta^{208}x^{16} + \zeta^{232}x^8 + \zeta^{244}x^4 + \zeta^{250}x^2 + \zeta^{253}x$
1.4	$\zeta^{232}x^{128} + \zeta^{238}x^{64} + \zeta^{11}x^{32} + \zeta^{167}x^{16} + \zeta^{200}x^8 + \zeta^{251}x^4 + \zeta^{128}x^2 + \zeta^{65}x$
1.5	$\zeta^{221}x^{128} + \zeta^{187}x^{64} + \zeta^{119}x^{16} + \zeta^{221}x^8 + \zeta^{187}x^4 + \zeta^{119}x$
1.6	$\zeta^{110}x^{128} + \zeta^{30}x^{64} + \zeta^{140}x^{16} + \zeta^{215}x^8 + \zeta^{210}x^4 + \zeta^{185}x$
1.8	$\zeta^{136}x^{128} + \zeta^{17}x^{64} + x^{32} + \zeta^{34}x^{16} + \zeta^{136}x^8 + \zeta^{17}x^4 + x^2 + \zeta^{34}x$
1.9	$\zeta^{25}x^{128} + \zeta^{200}x^{64} + \zeta^{75}x^{32} + \zeta^{225}x^{16} + \zeta^{130}x^8 + \zeta^{125}x^4 + \zeta^{165}x^2 + \zeta^{15}x$
1.10	$\zeta^{60}x^{128} + \zeta^{226}x^{64} + \zeta^{76}x^{32} + \zeta^{34}x^{16} + \zeta^{192}x^8 + \zeta^{214}x^4 + \zeta^{251}x^2 + \zeta^{11}x$
1.11	$\zeta^{204}x^{128} + \zeta^{153}x^{64} + \zeta^{51}x^{16} + \zeta^{204}x^8 + \zeta^{153}x^4 + \zeta^{51}x$
1.12	$\zeta^{161}x^{128} + \zeta^{217}x^{64} + \zeta^{160}x^{32} + \zeta^{4}x^{16} + \zeta^{11}x^8 + \zeta^{142}x^4 + \zeta^{250}x^2 + \zeta^{49}x$

listed in Table 3.3.

Table 3.3: Remaining APN function of the form $L_1(x^3) + L_2(x^9)$ from Table 2.5

No. in Table 2.5	$L_1(x)$	$L_2(x)$
1.7	$\zeta^{143}x^{128} + \zeta^{151}x^{64} + \zeta^{110}x^{32} + \zeta^{26}x^{16}$ $+\zeta^{69}x^8 + \zeta^{201}x^4 + \zeta^{19}x^2 + \zeta^{107}x$	$\zeta^{58}x^{128} + \zeta^{244}x^{64} + \zeta^{8}x^{32} + \zeta^{13}x^{16}$ $+\zeta x^8 + \zeta^{180}x^4 + \zeta^{76}x^2 + \zeta^{201}x$
1.14	$\zeta^{106}x^{128} + \zeta^{91}x^{64} + \zeta^{59}x^{32} + \zeta^{163}x^{16}$ $+\zeta^{32}x^8 + \zeta^{45}x^4 + \zeta^{241}x^2 + \zeta^{157}x$	$\zeta^{214}x^{128} + \zeta^{138}x^{64} + \zeta^{100}x^{32} + \zeta^{124}x^{16}$ $+\zeta^{172}x^8 + \zeta^{58}x^4 + \zeta^{250}x^2$
1.15	0	x
1.16	$\zeta^{77}x^{128} + \zeta^{155}x^{64} + \zeta^{88}x^{32} + \zeta^{142}x^{16}$ $+\zeta^{145}x^8 + \zeta^{202}x^4 + \zeta^{189}x^2 + \zeta^{241}x$	$\zeta^{223}x^{128} + \zeta^{69}x^{64} + x^{32} + \zeta^{96}x^{16}$ $+\zeta^{232}x^8 + \zeta^{168}x^4 + \zeta^{234}x^2 + \zeta^{94}x$
1.17	$\zeta^{188}x^{128} + \zeta^{132}x^{64} + \zeta^{76}x^{32} + \zeta^{252}x^{16}$ $+\zeta^{83}x^8 + \zeta^{185}x^4 + \zeta^{216}x^2 + \zeta^{181}x$	$\zeta^{91}x^{128} + \zeta^{46}x^{64} + \zeta^{81}x^{32} + \zeta^{37}x^{16}$ $+\zeta^{162}x^8 + \zeta^{42}x^4 + \zeta^{13}x^2 + \zeta^{163}x$
3.1	$\zeta^{25}x^{128} + \zeta^{194}x^4 + \zeta^{146}x^{2,}$	x

To finish the analysis we add two linear functions evaluated in x^5 and x^{17}, i.e. of the form $F(x) = L_1(x^3) + L_2(x^5) + L_3(x^9) + L_4(x^{17})$ (hence we consider now a generic quadratic function over $\mathbb{F}_{2^8}$).

When L_1 is a permutation we consider $L_1^{-1} \circ F$ (1.13 and 5.1) and when L_3 is a permutation, we consider $L_3^{-1} \circ F$ (4.1 and 6.1). Hence the last quadratic functions from the list are presented in Table 3.4 written in such form.

Table 3.4: Remaining APN function of the form $L_1(x^3) + L_2(x^5) + L_3(x^9) + L_4(x^{17})$ from Table 2.5

No. in Table 2.5	$L_1(x)$	$L_2(x)$	$L_3(x)$	$L_4(x)$
1.13	x	$\zeta^6x^{128} + \zeta^{162}x^{64}$ $+\zeta^{240}x^{32} + \zeta^{24}x^{16}$ $+\zeta^{171}x^8 + \zeta^{117}x^4$ $+\zeta^{90}x^2 + \zeta^{204}x$	$\zeta^{60}x^{128} + \zeta^{226}x^{64}$ $+\zeta^{76}x^{32} + \zeta^{34}x^{16}$ $+\zeta^{192}x^8 + \zeta^{214}x^4$ $+\zeta^{251}x^2 + \zeta^{11}x$	$\zeta^{115}x^{128} + \zeta^{184}x^{64}$ $+\zeta^{87}x^{32} + \zeta^{225}x^{16}$ $+\zeta^{162}x^8 + \zeta^{241}x^4$ $+\zeta^{44}x^2 + \zeta^{105}x$
2.1	$\zeta^{15}x^{16} + x$	0	$\zeta^{16}x^{32} + \zeta^{16}x^2$	x
4.1	$x^4 + x^2$	$x^{64} + x^{32}$	x	x^8
5.1	x	$x^8 + x$	$x^{64} + x^2$	0
6.1	$x^{16} + x^4$	$x^{32} + x^2$	x	0

We further analyse some results published in [109] by Yu, Wang and Li. In the cited paper, the authors gave a matrix approach to construct quadratic APN functions. They were able to extend previous lists of CCZ-inequivalent APN functions:

- For $\mathbb{F}_{2^7}$ Edel and Pott [66] listed 19 classes of CCZ-inequivalent APN functions. Yu, Wang and Li extended it to a list of 490 classes, none of the new ones is of the form $L_1(x^3) + L_2(x^9)$.
- For $\mathbb{F}_{2^8}$, in addition to the previous list of 23 classes, the authors gave 8157 new classes, providing a new list of 8180 classes of CCZ-inequivalent APN functions. None of the new functions is of the form $L_1(x^3) + L_2(x^9)$.

Regarding to the quadratic APN functions constructed in [102] by Weng, Tan and Gong, none of the 10 APN maps for $n = 7$ and the 10 APN maps for $n = 8$ is of the form $L_1(x^3) + L_2(x^9)$.

We leave as an open question whether any of the functions listed in [109] (and in [66, 102]) is EA-equivalent to an APN map of the form $L_1(x^3) + L_2(x^9)$.

Chapter 4

Constructing APN functions through isotopic shifts

In this chapter we move to the study of isotopic equivalence with respect to APN functions in characteristic 2. In particular, we introduce a new construction method for APN functions based on isotopic equivalence. We make the following formal definition, which is the central concept considered in this chapter (and which will appear natural after we state Theorem 4.1).

Definition 4.1. *Let p be a prime and n a positive integer. Let $F, L \in \mathbb{F}_{p^n}[x]$. The* isotopic shift of F by L, *denoted by F_L, is the polynomial given by*

$$F_L(x) = \Delta_F(x, L(x)) = F(x + L(x)) - F(x) - F(L(x)). \tag{4.1}$$

In Section 4.1 we show how isotopic shifts arise naturally in the study of planar functions. This result acts as motivation for studying isotopic shifts in the parallel area of APN functions. Before narrowing our scope to APN maps, in Section 4.2 we make some general observations on isotopic shifts. We then restrict ourselves to considering isotopic shifts of APN functions. Firstly, in Section 4.3, we consider how we may obtain the same function by isotopically shifting a given APN map F in characteristic 2 by different L. Then, in Subsection 4.3.1, we begin our main study, that of isotopic shifts of quadratic APN functions by linear maps. We show that only bijective or 2-to-1 linear maps can possibly produce an APN function from the isotopic shift of a quadratic APN function. We then proceed, in Subsection 4.3.2, to concentrate specifically on isotopic shifts of Gold functions in characteristic 2. In Theorem 4.6 we present a construction for quadratic APN functions over $\mathbb{F}_{2^{km}}$ using the isotopic shift method with 2^m-polynomials. For $k = m = 3$, this construction provides an APN function which is not CCZ-equivalent to any APN function from the cur-

rently known infinite classes. For $k = 4$, $m = 2$, our construction covers the APN function $x^9 + \mathrm{Tr}(x^3)$, known since 2006 [22, 57] and which has not been part of any known family of APN functions up to now. We show that an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original one, even if we shift only Gold functions by linear monomials, see Lemma 4.1. We show that every quadratic APN function over $\mathbb{F}_{2^6}$ is EA-equivalent to an isotopic shift of any other quadratic APN function, see Proposition 4.3. Some of the aforementioned equivalence/inequivalence results, together with more computational data, are provided in Section 4.4.

4.1 Isotopic equivalence for planar quadratic functions revisited

The following result shows that the concept of isotopic shift is, in fact, a very natural concept. Recall that the isotopic shift F_L is defined in (4.1) and isotopic equivalence is defined in Section 2.4.

Theorem 4.1. *For p a prime and n a positive integer, let $F, F' \in \mathbb{F}_{p^n}[x]$ be quadratic planar functions (null at 0). If F and F' are isotopic equivalent then F' is EA-equivalent to some isotopic shift F_L of F by a linear permutation polynomial $L \in \mathbb{F}_{p^n}[x]$.*

Proof. By definition, quadratic planar functions are isotopic equivalent if the presemifields defined by them are isotopic. That is, the presemifields defined by multiplications $\star$ and $*$, with $x \star y = \Delta_{F'}(x,y)$ and $x * y = \Delta_F(x,y)$, respectively, are isotopic. Note that the linear parts of F and F' do not play a role in these operations. In the calculations below, we replace then the quadratic functions by their DO parts (that is, we erase their linear parts, without loss of generality up to EA-equivalence). Then we have $x \star x = 2F'(x)$ and $x * x = 2F(x)$. For some linear permutations $T, M, N \in \mathbb{F}_{p^n}[x]$, we get

$$T(x \star y) = M(x) * N(y),$$

for all $x, y \in \mathbb{F}_{p^n}$. Hence we have

$$\begin{aligned} T(x \star x) =& T(2F'(x)) = 2T(F'(x)) \\ =& M(x) * N(x) = \Delta_F(M(x), N(x)), \end{aligned}$$

which leads to

$$2T(F'(M^{-1}(x))) = \Delta_F(x, N(M^{-1}(x))).$$

As this holds for all $x \in \mathbb{F}_{p^n}$, we see that this is, in fact, a polynomial identity, and F' is EA-equivalent to F_L with $L = N \circ M^{-1}$, a linear permutation. □

Theorem 4.1 shows that, when considering two quadratic planar functions that are isotopic equivalent, one is always EA-equivalent to an isotopic shift of the second one by a linear permutation. This trivially comprehends the case when the two maps are CCZ-equivalent, for which $N = M$ and so $L = Id$. More interesting, it tells us that, for isotopic equivalent quadratic planar functions, what takes us beyond CCZ-equivalence is the isotopic shift by a linear permutation L. In fields of even characteristic the isotopic equivalence cannot be defined for APN functions. However, in the past years classes of APN mappings were used for constructing planar functions. For this reason we investigate whether the isotopic shift, which can lead to planar functions in fields of odd characteristic, can also construct APN maps in fields of even characteristic. For linear shifts of APN functions, we do not restrict L to being a permutation. As with planar quadratic functions, we will see that an isotopic shift of an APN map can lead to APN functions CCZ-inequivalent to the original map.

4.2 Generic results on isotopic shifts

With regards to isotopic shifts, an easy first observation is that for any $F \in \mathbb{F}_{p^n}[x]$ and any permutation $L \in \mathbb{F}_{p^n}[x]$, we have

$$F_L(L^{-1}(x)) = F_{L^{-1}}(x), \tag{4.2}$$

where L^{-1} is the compositional inverse of L. In particular, thanks to EA-equivalence, if L is a linear permutation polynomial, then F_L and $F_{L^{-1}}$ have the same differential uniformity. Along similar lines, we have the following theorem.

Theorem 4.2. *For p a prime and n a positive integer let $F, F' \in \mathbb{F}_{p^n}[x]$ be arbitrary polynomials. If F and F' are EA-equivalent, say $F = A_1 \circ F' \circ A_2 + A$, where $A_1, A_2 \in \mathbb{F}_{p^n}[x]$ are affine permutations and $A \in \mathbb{F}_{p^n}[x]$ is affine, in addition with the restriction $A_2(0) = 0$, then for $L \in \mathbb{F}_{p^n}[x]$, F_L is affine equivalent to F'_M where $M = A_2 \circ L \circ A_2^{-1}$.*

Proof. Since $F = A_1 \circ F' \circ A_2 + A$ with A_2 a linear permutation polynomial, we

have

$$\begin{aligned} F_L(x) &= \Delta_F(x, L(x)) = F(x + L(x)) - F(x) - F(L(x)) \\ &= A_1\left(F'(A_2(x) + A_2(L(x))) - F'(A_2(x)) - F'(A_2(L(x)))\right) + A(0) \\ &= A_1\left(F'(A_2(x) + M(A_2(x))) - F'(A_2(x)) - F'(M(A_2(x)))\right) + A(0), \end{aligned}$$

and with $A_3(x) = A_1(x) + A(0)$ we have $F_L = A_3 \circ F'_M \circ A_2$. □

When considering quadratic maps, we derive from Theorem 4.2 a more general result by removing the restriction on A_2.

Corollary 4.1. *If $F, F' \in \mathbb{F}_{p^n}[x]$ are EA-equivalent and quadratic, say $F(x) = A_1 \circ F' \circ A_2(x) + A(x)$, then for $L \in \mathbb{F}_{p^n}[x]$, F_L is EA-equivalent to F'_M where $M = \bar{A}_2 \circ L \circ {\bar{A}_2}^{-1}$, $\bar{A}_2(x) = A_2(x) + A_2(0)$.*

Proof. If F' is quadratic then $F' \circ A_2(x) = F'(\bar{A}_2(x)) + N(x)$, with N an affine map. Hence we have

$$F_L(x) = A_1 \circ F'_M \circ \bar{A}_2(x) + A_3(x),$$

with A_3 affine. □

We note the following observations related to the isotopic shift construction.

- For $F, L \in \mathbb{F}_{p^n}[x]$, with $\deg(L) = 1$, we have that $\deg(F_L) \leq \deg(F)$.
- For $F, L \in \mathbb{F}_{2^n}[x]$ we have that $F_L = F_{L'}$, with $L' = L + Id$.
- For F quadratic and L, M arbitrary polynomials over $\mathbb{F}_{p^n}$, we have that

$$F_L + F_M = F_{L+M}. \tag{4.3}$$

In the following sections we are mainly concerned with the case where F is a quadratic APN function and L is linear.

4.3 Isotopic shifts of APN functions

As already stated, we are mainly concerned with the case where F is an APN function and L is linear, both maps defined over $\mathbb{F}_{2^n}$. We first consider how an isotopic shift of an APN function may generate the zero polynomial. (We remind that throughout the chapter, we assume any APN function has zero constant term.)

Theorem 4.3. *Let $F \in \mathbb{F}_{2^n}[x]$ be an APN function and $L \in \mathbb{F}_{2^n}[x]$. Then F_L is the zero function if and only if $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_{2^n}^\star$. Furthermore, if L is linear, then F_L is the zero function if and only if L is either the zero polynomial or the polynomial x.*

Proof. Suppose $F_L(x) = 0$. As F is APN, we know that for all $a \in \mathbb{F}_{2^n}^\star$, $\Delta_F(x, a) = 0$ if and only if $x \in \{0, a\}$. Now $F_L(x) = \Delta_F(x, L(x))$, so that for all $a \in \mathbb{F}_{2^n}^\star$, $L(a) \in \{0, a\}$ is forced. Conversely, if $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_{2^n}^\star$, then clearly $F_L(a) = \Delta_F(a, L(a)) = 0$, while $F_L(0) = \Delta_F(0, L(0)) = 0$. Hence $F_L(x) = 0$.
Now suppose L is linear. Since $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_{2^n}$, we have $\mathbb{F}_{2^n} = \mathrm{Im}(L) \oplus \mathrm{Ker}(L)$. Suppose $0 < \dim(\mathrm{Ker}(L)) < n$. Then there exist $v \in \mathrm{Im}(L)$ (which implies $v = L(v)$) and $z \in \mathrm{Ker}(L)$ with $vz \neq 0$ and $v + z \neq 0$. Thus $v = v + 0 = L(v) + L(z) = L(v + z) \in \{0, v + z\}$, a contradiction. Hence $\mathrm{Ker}(L) = \mathbb{F}_{2^n}$ or $\mathrm{Ker}(L) = \{0\}$. In the former case, $L(x) = 0$, while in the latter case $L(x) = x$. □

Our motivation for establishing this result is not directly related to being concerned with generating the zero polynomial, but with the more practical problem of understanding how distinct L can yield the same isotopic shift of a given DO APN function.

Corollary 4.2. *Let $F \in \mathbb{F}_{2^n}[x]$ be a DO APN function and $L, M \in \mathbb{F}_{2^n}[x]$. The following statements hold.*

(i) $F_L = F_M$ if and only if $L(a) + M(a) \in \{0, a\}$ for all $a \in \mathbb{F}_{2^n}^\star$.

(ii) Suppose L, M are linear. Then $F_L = F_M$ if and only if $L = M$ or $L = M + Id$ as polynomials.

Proof. We have from (4.3) that $F_L = F_M$ if and only if $F_N(x) = 0$, where $N = L + M$. Both results now follow from Theorem 4.3. □

Notice that one implication of (ii) is directly obtained by an observation in the previous section, that is $F_L = F_{L+Id}$.

We conclude with the observation that the isotopic shift can lead to an APN function also starting from a non-APN function. So, in general, the isotopic shift does not preserve the differential uniformity.

Remark 4.1. *Consider* $\mathbb{F}_{2^6}$ *and the function* $F(x) = x^5$*, which is not APN. With* $L(x) = \zeta x^8$ *we construct the APN map*

$$F_L(x) = x^4 L(x) + xL(x)^4 = \zeta x^{12} + \zeta^4 x^{33},$$

where $F_L(x) = M(x^3)$ *for the linear permutation* $M(x) = \zeta x^4 + \zeta^4 x^{32}$*.*

4.3.1 Isotopic shifts of quadratic APN functions

In this subsection, we restrict ourselves to isotopic shifts of quadratic APN functions by linear polynomials. In the planar case, for the isotopic shift to be planar we require the linear polynomial involved to be a permutation polynomial, see Proposition 7.1 in Chapter 7. The corresponding result for the APN case is as follows.

Theorem 4.4. *Let* $F \in \mathbb{F}_{2^n}[x]$ *be a quadratic APN function and* $L \in \mathbb{F}_{2^n}[x]$ *be linear. Set* $M = L + Id$*. If* F_L *is APN, then both following statements hold.*

(i) L *is either a permutation or 2-to-1, and* L *is injective on* $\mathrm{Im}(L)$*.*

(ii) M *is either a permutation or 2-to-1, and* M *is injective on* $\mathrm{Im}(M)$*.*

Proof. We need only establish (i), as the duality spelled out in Corollary 4.2 (ii) will then imply (ii). As F is a quadratic polynomial, $\Delta_F(x,a)$ is a linear operator for all $a \in \mathbb{F}_{2^n}^\star$. Consequently, $\Delta_{F_L}(x,a)$ is also linear, and F_L being APN is equivalent to $\mathrm{Ker}(\Delta_{F_L}(x,a)) = \{0,a\}$ for all $a \in \mathbb{F}_{2^n}^\star$. Applying the linear operator identity to the difference operators involved one can show that, for any $a \in \mathbb{F}_{2^n}^\star$,

$$\Delta_{F_L}(x,a) = \Delta_F(x,L(a)) + \Delta_F(a,L(x)). \tag{4.4}$$

Suppose L is not a permutation polynomial, so that there exists some $z \in \mathrm{Ker}(L)$ with $z \neq 0$. Then $\Delta_{F_L}(x,z) = \Delta_F(z,L(x))$. Clearly, any $x \in \mathrm{Ker}(L)$ satisfies $\Delta_{F_L}(x,z) = 0$, so that $\{0,z\} \subseteq \mathrm{Ker}(L) \subseteq \mathrm{Ker}(\Delta_{F_L}(x,z)) = \{0,z\}$. Thus $\mathrm{Ker}(L) = \{0,z\}$ is forced and L is 2-to-1. Furthermore, since $\Delta_{F_L}(x,z) = \Delta_F(z,L(x))$ and $\Delta_F(z,z) = 0$, we must have $z \notin \mathrm{Im}(L)$. Thus, viewed as a vector space over $\mathbb{F}_2$, we have $\mathbb{F}_{2^n} = \mathrm{Im}(L) \oplus \langle z \rangle$. Since $L(x+z) = L(x)$ for all $x \in \mathbb{F}_{2^n}$, we must have $L(\mathrm{Im}(L)) = \mathrm{Im}(L)$. □

We have the following corollary, which eliminates some possibilities for L when the field has square order.

Corollary 4.3. *Set n to be an even integer. Let $F \in \mathbb{F}_{2^n}[x]$ be a quadratic APN function and $L \in \mathbb{F}_2[x]$ be linear. If F_L is APN over $\mathbb{F}_{2^n}$, then L is 2-to-1.*

Proof. Set $M(x) = L(x) + x$. Suppose, by way of contradiction, that F_L is APN over $\mathbb{F}_{2^n}$ and L is a permutation polynomial. Then $L(1) = 1$ is forced. Thus $M(1) = M(0) = 0$. Now $\mathbb{F}_4 = \{0, 1, \gamma, \gamma + 1\}$ is a subfield of $\mathbb{F}_{2^n}$, and since $L \in \mathbb{F}_2[x]$ is a permutation polynomial, we must have either $L(\gamma) = \gamma$ or $L(\gamma) = \gamma + 1$.

If $L(\gamma) = \gamma$, then $M(\gamma) = 0$, so that M has more than two roots, and this contradicts Theorem 4.4 (ii). If $L(\gamma) = \gamma + 1$, then $M(\gamma) = 1$, and so $1 \in \mathrm{Im}(M)$. But then $0, 1 \in \mathrm{Im}(M)$ and $M(0) = M(1)$, so that M is not injective on $\mathrm{Im}(M)$, again contradicting Theorem 4.4 (ii). Thus, L cannot be a permutation polynomial. □

4.3.2 Isotopic shifts of Gold functions

We recall that the DO monomials in characteristic 2 which are APN are the so-called Gold functions over $\mathbb{F}_{2^n}$ $\mathcal{G}_i(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. First studied by Gold [73] in the context of sequence design and rediscovered in 1993 by Nyberg in [92], Gold functions have played an important role in the study of APN functions, and, in particular, in understanding CCZ-equivalence [32]. For $\mathcal{G}_i$ and any $L \in \mathbb{F}_{2^n}[x]$, we use $\mathcal{G}_{i,L}$ to denote the isotopic shift of $\mathcal{G}_i$ by L; that is

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + x L^{2^i}(x). \tag{4.5}$$

It is an easy observation that $\mathcal{G}_i$ and $\mathcal{G}_{n-i}$ are linearly equivalent. In fact, this is a necessary and sufficient condition for Gold functions to be linear equivalent, and if they are not linear equivalent, then they are not CCZ-equivalent [106]. This linear equivalence extends to isotopic shifts as $\mathcal{G}_{i,L}(x)^{2^{n-i}} = \mathcal{G}_{n-i,L}(x)$.

General restrictions on L

We expand on (4.5) further. Let the linear polynomial L be represented as $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$. Then expanding in (4.5) we have

$$\mathcal{G}_{i,L}(x) = \sum_{j=0}^{n-1} \left(b_j x^{2^i+2^j} + b_j^{2^i} x^{2^{i+j}+1} \right),$$

$$\mathcal{G}_{i,L}(x^{2^{n-1}})^2 = \sum_{j=0}^{n-1} \left(b_j^2 x^{2^i+2^j} + b_j^{2^{i+1}} x^{2^{i+j}+1} \right) = x^{2^i} M(x) + x M^{2^i}(x) = \mathcal{G}_{i,M}(x),$$

where $M(x) = \sum_{j=0}^{n-1} b_j^2 x^{2^j}$. We also have, with ζ primitive and $N(x) = \sum_{j=0}^{n-1} b_j \zeta^{2^j-1} x^{2^j}$,

$$\zeta^{-(2^i+1)} \mathcal{G}_{i,L}(\zeta x) = \zeta^{-(2^i+1)} \sum_{j=0}^{n-1} \left(b_j \zeta^{2^i+2^j} x^{2^i+2^j} + b_j^{2^i} \zeta^{2^{i+j}+1} x^{2^{i+1}+1} \right)$$
$$= \sum_{j=0}^{n-1} \left(b_j \zeta^{2^j-1} x^{2^i+2^j} + (b_j \zeta^{2^j-1})^{2^i} x^{2^{i+1}+1} \right) = x^{2^i} N(x) + x N^{2^i}(x) = \mathcal{G}_{i,N}(x).$$

From the above two equivalences we can perform a restriction over one non-zero coefficient of the linear function L. Fixing an integer j such that $0 < j \leq n-1$, then we can restrict the search over all possible linear functions L with $b_j \neq 0$ to those with $b_j = \zeta^k$ with $0 \leq k < 2^j - 1$ and k either 0 or odd. We summarise with the following statement.

Proposition 4.1. *Let $\mathbb{F}_{2^n}^\star = \langle \zeta \rangle$ and $\mathcal{G}_i(x) = x^{2^i+1}$ be APN over $\mathbb{F}_{2^n}$. Suppose $\mathcal{G}_{i,L}$ as (4.5) is constructed with $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$. Then $\mathcal{G}_{i,L}$ is linear equivalent to $\mathcal{G}_{i,M}$, where $M(x) = \sum_{j=0}^{n-1} (b_j \zeta^{k(2^j-1)})^{2^t} x^{2^j}$ for any k, t integers.*

When L is a linear function, the linear operator of $\mathcal{G}_{i,L}$ has the following form:

$$\Delta_a(x) = \Delta_{\mathcal{G}_{i,L}}(x,a) = x\, L(a)^{2^i} + a L(x)^{2^i} + x^{2^i} L(a) + a^{2^i} L(x). \tag{4.6}$$

The next result is related to Theorem 4.4 and shows that in certain situations we may obtain, for Gold functions, slightly stronger restrictions on L than those outlined in Theorem 4.4. Recall the definition of a q-polynomial, presented in Section 2.2.

Definition 4.2. *For q a power of 2, we call L a q-polynomial over $\mathbb{F}_{q^k}$ if $L(x) = \sum b_i x^{q^i}$. Any q-polynomial over $\mathbb{F}_{q^k}$ is a linear transformation of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$.*

Theorem 4.5. *Let $q = 2^m$, with $m > 1$, and suppose $\mathcal{G}_i(x) = x^{2^i+1}$ is APN over $\mathbb{F}_{q^k} = \mathbb{F}_{2^n}$, with $n = km$. If $\mathcal{G}_{i,L}$ as in (4.5) is APN over $\mathbb{F}_{2^n}$ with L a q-polynomial, then L is a complete mapping over $\mathbb{F}_{2^n}$.*

Proof. Since $\mathcal{G}_{i,L}$ is a quadratic APN function, we have $\mathrm{Ker}(\Delta_a(ax)) = \{0,1\}$, for $a \in \mathbb{F}_{2^n}^\star$. For $x \in \mathbb{F}_q^\star$, we have $L(ax) = xL(a)$. So, if $x \in \mathbb{F}_q^\star \setminus \{0,1\}$, from (4.6) we

have

$$\begin{aligned} 0 \neq \Delta_a(ax) &= ax\,L(a)^{2^i} + ax^{2^i}L(a)^{2^i} + (ax)^{2^i}L(a) + a^{2^i}xL(a) \\ &= ax\,L(a)\big(L(a)^{2^i-1} + x^{2^i-1}L(a)^{2^i-1} + a^{2^i-1}x^{2^i-1} + a^{2^i-1}\big) \\ &= ax\,L(a)\big(L(a)^{2^i-1} + a^{2^i-1}\big)\,(x^{2^i-1}+1). \end{aligned}$$

As $\mathcal{G}_i$ is APN over $\mathbb{F}_{2^n}$, we know $\gcd(i,n)=1$, so that $z \mapsto z^{2^i-1}$ is a bijection. Consequently, $x^{2^i-1}=1$ if and only if $x=1$, which we have excluded. Hence, for all $a \in \mathbb{F}_{2^n}^\star$, we must have $L(a) \neq 0$ and $L(a)^{2^i-1} \neq a^{2^i-1}$. This latter condition is equivalent to $L(a) \neq a$ for all $a \in \mathbb{F}_{2^n}^\star$, again because $z \mapsto z^{2^i-1}$ is a bijection. Since L is a linear transformation, we conclude L is a complete mapping over $\mathbb{F}_{2^n}$. □

We now prove a theorem which provides a construction of quadratic APN functions containing new examples of such functions.

Theorem 4.6. *Let $n=km$, $\mathbb{F}_{2^n}^\star = \langle\zeta\rangle$ and $d = \gcd(q-1, \frac{q^k-1}{q-1})$, where $q=2^m$. Let d' be the positive integer having the same prime factors as d, each being raised at the same power as in $\frac{q^k-1}{q-1}$, hence such that $\gcd(q-1, \frac{q^k-1}{(q-1)d'}) = 1$. Let $U = \langle\zeta^{d'(q-1)}\rangle$ be the multiplicative subgroup of $\mathbb{F}_{q^k}^\star$ of order $\big(\frac{q^k-1}{(q-1)d'}\big)$ and consider the set $W = \{y\zeta^j : j = 0,\ldots,d'-1, y \in U\}$. Let $L \in \mathbb{F}_{q^k}[x]$ be a q-polynomial and let $\mathcal{G}_i(x) = x^{2^i+1}$ be an APN Gold function over $\mathbb{F}_{q^k}$ (i.e. such that $\gcd(i,n)=1$). Then $\mathcal{G}_{i,L}$ as in (4.5) is APN over $\mathbb{F}_{q^k}$ if and only if the following conditions are satisfied:*

(i) for any $u \in W$, $L(u) \notin \{0,u\}$;

(ii) if n is even then $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| \leq 1$;

(iii) for distinct $u,v \in W$ satisfying $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$, we have

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin \mathbb{F}_q^\star.$$

Proof. Any element $x \in \mathbb{F}_{q^k}^\star$ can be expressed in the form $x = ut$ with $u \in W$ and $t \in \mathbb{F}_q^\star$. Indeed, since $\mathbb{F}_{q^k}^\star = \langle\zeta\rangle$, we have $x = \zeta^{d'z+j}$, for some integers z and j where $0 \leq j \leq d'-1$. For ease of notation, set $l = \frac{q^k-1}{(q-1)d'}$. Since $\gcd(q-1,l)=1$, for any such z, there exist integers r and s such that $z = r(q-1)+sl$. Hence we have

$$x = \zeta^{d'z+j} = \zeta^{d'r(q-1)}\zeta^j\zeta^{d'sl} = ut, \tag{4.7}$$

where, denoting $y = \zeta^{d'r(q-1)} \in U$, we have $u = y\zeta^j \in W$ and $t = \zeta^{d'sl} = \zeta^{s(\frac{q^k-1}{q-1})} \in \mathbb{F}_q^\star$. Since $|W \times \mathbb{F}_q^\star| = |W| \cdot |\mathbb{F}_q^\star| = (d'|U|) \cdot (q-1) = d' \cdot \frac{q^k-1}{d'(q-1)} \cdot (q-1) = q^k - 1 = |\mathbb{F}_{q^k}^\star|$, two distinct elements in $\mathbb{F}_{q^k}^\star$ cannot have the same representation, u and t are unique. Using the representation (4.7) for x, we have $L(x) = tL(u)$.

Let $a \in \mathbb{F}_{q^k}^\star$ and Δ_a from (4.6). Then $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$ if and only if $\mathrm{Ker}(\Delta_a) = \{0, a\}$ for all $a \in \mathbb{F}_{q^k}^\star$. Now apply the representation (4.7) for both $x = ut$ and $a = vs$ with $u, v \in W$ and $t, s \in \mathbb{F}_q$. Then

$$\begin{aligned}\Delta_a(x) &= u^{2^i}t^{2^i}sL(v) + v^{2^i}s^{2^i}tL(u) + uts^{2^i}L(v)^{2^i} + vst^{2^i}L(u)^{2^i} \\ &= ts\left(t^{2^i-1}\left(u^{2^i}L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i}L(u) + uL(v)^{2^i}\right)\right).\end{aligned}$$

So in this representation, $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$ if and only if the only solutions to $\Delta_{vs}(ut) = 0$ are $t = 0$, or $u = v$ and $t = s$.

Assume $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$. Then L is a complete mapping on $\mathbb{F}_{q^k}$ by Theorem 4.5; hence Condition (i) is satisfied. For showing Condition (ii), suppose that n is even and $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| > 1$. Since L is a complete linear mapping, the elements of $\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}$ cannot be in $\mathbb{F}_2$ and since $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| > 1$ these elements are then α and α^2, where α is a primitive element of $\mathbb{F}_{2^2}^\star$. There exist then two (distinct) elements $u, v \in W$ such that $L(u) = \alpha u$ and $L(v) = \alpha^2 v$. In this case we have $u^{2^i}L(v) + vL(u)^{2^i} = u^{2^i}\alpha^2 v + v\alpha^2 u^{2^i} = 0$, because i being odd (n being even), we have $\alpha^{2^i} = \alpha^2$, and similarly $v^{2^i}L(u) + uL(v)^{2^i} = 0$. Hence $\Delta_{vs}(ut) = 0$ for any $s, t \in \mathbb{F}_q$. Therefore Condition (ii) must hold. To establish Condition (iii), assume $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. As $\mathrm{Ker}(\Delta_{vs}) = \{0, vs\}$, we know that for all $t \in \mathbb{F}_q^\star$, we must have

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}}\right) \neq 0.$$

As $\mathcal{G}_i$ is APN over $\mathbb{F}_{q^k}$ by hypothesis, we know $\gcd(2^i - 1, q-1) = 1$, and so t^{2^i-1} ranges over all of $\mathbb{F}_q^\star$ as t does. Consequently, we must have

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin \mathbb{F}_q^\star,$$

which is Condition (iii).

Conversely, assume that Conditions (i), (ii) and (iii) hold. Since $L(ut) = tL(u)$, we have that L is a complete mapping by (i). Assume that $\Delta_{vs}(ut) = 0$.

We must show $t = 0$, or $u = v$ and $t = s$. Assume that $t \neq 0$, we have:

$$t^{2^i-1}\left(u^{2^i}L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i}L(u) + uL(v)^{2^i}\right) = 0. \tag{4.8}$$

Firstly, suppose $u = v$. Then (4.8) becomes $\left(t^{2^i-1} + s^{2^i-1}\right)\left(u^{2^i}L(u) + uL(u)^{2^i}\right) = 0$. Thus $t^{2^i-1} = s^{2^i-1}$ or $u^{2^i}L(u) = uL(u)^{2^i}$. By (i), $L(u) \neq 0$, so the latter reduces further to $L(u)^{2^i-1} = u^{2^i-1}$. But this is equivalent to $L(u) = u$, which cannot hold by (i). Thus $t^{2^i-1} = s^{2^i-1}$, from which we deduce $t = s$, as required.

It remains to show that $\Delta_{vs}(ut) = 0$ has no solutions when $t \neq 0$ and $u \neq v$. Suppose $x = ut$ is a solution such that $u^{2^i}L(v) + vL(u)^{2^i} = 0$. Then (4.8) forces $v^{2^i}L(u) + uL(v)^{2^i} = 0$ also. So we have

$$\frac{L(v)}{v} + \frac{L(u)^{2^i}}{u^{2^i}} = 0 \text{ and } \frac{L(u)}{u} + \frac{L(v)^{2^i}}{v^{2^i}} = 0.$$

Combining, we find

$$\frac{L(u)}{u} = \frac{L(u)^{2^{2i}}}{u^{2^{2i}}},$$

so $\frac{L(u)}{u} \in \mathbb{F}_{2^{2i}}$. If n is odd we have $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which implies that $\frac{L(u)}{u}$ is equal to 0 or 1. This is not possible due to Condition (i). On the other hand, if n is even then $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^2}$. Hence $\frac{L(u)}{u} = \alpha$, primitive element in $\mathbb{F}_{2^2}^\star$, and $\frac{L(v)}{v} = \left(\frac{L(u)}{u}\right)^{2^i} = \alpha^{2^i} = \alpha^2$. This leads to a contradiction for Condition (ii). Hence, if $x = ut$ is a solution, then $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. Now dividing by $u^{2^i}L(v) + vL(u)^{2^i}$ in (4.8) yields

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}}\right) = 0.$$

However, there are no solutions to this equation by (iii). This proves $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$. □

Following the same steps of Theorem 4.6 we can extend the previous result as follows.

Corollary 4.4. *Let $n = km$ and $d = \gcd(q-1, \frac{q^k-1}{q-1})$, where $q = 2^m$. Let d', U and W be defined as in Theorem 4.6. Let $L \in \mathbb{F}_{q^k}[x]$ be a q-polynomial and let $\mathcal{G}_i(x) = x^{2^i+1}$ be a Gold function over $\mathbb{F}_{q^k}$ (even not APN), with $n/\gcd(n,i)$ odd. Then $\mathcal{G}_{i,L}$ as in (4.5) is differentially 2^j-uniform over $\mathbb{F}_{q^k}$, where $j = \gcd(i,m)$, if and only if the following conditions are satisfied:*

(i) for any $u \in W$, $L(u)^{2^i-1} \notin \{0, u^{2^i-1}\}$;

(ii) for distinct $u, v \in W$ *satisfying* $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$, *we have*

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin U',$$

where $U' = \langle \bar{\zeta}^{\frac{q-1}{\bar{d}}} \rangle$, $\bar{\zeta} = \zeta^{\frac{q^k-1}{q-1}}$ *and* $\bar{d} = \gcd(2^i - 1, q-1)$.

Proof. Let $a \in \mathbb{F}_{q^k}^\star$ and Δ_a as (4.6). If we consider $x \in \mathbb{F}_q$, then we have

$$\Delta_a(ax) = ax\,L(a)\left(L(a)^{2^i-1} + a^{2^i-1}\right)\left(x^{2^i-1} + 1\right),$$

implying that $a\mathbb{F}_{2^j} \subseteq \mathrm{Ker}(\Delta_a)$. Then $\mathcal{G}_{i,L}$ is differentially 2^j-uniform over $\mathbb{F}_{q^k}$ if and only if $\mathrm{Ker}(\Delta_a) = a\mathbb{F}_{2^j}$ for all $a \in \mathbb{F}_{q^k}^\star$. Moreover, if $\mathcal{G}_{i,L}$ is differentially 2^j-uniform then we have that Condition (i) holds.

Now, consider any $x \in \mathbb{F}_{q^k}$, and apply the representation (4.7) for both $x = ut$ and $a = vs$ with $u, v \in W$ and $t, s \in \mathbb{F}_q$. Then

$$\begin{aligned}\Delta_a(x) &= u^{2^i}t^{2^i}sL(v) + v^{2^i}s^{2^i}tL(u) + uts^{2^i}L(v)^{2^i} + vst^{2^i}L(u)^{2^i} \\ &= ts\left(t^{2^i-1}\left(u^{2^i}L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i}L(u) + uL(v)^{2^i}\right)\right).\end{aligned}$$

So, $\mathcal{G}_{i,L}$ is differentially 2^j-uniform if and only if the only solutions to $\Delta_{vs}(ut) = 0$ are $t = 0$, or $u = v$ and $t \in s\mathbb{F}_{2^j}^\star$. For establishing Condition (ii), assume $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. As $\mathrm{Ker}(\Delta_{vs}) = vs\mathbb{F}_{2^j}$, we know that for all $t \in \mathbb{F}_q^\star$, we must have

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}}\right) \neq 0.$$

Since $U' = \{t^{2^i-1} : t \in \mathbb{F}_q^\star\}$, we must have

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin U',$$

which is Condition (ii).

Conversely, assume that Conditions (i), (ii) hold. Assume that $\Delta_{vs}(ut) = 0$. We must show $t = 0$, or $u = v$ and $t \in s\mathbb{F}_{2^j}^\star$. Assume that $t \neq 0$, we have:

$$t^{2^i-1}\left(u^{2^i}L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i}L(u) + uL(v)^{2^i}\right) = 0. \tag{4.9}$$

Supposing $u = v$, (4.9) becomes $\left(t^{2^i-1} + s^{2^i-1}\right)\left(u^{2^i}L(u) + uL(u)^{2^i}\right) = 0$. Thus $t^{2^i-1} = s^{2^i-1}$ or $u^{2^i}L(u) = uL(u)^{2^i}$. By (i), $u^{2^i}L(u) \neq uL(u)^{2^i}$, so $t^{2^i-1} = s^{2^i-1}$, from which we deduce $t \in s\mathbb{F}_{2^j}^\star$, as required.

Now, we need to show that $\Delta_{vs}(ut) = 0$ has no solutions when $t \neq 0$ and $u \neq v$. Suppose $x = ut$ is a solution such that $u^{2^i}L(v) + vL(u)^{2^i} = 0$. Then (4.9) implies $v^{2^i}L(u) + uL(v)^{2^i} = 0$ also. So, as in Theorem 4.6 we obtain $\frac{L(u)}{u} \in \mathbb{F}_{2^{2i}}$, which contradicts Condition (i) since $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^i}$. Thus, if $x = ut$ is a solution, $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. Dividing by $u^{2^i}L(v) + vL(u)^{2^i}$ in (4.9) we obtain

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}}\right) = 0.$$

However, there are no solutions to this equation by (ii). □

Proposition 4.2. *Set n an even integer. Suppose $\mathcal{G}_i(x) = x^{2^i+1}$ is APN over $\mathbb{F}_{2^n}$. Then for any $L \in \mathbb{F}_2[x]$ linear function, $\mathcal{G}_{i,L}$ defined as in (4.5) is not APN.*

Proof. Let $L(x) = \sum_{j\in J} x^{2^j}$, for some $J \subseteq \{0,\dots,n-1\}$. Then

$$\mathcal{G}_{i,L}(x) = \sum_{j\in J}[x^{2^{j+i}+1} + x^{2^j+2^i}].$$

Let Δ_1 from (4.6), so that $\Delta_1(x) = \sum_{j\in J}[(x^{2^{j+i}} + x) + (x^{2^j} + x^{2^i})]$. It is easy to check that $\mathbb{F}_4 \subset \mathrm{Ker}(\Delta_1)$. Indeed, let $\mathbb{F}_4 = \{0,1,\alpha,\alpha+1\}$, we have that $0,1 \in \mathrm{Ker}(\Delta_1)$. Since $\mathcal{G}_i$ is APN then i is odd, $\alpha^{2^i} = \alpha + 1$ and

$$(\alpha^{2^{j+i}} + \alpha) + (\alpha^{2^j} + \alpha^{2^i}) = ((\alpha+1)^{2^j} + \alpha) + (\alpha^{2^j} + \alpha + 1) = 0.$$

Thus, $\Delta_1(\alpha) = 0$, which implies $\mathbb{F}_4 \subset \mathrm{Ker}(\Delta_1)$. □

Restricting L to having 1 term

First we consider the case when the linear map is just a monomial, $L(x) = ux^{2^j}$. It follows from (4.2) that we need only to consider j where $j \leq n/2$.

Lemma 4.1. *Let $\mathcal{G}_i(x) = x^{2^i+1}$ be APN over $\mathbb{F}_{2^n}$, $L(x) = ux^{2^j} \in \mathbb{F}_{2^n}[x]$ and $\mathcal{G}_{i,L}$ as in (4.5). The following statements hold.*

(i) If $j = 0$ and $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_i$.

(ii) If n is odd, $j = i$, and $u \in \mathbb{F}_{2^n}^\star$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_{2i}$ and (provided $n > 3$) CCZ-inequivalent to $\mathcal{G}_i$.

(iii) *If $n = 2j$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_{|j-i|}$ whenever $ux^{2^i} + u^{2^i}x^{2^{j+i}}$ is a permutation. In such cases, $\mathcal{G}_{i,L}$ is CCZ-equivalent to $\mathcal{G}_i$ if and only if $j = 2i$ or $2i - j = n$.*

(iv) *If $\gcd(j,n) = 1$, then $\mathcal{G}_{i,L}$ is not APN over $\mathbb{F}_{2^n}$. Except for the case when n odd and $j = i$.*

(v) *If $\gcd(j+i, |j-i|, n) > 1$, then $\mathcal{G}_{i,L}$ is not APN over $\mathbb{F}_{2^n}$. In particular, if n is even and j is odd $\mathcal{G}_{i,L}$ is not APN.*

Proof. Firstly, set $L(x) = ux$ with $u \notin \mathbb{F}_2$. Then $\mathcal{G}_{i,L} = (u + u^{2^i})\mathcal{G}_i$, which is clearly linearly equivalent to $\mathcal{G}_i$. Now let $L(x) = ux^{2^j}$, $u \in \mathbb{F}_{2^n}^\star$. Then

$$\mathcal{G}_{i,L}(x) = ux^{2^i+2^j} + u^{2^i}x^{2^{i+j}+1}. \tag{4.10}$$

If $i = j$, then (4.10) becomes $\mathcal{G}_{i,L}(x) = ux^{2^{i+1}} + u^{2^i}\mathcal{G}_{2i}(x)$, which is equivalent to $\mathcal{G}_{2i}$ and APN provided $\gcd(2i,n) = 1$; i.e. provided n is odd. It was shown by Budaghyan, Carlet and Leander [28] that these two functions are CCZ-inequivalent provided $n > 3$. This proves (ii). For (iii), it is easily checked that

$$\mathcal{G}_{i,L}(x) = (ux^{2^i} + u^{2^i}x^{2^{j+i}}) \circ \mathcal{G}_{|j-i|}(x).$$

The statement in (iii) on equivalence is clear.

Now, let $\gcd(j,n) = 1$. For $a \in \mathbb{F}_q^\star$, set Δ_a as in (4.6). Then

$$\Delta_a(ax) = ua^{2^j+2^i}(x^{2^{j-i}} + x)^{2^i} + u^{2^i}a^{2^{j+i}+1}(x^{2^{j+i}} + x).$$

Now, $\mathcal{G}_{i,L}$ is APN if and only if $\mathrm{Ker}(\Delta_a(ax)) = \{0,1\}$ for all $a \in \mathbb{F}_q^\star$. Let $L_1(x) = x^{2^{j-i}} + x$ and $L_2(x) = x^{2^{j+i}} + x$, so that

$$\Delta_a(ax) = ua^{2^j+2^i}L_1(x)^{2^i} + u^{2^i}a^{2^{j+i}+1}L_2(x).$$

If n is even, j and i are odd numbers and the obtained function cannot be APN since $\mathbb{F}_4 \subseteq \mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$, and for all $x \in \mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$ we have that x is a solution of $\Delta_a(ax) = 0$. If n is odd, from (ii) we have that for $j = i$, $\mathcal{G}_{i,L}$ is APN. Then, let us consider $j \neq i$. In this case, $\mathrm{Ker}(L_1) \subsetneq \mathbb{F}_{2^n}$ and $\mathrm{Ker}(L_2) \subsetneq \mathbb{F}_{2^n}$ since $0 < |j-i| < n$ and $0 < j+i < n$, so there exists some element $\bar{x} \in \mathbb{F}_{2^n}^\star \setminus \{1\}$ (note that $\mathbb{F}_2 \subseteq \mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$) such that $L_1(\bar{x})\,L_2(\bar{x}) \neq 0$. Now $\Delta_a(ax) = 0$ is equivalent to

$$L_1(x)^{2^i} + u^{2^i-1}a^{(2^j-1)(2^i-1)}L_2(x) = 0.$$

Since $a \mapsto a^{(2^j-1)(2^i-1)}$ is a permutation of $\mathbb{F}_{2^n}$ (both i and j are coprime with n), there exists a such that $a^{(2^j-1)(2^i-1)} = \frac{L_1(\bar{x})^{2^i}}{u^{2^i-1}L_2(\bar{x})}$, implying $\bar{x} \in \mathrm{Ker}(\Delta_a(ax))$. So $\mathcal{G}_{i,L}$ is not APN. Then, statement (iv) is proved.

Let us consider statement (v). From the proof of (iv), we have that for all $x \in \mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$, x is a solution of $\Delta_a(ax) = 0$. Then, since $\gcd(j+i, |j-i|, n) = d > 1$, for some integer d, we have $\mathbb{F}_{2^d} \subseteq \mathrm{Ker}(L_1) \cap \mathrm{Ker}(L_2)$ and so $\mathcal{G}_{i,L}$ cannot be APN. □

Restricting L to having 2 terms

Consider now L as a linear binomial.

Lemma 4.2. *Let m be a positive integer, $n = 2m$ and*

$$L(x) = ux^{2^m} + vx, \tag{4.11}$$

with $u, v \in \mathbb{F}_{2^n}^\star$ and $v \neq 1$. Set $z = v + v^{2^i}$. If $\mathcal{G}_{i,L}$ is APN, then $\mathcal{G}_{i,M}$ is an APN function EA-equivalent to $\mathcal{G}_{i,L}$ for the following choices of linear $M \in \mathbb{F}_{2^n}[x]$:

(i) $M(x) = u\zeta^{2^m-1}x^{2^m} + vx$.

(ii) $M(x) = ux^{2^m} + wx$, *where* $w + w^{2^i} = z^{2^m}$;

(iii) $M(x) = u^2x^{2^m} + wx$ *where* $w + w^{2^i} = z^2$.

Proof. Given linear L as in (4.11), equation (4.5) is of the form

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + zx^{2^i+1}. \tag{4.12}$$

We want to prove that in each case the obtained function is EA-equivalent to the original map.

(i). If instead of u we consider $u\zeta^{2^m-1}$ in (4.12), then we obtain
$\mathcal{G}_{i,M}(x) = u^{2^i}\zeta^{2^i(2^m-1)}x^{2^{m+i}+1} + u\zeta^{2^m-1}x^{2^m+2^i} + zx^{2^i+1}$,
which is linear equivalent to $\mathcal{G}_{i,L}$ as $\mathcal{G}_{i,M}(\zeta^{-1}x) = \zeta^{-2^i-1}\mathcal{G}_{i,L}(x)$.

(ii). For M as specified, we have $\mathcal{G}_{i,M}$ is linear equivalent to $\mathcal{G}_{i,L}$ since
$\mathcal{G}_{i,M}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + z^{2^m}x^{2^i+1}$,
$\mathcal{G}_{i,M}(u^{-2^m}x^{2^m})^{2^m} = u^{-2^i-1}\mathcal{G}_{i,L}(x)$.

(iii). In this last case we obtain $\mathcal{G}_{i,M}(x^2)^{2^{2m-1}} = \mathcal{G}_{i,L}(x)$ since
$\mathcal{G}_{i,M}(x) = u^{2^{i+1}}x^{2^{m+i}+1} + u^2x^{2^m+2^i} + z^2x^{2^i+1}$.

□

Lemma 4.3. *Let m be an even positive integer and $n = 2m$. Suppose $\mathcal{G}_i$ is APN over $\mathbb{F}_{2^n}$. Set $L(x) = ux^{2^m} + vx$ with $v \in \mathbb{F}_{2^n}$ satisfying $v + v^{2^i} = 1$ and $u = w^{2^m-1}$ for $w \in \mathbb{F}_{2^n}^\star$. Then $\mathcal{G}_{i,L}$ is an APN function over $\mathbb{F}_{2^n}$ EA-equivalent to $\mathcal{G}_{m-i}$.*

Proof. In this case the isotopic shift of $\mathcal{G}_i$ by L is given by

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + x^{2^i+1} \quad = w^{2^{m+i}-2^i}x^{2^{m+i}+1} + w^{2^m-1}x^{2^m+2^i} + x^{2^i+1}.$$

Now note $w^{2^i+1}\mathcal{G}_{i,L}(xw^{-1}) = x^{2^{m+i}+1} + x^{2^m+2^i} + x^{2^i+1}$, and this latter function was shown to be EA-equivalent to $x^{2^{m-i}+1}$ in [35]. □

We end this subsection by deriving a necessary condition for specific $\mathcal{G}_{i,L}$ in certain restricted settings.

Lemma 4.4. *Let m be a positive integer and $n = 2m$. Let $u, v \in \mathbb{F}_{2^n}^\star$. If $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{2^n}$ with $L(x) = ux^{2^m} + vx$, then $u^{2^i}x^{2^i} + ux + v^{2^i} + v = 0$ has no solution x such that $x^{2^m+1} = 1$.*

Proof. From the given L we obtain in (4.5) that

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + (v^{2^i} + v)x^{2^i+1}.$$

If $\mathcal{G}_{i,L}$ is APN, then

$$\begin{aligned} 0 \neq & a^{-(2^i+1)}\Delta_a(ax) \\ \neq & (ua^{2^m-1})^{2^i}(x^{2^{m+i}} + x) + (ua^{2^m-1})(x^{2^m} + x^{2^i}) + (v^{2^i} + v)(x^{2^i} + x) \end{aligned}$$

for any $a \neq 0$ and $x \neq 0, 1$. Assume $x \in \mathbb{F}_{2^m}$. Then we have

$$a^{-(2^i+1)}\Delta_a(ax) = \left(u^{2^i}a^{(2^m-1)2^i} + ua^{2^m-1} + v^{2^i} + v\right)(x^{2^i} + x) \neq 0$$

Let $y = a^{2^m-1}$, then $u^{2^i}y^{2^i} + uy + v^{2^i} + v \neq 0$ for all $y \in \mathbb{F}_q$ such that $y^{2^m+1} = 1$. □

In particular when we consider the function $\mathcal{G}_1(x) = x^3$ we obtain the following.

Lemma 4.5. *Let m be an even positive integer and $n = 2m$. Set $u = \zeta^i$, with $0 \leq i < 2^m - 1$. If $v \in \mathbb{F}_{2^n}$ is such that $v(v+1) = \zeta^{j(2^m+1)}$ for some $0 \leq j < 2^m - 1$ and $\mathcal{G}_{1,L}$ is APN over $\mathbb{F}_{2^n}$ with $L(x) = ux^{2^m} + vx$, then $\zeta^{(2^m+1)(2j-i)} + \zeta^{i(2^m+1)} \neq 1$. Moreover, if there exists a positive integer l such that $\zeta^{i+l(2^m-1)} + \zeta^{2^m i+l(1-2^m)} = 1$, then $i \neq j$.*

Proof. From the given L we obtain in (4.5) that

$$\mathcal{G}_{1,L}(x) = \zeta^{2i}x^{2^{m+1}+1} + \zeta^i x^{2^m+2} + \zeta^{j(2^m+1)}x^3.$$

If $\mathcal{G}_{1,L}$ is APN, then

$$a^{-3}\Delta_a(ax) = (\zeta^i a^{2^m-1})^2(x^{2^{m+1}} + x) + (\zeta^i a^{2^m-1})(x^{2^m} + x^2) + \zeta^{j(2^m+1)}(x^2 + x) \neq 0$$

for any $a \neq 0$ and $x \neq 0, 1$. Assume $x \in \mathbb{F}_{2^m}$. Then we have

$$a^{-3}\Delta_a(ax) = ((\zeta^i a^{2^m-1})^2 + \zeta^i a^{2^m-1} + \zeta^{j(2^m+1)})(x^2 + x) \neq 0.$$

Let $a = \zeta^l$ for a positive integer l. Then

$$a^{-3}\Delta_a(ax) = (\zeta^{2(i+l(2^m-1))} + \zeta^{i+l(2^m-1)} + \zeta^{j(2^m+1)})(x^2 + x) \neq 0. \tag{4.13}$$

Suppose that $\zeta^{(2^m+1)(2j-i)} + \zeta^{i(2^m+1)} + 1 = 0$. Multiplying this equality by $\zeta^{i(2^m+1)}$ and then taking its 2^{n-1}th power we get $\zeta^{i(2^m+1)} + \zeta^{2^{n-1}i(2^m+1)} + \zeta^{j(2^m+1)} = 0$. For $l = 2^{n-1}i$, we have $i + l(2^m - 1) = i2^{n-1}(2^m + 1)$, and so we have a choice of a for which $a^{-2}\Delta_a(ax) = 0$, contradicting the hypothesis.

Assume now that there exists an integer l such that $\zeta^{i+l(2^m-1)} + \zeta^{2^m i+l(1-2^m)} = 1$. Then using (4.13) we find

$$\begin{aligned} 0 \neq &\zeta^{2(i+l(2^m-1))} + \zeta^{(i+l(2^m-1))} + \zeta^{j(2^m+1)} = \zeta^{i+l(2^m-1)}(\zeta^{i+l(2^m-1)} + 1) + \zeta^{j(2^m+1)} \\ \neq &\zeta^{i+l(2^m-1)}\zeta^{2^m i+l(1-2^m)} + \zeta^{j(2^m+1)} = \zeta^{i(2^m+1)} + \zeta^{j(2^m+1)}, \end{aligned}$$

implying $i \neq j$. □

Restricting L to having 3 terms

From the computational analysis performed for the Gold function $\mathcal{G}_1(x) = x^3$, see Section 4.4 below, we observed that, when L has 3 terms and $n = 3m$, the linear polynomial

$$L(x) = ax^{2^{2m}} + bx^{2^m} + cx \tag{4.14}$$

is a good generator of APN functions via shifts of $\mathcal{G}_1$. In this case, we have

$$\mathcal{G}_{1,L}(x) = a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2 + c)x^3. \tag{4.15}$$

As proved in Proposition 4.1, the polynomial L generates an isotopic shift of $\mathcal{G}_i$ equivalent to the one generated by

$$M(x) = (a\zeta^{(2^{2m}-1)j})^{2^k}x^{2^{2m}} + (b\zeta^{(2^m-1)j})^{2^k}x^{2^m} + c^{2^k}x. \tag{4.16}$$

Consideration of this case led to Theorem 4.6. The case with $q = 2^m$, $n = 3m$, in Theorem 4.6 is exactly the situation that we observed in our computational results. As we shall note in Section 4.4, this specific case provides a new APN function when $n = 9$ which is CCZ-inequivalent to any known APN function.

4.4 Computational results

We studied the possible linear functions L for which $\mathcal{G}_{i,L}$, as in (4.5), is an APN function over $\mathbb{F}_{2^n}$. The obtained APN functions have been compared, using CCZ-equivalence, to those presented in tables of [66]. For purposes of comparison, we will refer to the numbering given in those lists. In [102, 109] many more quadratic APN functions are constructed, however, none of our newly constructed functions is equivalent to any of them.

Note that, since for any linear L isotopic shifts by L and $L + Id$ give the same function F_L, whenever we have $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$ with $b_0 = 1$ we can consider $L'(x) = \sum_{j=1}^{n-1} b_j x^{2^j}$ instead.

Data for $\mathcal{G}_{i,L}$ where L has 1 or 2 terms

When L has just one term, all possible cases with $3 \leq n \leq 12$ considering all APN Gold functions $\mathcal{G}_i(x) = x^{2^i+1}$, with $\gcd(i,n) = 1$, have been analysed and the only APN functions arising are those presented in Lemma 4.1.

When L has exactly two terms, we determined those isotopic shifts of $\mathcal{G}_i$ by L that are APN over $\mathbb{F}_{2^n}$ for $6 \leq n \leq 11$. Apart from the $n = 6$ case, we obtained APN functions only for $n = 2m$ and $L(x) = ux^{2^m} + vx$. For $n \in \{12, 14, 16\}$ we only considered L of the form $ux^{2^m} + vx$. In particular, we found that if $n \in \{8, 12, 16\}$, then $\mathcal{G}_{i,L}$ from (4.5) is either equivalent to $\mathcal{G}_i$ or to $\mathcal{G}_{m-i}$. In the other cases, $n \in \{10, 14\}$, the obtained APN maps are all equivalent to the original Gold function $\mathcal{G}_i$.

When $n = 6$, with $\mathbb{F}_{2^6}^\star = \langle \zeta \rangle$, considering $\mathcal{G}_{L,1}$ more APN cases occur:

- $L(x) = ux^8 + vx = ux^{2^m} + vx$ can give functions equivalent to $\mathcal{G}_1$ or to function number 2.1 in Table 2.3 ($x^3 + x^{10} + \zeta x^{24}$).
- $L(x) = ux^{16} + vx$, where u is not a cube and $v + v^2 = 1$, gives a function equivalent to number 1.2 in Table 2.3 ($x^3 + \zeta^{11} x^6 + \zeta x^9$).

- $L(x) = ux^{16} + vx^4$, where u is not a cube and $v = u^{26}$, gives a function equivalent to number 1.2 in Table 2.3.

Data for $\mathcal{G}_{i,L}$ where L has 3 terms and new APN functions

When the function L has 3 terms, none of them equal to x, we analysed $\mathcal{G}_{i,L}$ for the cases $n \in \{6,7,8,9\}$. For $n = 7$ no valid trinomial was found. For the cases $n = 6,8,9$, all the trinomials found are 2^m-polynomials, where $n = km$ with $k > 1$, and thus instances of Theorem 4.6. In particular we obtain:

$n = 6$: ($k = 3$, $m = 2$) from $\mathcal{G}_1$ we can construct APN functions CCZ-equivalent to $\mathcal{G}_1$ and to number 1.2 in Table 2.3 ($x^3 + \zeta^{-1}\mathrm{Tr}(\zeta^3 x^9)$).

$n = 8$: ($k = 4$, $m = 2$) from $\mathcal{G}_1$ we can construct APN functions CCZ-equivalent to number 1.2 in Table 2.5 ($x^3 + \mathrm{Tr}(x^9)$); from $\mathcal{G}_3$ we can construct APN functions CCZ-equivalent to number 1.11 in Table 2.5 ($x^9 + \mathrm{Tr}(x^3)$), map not in any known family of APN functions until now.

$n = 9$: ($k = 3$, $m = 3$) from $\mathcal{G}_1$ we can construct APN functions not CCZ-equivalent to any function from the known APN families (all CCZ-equivalent to N. 12 in Table 4.1).

Due to the inequivalence result obtained for $\mathbb{F}_{2^9}$, for $n = 3m$, we analysed the possible APN functions $\mathcal{G}_{i,L}$ as in (4.5) constructed using the linear function L of the form $ax^{2^{2m}} + bx^{2^m} + cx$. Considering Proposition 4.1 and setting to $d = c^{2^i} + c$, we obtained, up to EA-equivalence, the following results:

$m = 2$: The obtained $\mathcal{G}_{1,L}$'s APN cases are equivalent to $\mathcal{G}_1$ or to $x^3 + \zeta^{-1}\mathrm{Tr}(\zeta^3 x^9)$.

$m = 3$: We obtain for $\mathcal{G}_{1,L}$ the values $\{[\zeta^{424},\zeta,\zeta^{34}],[\zeta^{263},\zeta,\zeta^{272}],[\zeta^{508},\zeta,\zeta^{132}]\}$. Using iteratively Proposition 4.1 it is possible to prove that the three cases are EA-equivalent to each other and, as mentioned above, $\mathcal{G}_{1,L}$ is not equivalent to any APN function from the known APN families. For $\mathcal{G}_{i,L}$ with $i \neq 1$ no APN map can be constructed.

$m = 4$: $\mathcal{G}_{1,L}$ is APN for $[a,b,d] \in \{[\zeta^{1962},\zeta^3,\zeta^{1365}],[\zeta^{290},\zeta,\zeta^{2184}],[\zeta^{904},\zeta^5,\zeta^{546}]\}$. For these cases, it is possible to prove that they are equivalent to $\mathcal{G}_1$. In particular, for any of these shifts $\mathcal{G}_{1,L}$ it is possible to find L_1 and L_2 2^4-polynomials such that $L_1(\mathcal{G}_{1,L}(x)) = \mathcal{G}_1(L_2(x))$. Using the same L's, identical results are obtained for $\mathcal{G}_{i,L}$ with $i = 5$.

With the restriction on the subfield $\mathbb{F}_{2^m}$ no choice was found for $m = 5$ but for $m = 6$ we obtain that $\mathcal{G}_{1,L}$ is APN for $[a,b,d] \in \{[\zeta^{37449},1,\zeta^{112347}],[\zeta^{149796},1,\zeta^{187245}],[\zeta^{74898},1,\zeta^{224694}]\}$. The same results, using the identical L's, can be obtained also for $\mathcal{G}_{i,L}$ for $i = 5,7$.

Remark 4.2. *As shown above, the conditions of Theorem 4.6 are satisfied for many functions in dimensions $n = 6,8,9,12,18$. In particular with $k = m = 3$ we obtain a map $\mathcal{G}_{1,L}$ not CCZ-equivalent to any known map so far. In addition for $k = 4$ and $m = 2$ we obtain a map $\mathcal{G}_{3,L}$ equivalent to $x^9 + Tr(x^3)$, an APN map known since 2006 [22, 57] which has not been part of any known family of APN functions up to now. Both functions have classical Walsh spectrum (the same as Gold functions). Computations for larger n are complicated and we leave this as an open problem indicated in a conjecture below.*

Conjecture 4.1. *The conditions of Theorem 4.6 are satisfied by infinitely many APN functions. That is, Theorem 4.6 covers APN functions for an infinite number of dimensions n.*

In Table 4.1 we list, up to CCZ-equivalence, all known quadratic APN maps defined over $\mathbb{F}_{2^9}$ (with references to families to which they belong). Note that we also have families of non-quadratic power APN functions defined over $\mathbb{F}_{2^9}$ but, as proven in [106], if a quadratic APN function is CCZ-equivalent to a power function then it is EA-equivalent to a Gold functions, and, therefore, we do not need to compare the constructed functions with these power functions. In the table we also list Γ-rank, Δ-rank and $|\mathcal{M}_{G_F}|$ of the functions (CCZ-invariant parameters, see Subsection 2.3.1). To this list we added the new function found with Theorem 4.6.

The cases $3 \leq n \leq 5$

For these cases, all APN functions are classified [21] and they are all CCZ-equivalent to the Gold functions and to the inverse function. So, from Lemma 4.1 we have that all quadratic APN functions can be obtained from the isotopic shifts of $\mathcal{G}_1$.

The case $n = 6$

From the linear isotopic shift of the Gold function $\mathcal{G}_1$, with both choices for L being a permutation and a 2-to-1 map, we obtained (computationally) all

Table 4.1: CCZ-inequivalent quadratic APN polynomials over $\mathbb{F}_{2^9}$ and their relation to previously known families of APN functions

N.	Function	Family	no. in Table 2.6	Γ-rank	Δ-rank	$\lvert\mathcal{M}_{G_F}\rvert$
1	x^3	Gold	1.1	38470	872	$9 \cdot 2^9 \cdot 511$
2	x^5	Gold	2.1	41494	872	$9 \cdot 2^9 \cdot 511$
3	x^{17}	Gold	3.1	38470	872	$9 \cdot 2^9 \cdot 511$
4	x^{13}	Kasami	4.1	58676	3086	$9 \cdot 511$
5	x^{241}	Kasami	6.1	61726	3482	$9 \cdot 511$
6	x^{19}	Welch	5.1	60894	3956	$9 \cdot 511$
7	x^{255}	Inverse	7.1	130816	93024	$2 \cdot 9 \cdot 511$
8	$Tr_1^9(x^9) + x^3$	[30]	1.2	47890	920	$9 \cdot 2^9$
9	$Tr_3^9(x^{18} + x^9) + x^3$	[31]	1.3	48428	930	$9 \cdot 2^9$
10	$Tr_3^9(x^{36} + x^{18}) + x^3$	[31]	1.4	48460	944	$9 \cdot 2^9$
11	$x^3 + x^{10} + \zeta^{438}x^{136}$	–	8.1	48608	938	$3 \cdot 7 \cdot 2^9$
12	$\zeta^{337}x^{129} + \zeta^{424}x^{66} + \zeta^2x^{17} + \zeta x^{10} + \zeta^{34}x^3$	Theorem 4.6	–	48596	944	$3 \cdot 7 \cdot 2^9$

the quadratic APN functions over $\mathbb{F}_{2^6}$ (up to EA-equivalence). That is, for any given quadratic APN function F over $\mathbb{F}_{2^6}$ there exist a linear permutation L and a 2-to-1 linear map L' such that the isotopic shifts $\mathcal{G}_{1,L}$ and $\mathcal{G}_{1,L'}$ are EA-equivalent to F. The same result was computationally obtained for any quadratic APN map over $\mathbb{F}_{2^6}$ listed in [57] in place of $\mathcal{G}_1$. The computations can be seen in Appendix A. Up to EA-equivalence (and thus CCZ-equivalence) the list is complete and, since for two quadratic maps EA-equivalence implies EA-equivalence of the isotopic shifts (see Corollary 4.1), we can state the following result.

Proposition 4.3. *Over $\mathbb{F}_{2^6}$ for any two quadratic APN maps F and G, there exist a linear permutation L and a linear 2-to-1 map L' such that F_L and $F_{L'}$ are EA-equivalent to G.*

Note that, in general, the number of all the DO-polynomials over $\mathbb{F}_{2^n}$ is $q^{\binom{n}{2}}$, where $q = 2^n$, and the number of all the possible shifts of a fixed function F is q^n. So, also for small values of n the number of the linear shifts that we can obtain from one fixed function is much smaller than the number of the DO-polynomials. Moreover, for isotopic shifts we are restricted to only shifts by linear permutation or 2-to-1 maps which further constrains the search area. Hence, obtaining all possible quadratic APN functions for $n = 6$ as an isotopic shift of a single function, indicates that the isotopic shift is a powerful method for constructing APN functions.

Additional data for isotopic shifts of $x^3 + \mathrm{Tr}(x^9)$

In this case, the isotopic shift of F by a linear function L is of the form

$$F_L(x) = xL(x)(x + L(x)) + \mathrm{Tr}(xL(x)(x^7 + L^7(x))). \tag{4.17}$$

We may immediately observe some trivial constructions.

For n even, set $L(x) = ux$ with u a primitive cubed root of unity in $\mathbb{F}_{2^n}$, so that $u^2 + u + 1 = 0$. Then we have $F_L(x) = x^3 + \mathrm{Tr}(x^9)$.

Remark 4.3. *For n a multiple of 3, the APN function x^3 can be obtained as an isotopic shift of $x^3 + \mathrm{Tr}(x^9)$ (set $L(x) = ux$ with u primitive 7-th root of unity, $F_L(x) = u(u + 1)x^3$).*

Computational results, which are different from the two cases above, can be summarised as follows. When the function L has 1 term:

$n = 7$: the obtained F_L's are CCZ-equivalent to number 2.2 in Table 2.4 ($x^3 + x^{17} + x^{33} + x^{34}$);

$n = 8$: the obtained F_L's are CCZ-equivalent to F or to $x^9 + \mathrm{Tr}(x^3)$;

$n = 11$: no valid monomial was found.

When the function L has 2 terms, different from x:

$n = 8$: the obtained F_L's are CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$.

Restricting the coefficients of L to $\mathbb{F}_2$

Proposition 4.2 shows that a linear function L with coefficients in $\mathbb{F}_2$ cannot generate an APN function from isotopic shift of Gold functions over extension fields of even degree. This was investigated further computationally, over extension fields of odd degree. We looked at $\mathcal{G}_{i,L}$ for valid $\mathcal{G}_i$ and $L \in \mathbb{F}_2[x]$. Except the case $n = 5$, for $3 \leq n \leq 11$ we obtained APN shifts only for $L(x) = x^{2^i}$ which is the case (ii) in Lemma 4.1. For $n = 5$ there are several polynomials which take $\mathcal{G}_i$ to $\mathcal{G}_j$ for $1 \leq i, j \leq 2$.

We also looked at isotopic shifts of $x^3 + \mathrm{Tr}(x^9)$ by linear $L \in \mathbb{F}_2[x]$. For $7 \leq n \leq 12$, the only linear functions for which APN functions were obtained were for $n = 7$, with $L(x) = x^8$ or $L(x) = x^{16}$. In both cases, the obtained APN functions are CCZ-equivalent to $x^3 + x^{17} + x^{33} + x^{34}$, number 2.2 in Table 2.4.

Chapter 5

Generalised isotopic shift construction for APN functions

From the concept of isotopic shift presented in Chapter 4, in the following we introduce two different constructions that can be seen as generalisations of the linear isotopic shift construction when the starting function is a monomial with a Gold exponent,

$$\mathcal{G}_{i,L}(x) = xL(x)^{2^i} + x^{2^i}L(x) \tag{5.1}$$

with L a linear function. There are different possibilities to generalise function (5.1). One of them is to consider $xL_1(x)^{2^i} + x^{2^i}L_2(x)$, with L_1 and L_2 linear maps, while another one is to consider $\mathcal{G}_{i,L}$ with L not linear.

The first generalisation is studied in Section 5.1. In particular, in Theorem 5.1 we give a construction for APN functions with L_1 and L_2 q-polynomials. From this construction we obtain fifteen new APN functions for $n = 9$. Moreover, we cover some of the functions in the lists given in [66] and [102] which are not contained in any of the known infinite families.

To show the inequivalence between some of the obtained maps, we introduce in Proposition 5.2 a new EA-invariant (this invariant was also noticed independently in [72]). We recall that for quadratic APN functions CCZ-equivalence coincides with EA-equivalence. Hence EA-invariants are useful for determining CCZ-inequivalence for quadratic APN functions.

For the case when L is not necessarily linear, all known APN power functions in odd dimensions, except the Dobbertin function, can be obtained as nonlinear shifts of Gold functions, see Theorem 5.2.

5.1 On generalisations of the form $xL_1(x)^{2^i} + x^{2^i}L_2(x)$

In this section we consider the generalised isotopic shift of the form

$$F(x) = xL_1(x)^{2^i} + x^{2^i}L_2(x), \tag{5.2}$$

for L_1, L_2 linear functions. It is possible, for some results presented in Chapter 4, to get a similar result for this construction.

Given two positive integers k, m, let us consider the finite field $\mathbb{F}_{2^n}$ with $n = km$. Denoting $d = \gcd(2^m - 1, \frac{2^{km}-1}{2^m-1})$, let d' be the positive integer with the same prime factors as d , satisfying $\gcd(2^m - 1, \frac{2^{km}-1}{(2^m-1)d'}) = 1$. Now, let $U = \langle \zeta^{d'(2^m-1)} \rangle$ be the multiplicative subgroup of $\mathbb{F}_{2^n}^\star$ of order $\left(\frac{2^{km}-1}{2^m-1}\right)/d'$. Note that it is possible to write every element $x \in \mathbb{F}_{2^n}^\star$ as $x = ut$ with $u \in W$ and $t \in \mathbb{F}_{2^m}^\star$, where $W = \{\zeta^s y : y \in U,\ 0 \le s \le d' - 1\}$.
Then it is possible to obtain the following generalisation of Theorem 4.6.

Theorem 5.1. *Let $n = km$ for $m > 1$. Let $L_1(x) = \sum_{j=0}^{k-1} A_j x^{2^{jm}}$ and $L_2(x) = \sum_{j=0}^{k-1} B_j x^{2^{jm}}$ be two 2^m-polynomials. Fix i so that $\gcd(i, m) = 1$ and $F \in \mathbb{F}_{2^n}[x]$ the function given by (5.2). Then F is APN over $\mathbb{F}_{2^n}$ if and only if each of the following statements holds for any $v \in W$:*

- $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(v)}{v}$;
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} = \frac{L_2(v)}{v}$, then $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(uv)}{uv}$;*
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} \neq \frac{L_2(v)}{v}$, then $\frac{L_1(v)^{2^i}(uv)+L_2(uv)v^{2^i}}{L_1(uv)^{2^i}v+L_2(v)(uv)^{2^i}} \notin \mathbb{F}_{2^m}^\star$.*

Proof. We need that, for any $a \in \mathbb{F}_{2^n}^\star$, the function $\Delta_a(x) = F(x + a) + F(x) + F(a)$ is a 2-to-1 map, or equivalently, that $\ker(\Delta_a(ax)) = \{0, 1\}$. Since $\mathbb{F}_{2^n}^\star = W \times \mathbb{F}_{2^m}^\star$, we can rewrite $a = st$ and $x = uv$ with $s, u \in \mathbb{F}_{2^m}^\star$ and $t, v \in W$. Since L_1 and L_2 are 2^m-polynomials, we have:

$$\begin{aligned}
\Delta_a(ax) =& L_1(a)^{2^i}ax + L_2(a)(ax)^{2^i} + L_1(ax)^{2^i}a + L_2(ax)a^{2^i} \\
=& s^{2^i}L_1(t)^{2^i}st \cdot uv + sL_2(t)s^{2^i}t^{2^i} \cdot u^{2^i}v^{2^i} + s^{2^i}u^{2^i}L_1(tv)^{2^i}st + suL_2(tv)s^{2^i}t^{2^i} \\
=& us^{2^i+1}[(L_1(t)^{2^i}tv + L_2(tv)t^{2^i}) + u^{2^i-1}(L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t)].
\end{aligned}$$

Without loss of generality we can assume that $s = 1$. So, F is APN over $\mathbb{F}_{2^n}$ if and only if $u = 0$ or $u = v = 1$ are the only solutions to $\Delta_t(uvt) = 0$ for any $t \in U$.

If $v = 1$, then

$$\Delta_t(tx) = u(L_1(t)^{2^i}t + L_2(t)t^{2^i})[1 + u^{2^i-1}].$$

Since $\gcd(i,m) = 1$, x^{2^i-1} is a permutation over $\mathbb{F}_{2^m}$ and thus $\ker(\Delta_t(tx)) = \{0,1\}$ if and only if $\frac{L_1(t)^{2^i}}{t^{2^i}} \neq \frac{L_2(t)}{t}$.

Assume now that $v \neq 1$. If $L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t = 0$, then we have:

$$\Delta_t(tx) = u[(L_1(t)^{2^i}tv + L_2(tv)t^{2^i})].$$

This implies $\frac{L_1(t)^{2^i}}{t^{2^i}} \neq \frac{L_2(tv)}{tv}$.

If $L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t \neq 0$, then

$$[(L_1(t)^{2^i}tv + L_2(tv)t^{2^i}) + u^{2^i-1}(L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t)] = 0$$

implies $u^{2^i-1} = \frac{L_1(t)^{2^i}tv + L_2(tv)t^{2^i}}{L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t}$. Since x^{2^i-1} is a permutation over $\mathbb{F}_{2^m}$ this equation admits a solution different from zero if and only if $\frac{L_1(t)^{2^i}tv + L_2(tv)t^{2^i}}{L_2(t)t^{2^i}v^{2^i} + L_1(tv)^{2^i}t}$ is contained in $\mathbb{F}_{2^m}^\star$. □

The obtained APN function (5.2) is of the form

$$F(x) = (A_0^{2^i} + B_0)x^{2^i+1} + \sum_{j=1}^{k-1}[A_j^{2^i}x^{2^{i+jm}+1} + B_j x^{2^{jm}+2^i}].$$

Let us see now necessary conditions on the linear functions L_1 and L_2 for F to be APN.

Proposition 5.1. *Let n, L_1, L_2 and F be as in Theorem 5.1. If F is APN over $\mathbb{F}_{2^n}$, then the following statements hold:*

(i) $\ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i}x) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$;

(ii) $|\ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i}x^{2^i})| \leq 2$ *for any* $r, w \in \mathbb{F}_{2^n}$;

(iii) If $\ker(L_1) \cap \ker(L_2(x) + x) \neq \{0\}$, *then* $\ker(L_1(x) + x) \cap \ker(L_2) = \{0\}$;

(iv) $\ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i}x^{(2^j-1)2^i+1}) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$ *and* $j \geq 0$.

Proof. For any non-zero a, we define the function $\Delta_a(x) = F(x+a) + F(x) + F(a)$. Suppose there exists a non-zero $a \in \ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i}x)$. As

$$\Delta_a(x) = aL_1(x)^{2^i} + xL_1(a)^{2^i} + x^{2^i}L_2(a) + a^{2^i}L_2(x),$$

we clearly have $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, but since $m > 1$, this contradicts $|\ker(\Delta_a)| = 2$. This establishes (i).

For (ii), suppose $\{0, a, b\} \subseteq \ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i} x^{2^i})$. Then

$$\Delta_a(b) = a(rb) + b(ra) + a^{2^i}(w^{2^i} b^{2^i}) + b^{2^i}(w^{2^i} a^{2^i}) = 0.$$

Next suppose $a \in \ker(L_1) \cap \ker(L_2(x) + x)$. Then we have $\Delta_a(x) = a(L_1(x) + x)^{2^i} + a^{2^i} L_2(x)$. Clearly any $b \in \ker(L_1(x) + x) \cap \ker(L_2)$ satisfies $\Delta_a(b) = 0$. Since f is APN, $\ker(\Delta_a) = \{0, a\}$, so that $\ker(L_1(x) + x) \cap \ker(L_2) \subset \{0, a\}$. However, $\ker(L_1) \cap \ker(L_1(x) + x) = \{0\}$, so that no non-zero element of $\mathbb{F}_{2^n}$ can lie in both $\ker(L_1) \cap \ker(L_2(x) + x)$ and $\ker(L_1(x) + x) \cap \ker(L_2)$. This establishes (iii).

For (iv), suppose $a \in \ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i} x^{(2^j-1)2^i+1})$ is non-zero. Then for any $t \in \mathbb{F}_{2^m}$ we have

$$\begin{aligned}\Delta_a(ta) &= ar^{2^i} t^{2^i} a^{2^{j+i}} + tar^{2^i} a^{2^{j+i}} + (ta)^{2^i} r^{2^i} a^{(2^j-1)2^i+1} + a^{2^i} r^{2^i} ta^{(2^j-1)2^i+1} \\ &= r^{2^i} a^{2^{j+i}+1} \left(t^{2^i} + t + t^{2^i} + t\right) = 0,\end{aligned}$$

so that $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, a contradiction. □

5.1.1 The case $n = 8$

Applying the construction of Theorem 5.1 in dimension 8 with $k = 4$ and $m = 2$, restricting the coefficients of L_1 and L_2 to the subfield $\mathbb{F}_{2^4}$, we obtained several APN functions given in Table 2.5 and one in [102, Table 5] which have not been previously identified as a part of any APN family. The functions mentioned are listed in Table 5.1.

The following results were obtained for $n = 8$.

- Considering generalised isotopic shifts of x^3 it is possible to obtain maps EA-equivalent to nos. 1.2, 1.5, 1.7, 1.8, 1.10, 1.11, 1.12, 1.16, 1.17, 3.1 in Table 2.5 and to no. 9 in Table 5 [102].
- Considering generalised isotopic shifts of x^9 it is also possible to obtain maps EA-equivalent to no. 1.3 in Table 2.5.

Remark 5.1. *Function no. 9 in Table 5 [102] has the same CCZ-invariants (Γ-rank, Δ-rank and $|\mathcal{M}_{G_F}|$) as function number 1.9 in Table 2.5 (we note that the value of the Γ-rank given in [102, Table 6] is not correct, indeed the function has Γ-rank=14034,*

Table 5.1: APN polynomials over $\mathbb{F}_{2^8}$ derived from Theorem 5.1. They all correspond to known but unclassified cases.

Functions	equiv. to no. in Table 2.5
$\zeta^{136}x^{66} + \zeta^{85}x^{33} + \zeta^{85}x^{18} + \zeta^{102}x^9 + \zeta^{221}x^6 + x^3$	no. 9 in Table 5 [102]
$\zeta^{102}x^{66} + \zeta^{204}x^9 + x^3$	1.2
$\zeta^{153}x^{129} + \zeta^{204}x^{66} + \zeta^{170}x^{33} + \zeta^{85}x^{18} + \zeta^{204}x^6 + x^3$	1.5
$\zeta^{102}x^{129} + \zeta^{153}x^{66} + \zeta^{170}x^{33} + \zeta^{221}x^{18} + \zeta^{221}x^9 + \zeta^{187}x^6 + x^3$	1.7
$x^{66} + \zeta^{85}x^{33} + x^{18} + x^9 + x^3$	1.8
$\zeta^{204}x^{129} + \zeta^{170}x^{66} + \zeta^{153}x^{33} + \zeta^{85}x^{18} + \zeta^{153}x^9 + \zeta^{17}x^6 + x^3$	1.10
$\zeta^{204}x^{66} + x^{33} + x^{18} + \zeta^{153}x^9 + x^3$	1.11
$\zeta^{170}x^{129} + \zeta^{204}x^{66} + \zeta^{17}x^{33} + \zeta^{68}x^{18} + \zeta^{221}x^9 + \zeta^{204}x^6 + x^3$	1.12
$\zeta^{238}x^{129} + \zeta^{204}x^{66} + \zeta^{119}x^{33} + \zeta^{68}x^{18} + \zeta^{85}x^9 + \zeta^{119}x^6 + x^3$	1.16
$\zeta^{17}x^{129} + \zeta^{85}x^{66} + \zeta^{34}x^{33} + \zeta^{34}x^{18} + \zeta^{187}x^9 + \zeta^{187}x^6 + x^3$	1.17
$\zeta^{17}x^{129} + \zeta^{238}x^{66} + \zeta^{153}x^{33} + \zeta^{85}x^{18} + \zeta^{238}x^9 + \zeta^{102}x^6 + x^3$	3.1
$\zeta^{153}x^{129} + \zeta^{221}x^{72} + \zeta^{170}x^{33} + \zeta^{102}x^{24} + x^{12} + x^9 + \zeta^{136}x^3$	1.3

see Table 2.7 for the correct values).

Since two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [105], the CCZ-inequivalence between these two functions can be obtained by checking another invariant with respect to EA-equivalence that we shall introduce in the next subsection.

5.1.2 A new EA-equivalence invariant

Let $S(F) = \{b \in \mathbb{F}_{2^n} : \exists a \in \mathbb{F}_{2^n} \text{ s.t. } \mathcal{W}_F(a,b) = 0\}$, where $\mathcal{W}_F(a,b)$ is the Walsh coefficient of F in a and b. This set was used in [25] to study some relations between CCZ-equivalence and EA-equivalence.

It is easy to check that:

- if $F' = F + L$ with L linear, then $S(F) = S(F')$.
- If $F' = A_1 \circ F \circ A_2$ with A_1, A_2 affine permutations, then $S(F') = \bar{A}_1^*(S(F))$, where $\bar{A}_1^*$ is the adjoint operator of the linear map $A_1(x) + A_1(0)$.

From this we have the following.

Proposition 5.2. *Let N_i be the number of the $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$ contained in $S(F)$ of dimension i. Then, the values N_i for $i = 1, \ldots, n$ are EA-invariant.*

Proof. If F' is EA-equivalent to F, then there exist A_1, A_2 affine permutations and L linear such that $F'(x) = A_1 \circ F \circ A_2(x) + L(x)$. From the arguments above, denoting $\bar{A}_1(x) = A_1(x) + A_1(0)$ we have that $S(F') = \bar{A}^*(S(F))$. □

Remark 5.2. *We computed the values N_i for the two functions and we got $N_1 = 86$, $N_2 = 340$ and $N_3 = 4$ for function no. 9 in [102, Table 5], and $N_1 = 86$, $N_2 = 340$ and $N_3 = 8$ for function no. 1.9 in Table 2.5. Thus from Proposition 5.2 we have that the two functions are not EA-equivalent.*

Remark 5.3. *Note that when n is odd, a quadratic APN function F is AB (i.e. for all $b \in \mathbb{F}_{2^n}^\star$ we have $\{\mathcal{W}_F(a,b) : a \in \mathbb{F}_{2^n}\} = \{0, \pm 2^{(n+1)/2}\}$), which implies $S(F) = \mathbb{F}_{2^n}$. Thus, this new invariant cannot be used for testing the CCZ-equivalence of quadratic APN functions in the case n odd.*

Remark 5.4. *In fact, this EA-invariant was tackled independently by Göloğlu and Pavlů in [72]. In their work, they focused on plateaued functions and looked at the subspaces in the set $\{b s.t. \mathcal{W}_F(0,b) \neq \pm 2^{n/2}\}$ (n even). For plateaued functions, this set coincides with $S(F)$.*

Remark 5.5. *A similar invariant was introduced in [39] where the authors consider the set*

$$\mathcal{Z}_F = \{(\alpha,\beta) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \; s.t. \; \mathcal{W}_F(\alpha,\beta) = 0\} \cup \{0,0\}.$$

Lemma 2 in [39] states that for two CCZ-equivalent functions F and G, there exists a linear permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\mathcal{L}(\mathcal{Z}_F) = \mathcal{Z}_G$. Therefore the number of vector subspaces of $\mathcal{Z}_F$ of a fixed dimension i is invariant under CCZ-equivalence. Notice that the set $S(F)$ is the projection, over one coordinate, of the set $\mathcal{Z}_F$ and the invariants introduced in Proposition 5.2 could be not invariant under CCZ-equivalence. From [39] we have also the following: setting $\mathcal{V}^\perp = \{(0,x) : x \in \mathbb{F}_{2^n}\}$ and Σ_F the set of all vector spaces of dimension n in $\mathcal{Z}_F$, the values

$$n_i = |\{V \in \Sigma_F : \dim(V') = i\}|$$

are EA-invariants, where V' is its projection of V on $\mathcal{V}^\perp$ [1].

[1] In general we have $n_i \leq N_i$. Consider for example $i = 1$. Then N_1 corresponds to the number of elements $b \neq 0$ such that there exists an a for which $\mathcal{W}_F(a,b) = 0$. Instead n_1 is the number of elements $b \neq 0$ such that $\mathcal{W}_F(a,b) = 0$ for at least 2^{n-1} different elements a.

5.1.3 The case $n = 9$

For the case $k = m = 3$ we consider the generalised linear shift as in (5.2) with L_1 and L_2 having coefficients in the subfield $\mathbb{F}_{2^3}$. In Table 4.1 we have listed all known APN functions for $n = 9$. In Table 5.2, we list all new APN functions obtained from Theorem 5.1. We observe that the family of Theorem 5.1 covers the only known example of an APN function for $n = 9$, function N. 11 of Table 4.1, which had not been previously identified as part of an APN family. Hence, currently, all known APN functions for $n = 9$ are now covered by an APN family. Note that this latter function was not obtained from the approach studied in [66] (it does not belong to a switching class of a previously known APN map). Moreover, Table 5.2 indicates 15 new CCZ-inequivalent APN functions, all obtained from Theorem 5.1. We include, for each function, the CCZ-invariants Γ-rank, Δ-rank and $|\mathcal{M}_{G_F}|$.

Table 5.2: CCZ-inequivalent APN polynomials over $\mathbb{F}_{2^9}$ derived from Theorem 5.1. All, except for the first one, are either new or correspond to the one known but unclassified case.

$\mathcal{G}_i$	Function	Eq. to known ones	Γ-rank	Δ-rank	$\lvert\mathcal{M}_{G_F}\rvert$
$i=1$	$x^{129}+\zeta^{146}x^{66}+x^{17}+\zeta^{365}x^{10}+x^3$	eq. to N. 12 in Table 4.1	48596	944	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{219}x^{129}+\zeta^{292}x^{66}+\zeta^{292}x^{17}+\zeta^{219}x^{10}+x^3$	new	48506	936	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{292}x^{66}+\zeta^{365}x^{17}+\zeta^{73}x^{10}+x^3$	new	48610	938	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{365}x^{66}+\zeta^{146}x^{17}+\zeta^{365}x^{10}+x^3$	new	48612	938	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{219}x^{66}+\zeta^{292}x^{17}+\zeta^{73}x^{10}+x^3$	new	48548	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+\zeta^{365}x^{66}+\zeta^{73}x^{17}+\zeta^{73}x^{10}+x^3$	new	48548	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+\zeta^{438}x^{66}+\zeta^{292}x^{10}+x^3$	new	48506	936	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{365}x^{129}+x^{66}+\zeta^{438}x^{10}+x^3$	new	48604	928	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+\zeta^{292}x^{66}+x^{10}+x^3$	new	48564	942	$2^9\cdot 3\cdot 7$
$i=1$	$\zeta^{73}x^{129}+x^{66}+\zeta^{219}x^{17}+x^3$	new	48604	928	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{438}x^{68}+\zeta^{438}x^{12}+x^5$	new	48546	938	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{365}x^{33}+\zeta^{365}x^{12}+x^5$	eq. to 8.1 in Table 2.6	48608	938	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{73}x^{257}+\zeta^{146}x^{68}+x^{33}+x^5$	new	48564	942	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{365}x^{257}+\zeta^{438}x^{68}+\zeta^{365}x^{33}+\zeta^{438}x^{12}+x^5$	new	48594	944	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{146}x^{257}+\zeta^{219}x^{68}+\zeta^{73}x^{33}+x^{12}+x^5$	new	48520	932	$2^9\cdot 3\cdot 7$
$i=2$	$\zeta^{73}x^{257}+\zeta^{219}x^{68}+\zeta^{365}x^{33}+x^5$	new	48602	938	$2^9\cdot 3\cdot 7$
$i=4$	$\zeta^{292}x^3+\zeta^{146}x^{80}+\zeta^{73}x^{24}+x^{17}$	new	48520	932	$2^9\cdot 3\cdot 7$

The CCZ-inequivalence of some of these functions was obtained by checking with MAGMA the equivalence of some linear code which can be associated to an APN function (see [22]).

5.2 Isotopic shifts with nonlinear functions

In this section we consider the case when the function L used in the shift is not necessarily linear.

In Proposition 4.2, it has been proved that, in even dimension, an isotopic shift of the Gold function with a linear function defined over $\mathbb{F}_2[x]$ cannot be APN. In the following, we show that for any quadratic function F in even dimension, we cannot obtain APN functions by shifting F with a polynomial whose coefficients belong to $\mathbb{F}_2$.

Proposition 5.3. *For two integers k and m let $n = km$ and $q = 2^k$. Consider a function $F \in \mathbb{F}_{2^n}[x]$ of the form*

$$F(x) = \sum_{i<j} b_{ij} x^{q^i+q^j} + \sum_i b_i x^{2^i} + c,$$

If $\mathbb{F}_4 \subseteq \mathbb{F}_{2^n}$ or $k > 1$, then any isotopic shift F_L with $L \in \mathbb{F}_{2^k}[x]$ cannot be APN. In particular, this holds for any quadratic function $F \in \mathbb{F}_{2^n}[x]$ with n even and $L \in \mathbb{F}_2[x]$.

Proof. For F and L as outlined, we have

$$F_L(x) = \sum_{i<j} b_{ij}[x^{q^i} L(x)^{q^j} + x^{q^j} L(x)^{q^i}] + c$$

and $L(x^q) = L(x)^q$. Note that for any $x \in \mathbb{F}_{2^k}$, $F_L(x) = c$. For $a \in \mathbb{F}_{2^n}$, we set $\Delta_a(x) = F_L(x+a) + F_L(x) + F_L(a)$.

If $k > 1$, then $\Delta_a(x) = c$ for all $x, a \in \mathbb{F}_{2^k}$, so that F_L is not APN. If $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\} \subseteq \mathbb{F}_{2^n}$, then consider $\Delta_\alpha(x)$. Clearly $\Delta_\alpha(0) = c$, while it is easily observed that $\Delta_\alpha(\alpha+1) = \Delta_\alpha(1)$. We have

$$\begin{aligned}
\Delta_\alpha(\alpha+1) =& F_L(\alpha+1) + F_L(\alpha) + c \\
=& c + \sum_{i<j} b_{ij}[L(\alpha+1)^{q^i}(\alpha+1)^{q^j} + (\alpha+1)^{q^i} L(\alpha+1)^{q^j} \\
& + L(\alpha)^{q^i}\alpha^{q^j} + \alpha^{q^i} L(\alpha)^{q^j}] \\
=& c + \sum_{i<j} b_{ij}[L(\alpha+1)(\alpha+1)^{q^j-i} + (\alpha+1)L(\alpha+1)^{q^j-i} \\
& + L(\alpha)\alpha^{q^j-i} + \alpha L(\alpha)^{q^j-i}]^{q^i}.
\end{aligned}$$

When $j-i$ is odd and $\mathbb{F}_4 \not\subseteq \mathbb{F}_{2^k}$, the term in the sum is zero as $\alpha^{q^j-i} = \alpha^2 = \alpha+1$, $L(\alpha)^{q^j-i} = L(\alpha+1)$ and $L(\alpha+1)^{q^j-i} = L(\alpha)$. If $j-i$ even or $\mathbb{F}_4 \subseteq \mathbb{F}_{2^k}$, then the term in the sum is again zero due to the fact that $\alpha^{q^j-i} = \alpha$ and $L(\alpha)^{q^j-i} = L(\alpha)$. In either case, we have $\Delta_\alpha(x) = c$ for $x = 0, 1, \alpha+1$, so F_L is not APN. □

5.2.1 Nonlinear shift for the Gold functions

If we consider an isotopic shift of a Gold function without the restriction that L is a linear function, then $L(x) = \sum_{j=0}^{2^n-1} c_j x^j$ and the isotopic shift will be of the form

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + xL(x)^{2^i}. \tag{5.3}$$

We have $\mathcal{G}_{i,L}(x^2)^{2^{-1}} = x^{2^i} M(x) + xM(x)^{2^i}$, where $M(x) = \sum c_j^{2^{-1}} x^j$, and also $\zeta^{-2^i-1}\mathcal{G}_{i,L}(\zeta x) = x^{2^i} N(x) + xN(x)^{2^i}$, where $N(x) = \sum c_j \zeta^{j-1} x^j$. Hence we obtain the following.

Proposition 5.4. *Let $\mathbb{F}_{2^n}^\star = \langle \zeta \rangle$. Assume that $\mathcal{G}_{i,L}$ is constructed with $L(x) = \sum_{j=0}^{2^n-1} c_j x^j$. Then, for any integers k, t, we have that $\mathcal{G}_{i,L}$ is linear equivalent to $\mathcal{G}_{i,M}$, where $M(x) = \sum_{j=0}^{2^n-1} (c_j \zeta^{k(j-1)})^{2^t} x^j$.*

As for the linear shifts, it is possible to restrict the search of one possible non-zero coefficient of the function.

In the following table we recall the list of known APN power maps (already presented in Table 2.1). In odd dimension it is possible to obtain all power

Table 5.3: Known APN power functions x^d over $\mathbb{F}_{2^n}$

Name	Exponent d	Conditions	Degree	Proven
Gold	$2^i + 1$	gcd(i,n)=1	2	[73, 92]
Kasami	$2^{2i} - 2^i + 1$	gcd(i,n)=1	i+1	[75, 76]
Welch	$2^t + 3$	$n = 2t + 1$	3	[60]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	$\frac{t+2}{2}$ t+1	[59]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[7, 92]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[61]

APN functions, except the Dobbertin functions, as the isotopic shifts of a Gold function by a monomial.

Theorem 5.2. *Over $\mathbb{F}_{2^n}$ with n an odd integer, let F be any known APN power function outside the class of Dobbertin functions. Then there exists a monomial $L(x) = ax^d$ and a Gold function $\mathcal{G}_i = x^{2^i+1}$ such that the shift $\mathcal{G}_{i,L}$ is EA-equivalent to F.*

Proof. As shown in Table 5.3, excluding the Dobbertin function, the known APN power functions are the Gold functions, the Kasami functions, the Welch

function, the Niho functions and the inverse function. In the following we show that it is possible for any of the mentioned functions, to construct an isotopic shift of a Gold function that is EA-equivalent to it.

1. Consider the Kasami function $x^{2^{2t}-2^t+1}$. If t is odd, then let i be an integer such that $n = 2i + t$. Then, considering $L(x) = ax^{2^{n-i}+2^{n-i+1}...+2^{n-i+t-1}}$ we have
$$\begin{aligned}\mathcal{G}_{i,L}(x) &= a^{2^i}x^{2^t} + ax^{2^{n-i}+2^{n-i+1}...+2^{n-i+t-1}+2^i}\\ &= a^{2^i}x^{2^t} + ax^{2^i(2^t+2^{t+1}...+2^{2t-1}+1)}\\ &= a^{2^i}x^{2^t} + ax^{2^i(2^{2t}-2^t+1)}.\end{aligned}$$
If t is even, let i be an integer such that $t = 2i$. Then, with $L(x) = ax^{2^i+2^{i+1}+...+2^{3i-1}}$ we have $\mathcal{G}_{i,L}(x) = a^{2^i}x^{2^{2t}-2^t+1} + ax^{2^{3i}}$.

2. For the inverse function, x^{2^n-2}, considering $L(x) = ax^{2^{2t}-2}$, where t is such that $n = 2t + 1$, we have $\mathcal{G}_{1,L}(x) = a^2x^{2(2^n-2)} + ax^{2^{2t}}$.

3. Let $n = 2t + 1$ and consider the Welch function x^{2^t+3}. If t is odd, then consider i such that $t = 2i - 1$. With $L(x) = ax^{2^i+2^{2i+1}}$ we obtain $\mathcal{G}_{i,L}(x) = a^{2^i}x^{2^{2i}(2^{2i-1}+3)} + ax^{2^{i+2}}$. If t is even, then consider i such that $t = 2i$. Using $L(x) = ax^{2^{3i+1}+2^{3i+2}}$ we obtain $\mathcal{G}_{i,L}(x) = a^{2^i}x^4 + ax^{2^{3i+1}(2^{2i}+3)}$.

4. For $n = 2t + 1$, with t odd, let $t = 2i - 1$. Then, with $L(x) = ax^{2^n-2^i}$ we obtain that
$$\begin{aligned}\mathcal{G}_{i,L}(x) &= a^{2^i}x^{2^i-2^{2i}+1} + ax = a^{2^i}x^{2^{2i}(2^{-i}+2^{-2i}-1)} + ax\\ &= a^{2^i}x^{2^{2i}(2^{3i-1}+2^{2i-1}-1)} + ax = a^{2^i}x^{2^{2i}(2^{(3t+1)/2}+2^t-1)} + ax\end{aligned}$$
is equivalent to the Niho function (indeed $(3t+1)/2 = (6i-3+1)/2 = 3i-1$). If t is even, let $t = 2i$. Then with $L(x) = ax^{2^{n-i}+2^{n-i+1}...+2^{n-1}}$
$$\begin{aligned}\mathcal{G}_{i,L}(x) = &\ a^{2^i}x^{2^i} + ax^{2^{n-i}+2^{n-i+1}...+2^{n-1}+2^i}\\ = &\ a^{2^i}x^{2^i} + ax^{2^{n-i}(1+2...+2^{i-1}+2^{2i})}\\ = &\ a^{2^i}x^{2^i} + ax^{2^{n-i}(2^i-1+2^{2i})}\end{aligned}$$
is equivalent to the Niho function.

5. Let $n = 2i + 1$ and j be an integer such that $\gcd(n, j) = 1$. Then with $L(x) = ax^{2^{i+j}-2^i}$
$$\begin{aligned}\mathcal{G}_{i,L}(x) &= a^{2^i}x^{2^{2i+j}-2^{2i}+1} + ax^{2^{i+j}} = a^{2^i}x^{2^{2i}(2^j+2^{-2i}-1)} + ax^{2^{i+j}}\\ &= a^{2^i}x^{2^{2i}(2^j+1)} + ax^{2^{i+j}}\end{aligned}$$

is equivalent to the Gold function with parameter j.

□

Remark 5.6. *From computational results, for n even, it seems that it is not possible to obtain APN functions as the isotopic shifts of a Gold map by (non-linear) monomials. The search has been performed for* $n = 4,6,8,10$*, considering also non-APN Gold exponents.*

Chapter 6

On equivalence between known families of quadratic APN functions

In Table 6.1 we recall the fifteen known infinite families of quadratic APN polynomials CCZ-inequivalent to power functions, listed previously in Table 2.2, with the addition of the results from Chapter 4 and Chapter 5 (family C13). Note that there is also a family of APN functions constructed by Göloğlu [70] which was proven to be CCZ-equivalent to Gold power functions in [35]. In this chapter we reduce the list of known families of polynomial APN functions by excluding all equivalent cases. Indeed, we show that the class of trinomial APN functions introduced in [26], family C3, and the class of multinomials studied in [17], family C11, are equivalent. Moreover, we prove that also their generalisations given in [62] coincide with the original ones. Finally we show that these classes can be reduced to the hexanomials introduced in [26], family C4. Note that CCZ-equivalence between APN quadratic functions reduces to EA-equivalence [105], so all the equivalences that we prove in the next sections are EA-equivalences. According to the table of CCZ-inequivalent functions which arise from known APN families (in dimensions up to 11) [35], the remaining families of APN functions are pairwise inequivalent in general. We present a complete list of the 13 known families of APN polynomials, which are pairwise CCZ-inequivalent, in Table 6.2.

6.1 On some known families

Note that functions in Table 6.1 are given with different choices for parameters and coefficients, which in some cases can provide a huge number of different functions. In [35], the authors present a table of all possible pairwise CCZ-

Table 6.1: Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions	Conditions	In
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}$, $i=sk \mod p$, $m=p-i$, $n\geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[29]
C3	$x^{2^{2i}+2^i}+cx^{q+1}+dx^{q(2^{2i}+2^i)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $\gcd(2^i+1,q+1)\neq 1$, $dc^q+c\neq 0$, $d\notin\{\lambda^{(2^i+1)(q-1)} : \lambda\in\mathbb{F}_{2^n}\}$, $d^{q+1}=1$	[26]
C4	$x(x^{2^i}+x^q+cx^{2^iq})$ $+x^{2^i}(c^qx^q+sx^{2^iq})+x^{(2^i+1)q}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}$, $s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q$, $X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[26]
C5	$x^3+a^{-1}Tr(a^3x^9)$	$a\neq 0$	[30]
C6	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$	$3\mid n$, $a\neq 0$	[31]
C7	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$	$3\mid n$, $a\neq 0$	[31]
C8-C10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+$ $vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in\mathbb{F}_{2^k}$, $vw\neq 1$, $3\mid(k+s)$ u primitive in $\mathbb{F}_{2^n}^*$	[17]
C11	$dx^{2^i+1}+d^qx^{q(2^i+1)}+$ $cx^{q+1}+\sum_{s=1}^{m-1}\gamma_s x^{2^s(q+1)}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, i,m odd, $c\notin\mathbb{F}_{2^m}$, $\gamma_s\in\mathbb{F}_{2^m}$, d not a cube	[17]
C12	$(x+x^q)^{2^i+1}+$ $u'(ux+u^qx^q)^{(2^i+1)2^j}+$ $u(x+x^q)(ux+u^qx^q)$	$q=2^m$, $n=2m$, $m\geq 2$ even, $\gcd(i,m)=1$ and j even u primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not a cube	[112]
C13	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$	$n=km$, $\gcd(n,i)=1$ $L_1(x),L_2(x)$ 2^m-polynomials satisfing the conditions in Theorem 5.1, Chapter 5	[24]
C14	$ut(x)(x^q+x)+t(x)^{2^{2i}+2^{3i}}+$ $at(x)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$ $a,b\in\mathbb{F}_{2^m}$, $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$, $u\notin\mathbb{F}_{2^m}$ and $t(x)=u^qx+x^qu$	[99]
C15	$x^3+ax^{2^k(2^i+1)}$ $+bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$	$n=2m=10$, $(a,b,c)=(\beta,1,0)$, $i=3$, $k=2$, $\mathbb{F}_4^*=\langle\beta\rangle$	[34]
		$n=2m$, m odd, $3\not\mid m$, $(a,b,c)=(\beta,\beta^2,1)$, $\mathbb{F}_4^*=\langle\beta\rangle$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \mod n\}$	

inequivalent functions which can be derived from the known families of APN functions, up to dimension $n=11$. According to this table, families C3 and C11 coincide on small dimensions and are contained in C4.

We recall the conditions for the families C3 and C11 in the following results.

Theorem 6.1 ([26]). *Let $n=2m$ with $m>1$. Let i be such that $\gcd(i,m)=1$. Let F*

be the function over $\mathbb{F}_{2^n}$ defined by

$$cx^{2^m+1} + x^{2^{2i}+2^i} + dx^{2^m(2^{2i}+2^i)} \tag{C3}$$

where $c,d \in \mathbb{F}_{2^n}$ are such that $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+1)(2^m-1)} : \lambda \in \mathbb{F}_{2^n}\}$ and $dc^{2^m} + c \neq 0$. Then, F is APN over $\mathbb{F}_{2^n}$.

Theorem 6.2 ([17]). *Let $n = 2m$ with m an odd integer. Let i be an odd integer such that $\gcd(i,m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1} + \sum_{s=1}^{m-1} \gamma_s x^{2^s(2^m+1)} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)} \tag{C11}$$

where $c \notin \mathbb{F}_{2^m}$, $d \in \mathbb{F}_{2^n}$ not a cube and $\gamma_s \in \mathbb{F}_{2^m}$ for each s. Then, F is APN over $\mathbb{F}_{2^n}$.

Remark 6.1. *Note that, considering family C11, for i such that $\gcd(i,m) = 1$, with m odd, the condition given in Theorem 6.2, that is i odd and d not a cube, is equivalent to requesting just $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, if i is odd, then $\{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \{x^3 : x \in \mathbb{F}_{2^{2m}}\}$. If i is even, recalling that (cf. Lemma 11.1 in [89])*

$$\gcd(2^i+1, 2^n-1) = \begin{cases} 1 & \text{if } \gcd(i,n) = \gcd(2i,n) \\ 2^{\gcd(i,n)} + 1 & \text{if } 2\gcd(i,n) = \gcd(2i,n), \end{cases}$$

we get $\{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \mathbb{F}_{2^{2m}}$, implying existence of no choice for d.

Moreover, for family C3 we have that coefficients c and d, satisfying the constraints in Theorem 6.1, exist if and only if $\gcd(2^i+1, 2^m+1) \neq 1$ (see [26]). This implies that m is odd since i and m are coprime (it can be easily deduced from $\gcd(2^{2i}-1, 2^{2m}-1) = 2^{\gcd(2i,2m)} - 1 = 3$). Moreover, as above, if i is even we have no choice for d, so also i must be odd.

In [62], the authors generalise these two families. In the following, we report the statements of the results given in [62]. However, as we will show in the next section, the parameters of these functions need some adjustments.

Family C11*: Let $n = 2m$, with $m > 1$. Let i,j be such that $i > j$ and $\gcd(i-j,m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}), \tag{6.1}$$

where $c \notin \mathbb{F}_{2^m}$, d is not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$, $\gamma_\ell \in \mathbb{F}_{2^m}$ for all ℓ and $L(x) = \sum_{k\in K} x^{2^k}$ such that $\{0,1\} \neq K \subseteq \{0,...,n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Family C3*: Let $n = 2m$, with $m > 1$. Let i, j be such that $i > j$ and $\gcd(i-j, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(x^{2^i+2^j}) + dL(x^{2^m(2^i+2^j)}), \tag{6.2}$$

where $c, d, \gamma_\ell \in \mathbb{F}_{2^n}$ are such that $d^{2^m+1} = 1$, $d \notin \{\lambda^{(2^i+2^j)(2^m-1)} : \lambda \in \mathbb{F}_{2^n}\}$, $dc^q + c \neq 0$, $d = \gamma_\ell^{1-2^m}$ for all ℓ and $L(x) = \sum_{k\in K} x^{2^k}$ such that $\{0,1\} \neq K \subseteq \{0,...,n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Note that, these types of functions are of the form (or can be reduced to)

$$F(x) = wx^{2^m+1} + Q(x), \tag{6.3}$$

where Q is a quadratic function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ and $w \notin \mathbb{F}_{2^m}$. This type of construction for APN and differentially 4-uniform functions has been further studied in [41, 43].

Remark 6.2. *The general idea used in this chapter for proving the equivalence between these families is based on the fact that for any element w not in $\mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^n} = w\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. At this point, considering two functions as in (6.3)*

$$F_1(x) = w_1x^{2^m+1} + Q_1(x), \quad F_2(x) = w_2x^{2^m+1} + Q_2(x),$$

to prove the equivalence we need to individuate a linear permutation L for which $L(F_1(x)) = F_2(x)$. Since $\mathbb{F}_{2^n} = w_1\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m} = w_2\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ the action of L can be given by defining the images of $w_1\mathbb{F}_{2^m}$ and of $\mathbb{F}_{2^m}$ separately. In particular, L should be such that the vector space $w_1\mathbb{F}_{2^m}$ is mapped into $w_2\mathbb{F}_{2^m}$ with the trivial action $w_1y \mapsto w_2y$ (for any $y \in \mathbb{F}_{2^m}$) and $L(Q_1(x)) = Q_2(x)$.

Before proving the equivalence of these families, we correct the results of [62]. Indeed, the first family when m is even cannot be APN. While, the second one, in addition to restriction of m to be odd, in general is not APN if $L(x) \neq x^{2^k}$ (tested by MAGMA in small dimensions).

6.1.1 Correction of family C11* and family C3*

For the family C11* we have the following result.

Proposition 6.1. *Let $n = 2m$. Let F be a function defined over $\mathbb{F}_{2^n}$ as in (6.1). Then, if m is even F cannot be APN.*

Proof. Consider the function

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_l x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}),$$

satisfying the properties given in (6.1).

By hypothesis, $L(x) = x(\sum_{k\in K} x^{2^k-1})$ where $\{0,1\} \neq K \subseteq \{0,\ldots,n\}$ and $\sum_{k\in K} x^{2^k-1}$ is irreducible over $\mathbb{F}_{2^n}$. Since $\deg(\sum_{k\in K} x^{2^k-1}) > 1$ we have that 0 is the only root of $L(x) = 0$. This implies that L is a linear permutation and, moreover, $L(x^{2^m}) = L(x)^{2^m}$. To prove that F cannot be APN for m even we need to prove that there exists $a \in \mathbb{F}_{2^n}$ non-zero such that

$$\Delta_a(x) = F(x) + F(x+a) + F(a) = 0 \tag{6.4}$$

admits more than two solutions.

Suppose that x is a solution of (6.4). Then we obtain

$$\Delta_a(x) + \Delta_a(x)^{2^m} = (c + c^{2^m})(x^{2^m} a + a^{2^m} x) = 0.$$

Since $c \notin \mathbb{F}_{2^m}$ we have $x^{2^m} a + a^{2^m} x = 0$, which implies $x = at$ for some $t \in \mathbb{F}_{2^m}$. Substituting $x = at$ in (6.4) we have

$$L((da^{2^i+2^j} + d^{2^m} a^{2^m(2^i+2^j)})(t^{2^i} + t^{2^j})) = 0.$$

Since L is a linear permutation, this implies that $(da^{2^i+2^j} + d^{2^m} a^{2^m(2^i+2^j)})(t^{2^i} + t^{2^j}) = 0$. Now, from the fact that $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$ the authors in [62] claim that $(da^{2^i+2^j} + d^{2^m} a^{2^m(2^i+2^j)}) \neq 0$ for all non-zero a. However, while for m odd the condition $d \notin \{x^{2^i+2^j} : x \in \mathbb{F}_{2^n}\}$ is sufficient to guarantee $da^{2^i+2^j} \notin \mathbb{F}_{2^m}$, such claim is incorrect when m is even.

Indeed, if m is even, then $3 \mid (2^m - 1)$ and $3 \nmid (2^m + 1)$. Now, let $d = \alpha^k$, with α a primitive element of $\mathbb{F}_{2^n}$, and k some integer. Since $\gcd(i-j, m) = 1$ we have that $i - j$ is odd and thus $\gcd(2^{i-j} + 1, 2^n - 1) = 3$. So, finding a such that $da^{2^i+2^j} \in \mathbb{F}_{2^m}$ is equivalent to finding a' such that $da'^3 \in \mathbb{F}_{2^m}$. Let $a' = \alpha^h$, we want to determine h such that $(2^m + 1) \mid (3h + k)$. Suppose $d \notin \mathbb{F}_{2^m}$, otherwise

a' can be just 1. We have two cases, $k \equiv 1,2 \mod 3$. If $k \equiv 1 \mod 3$, then $3h+k = 3(h+k')+1$ for some k'. Since m is even $2^{m+1}+1$ is equal to $3h'$ for some h', thus considering $h = h'-k'$ we would have $3h+k = 3(h+k')+1 = 3h'+1 = 2(2^m+1)$. If $k \equiv 2 \mod 3$, then $3h+k = 3(h+k')+2$ for some k'. Since m is even 2^m-1 is equal to $3h'$ for some h', thus considering $h = h'-k'$ we would have $3h+k = 3(h+k')+2 = 3h'+2 = 2^m+1$. This concludes our proof. □

We can note that, in the previous proof, for analysing the solutions of (6.4), we used only the fact that L is a linear permutation with coefficients over $\mathbb{F}_{2^m}$. So, we restate the conditions for family C11* as follows.

Theorem 6.3. *Let $n = 2m$ with m odd. Let i, j be such that $i > j$ and $\gcd(i-j, m) = 1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(dx^{2^i+2^j} + d^{2^m} x^{2^m(2^i+2^j)}), \qquad \text{(C11*)}$$

where $c \notin \mathbb{F}_{2^m}$, d is not in $\{x^{2^i+2^j} : x \in \mathbb{F}_{2^{2m}}\}$, $\gamma_\ell \in \mathbb{F}_{2^m}$ for all ℓ and L a linear permutation with coefficients over $\mathbb{F}_{2^m}$. Then, F is APN over $\mathbb{F}_{2^n}$.

Remark 6.3. *For the second family C3*, some steps of the proof in [62, Theorem 2] do not work in general. When $L(x) = x^{2^k}$, family (C3*) results to be APN, this can be proved following the steps given in [62], which became legit when L has only one monomial.*
While if L is not of type x^{2^k}, from computational tests done using MAGMA in small dimensions, the function in (6.2) in general is not APN.

More precisely, let

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + L(x^{2^i+2^j}) + dL(x^{2^m(2^i+2^j)}),$$

satisfying the properties given in (6.2) . Then, F is APN if and only if the equation $\Delta_a(x) = F(x) + F(x+a) + F(a) = 0$ admits at most two solutions for any non-zero $a \in \mathbb{F}_{2^n}$. It is is easy to check that $\Delta_a(x) + d\Delta_a(x)^{2^m} = (c + dc^{2^m})(x^{2^m}a + a^{2^m}x)$. Thus, if x is a solution of $\Delta_a(x) = 0$ we have that $x = at$ for some $t \in \mathbb{F}_{2^m}$. Substituting $x = at$, we obtain

$$L(a^{2^i+2^j}(x^{2^i} + x^{2^j})) + dL(a^{2^m(2^i+2^j)}(x^{2^i} + x^{2^j})^{2^m}) = 0.$$

At this point, in [62, Theorem 2] the authors claim that

$$L(a^{2^i+2^j}(t^{2^i}+t^{2^j}))+dL(a^{2^m(2^i+2^j)}(t^{2^i}+t^{2^j}))=L((a^{2^i+2^j}+da^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j})),$$

which is not true in general. For the case of $L(x)=x^{2^k}$ for some k, we have that

$$\begin{aligned}&L(a^{2^i+2^j}(t^{2^i}+t^{2^j}))+dL(a^{2^m(2^i+2^j)}(t^{2^i}+t^{2^j}))\\&=L((a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j})).\end{aligned}$$

So, in this case we would obtain

$$\Delta_a(x)=L(a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j}))=0,$$

which is equivalent to $(a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)})(t^{2^i}+t^{2^j})=0$. Now, $d^{2^{n-k}}\notin\{\lambda^{(2^i+2^j)(2^m-1)}:\lambda\in\mathbb{F}_{2^n}\}$ implies $a^{2^i+2^j}+d^{2^{n-k}}a^{2^m(2^i+2^j)}\neq 0$ and so we can have at most two solutions.

Thus, we consider C3* only with $L(x)=x^{2^k}$, and in this case the exponent k can be included in i and j. Moreover, as for the family C3, from the constraints on c and d we need m odd. So, in this case we have the following.

Theorem 6.4. *Let $n=2m$ with m odd. Let i,j be such that $i>j$ and $\gcd(i-j,m)=1$. Let F be the function over $\mathbb{F}_{2^n}$ defined by*

$$cx^{2^m+1}+\sum_{\ell=1}^{m-1}\gamma_\ell x^{2^\ell(2^m+1)}+x^{2^i+2^j}+dx^{2^m(2^i+2^j)},\tag{C3*}$$

where $c,d,\gamma_\ell\in\mathbb{F}_{2^n}$ are such that $d^{2^m+1}=1$, $d\notin\{\lambda^{(2^i+2^j)(2^m-1)}:\lambda\in\mathbb{F}_{2^n}\}$, $dc^{2^m}+c\neq 0$, $d=\gamma_\ell^{1-2^m}$ for all ℓ. Then, F is APN over $\mathbb{F}_{2^n}$.

6.2 Equivalence between known families

6.2.1 C11 and C3 are equivalent

Computational results performed in [35] for $m=3,4,5$ show that all APN functions of family C11 are equivalent to functions of C3. This led us to the idea that family C11 is contained in family C3. In the following we are going to show that it is true, firstly showing that family C11 without the sum $\sum_{\ell=1}^{m-1}\gamma_\ell x^{2^\ell(2^m+1)}$ is equivalent to family C3, secondly that every function in family C11 is equivalent to a function in the same family without the sum.

Lemma 6.1. *Let $n = 2m$, with m odd. Let i odd be such that $\gcd(i,m) = 1$ and consider the APN function*

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \tag{6.5}$$

where $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$. That is, F belongs to C11. Then, F is EA-equivalent to a function F' of C3.

Proof. Since $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ we have $\mathbb{F}_{2^{2m}} = c\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$. Let L be the linear permutation which is the identity map on $c\mathbb{F}_{2^m}$ and the power linear function x^{2^i} on $\mathbb{F}_{2^m}$, that is $L(cy+z) = cy + z^{2^i}$ for all $y,z \in \mathbb{F}_{2^m}$. Then, we obtain

$$F'(x) = \frac{L(F(x))}{d^{2^i}} = c'x^{2^m+1} + x^{2^{2i}+2^i} + d'x^{2^m(2^{2i}+2^i)},$$

with $c' = \dfrac{c}{d^{2^i}}$ and $d' = d^{2^i(2^m-1)}$. Since, m is odd and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\} = \{x^3 : x \in \mathbb{F}_{2^{2m}}\}$ (recall that i is odd) we have $d' \notin \{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$. Indeed, if $d' \in \{x^{(2^i+1)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have that d' is a cube, but $3 \nmid (2^m-1)$ and d is not a cube.

Moreover, since $c \notin \mathbb{F}_{2^m}$

$$c'^{2^m}d' + c' = \frac{c^{2^m}}{d^{2^i}} + \frac{c}{d^{2^i}} \neq 0,$$

implying that F in (6.5) is EA-equivalent to an APN function contained in C3 (F' satisfies the conditions of Theorem 6.1). □

Lemma 6.2. *Let $n = 2m$, with m odd. Let i odd be such that $\gcd(i,m) = 1$ and consider an APN function*

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}$$

as in Theorem 6.2. Then, F is EA-equivalent to a function as in (6.5)

$$F'(x) = c'x^{2^m+1} + d'x^{2^i+1} + d'^{2^m}x^{2^m(2^i+1)},$$

where c' and d' satisfy the conditions in Theorem 6.2.

Proof. Assume $1 \leq t \leq m-1$ be such that $\gamma_t \neq 0$. We can suppose that $\gamma_t = 1$. Indeed, since $\gamma_t \in \mathbb{F}_{2^m}$, dividing F by γ_t the function F/γ_t would satisfy the hypothesis of Theorem 6.2. Consider the following linear function with $w \in \mathbb{F}_{2^m}^*$ (we will study its permutation property later)

$$L(x) = (w + (c + c^{2^m})^{2^t})x + x^{2^t} + wx^{2^m} + x^{2^{m+t}}. \tag{6.6}$$

Let $u = dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)} \in \mathbb{F}_{2^m}$, then we obtain

$$\begin{aligned}
L(F(x)) &= (w + (c + c^{2^m})^{2^t})[u + cx^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)}] \\
&\quad + u^{2^t} + c^{2^t}x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l^{2^t} x^{2^{l+t}(2^m+1)} \\
&\quad + w[u + c^{2^m}x^{2^m+1} + \sum_{l=1}^{m-1} \gamma_l x^{2^l(2^m+1)}] \\
&\quad + u^{2^t} + c^{2^{m+t}}x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l^{2^t} x^{2^{l+t}(2^m+1)} \\
&= (w + (c + c^{2^m})^{2^t} + w)u + ((w + (c + c^{2^m})^{2^t})c + wc^{2^m})x^{2^m+1} \\
&\quad + (c + c^{2^m})^{2^t}x^{2^t(2^m+1)} + \sum_{l=1}^{m-1} \gamma_l (w + (c + c^{2^m})^{2^t} + w)x^{2^l(2^m+1)} \\
&= (c + c^{2^m})^{2^t}u + (w(c + c^{2^m}) + c(c + c^{2^m})^{2^t})x^{2^m+1} \\
&\quad + \sum_{l=1, l\neq t}^{m-1} \gamma_l (c + c^{2^m})^{2^t} x^{2^l(2^m+1)}
\end{aligned}$$

Hence

$$\frac{L(F(x))}{(c + c^{2^m})^{2^t}} = u + (w(c + c^{2^m})^{1-2^t} + c)x^{2^m+1} + \sum_{l=1, l\neq t}^{m-1} \gamma_l x^{2^l(2^m+1)}.$$

Let $c' = w(c + c^{2^m})^{1-2^t} + c$, also the condition on c', that is $c' \notin \mathbb{F}_{2^m}$, is satisfied since we have

$$\begin{aligned}
c'^{2^m} + c' &= w^{2^m}(c + c^{2^m})^{1-2^t} + c^{2^m} + w(c + c^{2^m})^{1-2^t} + c \\
&= (w^{2^m} + w)(c + c^{2^m})^{1-2^t} + (c + c^{2^m}) \;=\; (c + c^{2^m}).
\end{aligned}$$

Therefore we managed, from the original general formula C11, to obtain a similar one in which the monomial $x^{2^t(2^m+1)}$ is not present any more and the rest of the components of the sum is left unchanged. If the same procedure is applied for any j such that $\gamma_j \neq 0$ we are able to obtain a function of the form (6.5).

Now we only need to show that L of equation (6.6) is a permutation, where

$$L(x) = (x + x^{2^m})^{2^t} + w(x + x^{2^m}) + (c + c^{2^m})^{2^t}x.$$

Assume that $x \in \mathbb{F}_{2^m}$ then $L(x) = (c + c^{2^m})^{2^t}x$ is null if and only if $x = 0$. Otherwise consider $x \notin \mathbb{F}_{2^m}$ and let $y = x + x^{2^m} \in \mathbb{F}_{2^m}^*$, obtaining $L(x) = y^{2^t} + wy +$

$(c+c^{2^m})^{2^t}x$. If $L(x)=0$ then

$$x=\frac{y^{2^t}+wy}{(c+c^{2^m})^{2^t}}.$$

Since $w\in\mathbb{F}_{2^m}$ then also the right hand-side of the above equation belongs to $\mathbb{F}_{2^m}$, that leads to a contradiction. Therefore L is a linear permutation. □

Also C3 can be reduced to C11 reversing the computation done for (6.5) (an explicit computation is given in the subsection where we prove that C3* is included in C11*). So we have proved:

Proposition 6.2. *Families C3 and C11 are EA-equivalent.*

6.2.2 C11* is equivalent to C11

Using Remark 6.2 the equivalence is almost straightforward, however we want to make clear to the reader how to construct such equivalence. Obviously, C11 is a particular case of C11*. We show that also C11* can be reduced to C11.

Without loss of generality, we can consider C11* with $j=0$. From both functions it is possible, using the same technique as in Subsection 6.2.1, to remove the summation $\sum_{l=1}^{m-1}\gamma_l x^{2^l(2^m+1)}$. Hence we end up with

$$F_1(x)=cx^{2^m+1}+dx^{2^i+1}+d^{2^m}x^{2^m(2^i+1)}=cx^{2^m+1}+Q(x) \qquad \text{(C11)}$$
$$F_2(x)=cx^{2^m+1}+L(dx^{2^i+1}+d^{2^m}x^{2^m(2^i+1)})=cx^{2^m+1}+Q'(x), \qquad \text{(C11*)}$$

where $c\notin\mathbb{F}_{2^m}$, $d\notin\{x^{2^i+1}:x\in\mathbb{F}_{2^{2m}}\}$ and L a linear permutation with coefficients over $\mathbb{F}_{2^m}$.

Therefore, as explained in Remark 6.2, with the linear map L' which acts as the identity map on $c\mathbb{F}_{2^m}$ and as the linear function L^{-1} on $\mathbb{F}_{2^m}$, we obtain

$$L'\circ F_2(x)=F_1(x).$$

Since the constraints on the coefficients are the same for C11* and C11, we have obtained our claim.

Proposition 6.3. *Families C11* and C11 are EA-equivalent.*

6.2.3 C3* is equivalent to C11

Now we prove that family C3* as in Theorem 6.4, which contains C3, is equivalent to C11.

Let $n = 2m$ with m odd and consider the APN function defined over $\mathbb{F}_{2^n}$

$$F(x) = cx^{2^m+1} + \sum_{\ell=1}^{m-1} \gamma_\ell x^{2^\ell(2^m+1)} + x^{2^i+2^j} + dx^{2^m(2^i+2^j)},$$

where $c, d, \gamma_\ell \in \mathbb{F}_{2^n}$ satisfy the constraints of Theorem 6.4.

Since $d^{2^m+1} = 1$, there exists d' such that $d'^{2^m-1} = d$. Moreover, since d is not contained in $\{x^{(2^i+2^j)(2^m-1)} : x \in \mathbb{F}_{2^{2m}}\}$ we have $d' \notin \{x^{(2^i+2^j)} : x \in \mathbb{F}_{2^{2m}}\}$. Multiplying F by d', we obtain

$$F'(x) = d'F(x) = d'cx^{2^m+1} + \sum_{\ell=1}^{m-1} d'\gamma_\ell x^{2^\ell(2^m+1)} + d'x^{2^i+2^j} + d'^{2^m} x^{2^m(2^i+2^j)}.$$

Since $c + c^{2^m} d \neq 0$ we have that $d'c + (d'c)^{2^m} = d'(c + c^{2^m} d) \neq 0$, so $d'c \notin \mathbb{F}_{2^m}$. Moreover, since $d = \gamma_\ell^{1-2^m}$ for all ℓ such that $\gamma_\ell \neq 0$, we have that $(d'\gamma_\ell)^{2^m} = d'(d\gamma_\ell^{2^m}) = d'(\gamma_\ell^{1-2^m}\gamma_\ell^{2^m})$ which implies $d'\gamma_\ell \in \mathbb{F}_{2^m}$ for all $\gamma_\ell \neq 0$. Thus, F' is an element of C11*, which is EA-equivalent to C11 from Proposition 6.3. Then, from Proposition 6.2 we can conclude the following.

Proposition 6.4. *Families C11 and C3* are EA-equivalent.*

We summarise our results in the following theorem.

Theorem 6.5. *Families C3, C11, C3* and C11* are all EA-equivalent to each other.*

We conclude showing that for any fixed i, all the functions contained in these families are EA-equivalent to each other.

Proposition 6.5. *Let $n = 2m$ with m odd and let i be such that $\gcd(n, i) = 1$. Let*

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)},\ F'(x) = c'x^{2^m+1} + d'x^{2^i+1} + d'^{2^m} x^{2^m(2^i+1)}.$$

be two APN functions of family C11, that is, $c, c' \notin \mathbb{F}_{2^m}$ and $d, d' \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^n}\}$. Then, F and F' are affine equivalent.

Proof. Let us fix d not a cube, consider $c, c' \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and the functions

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)},\ F'(x) = c'x^{2^m+1} + dx^{2^i+1} + d^{2^m} x^{2^m(2^i+1)}.$$

Then, considering the linear permutation L which is the identity on $\mathbb{F}_{2^m}$ and that maps $c\mathbb{F}_{2^m}$ into $c'\mathbb{F}_{2^m}$, we immediately have $L \circ F = F'$.

Now, let us fix the coefficient $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and d not a cube. Consider the two functions

$$\begin{aligned} F(x) =& cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \\ F'(x) =& cx^{2^m+1} + d^2x^{2^i+1} + (d^2)^{2^m}x^{2^m(2^i+1)}. \end{aligned}$$

Then, we have that

$$F(x^{1/2})^2 = c^2x^{2^m+1} + d^2x^{2^i+1} + (d^2)^{2^m}x^{2^m(2^i+1)}$$

is equivalent to F' from the argument above. Thus, F is equivalent to F'.

Now, let $U := \{x^{2^i+1} : x \in \mathbb{F}_{2^n}^*\} = \{x^3 : x \in \mathbb{F}_{2^n}^*\}$ (i is odd), for any $u \in U$,

$$F(x) = cx^{2^m+1} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}$$

and

$$F'(x) = cx^{2^m+1} + dux^{2^i+1} + (du)^{2^m}x^{2^m(2^i+1)}$$

are equivalent. Indeed, we can apply the substitution $x \mapsto \lambda x$ for some $\lambda \in \mathbb{F}_{2^n}^*$ such that $\lambda^{2^i+1} = u$, and we have that $F(\lambda x) = c\lambda^{2^m+1}x^{2^m+1} + dux^{2^i+1} + (du)^{2^m}x^{2^m(2^i+1)}$ is equivalent to F'.

Now, since we can partition all non-cube elements as $dU \cup d^2U$ for some d not a cube, from the arguments above we have our claim. □

6.2.4 Equivalence with hexanomials (family C4)

The following family of APN hexanomials was constructed in [26].

Theorem 6.6. *Let n and i be any positive integers, $n = 2m$, $\gcd(i,m) = 1$, and $\bar{c}, \bar{d} \in \mathbb{F}_{2^n}$ be such that $\bar{d} \notin \mathbb{F}_{2^m}$. Then, the function*

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m})$$

is APN if and only if the equation

$$x^{2^i+1} + \bar{c}x^{2^i} + \bar{c}^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

The existence of coefficients $\bar{c}$ satisfying the conditions of the theorem above has been studied in [14]. In [70], Göloğlu characterised and compute the number of such $\bar{c}$'s.

We are going to show below that C11 (and thus C3) is contained in C4.

Without loss of generality, from the arguments given in Lemma 6.2, we can consider functions of the form

$$F(x) = cx^{2^m+1} + x^{2^i(2^m+1)} + dx^{2^i+1} + d^{2^m}x^{2^m(2^i+1)}, \tag{6.7}$$

with $c \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ and $d \notin \{x^{2^i+1} : x \in \mathbb{F}_{2^{2m}}\}$.

Consider a linear permutation of the type $x + \gamma x^{2^m}$ ($\gamma^{2^m+1} \neq 1$). Evaluating $F(x + \gamma x^{2^m})$ and deleting terms of algebraic degree less than 2, we obtain

$$\left.\begin{aligned}\widetilde{F}(x) = \quad & (c + c\gamma^{2^m+1})x^{2^m+1} + (1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)} \\ & +(d + d^{2^m}\gamma^{2^m(2^i+1)})x^{2^i+1} + (d^{2^m} + d\gamma^{2^i+1})x^{2^m(2^i+1)} \\ & +(d\gamma^{2^i} + d^{2^m}\gamma^{2^m})x^{2^{m+i}+1} + (d^{2^m}\gamma^{2^{m+i}} + d\gamma)x^{2^i+2^m}\end{aligned}\right\} = u.$$

Now, using a linear permutation as in (6.6), it is possible to delete the monomial $(1 + \gamma^{2^i(2^m+1)})x^{2^i(2^m+1)}$ since $(1 + \gamma^{2^i(2^m+1)})$ and u are in $\mathbb{F}_{2^m}$. Indeed, let $\gamma' = (1 + \gamma^{2^i(2^m+1)})$ and $L(x) = (w + (c + c^{2^m})^{2^i}\frac{\gamma'}{\gamma'^{2^i}})x + x^{2^i} + wx^{2^m} + x^{2^{m+i}}$ for some $w \in \mathbb{F}_{2^m}^*$. Then, following the same steps as in Lemma 6.2, we have

$$F'(x) = \frac{L(\widetilde{F}(x)/\gamma')}{\left(\frac{c}{\gamma'} + \frac{c^{2^m}}{\gamma'}\right)^{2^i}} = c'x^{2^m+1} + u,$$

for some $c' \notin \mathbb{F}_{2^m}$ depending on L. Denoting by $a = (d + d^{2^m}\gamma^{2^m(2^i+1)})$ and $b = (d\gamma^{2^i} + d^{2^m}\gamma^{2^m})$ we get

$$F'(x) = c'x^{2^m+1} + (ax^{2^i+1} + a^{2^m}x^{2^m(2^i+1)} + bx^{2^{m+i}+1} + b^{2^m}x^{2^i+2^m}). \tag{6.8}$$

Now, since i and m are odd and $\gcd(i, m) = 1$ then $x^{2^{m+i}+1}$ is a permutation of $\mathbb{F}_{2^n}$, which means that there exists $\lambda \in \mathbb{F}_{2^n}^*$ such that $\lambda^{2^{m+i}+1} = b$. Then, substituting $x \mapsto \lambda^{-1}x$ in (6.8) we obtain

$$F''(x) = \underbrace{c''x^{2^m+1}}_{c''\mathbb{F}_{2^m}} + \underbrace{\frac{a}{\lambda^{2^i+1}}x^{2^i+1} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m}x^{2^m(2^i+1)} + x^{2^{m+i}+1} + x^{2^i+2^m}}_{\mathbb{F}_{2^m}},$$

where $c'' = c'/\lambda^{2^m+1}$. Since $\mathbb{F}_{2^n} = c''\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can perform a substitution $x \mapsto x^{2^{m-i}}$ and then apply a linear map L which is $x^{2^{m+i}}$ on $c''\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$. Thus, denoting by $\tilde{c} = (c'')^{2^{m+i}}$, we obtain the EA-equivalent function

$$\begin{aligned}\bar{F}(x) =& L(F''(x^{2^{m-i}}))\\ =& \tilde{c}x^{2^m+1} + \frac{a}{\lambda^{2^i+1}}x^{2^m+2^j} + \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m} x^{(2^{m+j}+1)} + x^{2^j+1} + x^{2^m(2^j+1)}, \quad (6.9)\end{aligned}$$

where $j = m - i$ is even and $\gcd(j, m) = 1$.

On the other hand, let i be an integer with $\gcd(i, m) = 1$ and consider a hexanomial

$$H(x) = \bar{d}x^{2^i(2^m+1)} + x^{(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}),$$

with $\bar{c}$ and $\bar{d}$ satisfy the condition given in Theorem 6.6.

Applying the linear permutation (as in (6.6)) $L(x) = (w + (\bar{d} + \bar{d}^{2^m})^{2^{n-i}})x + wx^{2^m} + x^{2^{n-i}} + x^{2^{m-i}}$ for some $w \in \mathbb{F}_{2^m}^*$, we obtain

$$H'(x) = \frac{L(H(x))}{(\bar{d} + \bar{d}^{2^m})^{2^{n-i}}} = \bar{d}'x^{2^i(2^m+1)} + (x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}),$$

where $\bar{d}' = w(\bar{d} + \bar{d}^{2^m})^{1-2^{n-i}} + \bar{d} \notin \mathbb{F}_{2^m}$. Since $\mathbb{F}_{2^{2m}} = \bar{d}'\mathbb{F}_{2^m} \oplus \mathbb{F}_{2^m}$ we can apply a linear permutation which is $x^{2^{n-i}}$ on $\bar{d}'\mathbb{F}_{2^m}$ and the identity on $\mathbb{F}_{2^m}$ in order to obtain the EA-equivalent function

$$H''(x) = d''x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m}, \quad (6.10)$$

where $d'' = \bar{d}'^{2^{n-i}}$. Then, the family of the hexanomials can be expressed as pentanomials and the constraint on the coefficient $\bar{c}$ is the same of the hexanomials. Indeed, following the same steps of the proof of [26, Theorem 2], a function H'' as in (6.10), with $d'' \notin \mathbb{F}_{2^m}$ and $\gcd(i, m) = 1$, is APN if and only if

$$x^{2^i+1} + \bar{c}x^{2^i} + \bar{c}^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

Coming back to our function in (6.9), from the arguments above, since $\bar{F}$ is APN and $c'' \notin \mathbb{F}_{2^m}$, denoting $\bar{a} = \left(\frac{a}{\lambda^{2^i+1}}\right)^{2^m}$, we have that

$$x^{2^j+1} + \bar{a}x^{2^j} + \bar{a}^{2^m}x + 1 = 0$$

has no non-zero solution such that $x^{2^m+1} = 1$. So, the function $\bar{F}$ is equivalent to a hexanomials.

Hence we have proved the following result:

Theorem 6.7. *The families C3, C3*, C11 and C11* coincide and they are included in C4. In particular, the hexanomials admit a representation as pentanomials in the following form*

$$H'(x) = \bar{d}x^{2^m+1} + x^{2^i+1} + x^{2^m(2^i+1)} + \bar{c}x^{2^{m+i}+1} + \bar{c}^{2^m}x^{2^i+2^m},$$

with $\bar{d} \notin \mathbb{F}_{2^m}$ and $\bar{c}$ such that the equation

$$x^{2^i+1} + \bar{c}x^{2^i} + \bar{c}^{2^m}x + 1 = 0$$

has no solution x such that $x^{2^m+1} = 1$.

Moreover, when m and i are odd, H' is EA-equivalent to a pentanomial of type

$$\bar{H}(x) = dx^{2^m+1} + x^{2^j+1} + x^{2^m(2^j+1)} + cx^{2^{m+j}+1} + c^{2^m}x^{2^j+2^m},$$

where d and c satisfy the same conditions as $\bar{d}$ and $\bar{c}$ above, and $j = m - i$.

Proof. We need to prove only that when m is odd the pentanomial H' with i odd is equivalent to a pentanomial $\bar{H}$ with $j = m - i$ even. This can be done with the same steps as used above to compute $\bar{F}$ in (6.9) from F'' of (6.8), with the only difference that in this case the coefficient a of F'' is equal to 1. □

6.3 The updated list

Using the obtained results we reduce the list of known families of APN polynomials (which are CCZ-inequivalent to power functions) to those pairwise CCZ-inequivalent to each other. This refined list is presented in Table 6.2.

Table 6.2: Known classes of quadratic APN polynomial over $\mathbb{F}_{2^n}$ CCZ-inequivalent to power functions

N°	Functions	Conditions	In
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}$, $i=sk \mod p$, $m=p-i$, $n\geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[29]
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. $x^{q+1}=1$	[26]
F4	$x^3+a^{-1}Tr(a^3x^9)$	$a\neq 0$	[30]
F5	$x^3+a^{-1}Tr_n^3(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[31]
F6	$x^3+a^{-1}Tr_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n$, $a\neq 0$	[31]
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 $\mathbb{F}_{2^n}^*$	[17]
F10	$(x+x^{2^m})^{2^i+1}+$ $u'(ux+u^{2^m}x^{2^m})^{(2^i+1)2^j}+$ $u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m$, $m\geq 2$ even, $\gcd(i,m)=1$ and $j\geq 2$ even u primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not a cube	[112]
F11	$L_1(x)^{2^i}x+L_2(x)x^{2^i}$	$n=km$, $\gcd(n,i)=1$ $L_1(x),L_2(x)$ 2^m-polynomials satisfing the conditions in Theorem 5.1, Chapter 5	[24]
F12	$ut(x)(x^q+x)+t(x)^{2^{2i}+2^{3i}}+$ $at(x)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$ $a,b\in\mathbb{F}_{2^m}$, $X^{2^i+1}+aX+b$ has no solution over $\mathbb{F}_{2^m}$, $u\notin\mathbb{F}_{2^m}$ and $t(x)=u^qx+x^qu$	[99]
F13	$x^3+ax^{2^k(2^i+1)}$ $+bx^{3\cdot 2^m}+cx^{2^{n+k}(2^i+1)}$	$n=2m=10,(a,b,c)=(\beta,1,0),i=3,k=2,\mathbb{F}_4^*=\langle\beta\rangle$	[34]
		$n=2m,m$ odd, $3\not\|\, m,(a,b,c)=(\beta,\beta^2,1)$, $\mathbb{F}_4^*=\langle\beta\rangle$, $i\in\{m-2,m,2m-1,(m-2)^{-1} \mod n\}$	

Chapter 7

Isotopic shift construction for planar functions

In this chapter we consider fields of odd characteristic. In particular we extend some of the results on the isotopic shift

$$F_L(x) = \Delta_F(x, L(x)) = F(x + L(x)) - F(x) - F(L(x)) \tag{7.1}$$

of Chapter 4 to the case of p odd. In Theorem 4.1, it is proved that if F and G are isotopic equivalent quadratic planar functions, then G is EA-equivalent to an isotopic shift of F by some linear permutation L. We show in Section 7.1 that the converse does not hold, that is, an isotopic shift of a quadratic planar function by a linear permutation does not necessarily produce an isotopic equivalent function (and it is not always planar either). Moreover, we extend the isotopic shift construction of APN functions given in Chapter 4 for the even characteristics to the case of odd characteristics for PN functions. For an Albert-like planar function (i.e x^{p^i+1}) we study the planarity for some particular functions of the type

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i},$$

with L_1 and L_2 linearised polynomials, see Theorem 7.1. When $x^{p^i+1} = x^2$, this result gives some conditions on planar functions of the type $xL(x)$ with L linear. This characterisation permits to determine that the planar functions classified in [5] are affine equivalent to the function x^2 or to an Albert function, see Proposition 7.9.

7.1 On the linear shifts over fields of odd characteristic

In even characteristics, the isotopic shift of an APN function can produce a CCZ-inequivalent APN function (see for example Lemma 4.1). This is also true

for the case of planar functions. For example, consider the planar quadratic function $F(x) = x^2$, defined over a finite field of characteristic $p > 2$. Consider its isotopic shift by the linear permutation $L(x) = x^{p^j}$,

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)) = 2x^{p^j+1}.$$

Now, F_L is planar over $\mathbb{F}_{p^n}$ if and only if $\frac{n}{\gcd(n,j)}$ is odd (Albert function [1]). Therefore we have an example of isotopic shift F_L that is not planar and also an example of isotopic shift that is planar and isotopic inequivalent to F. As for the case of APN maps in even characteristic, see Remark 4.1, in general the isotopic shift does not preserve the differential uniformity.

In even characteristic, we have some restrictions on L so that the isotopic shift of a function F is APN. This is also the case in odd characteristic for obtaining planar functions.

Proposition 7.1. *Given $F, L \in \mathbb{F}_{p^n}[x]$, where L is a linear function which is not a permutation, the map F_L is not planar.*

Proof. Without loss of generality assume $F(0) = 0$. Given F_L as in (7.1), the function is planar if and only if for any element $e \neq 0$

$$D_e F_L(x) = F_L(x + e) - F_L(x)$$

is a permutation. Equivalently, we can consider $\Delta_e(x) = D_e F_L(x) - F_L(e)$ to be a permutation. Since L is not a permutation, there exists $z \neq 0$ such that $L(z) = 0$. Then,

$$\Delta_z(z) = F_L(2z) - 2F_L(z) = 0 = \Delta_z(0)$$

since $F_L(2z) = F_L(z) = 0$. Thus Δ_z is not a permutation. □

Remark 7.1. *Note that F does not need to be planar in order to obtain a planar function from a shift. Indeed, consider the finite field $\mathbb{F}_{3^4}$ and the non-planar function $F(x) = x^{3+1} = x^4$. With the linear permutation $L(x) = x^{27} + \zeta^4 x^3$ we construct*

$$F_L(x) = x^3 L(x) + x L(x)^3 = x^{30} + \zeta^4 x^6 + x^2 + \zeta^{12} x^{10},$$

that is planar. This function is CCZ-equivalent to the Dickson function $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^3 - x)$ and $t(x) = x^{3^2} - x$.

Similarly to the case of finite fields with even characteristic we have the following proposition.

Proposition 7.2. *For a monomial DO polynomial F and a linear function $L(x) = \sum_{j=0}^{n-1} b_j x^{p^j}$, the isotopic shift F_L is affine equivalent to the isotopic shift F_M constructed with the linear function*

$$M(x) = \sum_{j=0}^{n-1} (b_j \zeta^{k(p^j-1)})^{p^t} x^{p^j},$$

where k and t can be any integers. Moreover, for any function F, if L is a permutation, then F_L is affine equivalent to $F_{L^{-1}}(x)$.

Proof. Without loss of generality let $F(x) = x^{p^i+1}$. Then, we have

$$F_M(x) = \sum_{j=0}^{n-1} [(b_j \zeta^{k(p^j-1)})^{p^t} x^{p^i+p^j} + (b_j \zeta^{k(p^j-1)})^{p^{i+t}} x^{p^{j+i}+1}]$$

and

$$\begin{aligned}
&(\zeta^{kp^t(1+p^i)} F_M(\zeta^{-kp^t} x^{p^t}))^{p^{-t}} = \\
=&\zeta^{k(1+p^i)} [\zeta^{-kp^i} x^{p^i} M(\zeta^{-kp^t} x^{p^t}))^{p^{-t}} + \zeta^{-k} x M(\zeta^{-kp^t} x^{p^t}))^{p^{i-t}}] \\
=&\zeta^{k(1+p^i)} \sum [\zeta^{-kp^i} x^{p^i} b_j \zeta^{k(p^j-1)} \zeta^{-kp^j} x^{p^j} + \zeta^{-k} x b_j^{p^i} \zeta^{k(p^j-1)p^i} \zeta^{-kp^j p^i} x^{p^j p^i}] \\
=&\zeta^{k(1+p^i)} \sum [\zeta^{-k(p^i+1)} b_j x^{p^j+p^i} + \zeta^{-k(p^i+1)} b_j^{p^i} x^{p^j p^i+1}] \\
=&\sum [b_j x^{p^j+p^i} + b_j^{p^i} x^{p^{j+i}+1}] = F_L(x).
\end{aligned}$$

For the last part, it is easy to check that if L is a permutation, then $F_L(L^{-1}(x)) = F_{L^{-1}}(x)$. □

7.1.1 The reciprocity of the isotopic shift

We consider here the following question.

Question 7.1. *Given $F, G \in \mathbb{F}_{p^n}[x]$ quadratic maps, does the existence of an isotopic shift connecting F to G imply the existence of an isotopic shift connecting G to F?*

We refer to the property mentioned in the above question as to the reciprocity of the isotopic shift. With the existence of an isotopic shift connecting F to G we refer to the existence of a linear permutation L such that F_L is EA-equivalent to G. Recall that, from Corollary 4.1, if F and F' are EA-equivalent quadratic maps then for any $M \in \mathbb{F}_{p^n}[x]$ there exists a map $N \in \mathbb{F}_{p^n}[x]$ such that F_M is EA-equivalent to F'_N. Hence, if G is EA-equivalent to F_L, then given M there exists N such that G_M is EA-equivalent to $(F_L)_N$. Therefore Question 7.1 is equivalent to the following question.

Question 7.2. *Given $F, L \in \mathbb{F}_{p^n}[x]$ with L linear permutation, F quadratic map and such that F_L is quadratic too, does there exist a linear permutation $M \in \mathbb{F}_{p^n}[x]$ such that $(F_L)_M$ is EA-equivalent to F?*

If F and G are isotopic equivalent quadratic planar functions, Theorem 4.1 implies that Question 7.1 has a positive answer. In particular, for F a quadratic planar map, if F_L is isotopic equivalent to F then there exists a linear permutation M such that $(F_L)_M$ is EA-equivalent to F.

In general, considering F and G quadratic maps not isotopic equivalent, the reciprocity of the isotopic shift is not always satisfied. Indeed there are cases in which the isotopic shift is reciprocal and cases in which it is not. In the following we report some computational results obtained, which show the different behaviours of the isotopic shift. Over $\mathbb{F}_{p^n}$, we consider $F(x) = x^2$ and $G(x) = x^{p^j+1}$, for which F_L is EA-equivalent to G with $L(x) = x^{p^j}$. Without loss of generality, we can always assume $j \leq n/2$. We analyse then whether there exists also an isotopic shift connecting G to F and, in small dimensions, we obtained the following results.

- Over $\mathbb{F}_{p^3}$ (with $p = 3,5,7$) for $G(x) = x^{p+1}$ there exists a linear permutation M such that G_M is EA-equivalent to x^2.[1]
- Over $\mathbb{F}_{3^4}$ for both $G(x) = x^{p+1}$ and $G(x) = x^{p^2+1}$ no isotopic shift of G is EA-equivalent to x^2.
- Over $\mathbb{F}_{3^5}$ for both $G(x) = x^{p+1}$ and $G(x) = x^{p^2+1}$ no isotopic shift of G is EA-equivalent to x^2.[2]

Notice that, over $\mathbb{F}_{3^4}$, x^{p+1} and x^{p^2+1} are not planar. Instead, over $\mathbb{F}_{3^5}$, both maps are planar. Hence there are cases of isotopic shift not reciprocal when F, G are both quadratic planar maps and cases when F is planar and G is not.

Remark 7.2. *The obtained results imply that the isotopic shift (together with EA-transformation), even when restricted to planar maps, does not represent an equivalence notion.*

[1] The mentioned linear permutations M are the following: $M(x) = x^p + x$ for $p = 3$, $M(x) = x^{p^2} + x$ for $p = 5$ and $M(x) = x^{p^2} + x^p$ for $p = 7$.

[2] To perform the last two analyses, we consider all possible linear permutations M over $\mathbb{F}_{3^4}$ and $\mathbb{F}_{3^5}$, up to some restrictions over the coefficients given by Proposition 7.2. Then we verify, for those M which generate planar maps G_M, whether G_M is EA-equivalent to x^2.

7.1.2 Comparison on linear shifts in odd and even characteristic

Assume F is a quadratic polynomial satisfying $F(0) = 0$ and L a linear function over $\mathbb{F}_{p^n}$ where p is odd. Let $\Delta(x,y)$ be the symmetric bilinear operator

$$\Delta(x,y) = F(x+y) - F(x) - F(y).$$

Then

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)) = \Delta(x, L(x))$$

is an isotopic shift of a quadratic polynomial and then is a DO polynomial itself, and its differential property is given by $\Delta(c, L(x)) + \Delta(L(c), x)$ for $c \neq 0$. Indeed, since $\Delta(x,y)$ is symmetric and bilinear we have

$$\begin{aligned} F_L(x+c) - F_L(x) - F_L(c) =& \Delta(L(x+c), x+c) - \Delta(L(x), x) - \Delta(L(c), c) \\ =& \Delta(L(x), x) + \Delta(L(c), x) + \Delta(L(x), c) + \\ & \Delta(L(c), c) - \Delta(L(x), x) - \Delta(L(c), c) \\ =& \Delta(c, L(x)) + \Delta(L(c), x). \end{aligned}$$

In order F_L to be planar we want that

$$\text{for any } c \neq 0 \qquad |\mathrm{Im}(\Delta(c, L(x)) + \Delta(L(c), x))| = p^n.$$

In particular, combining it with Proposition 7.1, we have the following.

Proposition 7.3. *Given $F, L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where F is a quadratic polynomial satisfying $F(0) = 0$ and L is a linear map, consider the isotopic shift of F by L, F_L defined as in (7.1). If the map F_L is planar then for any element $c \neq 0$ we have*

$$\mathrm{Ker}(\Delta(c, L(x))) \cap \mathrm{Ker}(\Delta(L(c), x)) = \{0\}.$$

Moreover, L is a permutation.

In the following table we compare the characteristics of the linear functions L for the case p even (taken from Chapter 4) and p odd.

	p **even**	p **odd**
if	F_L is APN	F_L is PN
then		
$\forall c \in \mathbb{F}_{p^n}^\star$	$\Delta(c, L(x)) + \Delta(L(c), x)$ 2-to-1	$\Delta(c, L(x)) + \Delta(L(c), x)$ 1-to-1
	L 1-to-1 or 2-to-1	L 1-to-1
	if $\mathrm{Ker}(L) = \{0, z\}$ then $\Delta(z, L(c)) \neq 0$ $\forall c \notin \mathrm{Ker}(L)$	$\Delta(c, L(c)) \neq 0$ ($F_L(c) \neq 0$)
	$\mathrm{Ker}(\Delta(c, L(x))) \cap \mathrm{Ker}(\Delta(L(c), x)) = \{0, c\}$	$\mathrm{Ker}(\Delta(c, L(x))) \cap \mathrm{Ker}(\Delta(L(c), x)) = \{0\}$

7.1.3 Shifting Albert-like functions by monomials

Starting from an Albert like function x^{p^i+1} over $\mathbb{F}_{p^n}$ by a linear monomial $L(x) = ax^{p^t}$ we obtain the map

$$F_L(x) = a^{p^i} x^{p^{i+t}+1} + ax^{p^i+p^t}.$$

For this case we can obtain the following result.

Proposition 7.4. *Let p be an odd prime, $a \in \mathbb{F}_{p^n}^\star$ and $F_L(x) = a^{p^i} x^{p^{i+t}+1} + ax^{p^i+p^t}$ be an isotopic shift of x^{p^i+1} over $\mathbb{F}_{p^n}$. Then:*

(i) If $i = 0$, then F_L is planar if and only if $n/\gcd(n,t)$ is odd, moreover F_L is linear equivalent to an Albert-like function;

(ii) If $t = 0$, then F_L is planar if and only if $n/\gcd(n,i)$ is odd and $a \notin \mathbb{F}_{p^i}$, moreover F_L is linear equivalent to an Albert-like function;

(iii) If $n = 2m$ with m odd and $t = m$, then for any $i \leq m$ odd the shift F_L is planar if and only if a is such that $a^{p^m+1} \notin \mathbb{F}_{p^m} \cap \mathbb{F}_{p^i}$. Moreover, F_L is affine equivalent to the planar function $x^{p^{m-i}+1}$;

(iv) If $n = 4k$ for some integer k, $p^k \equiv 1 \mod 4$ and $L(x) = \zeta^s x^{p^k}$ with s odd, then the isotopic shift of x^{p^k+1}, $F_L(x) = \zeta^{s\cdot p^k} x^{p^{2k}+1} + \zeta^s x^{2p^k}$ is planar and isotopic equivalent to the planar function of a Dickson semifield.

Proof. For the first two cases we have, when $i = 0$, $F_L(x) = 2ax^{p^t+1}$ and $F_L(x) = (a^{p^i} + a)x^{p^i+1}$ for $t = 0$, so these are planar if and only if $n/\gcd(n,t)$ and $n/\gcd(n,i)$ are odd.

For the third case we have that

$$F_L(x) = a^{p^i} x^{p^{i+m}+1} + ax^{p^i+p^m} = a^{p^i}(x^{p^i+p^m})^{p^m} + ax^{p^i+p^m}.$$

Then, $F_L(x) = L_1 \circ x^{p^{m-i}+1} \circ L_2(x)$ where $L_1(x) = a^{p^i} x^{p^m} + ax$ and $L_2(x) = x^{p^i}$. Since $x^{p^m+p^i}$ is planar ($n/\gcd(m-i,n)$ is odd) F_L can be planar if and only if L_1 is a permutation. From $a^{p^m+1} \notin \mathbb{F}_{p^m} \cap \mathbb{F}_{p^i}$ we have that L_1 is a permutation. Indeed, L_1 is a permutation if and only if

$$A = \begin{bmatrix} a & a^{p^{m+i}} \\ a^{p^i} & a^{p^m} \end{bmatrix}$$

is full rank, which is equivalent to $\det(A) = a^{p^m+1} - a^{p^i(p^m+1)} \neq 0$.

For the last case, $F_L(x) = \zeta^{s\cdot p^k} x^{p^{2k}+1} + \zeta^s x^{2p^k}$ is equivalent to $x^{p^{2k}+1} + \frac{1}{\zeta^{s(p^k-1)}} x^{2p^k} = x^{p^{2k}+1} + \zeta^{s\cdot p^{4k-2}(p^k-1)} x^{2p^k}$. Since $s \cdot p^{4k-2}$ is odd we have from Theorem 4.2 in [50] that F_L is planar. From Theorem 4.3 in [50] we have that the semifield associated to $x^{p^{2k}+1} + \zeta^{p^{4k-2}(p^k-1)} x^{2p^k}$ is isotopic to the Dickson semifield $-\frac{1}{8}L'(t^2(x)) + \frac{1}{2}x^2$, with $L'(x) = x^{p^k} + x$ and $t(x) = x^{p^{2k}} - x$. □

7.2 Generalised isotopic shift

7.2.1 For general Albert-like functions

If we consider an Albert-like function x^{p^i+1}, an isotopic shift by a linear function L is given by

$$x^{p^i} L(x) + xL(x)^{p^i}.$$

In the following we consider a slight generalisation of such functions, as in Section 5.1. That is, we consider two linear maps

$$L_1(x) = \sum_{j=0}^{k-1} A_j x^{p^{jm}} \text{ and } L_2(x) = \sum_{j=0}^{k-1} B_j x^{p^{jm}}$$

defined over the finite field $\mathbb{F}_{p^{km}}$ and construct the function

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i}.$$

A necessary condition for F to be planar is the following.

Proposition 7.5. *For two positive integers m, k, consider the function*

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i}$$

defined over $\mathbb{F}_{p^{km}}$, where $L_1, L_2 \in \mathbb{F}_{p^{km}}[x]$ are p^m-linear polynomials. Then, F can be planar only if $\frac{m}{\gcd(i,m)}$ is odd.

Proof. Since F is planar then for any $e \in \mathbb{F}_{p^{km}}^\star$ the function $\Delta_e(x) = F(x+e) - F(x) - F(e)$ is a permutation. In particular, for any $e \in \mathbb{F}_{p^m}^\star$ we have

$$\Delta_e(1) = (L_1(1)^{p^i} + L_2(1))(e^{p^i} + e).$$

Since $\Delta_e(0) = 0$, in order to be a permutation, $\Delta_e(1)$ must be different from 0, implying that $e^{p^i} \neq -e$, for any $e \in \mathbb{F}_{p^m}^\star$. This implies that $\frac{m}{\gcd(i,m)}$ is odd. □

Remark 7.3. *Note that for this construction the necessary condition* $\frac{m}{\gcd(i,m)}$ *odd implies that* x^{p^i+1} *is planar over the subfield* $\mathbb{F}_{p^m}$*, but it does not necessarily mean planarity over* $\mathbb{F}_{p^{km}}$*.*

Let $W = \{y\zeta^j : y \in U, 0 \le j \le d'-1\}$, where $U = \langle \zeta^{d'(p^m-1)} \rangle$, $d = \gcd(p^m - 1, \frac{p^{km}-1}{p^m-1})$ and d' is an integer with the same prime factor as d, each being raised at the power as in $\frac{p^{km}-1}{p^m-1}$ (hence such that $\gcd(p^m-1, \frac{p^{km}-1}{d'(p^m-1)}) = 1$). We obtain the following result.

Theorem 7.1. *Let* k, m *and* i *be positive integers and consider two* p^m*-linear polynomials* L_1, L_2 *over* $\mathbb{F}_{p^{km}}$*. Then, the function* $F(x) = L_1(x)^{p^i}x + L_2(x)x^{p^i}$ *is planar over* $\mathbb{F}_{p^{km}}$ *if and only if* $\frac{m}{\gcd(m,i)}$ *is odd and the following conditions are satisfied:*

(i) $F(t) \neq 0$ *for any* $t \in W$*;*

(ii) $L_1(v)^{p^i}t + L_2(t)v^{p^i} \neq 0$ *for any* $t, v \in W$ *such that* $L_1(t)^{p^i}v + L_2(v)t^{p^i} = 0$*;*

(iii) $\frac{L_1(v)^{p^i}t + L_2(t)v^{p^i}}{L_1(t)^{p^i}v + L_2(v)t^{p^i}} \neq -r^{p^i-1}$ *for any* $t, v \in W$ *and any* $r \in \mathbb{F}_{p^m}^\star$ *such that* $L_1(t)^{p^i}v + L_2(v)t^{p^i} \neq 0$*.*

Proof. From Proposition 7.5 we have the condition on the parity of $\frac{m}{\gcd(m,i)}$. Moreover, for planarity, we need that for any $e \in \mathbb{F}_{p^{km}}^\star$ the function $\Delta_e(x) = F(x+e) - F(x) - F(e)$ is a permutation (or equivalently 0 is the only root of $\Delta_e(x)$). Since $\mathbb{F}_{p^{km}}^\star = W \times \mathbb{F}_{p^m}^\star$ we can rewrite $e = st$ and $x = uv$ with $s, u \in \mathbb{F}_{p^m}^\star$ and $t, v \in W$. Hence,

$$\begin{aligned}\Delta_e(x) =& L_1(e)^{p^i}x + L_2(e)x^{p^i} + L_1(x)^{p^i}e + L_2(x)e^{p^i}\\ =& s^{p^i}L_1(t)^{p^i}uv + sL_2(t)u^{p^i}v^{p^i} + u^{p^i}L_1(v)^{p^i}st + uL_2(v)s^{p^i}t^{p^i}\\ =& us[s^{p^i-1}(L_1(t)^{p^i}v + L_2(v)t^{p^i}) + u^{p^i-1}(L_1(v)^{p^i}t + L_2(t)v^{p^i})].\end{aligned}$$

If $v = t$, then

$$\Delta_e(x) = us(L_1(t)^{p^i}t + L_2(t)t^{p^i})[s^{p^i-1} + u^{p^i-1}].$$

Then $L_1(t)^{p^i}t + L_2(t)t^{p^i} = F(t) \neq 0$ must hold for any $t \in W$. Moreover $(\frac{s}{u})^{p^i-1} \neq -1$, for any $s, u \in \mathbb{F}_{p^m}^\star$.
For the case $v \neq t$, when $L_1(t)^{p^i}v + L_2(v)t^{p^i} = 0$, we have

$$\Delta_e(x) = u^{p^i}s(L_1(v)^{p^i}t + L_2(t)v^{p^i}),$$

and thus we must have $L_1(v)^{p^i}t + L_2(t)v^{p^i} \neq 0$. While, if $L_1(t)^{p^i}v + L_2(v)t^{p^i} \neq 0$ then we must have $\frac{L_1(v)^{p^i}t + L_2(t)v^{p^i}}{L_1(t)^{p^i}v + L_2(v)t^{p^i}} \neq -(\frac{s}{u})^{p^i-1}$. □

7.2.2 The particular case of x^2

If we consider the particular case of x^2, we obtain the function

$$F(x) = L_1(x)x + L_2(x)x = xL(x),$$

where $L(x) = L_1(x) + L_2(x)$.

Some existence results on planar functions of type $xL(x)$ are discussed in [81, 103]. For example, in these works the authors study the planar property of functions of type $x(x^q + ux)$ over $\mathbb{F}_{q^2}$ and $x(\mathrm{Tr}_n(x) + ax)$. In particular, we have the following.

Proposition 7.6 ([81]). *Let q be a power of a prime, and $L_1, L_2 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be q-linear mappings. If the mapping $L_1(x) \cdot L_2(x)$ is planar, then the maps L_1 and L_2 are bijective.*

This proposition implies that it is sufficient to study planar function of type $xL(x)$ where L is a bijection.

Remark 7.4. *The fact that L is bijective can be obtained also from the previous section. Indeed, we can consider the isotopic shift of x^2 with a linear function L, obtaining the function $F(x) = 2xL(x)$. If F is planar then the function L needs to be a permutation.*

We can restate Theorem 7.1 for the case of x^2 as follows.

Theorem 7.2. *Let k and m be positive integers. Consider a p^m-linear polynomial L over $\mathbb{F}_{p^{km}}$. Then the function $F(x) = xL(x)$ is planar if and only if the following conditions are satisfied:*

- *$F(t) \neq 0$ for any $t \in W$;*
- *$\frac{L(v)}{v} \neq -\frac{L(t)}{t}$ for any $t, v \in W$.*

For the case $k = 3$, we obtain some equivalence results for some specific p^m-linear polynomials L.

Proposition 7.7. *Over $\mathbb{F}_{p^{3m}}$, consider the isotopic shift of x^2 by the linear permutation $L(x) = ax^{p^{2m}} + bx^{p^m} + x$, $F_L(x) = 2(ax^{p^{2m}+1} + bx^{p^m+1} + x^2)$. Denoting by N the norm function from $\mathbb{F}_{p^{3m}}$ to $\mathbb{F}_{p^m}$, assume that $a = \frac{2e^{p^{2m}+1}}{N(e)+1}$ and $b = \frac{2e^{p^{2m}}}{N(e)+1}$, where e is such that $N(e) \neq \pm 1$.Then, F_L is planar and affine equivalent to x^2.*

Proof. Let $A_1(x) = \frac{e^{2p^{2m}}}{1-N(e)^2}(x^{p^{2m}} - e^2x)$ and $A_2(x) = x^{p^{2m}} + \frac{1}{e}x^{p^m} + e^{p^m}x$. The map A_1 is a permutation since $x^{p^{2m}-1} = e^2$ would imply $1 = N(x)^{(p^m+1)(p^m-1)} = N(e)^2$. Also A_2 is a permutation. Indeed, A_2 is a permutation if and only if the determinant of the matrix

$$\begin{bmatrix} e^{p^m} & 1 & \frac{1}{e^{p^{2m}}} \\ \frac{1}{e} & e^{p^{2m}} & 1 \\ 1 & \frac{1}{e^{p^m}} & e \end{bmatrix}$$

is not zero. That is, $N(e) + \frac{1}{N(e)} - 2 \neq 0$, implying $N(e)^2 + 1 - 2N(e) = (N(e) - 1)^2 \neq 0$.

Now, it is easy to verify that $A_1 \circ x^2 \circ A_2 = F_L(x)/2$. □

Proposition 7.8. *Over $\mathbb{F}_{p^{3m}}$ consider the isotopic shift of x^2 by the linear permutation $L(x) = ax^{p^{2m}} + bx^{p^m} + x$, $F_L(x) = 2(ax^{p^{2m}+1} + bx^{p^m+1} + x^2)$. Denoting by N the norm function from $\mathbb{F}_{p^{3m}}$ to $\mathbb{F}_{p^m}$, assume that $a = 1/b^{p^{2m}}$, $N(b) \neq 1$. Then, F_L is planar and affine equivalent to x^{p^m+1}.*

Proof. Let $A_1(x) = \frac{b^{p^m+1}}{N(b)-1}(x^{p^{2m}} - \frac{1}{b^{p^m}}x)$ and $A_2(x) = \frac{1}{b^{p^{2m}}}(x^{p^{2m}} + b^{p^{2m}+1}x^{p^m} + b^{p^{2m}}x)$. A_1 is a permutation since $x^{p^{2m}-1} = \frac{1}{b^{p^m}}$ would imply

$$1 = N(x)^{(p^m+1)(p^m-1)} = 1/N(b)^{p^m} = 1/N(b)$$

and, with similar arguments as in Proposition 7.7, A_2 is a permutation. Then, $A_1 \circ x^{p^m+1} \circ A_2 = F_L(x)/2$. □

In [5], the authors completely classified the planar functions of type $x(x^{p^{2m}} + Ax^{p^m} + Bx)$ when the coefficients are restricted to $\mathbb{F}_{p^m}$. In particular, they obtained the following result.

Theorem 7.3 ([5])**.** *Let m be a positive integer, p an odd prime and consider the function $f_{A,B} \in \mathbb{F}_{p^{3m}}[x]$ of the type*

$$f_{A,B}(x) = x(x^{p^{2m}} + Ax^{p^m} + Bx)$$

where $A, B \in \mathbb{F}_{p^m}$. Then, $f_{A,B}$ is planar if and only if one of the following conditions holds:

1. *$A^3 \neq \pm 1$ and $A^3 - 2AB + 1 = 0$;*
2. *$A = B^2$ and $B^3 \neq \pm 1$;*

3. $B = 0$ *and* $A^3 + 1 \neq 0$.

From Proposition 7.7 and Proposition 7.8 we can prove that all the planar functions in Theorem 7.3 are affine equivalent to x^2 or x^{p^m+1}.

Proposition 7.9. *Let m be a positive integer, p an odd prime and consider the function $f_{A,B} \in \mathbb{F}_{p^{3m}}[x]$ of the type*

$$f_{A,B}(x) = x(x^{p^{2m}} + Ax^{p^m} + Bx)$$

where $A, B \in \mathbb{F}_{p^m}$. If $f_{A,B}$ is planar then it is affine equivalent to x^2 or to x^{p^m+1}.

Proof. Let $q = p^m$. From Theorem 7.3 we have that A and B satisfy one of the following conditions

1. $A^3 \neq \pm 1$ and $A^3 - 2AB + 1 = 0$;
2. $A = B^2$ and $B^3 \neq \pm 1$;
3. $B = 0$ and $A^3 + 1 \neq 0$.

Suppose we are in the first case. Then, $B = \frac{A^3+1}{2A}$ and dividing $f_{A,B}(x)$ by B we obtain

$$f'(x) = \frac{2A}{A^3+1}x^{q^2+1} + \frac{2A^2}{A^3+1}x^{q+1} + x^2.$$

Denoting by $e = \frac{1}{A}$, we have $N(e) = \frac{1}{A^3} \neq \pm 1$ and

$$f'(x) = \frac{2A}{A^3+1}x^{q^2+1} + \frac{2A^2}{A^3+1}x^{q+1} + x^2 = \frac{2e^2}{1+e^3}x^{q^2+1} + \frac{2e}{1+e^3}x^{q+1} + x^2.$$

Now, as shown in Proposition 7.7, the function f' is equivalent to x^2 and so does $f_{A,B}$.

Suppose now that we have the second case. Dividing $f_{A,B}(x)$ by B we obtain

$$f'(x) = \frac{1}{B}x^{q^2+1} + Bx^{q+1} + x^2.$$

Since $N(B) = B^3 \neq \pm 1$ from Proposition 7.8 we obtain that $f_{A,B}$ is equivalent to x^{q+1}.

For the last case we have the function $f_{A,0}(x) = x^{q^2+1} + Ax^{q+1} = x^{q^2(q+1)} + Ax^{q+1}$. Since $f_{A,0}$ is planar the linearised polynomial $x^{q^2} + Ax$ is a permutation and thus $f_{A,0}$ is equivalent to x^{q+1}. □

7.3 Computational results over $\mathbb{F}_{p^n}$

In this section we report some computational results obtained on the linear shifts for odd characteristics and small dimensions.

As seen before, from the linear shift of x^2 by a linear monomial we can obtain the Albert functions x^{p^t+1} (for any $t \geq 1$). For any p odd, over $\mathbb{F}_{p^n}$ with $n \leq 3$, these are the only planar DO functions possible (see [56, 90]).

Isotopic shifts by a linear monomial

Starting from an Albert like function x^{p^t+1} over $\mathbb{F}_{p^n}$ by a linear monomial $L(x) = ax^{p^i}$ we obtain the map

$$F_L(x) = a^{p^t} x^{p^{t+i}+1} + ax^{p^t+p^i}.$$

As shown in Proposition 7.4, we can obtain an inequivalent Albert planar function or also the Dickson function over some fields $\mathbb{F}_{p^{4k}}$. We considered $t > 0$ and performed some computations over small dimensions. From Proposition 7.2 we can restrict to $1 \leq t, i \leq \frac{n}{2}$ (since F_L is equivalent to $F_{L^{-1}}$) and also restrict the coefficient a. Over the finite fields $\mathbb{F}_{p^n}$ with $p = 3$ and $3 \leq n \leq 10$, with $p = 5$ and $3 \leq n \leq 6$, with $p = 7$ and $3 \leq n \leq 5$, the only planar functions constructed are those presented in Proposition 7.4. The field $\mathbb{F}_{7^3}$ is the only exception since it is possible to construct, for $t = i = 1$, a planar map affine equivalent to x^2. We checked over $\mathbb{F}_{p^3}$ with $p \leq 67$ if we could obtain different cases from Proposition 7.4 as for $\mathbb{F}_{7^3}$, but no planar functions were obtained.

The case $p = 3$

We consider the isotopic shift of x^2 by a linear function L, that is the function $2xL(x)$ with L a linear permutation.

Over $\mathbb{F}_{3^4}$ from the shift of x^2 we can obtain planar maps CCZ-equivalent to x^2 and to $x^{28} + x^{10} + \zeta^{20}x^4 + \zeta^5 x^2$, which is equivalent to the Dickson function [55] $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^p - x)$ and $t(x) = x^{p^2} - x$.
Over $\mathbb{F}_{3^5}$, from the shift of x^2 we can obtain only the planar functions x^4 and x^{10} (Albert cases). From the shift of $F(x) = x^{90} + x^2$ (see [4]), for $L(x) = x^{81} + x^9 + 2x^3 + x$ we obtain that F_L is equivalent to $x^{10} - x^6 - x^2$ [58].
Over $\mathbb{F}_{3^6}$, with restriction of coefficients over $\mathbb{F}_{3^2}$ and $\mathbb{F}_{3^3}$, from the shift of x^2 we can obtain the planar functions x^2 and x^{10} (Albert cases) and the planar functions BH and LMPT (see Table 7.1).

The case $p = 5$

Over $\mathbb{F}_{5^4}$, from the shift of x^2 we can obtain planar maps equivalent to x^2 and to $x^{126} + \zeta^{12}x^6 + \zeta^2 x^2$, which is CCZ-equivalent to the Dickson function $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^p - x)$ and $t(x) = x^{p^2} - x$.

Isotopic shift with q-polynomials

We report some computational results, done in characteristic 3, for the (generalised) isotopic shift constructed in Section 7.2.

Consider the field $\mathbb{F}_{3^6}$. In Table 7.1 we list all known isotopic inequivalent planar functions over $\mathbb{F}_{3^6}$.

Table 7.1: All known isotopic inequivalent planar functions over $\mathbb{F}_{3^6}$

x^2	Finite Field
x^{p^2+1}	Albert [1]
$\frac{1}{8}(x^{2p^4} + x^{2p} - 2x^{p^4+p} - x^{2p^3} - x^2 + 2x^{p^3+1}) + \frac{1}{2}x^2$	Dickson [55]
$\zeta^{27}x^{270} + \zeta x^{28} + \zeta x^{10}$	BH [33]
$2x^{270} + x^{246} + 2x^{90} + x^{82} + x^{54} + 2x^{30} + x^{10} + x^2$	LMPT [86]
$\zeta^{336}x^{270} + \zeta^{700}x^{244} + \zeta^{350}x^{162} + \zeta^{350}x^{84} +$ $+x^{54} + \zeta^{700}x^{36} + x^{28} + \zeta^{336}x^{10} + \zeta^{350}x^6$	Ganley [69]
$2x^{486} + 2x^{252} + \zeta^{294}x^{162} + \zeta^{294}x^{84} +$ $+\zeta^{28}x^{54} + \zeta^{28}x^{28} + 2x^{18} + \zeta^{294}x^6 + \zeta^{84}x^2$	CG [48]
$\zeta^{140}x^{324} + \zeta^{504}x^{246} + \zeta^{284}x^{108} + \zeta^{504}x^{90} + \zeta^{674}x^{82} +$ $+\zeta^{506}x^{54} + \zeta^{726}x^{30} + \zeta^{225}x^{28} + \zeta^{140}x^{12} + \zeta^{388}x^4 + \zeta^{532}x^2$	ZP [112]
x^{122}	CM [51]

Considering $k = 2$ and $m = 3$, a p^m-polynomial is of the form $L(x) = ax^{3^3} + bx$. With $F(x) = x^{p+1}$ (it is not planar over $\mathbb{F}_{3^6}$) the isotopic shift with $L(x) = \zeta^2 x^{3^3} + x$ (i.e. the case $L_1(x) = L_2(x)$),

$$F_L(x) = \zeta^6 x^{82} + \zeta^2 x^{30} + 2x^4$$

is planar and affine equivalent to the ZP function.

We searched for similar structures in other even dimensions. Over $\mathbb{F}_{3^{2m}}$ with $L(x) = ax^{p^m} + x$, $a \neq 0$, and $F(x) = x^{p^i+1}$ we obtained the following results:

- with $m = 3$ over $\mathbb{F}_{3^6}$ for $i = 1$ all the planar maps constructed are affine equivalent to the ZP map.

- with $m = 4,5$ no planar maps are constructed;
- with $m = 6$, over $\mathbb{F}_{3^{12}}$ for $i = 2,4$ planar maps are constructed. Due to the large dimension of the finite field, it was not possible to check with MAGMA the equivalence to known families.

Over $\mathbb{F}_{3^{2m}}$ with $m = 3,4,5,6$ we consider also the generalised isotopic shifts with $L_1(x) = a_1x^{3^3} + x$ and $L_2(x) = a_2x^{3^3} + x$. So the isotopic shift of x^{p^i+1} is given by

$$F(x) = a_1x^{p^i+p^m} + a_2^{p^m}x^{p^{m+i}+1} + 2x^{p^i+1}.$$

Over $\mathbb{F}_{3^6}$ the obtained planar functions are equivalent to the Albert function x^{10} or to the ZP function. Over all the other fields we obtained several planar functions, but it is not currently possible to check with MAGMA the CCZ-equivalence to the known families, with the exception of some particular cases over $\mathbb{F}_{3^8}$. Indeed for x^{3^4+1} when $a_1 = 0$ we obtain the functions $a_2^{3^4}x^2 + 2x^{3^4+1}$ which are equivalent to x^2 (see for instance [81]).

Chapter 8

On the boomerang uniformity of some permutation polynomials

The boomerang uniformity and the boomerang connectivity table are important cryptographic properties of S-boxes which were first introduced and studied in [16, 46]. In [16] the authors also gave the classification of all differentially 4-uniform permutations of 4 bits. Moreover, they obtained the boomerang uniformities for two classes of differentially 4-uniform functions, the inverse function and the Gold functions over $\mathbb{F}_{2^n}$ for n even.

Recently, Li et al. [84] gave an equivalent definition for the BCT (and the boomerang uniformity) and provided a characterisation by means of the Walsh transform of functions with a fixed boomerang uniformity. Moreover, they gave an upper bound for the boomerang uniformity of quadratic permutations, and provided also a class of quadratic permutations (related to the Gold functions), defined for $n \equiv 2 \mod 4$, with differential 4-uniformity and boomerang 4-uniformity. The boomerang uniformity of differentially 4-uniform permutations obtained from the inverse function by swapping the image of 0 and 1 is also obtained in [84].

Another recent paper by Mesnager et al. [91] studies the boomerang uniformity of quadratic permutations. In particular, from their results it is possible to obtain the boomerang uniformity of the Gold functions and the class studied in [84], and also the boomerang uniformity of the binomials studied in [19].

In this chapter we continue the study of the boomerang uniformity of the known classes of differentially 4-uniform permutations listed in Table 2.8. In particular, in Section 8.1, we consider the Bracken-Leander cubic function $x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{2^n}$ with $n = 4k$, presented in [18]. In [84], the value

of its boomerang uniformity, when $k = 1,3$, is obtained computationally: it is equal to 4 for $k = 1$ and to 14 for $k = 3$. The observation of only two values does not give much information about the general behaviour of the boomerang uniformity of the Bracken-Leander map. We further study this function and, in Theorem 8.1, we show that its boomerang uniformity is upper bounded by 24. Using the software MAGMA and Proposition 8.1 it is possible to verify that in small dimensions this upper bound can be attained. Further, in Section 8.2 we consider three other promising classes of differentially 4-uniform permutations. These classes have maximum algebraic degree $n-1$ and are obtained in [85, 108] by modifying the inverse function. In Theorems 8.3, 8.4 and 8.5 we show that the boomerang uniformity of these permutations is either 6, 8 or 10.

8.1 On the Bracken-Leander map

For an odd integer k, let $q = 2^k$ and consider the finite field with 2^{4k} elements $\mathbb{F}_{2^{4k}} = \mathbb{F}_{q^4}$. Over this field consider the differentially 4-uniform permutation

$$F(x) = x^{2^{2k}+2^k+1} = x^{q^2+q+1}.$$

In the following we show that

Theorem 8.1. *Let $k > 1$ be odd. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{2^{4k}}$ is such that $\beta_F \leq 24$.*

Before proving Theorem 8.1 we prove two lemmata (the definition of $S_{a,b}$ has been given in Subsection 2.3.2).

Lemma 8.1. *Let $k > 1$ be odd and $q = 2^k$. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{q^4}$ is such that*

$$S_{1,b} \leq \begin{cases} 4 & \text{if } b \in \mathbb{F}_{q^2}^\star \text{ and } \mathrm{Tr}_1^{2k}(b) = 0 \\ 6 & \text{if } b \in \mathbb{F}_{q^2}^\star \text{ and } \mathrm{Tr}_1^{2k}(b) = 1 \\ 4m+4 & \text{if } b \notin \mathbb{F}_{q^2} \end{cases}$$

where m is the number of the solutions $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ of

$$b^{q^2} + b = \alpha^{q+1} \frac{(\alpha^{2q} + \alpha)(\alpha + 1)}{(\alpha^q + \alpha)^2}.$$

Proof. We want to study the number of solutions $(x,\alpha) \in \mathbb{F}_{q^4} \times \mathbb{F}_{q^4}$, for $b \in \mathbb{F}_{q^4}^\star$, of

$$\begin{cases} D_1 D_\alpha F(x) = 0 \\ D_\alpha F(x) = b \end{cases}$$

In particular, we have the following

$$\begin{aligned} D_\alpha F(x) =& (x+\alpha)^{q^2+q+1} + x^{q^2+q+1} \\ =& x^{q^2+q}\alpha + x^{q^2+1}\alpha^q + x^{q+1}\alpha^{q^2} + x^{q^2}\alpha^{q+1} + x^q\alpha^{q^2+1} + x\alpha^{q^2+q} + \alpha^{q^2+q+1}. \end{aligned}$$

And therefore

$$\begin{aligned} D_1 D_\alpha F(x) =& (x^{q^2} + x^q + 1)\alpha + (x^{q^2} + x + 1)\alpha^q + (x^q + x + 1)\alpha^{q^2} \\ &+ \alpha^{q+1} + \alpha^{q^2+1} + \alpha^{q^2+q} \\ =& y^q(\alpha + \alpha^q) + y(\alpha^q + \alpha^{q^2}) + \alpha + \alpha^q + \alpha^{q^2} + \alpha^{q+1} + \alpha^{q^2+1} + \alpha^{q^2+q}, \end{aligned}$$

where $y = x^q + x$. Hence, we have that $y^q + y = x^{q^2} + x$ is an element of $\mathbb{F}_{q^2}$, so $y^{q^3} = y^{q^2} + y^q + y$. For simplicity, let us denote $R = D_1 D_\alpha F(x) = 0$. Thus

$$R^q = y^{q^2}(\alpha^q + \alpha^{q^2}) + y^q(\alpha^{q^2} + \alpha^{q^3}) + \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \alpha^{q^2+q} + \alpha^{q^3+q} + \alpha^{q^3+q^2},$$

and using the fact that $y^{q^3} = y^{q^2} + y^q + y$

$$\begin{aligned} R^{q^2} =& y^{q^2}(\alpha^{q^2} + \alpha) + y^q(\alpha^{q^2} + \alpha^{q^3}) + y(\alpha^{q^2} + \alpha^{q^3}) \\ &+ \alpha^{q^2} + \alpha^{q^3} + \alpha + \alpha^{q^3+q^2} + \alpha^{q^2+1} + \alpha^{q^3+1}. \end{aligned}$$

Then

$$\begin{aligned} 0 =& R^q + R^{q^2} \\ =& y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} + \alpha^q + \alpha + \alpha^{q^2+q} + \alpha^{q^3+q} + \alpha^{q^2+1} + \alpha^{q^3+1} \\ =& y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} + \alpha^q + \alpha + (\alpha^q + \alpha)^{q^2+1}. \end{aligned}$$

Since $y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha)^{q^2} \in \mathbb{F}_{q^2}$ and $(\alpha^q + \alpha)^{q^2+1} \in \mathbb{F}_{q^2}$ then also $(\alpha^q + \alpha) \in \mathbb{F}_{q^2}$. Then, we can rewrite the equation as

$$\begin{aligned} 0 =& y^{q^2}(\alpha^q + \alpha) + y(\alpha^q + \alpha) + \alpha^q + \alpha + (\alpha^q + \alpha)^2 = (\alpha^q + \alpha)(y^{q^2} + y + \alpha^q + \alpha + 1) \\ =& (\alpha^q + \alpha)(x^{q^3} + x^{q^2} + x^q + x + \alpha^q + \alpha + 1). \end{aligned}$$

Therefore one of the following conditions is satisfied:

1. $\alpha^q + \alpha = 0$, that is, $\alpha \in \mathbb{F}_q$;

2. $\mathrm{Tr}_k^{4k}(x) = x^{q^3} + x^{q^2} + x^q + x = \alpha^q + \alpha + 1$.

Case 1: $\alpha \in \mathbb{F}_q$.
We have $R = \alpha + \alpha^2 = 0$, hence $\alpha \in \mathbb{F}_2$. We do not consider the case $\alpha = 0$, therefore for $\alpha = 1$ we know that the equation $D_\alpha F(x) = b$ admits at most 4 solutions. So, for any b the number of solutions of type (x,α) with $\alpha \in \mathbb{F}_q$ is at most 4.

Case 2: $\mathrm{Tr}_k^{4k}(x) = x^{q^3} + x^{q^2} + x^q + x = \alpha^q + \alpha + 1$.
In this case, we need to compute the number of solutions (x,α) with $\alpha \notin \mathbb{F}_q$. Since $\mathrm{Tr}_k^{4k}(x) \in \mathbb{F}_q$, we have that $\alpha^q + \alpha \in \mathbb{F}_q^\star$. Therefore, $\alpha^{q^2} + \alpha = 0$, so we have $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Then, we have $R = (\alpha^q + \alpha)(y^q + y) + \alpha^q + \alpha^2 = (\alpha^q + \alpha)(x^{q^2} + x) + \alpha^q + \alpha^2$, and the system that we have to analyse is the following

$$\begin{cases} \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \\ \mathrm{Tr}_k^{4k}(x) = \alpha^q + \alpha + 1 \\ (\alpha^q + \alpha)(x^{q^2} + x) = \alpha^q + \alpha^2 \\ D_\alpha F(x) = b. \end{cases} \tag{8.1}$$

It is clear that, for a fixed α, if $\bar{x}$ is a solution of the first three equations in (8.1), then all the other solutions (for these equations) are $\bar{x} + w$ for any $w \in \mathbb{F}_{q^2}$. Moreover, since $\alpha^q + \alpha \neq 0$, denoting by $\gamma = \frac{\alpha^q + \alpha^2}{\alpha^q + \alpha}$, we have $x^{q^2} = x + \gamma$.
The last equation is

$$\begin{aligned} b =& D_\alpha F(x) = x^{q^2+q}\alpha + x^{q^2+1}\alpha^q + x^{q+1}\alpha + x^{q^2}\alpha^{q+1} + x^q\alpha^2 + x\alpha^{q+1} + \alpha^{q+2} \\ =& (x+\gamma)x^q\alpha + (x+\gamma)x\alpha^q + x^{q+1}\alpha + (x+\gamma)\alpha^{q+1} + x^q\alpha^2 + x\alpha^{q+1} + \alpha^{q+2} \\ =& x^q\alpha(\gamma+\alpha) + x^2\alpha^q + x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha). \end{aligned}$$

For $w \in \mathbb{F}_{q^2}$, there exist unique $r,s \in \mathbb{F}_q$ such that $w = r\alpha + s$. Hence, we have

$$\begin{aligned} D_\alpha F(x+w) &= (x^q + r\alpha^q + s)\alpha(\gamma+\alpha) + (x^2 + r^2\alpha^2 + s^2)\alpha^q + (x + r\alpha + s)\alpha^q\gamma \\ &\quad + \alpha^{q+1}(\gamma+\alpha) \\ &= D_\alpha F(x) + \gamma(r\alpha^{q+1} + s\alpha + r\alpha^{q+1} + s\alpha^q) + r\alpha^{q+2} + s\alpha^2 + r^2\alpha^{q+2} + s^2\alpha^q \\ &= D_\alpha F(x) + \gamma s(\alpha + \alpha^q) + \alpha^{q+2}(r + r^2) + s(\alpha^2 + s\alpha^q) \\ &= D_\alpha F(x) + (\alpha^q + \alpha^2)s + \alpha^{q+2}(r + r^2) + s(\alpha^2 + s\alpha^q) \\ &= D_\alpha F(x) + \alpha^q(s + s^2) + \alpha^{q+2}(r + r^2). \end{aligned}$$

Then, $D_\alpha F(x+w) = D_\alpha F(x) = b$ if and only if $\alpha^q(s+s^2) + \alpha^{q+2}(r+r^2) = 0$. Since $\alpha \neq 0$, we have that $(s+s^2) + \alpha^2(r+r^2) = 0$ if and only if both $s+s^2$ and $r+r^2$ are zero ($r,s \in \mathbb{F}_q$ and $\alpha \notin \mathbb{F}_q$). Hence, fixed $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, if $\bar{x}$ is a solution of $D_\alpha F(x) = b$, then we can have only three more solutions, which are $\bar{x}+\alpha, \bar{x}+1, \bar{x}+\alpha+1$.

Consider now the following

$$\begin{aligned} b^{q^2} + b =& x^{q^3}\alpha(\gamma+\alpha) + x^{2q^2}\alpha^q + x^{q^2}\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) + x^q\alpha(\gamma+\alpha) + x^2\alpha^q \\ &+ x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ =&(x+\gamma)^q\alpha(\gamma+\alpha) + (x+\gamma)^2\alpha^q + (x+\gamma)\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ &+ x^q\alpha(\gamma+\alpha) + x^2\alpha^q + x\alpha^q\gamma + \alpha^{q+1}(\gamma+\alpha) \\ =&\gamma^q\alpha(\gamma+\alpha) = \frac{\alpha+\alpha^{2q}}{\alpha^q+\alpha}\alpha\frac{\alpha^q(\alpha+1)}{\alpha^q+\alpha} = \alpha^{q+1}\frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}. \end{aligned}$$

Now, if $b \in \mathbb{F}_{q^2}$ we have either $\gamma = 0$ or $\gamma = \alpha$.

- If $\gamma = 0$, then from (8.1) we obtain $\alpha^q = \alpha^2$, $x \in \mathbb{F}_{q^2}$ and $\alpha^q + \alpha + 1 = 0$, implying that $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$.
- If $\gamma = \alpha$ then $\frac{\alpha^q+\alpha^2}{\alpha^q+\alpha} + \alpha = \frac{\alpha^q(\alpha+1)}{\alpha^q+\alpha} = 0$. This leads to $\alpha = 1$ (already studied).

Thus, for the case $b \in \mathbb{F}_{q^2}$, we need to count the number of solutions x of the following systems:

$$(I)\begin{cases} D_1D_1F(x) = 0 \\ D_1F(x) = b, \end{cases} \qquad (II)\begin{cases} x^{q^2} + x = 0 \\ D_1D_\omega F(x) = 0 \\ D_\omega F(x) = b, \end{cases} \qquad (III)\begin{cases} x^{q^2} + x = 0 \\ D_1D_{\omega^2} F(x) = 0 \\ D_{\omega^2} F(x) = b, \end{cases}$$

where ω is a primitive element of $\mathbb{F}_4$.

Since we have the restriction $x^{q^2} + x = 0$, solving System (II) and (III) is equivalent to solve the systems

$$(II')\begin{cases} D_1D_\omega G(x) = 0 \\ D_\omega G(x) = b, \end{cases} \qquad (III')\begin{cases} D_1D_{\omega^2} G(x) = 0 \\ D_{\omega^2} G(x) = b, \end{cases}$$

defined over $\mathbb{F}_{q^2}$, where $G(x) = F_{|_{\mathbb{F}_{q^2}}}(x) = x^{q+2}$.

Note that, for all these systems the equations involving the second derivative are satisfied for any $x \in \mathbb{F}_{q^2}$. Moreover, the function $G : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is a Gold

function with boomerang uniformity 4 (see [16]) and we can have that at most one system between (II') and (III') admits 4 solutions.

Suppose now that $b \in \mathbb{F}_{q^2}$ and one between System (II) or (III) admits 4 solutions. We need to determine the number of solutions of System (I), that is, we need to study the number of solutions of $D_1F(x) = b$. Let us consider, therefore, the proof of Theorem 1 in [18], in which the authors study the differential uniformity of F. According to their notation, we have $c = b + 1 \in \mathbb{F}_{q^2}$ and $t = \mathrm{Tr}(x) = \mathrm{Tr}(c) = 0$. If we consider now Equation (5) in [18] we have the following condition:

$$0 = (x + x^{q^2})^2 + (t+1)(x + x^{q^2}) + c^q + c^{q^3} = (x + x^{q^2})^2 + (x + x^{q^2}).$$

Hence $x + x^{q^2} = 0, 1$. The only possibility is $x^{q^2} = x + 1$, otherwise we would obtain a solution $x \in \mathbb{F}_{q^2}$ of $D_1G(x) = b$ in contradiction with the boomerang uniformity of G. This restriction leads us to

$$\begin{aligned} D_1F(x) &= x^{q^2+q} + x^{q^2+1} + x^{q+1} + x^{q^2} + x^q + x + 1 \\ &= (x+1)x^q + (x+1)x + x^{q+1} + x + 1 + x^q + x + 1 = x^2 + x \\ 0 &= x^2 + x + b. \end{aligned}$$

This last equation implies that we have, for $\alpha = 1$, at most 2 solutions. Moreover, since from $x^2 = x + b$ we obtain that $x^{q^2} = x + \mathrm{Tr}_1^{2k}(b)$, we can have these two more solutions if and only if $\mathrm{Tr}_1^{2k}(b) = 1$. Hence, in total we can have at most 6 solutions when $\mathrm{Tr}_1^{2k}(b) = 1$.

On the other hand, if $b \in \mathbb{F}_{q^2}$ and $\mathrm{Tr}_1^{2k}(b) = 0$ we can have only solutions $x \in \mathbb{F}_{q^2}$ for all the three systems. Therefore, since $G(x) = F_{|_{\mathbb{F}_{q^2}}}(x)$ we can have at most only one of the systems admitting 4 solutions.

For $b \notin \mathbb{F}_{q^2}$, let m be the number of roots of the equation $b^{q^2} + b = \alpha^{q+1}\frac{(\alpha^{2q}+\alpha)(\alpha+1)}{(\alpha^q+\alpha)^2}$ such that $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then, for any of these roots we can have 4 possible x plus the 4 possible solutions when $\alpha = 1$. Hence, we have $S_{1,b} \leq 4 \cdot (m+1)$. □

Remark 8.1. *For the case $b \in \mathbb{F}_{q^2}$ it is possible to show that six solutions are possible. Consider $b = \omega$, where ω is a primitive element of $\mathbb{F}_4$. First of all, it is easy to check that any $x \in \mathbb{F}_4$ is a solution of System (II) in the proof of Lemma 8.1. Moreover, we have that $\mathrm{Tr}_1^{2k}(b) = 1$, so there exist two solutions in $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ of System (I) in Lemma 8.1. So, we have that $S_{1,\omega} = 6$.*

Lemma 8.2. *Let $k > 1$ be odd and $q = 2^k$. For any $b \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ the equation*

$$b^{q^2} + b = \alpha^{q+1} \frac{(\alpha^{2q} + \alpha)(\alpha + 1)}{(\alpha^q + \alpha)^2}$$

admits at most 5 solutions $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Proof. Consider the equation

$$b^{q^2} + b = \alpha^{q+1} \frac{(\alpha^{2q} + \alpha)(\alpha + 1)}{(\alpha^q + \alpha)^2}. \tag{8.2}$$

Then, we have also the relation

$$\mathrm{Tr}_k^{4k}(b) = \alpha^{q+1} \frac{(\alpha^{q+1} + 1)}{\alpha^q + \alpha}. \tag{8.3}$$

Let $d = b^{q^2} + b$ and $e = \mathrm{Tr}_k^{4k}(b) = d^q + d \in \mathbb{F}_q$.

If $d \in \mathbb{F}_q$, then $e = 0$ and therefore $\alpha^{q+1} = 1$ and $\alpha^q = \alpha^{-1}$. This leads to

$$d = 1 \cdot \frac{(\frac{1}{\alpha^2} + \alpha)(\alpha + 1)}{\frac{1}{\alpha^2} + \alpha^2} = \frac{1 + \alpha^3}{\alpha^2}(\alpha + 1)\frac{\alpha^2}{(1+\alpha)^4} = \frac{1 + \alpha^3}{(1+\alpha)^3} = \frac{\alpha^2 + \alpha + 1}{1 + \alpha^2}.$$

Hence $\alpha^2(d + 1) + \alpha + 1 + d = 0$, that has at most 2 solutions. in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ if and only if $\mathrm{Tr}_1^k(d) = 0$. Indeed, if $\mathrm{Tr}_1^k(d) = 1$ we would have $\mathrm{Tr}_1^k(d^2 + 1) = 0$ and thus the equation admits 2 solutions in $\mathbb{F}_q$.

Now, consider the case $d \notin \mathbb{F}_q$ and thus $e \neq 0$. Denoting by $\gamma = \frac{\alpha^q + \alpha^2}{\alpha^q + \alpha}$, we have $d = \gamma^q \alpha(\gamma + \alpha)$ and

$$e = d^q + d = \gamma^{q+1}(\alpha^q + \alpha) + \gamma\alpha^{2q} + \gamma^q\alpha^2.$$

Since $d \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ we can write α as $\alpha = rd + s$, with $r, s \in \mathbb{F}_q, r \neq 0$. Therefore, we have $\alpha^q + \alpha = r(d^q + d) = re$. From $d(\alpha^q + \alpha)^2 = \alpha^{q+1}(\alpha^{2q} + \alpha)(\alpha + 1)$ (Equation (8.2)) we get

$$\begin{aligned} s^5 =& s^4 r d^q + s^3(r^2e^2 + 1) + s^2(r^3 d^q e^2 + r^2 e^2 + r d^q) \\ &+ s(r^4 d^{2q+2} + r^3 e^3 + r^2 d^2) + r^5 d^{3q+2} + r^4 d^{q+1} e^2 + r^3 d^{q+2} + r^2 d e^2. \end{aligned} \tag{8.4}$$

From $e(\alpha^q + \alpha) = \alpha^{q+1}(\alpha^{q+1} + 1)$ (Equation (8.3)) we get

$$s^4 = s^2(r^2e^2 + 1) + sre + re^2 + r^4 d^{2q+2} + r^2 d^{q+1}. \tag{8.5}$$

To simplify the equation, let us introduce the variable $A = re + 1$. Then we can rewrite Equation (8.4) as

$$\begin{aligned} s^5 =& s^4 r d^q + s^3 A^2 + s^2(r d^q A^2 + A^2 + 1) + s(r^4 d^{2q+2} + r^3 e^3 + r^2 d^2) \\ &+ r^5 d^{3q+2} + r^4 d^{q+1} e^2 + r^3 d^{q+2} + r^2 d e^2, \end{aligned}$$

and Equation (8.5) as

$$s^4 = s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1}.$$

Substituting the second one in the first one we obtain

$$\begin{aligned}
0 =& s(s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1}) \\
&+ (s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1})rd^q + s^3A^2 + s^2(rd^qA^2 + A^2 + 1) \\
&+ s(r^4d^{2q+2} + r^3e^3 + r^2d^2) + r^5d^{3q+2} + r^4d^{q+1}e^2 + r^3d^{q+2} + r^2de^2 \\
=& s^3A^2 + s^2re + s(re^2 + r^4d^{2q+2} + r^2d^{q+1}) + s^2A^2rd^q + sr^2d^qe + r^2d^qe^2 \\
&+ r^5d^{3q+2} + r^3d^{2q+1} + s^3A^2 + s^2(rd^qA^2 + A^2 + 1) \\
&+ s(r^4d^{2q+2} + r^3e^3 + r^2d^2) + r^5d^{3q+2} + r^4d^{q+1}e^2 + r^3d^{q+2} + r^2de^2 \\
=& s^2(A^2 + A) + s(re^2 + r^3e^3 + r^2e^2) + r^2e^3 + r^4d^{q+1}e^2 + r^3d^{q+1}e \\
=& s^2reA + sre^2(1 + rA) + r^2e(e^2 + rd^{q+1}A) \\
=& re[s^2A + se(1 + rA) + r(e^2 + rd^{q+1}A)].
\end{aligned}$$

Since $r, e \neq 0$, denoting by $B = e(1 + rA)$ and by $C = r(e^2 + rd^{q+1}A)$ we have

$$0 = s^2A + sB + C. \tag{8.6}$$

Replacing (8.6), hence $s^2A = sB + C$, into (8.5) ($s^4 = s^2A^2 + sre + K$, with $K = re^2 + r^4d^{2q+2} + r^2d^{q+1}$) we have

$$s^4 = A(sB + C) + sre + K = s(AB + re) + AC + K.$$

Thus raising (8.6) to the power of two and substituting s^4 we obtain

$$s^2B^2 = s(A^3B + A^2re) + A^3C + A^2K + C^2.$$

Using (8.6) (multiplied by B^2) we obtain

$$As^2B^2 = sB^3 + B^2C = s(A^4B + A^3re) + A^4C + A^3K + AC^2,$$

which implies

$$0 = s(B^3 + A^4B + A^3re) + B^2C + A^4C + A^3K + AC^2 = s\bar{D} + \bar{E}.$$

Therefore

$$\begin{aligned}\bar{D} =& B^3 + A^4B + A^3re = (e + reA)^3 + A^4(e + reA) + A^3re\\ =& e[e^2 + Are^2 + A^2],\\ \bar{E} =& B^2C + A^4C + A^3K + AC^2\\ =& (e^2 + A^2r^2e^2)(re^2 + Ar^2d^{q+1}) + A^4(re^2 + Ar^2d^{q+1})\\ &+ A^3(re^2 + r^4d^{2q+2} + r^2d^{q+1}) + A(r^2e^4 + A^2r^4d^{2q+2})\\ =& e[A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3].\end{aligned}$$

Let $D = \bar{D}e^{-1}$ and $E = \bar{E}e^{-1}$, then $Ds = E$ with

$$D = e^2 + Are^2 + A^2 \text{ and } E = A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3.$$

Using this last relation inside (8.6) we have

$$\begin{aligned}0 =& D^2(s^2A + sB + C)\\ =& D^2s^2A + D^2sB + D^2C\\ =& E^2A + DEB + D^2C.\end{aligned}$$

Now, since

$$\begin{aligned}AE^2 =& A^5r^4e^4 + A^3r^4d^{2q+2}e^2 + A^3r^4e^6 + Ar^2e^6,\\ BDE =& A^5(r^3e^3 + r^3e^4 + r^2e^4 + d^{q+1}r^2e^2) + A^4(r^3d^{q+1}e^2 + r^2e^3),\\ &+ A^3(r^2e^4 + r^2e^5) + A^2re^4 + A(r^2e^6 + r^2d^{q+1}e^4) + re^6,\\ CD^2 =& A^5r^2d^{q+1} + A^4re^2 + A^3r^4d^{q+1}e^4 + A^2r^3e^6 + Ar^2d^{q+1}e^4 + re^6,\end{aligned}$$

we obtain

$$\begin{aligned}0 =& A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2)\\ &+ A^4(r^3d^{q+1}e^2 + re^4) + A^3(r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5)\\ =& A^3rP(r),\end{aligned} \tag{8.7}$$

with

$$\begin{aligned}P(r) =& A^2(r^3e^4 + r^2e^4 + r^2e^3 + rd^{q+1}e^2 + rd^{q+1} + e^2) + A(r^2d^{q+1}e^2 + e^4)\\ &+ r^3d^{2q+2}e^2 + r^3d^{q+1}e^4 + re^5\\ =& r^5e^6 + r^4(e^5 + e^6) + r^3(e^4 + d^{q+1}(e^2 + e^3) + d^{2q+2}e^2) + r^2(e^3 + d^{q+1}e^2)\\ &+ rd^{q+1}(e^2 + 1) + e^4 + e^2.\end{aligned}$$

We need to find solutions of Equation (8.7) related to some $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ that satisfies (8.2). Equation (8.7) is satisfied if either one of the following conditions is true

1. $A = 0$,
2. $r = 0$, not acceptable since $\alpha \notin \mathbb{F}_q$,
3. $P(r) = 0$.

Assume that $A = 0$ is a possible solution, therefore $r = \frac{1}{e}$ (it is related to an α for which (8.2) holds). From Equation (8.6) we obtain that $se + re^2 = 0$, therefore $s = 1$. From Equation (8.5) we have

$$\begin{aligned} s^4 &= s^2A^2 + sre + re^2 + r^4d^{2q+2} + r^2d^{q+1} \\ 1 &= 0 + 1 + e + \frac{d^{2q+2}}{e^4} + \frac{d^{q+1}}{e^2} \\ d^{2q+2} &= e^2d^{q+1} + e^5. \end{aligned}$$

Hence, we obtain that

$$\begin{aligned} r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5 &= r^4d^{q+1}e^4 + r^4e^7 + r^4d^{q+1}e^4 + r^2e^5 \\ &= r^2e^5(r^2e^2 + 1) = r^2e^5A^2 \end{aligned}$$

and using this equality we have that (8.7) becomes

$$\begin{aligned} 0 &= E^2A + DEB + D^2C \\ &= A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2) \\ &\quad + A^4(r^3d^{q+1}e^2 + re^4) + A^3(r^4d^{2q+2}e^2 + r^4d^{q+1}e^4 + r^2e^5) \\ &= A^5(r^4e^4 + r^3e^4 + r^3e^3 + r^2d^{q+1}e^2 + r^2d^{q+1} + re^2) + A^4(r^3d^{q+1}e^2 + re^4) + A^5r^2e^5 \\ &= A^4r[A(r^3e^4 + r^2e^4 + r^2e^3 + rd^{q+1}e^2 + rd^{q+1} + e^2 + re^5) + r^2d^{q+1}e^2 + e^4] \\ &= A^4rQ(r), \end{aligned}$$

where $Q(r)$ is a polynomial of degree at most 4. Therefore, if b is such that among the solution of (8.2) there is one for which $A = 0$, then at most we have 5 possible solutions r of (8.7).

Otherwise, if $A = 0$ is not a possible solution, then $P(r)$ can have at most 5 different roots. Hence, in total we have at most 5 different possible r.

We need to check, how many s there exist for any of these r. From the equation $Ds = E$ we know that, given a fixed r, unless $D = 0$, there exists only one

possible s. We need to study the case $D = A^2 + Are^2 + e^2 = 0$. From Equation (8.6), that is, $As^2 + Bs + C = 0$ we obtain that we can have at most two s for any r (in the case $D = 0$).

If $A = 0$, then (8.6) admits at most one solution since $B = Are + e = e \neq 0$. Also if $A \neq 0$ and $B = 0$, then the equation admits only one solution. In particular, (8.6) admits two solutions if and only if $B \neq 0$ and $\mathrm{Tr}\left(\frac{AC}{B^2}\right) = 0$. Hence, we need to study the system

$$\begin{cases} 0 \neq A \\ 0 \neq B = Are + e \\ 0 = D = A^2 + Are^2 + e^2 = A^2 + eB \\ 0 = E = A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 = re^2B + eC + B^2 + e^2A \end{cases}$$

Then, we have $A^2 = Are^2 + e^2$ and (substituting A) $r^2(e^2 + e^3) = re^2 + e^2 + 1$, that leads to the restriction $e \neq 1$. Using these relations inside E we obtain

$$\begin{aligned} 0 &= A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= (Are^2 + e^2)r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= Ar^3e^4 + r^2e^4 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 \\ &= r^4e^5 + r^3e^4 + r^2e^4 + r^3d^{q+1}e^2 + r^2d^{q+1}e + r^3e^4 + r^2e^3 + re^3 \\ &= re(r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2) \end{aligned} \tag{8.8}$$

which implies $r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2 = 0$ and thus

$$\begin{aligned} 0 &= (r^3e^4 + re^3 + r^2d^{q+1}e + rd^{q+1} + re^2 + e^2)(e^2 + e) \\ &= re^3r^2(e^2 + e^3) + r(e^5 + e^4) + d^{q+1}r^2(e^3 + e^2) + rd^{q+1}(e^2 + e) + (r + 1)(e^4 + e^3) \\ &= re^3(re^2 + e^2 + 1) + r(e^5 + e^4) + d^{q+1}(re^2 + e^2 + 1) + rd^{q+1}(e^2 + e) + (r + 1)(e^4 + e^3) \\ &= r^2e^5 + d^{q+1}(e^2 + 1) + rd^{q+1}e + e^3(e + 1) \\ 0 &= (r^2e^5 + d^{q+1}(e^2 + 1) + rd^{q+1}e + e^3(e + 1))(e + 1). \end{aligned}$$

Using the substitution $r^2(e^2 + e^3) = re^2 + e^2 + 1$ we have

$$\begin{aligned} 0 &= e^3(re^2 + e^2 + 1) + d^{q+1}(e + 1)^3 + rd^{q+1}(e^2 + e) + e^3(e + 1)^2 \\ &= r(e^5 + d^{q+1}(e^2 + e)) + d^{q+1}(e + 1)^3. \end{aligned}$$

Hence, we have only one possible r that satisfies the system. Now, from $r^2(e^2 +$

$e^3) + re^2 + e^2 + 1 = 0$ we have also

$$\begin{aligned}
0 =&(r^2(e^2+e^3) + re^2 + e^2 + 1)(e^4 + d^{q+1}(e+1)) \\
=&red^{q+1}(e+1)^3 + re^2d^{q+1}(e+1)^3 + ed^{q+1}(e+1)^3 + e^4(e+1)^2 + d^{q+1}(e+1)^3 \\
=&(e+1)^2(rd^{q+1}e(e+1)^2 + d^{q+1}(e+1)^2 + e^4) \\
=&(e+1)^2[(e+1)(re^5 + d^{q+1}(e+1)^3) + d^{q+1}(e+1)^2 + e^4] \\
=&(e+1)^2[re^5(e+1) + d^{q+1}(e+1)^4 + d^{q+1}(e+1)^2 + e^4] \\
=&(e+1)^2e^2[re^3(e+1) + d^{q+1}(e+1)^2 + e^2]
\end{aligned}$$

and thus $re^3(e+1) = d^{q+1}(e+1)^2 + e^2$. Moreover, from $re^3(e+1) + d^{q+1}(e+1)^2 + e^2 = 0$, we can obtain

$$\begin{aligned}
0 =&[re^3(e+1) + d^{q+1}(e+1)^2 + e^2](e^4 + d^{q+1}(e+1)) \\
=&e^2d^{q+1}(e+1)^4 + d^{q+1}e^4(e+1)^2 + e^6 + d^{2q+2}(e+1)^3 + d^{q+1}e^2(e+1) \\
=&e^3d^{q+1}(e+1) + e^6 + d^{2q+2}(e+1)^3 \\
d^{2q+2}(e+1)^3 =&e^3d^{q+1}(e+1) + e^6
\end{aligned}$$

From the two equations above we have also $re^3(1+e) = d^{q+1}(1+e)^2 + e^2$ and $d^{2q+2}(1+e)^3 = d^{q+1}e^3(1+e) + e^6$. We know that $e \neq 0, 1$ therefore

$$r = \frac{d^{q+1}(e+1)}{e^3} + \frac{1}{e(e+1)}.$$

Hence,

$$\begin{aligned}
A =&re + 1 \\
=&\frac{d^{q+1}(e+1)}{e^2} + \frac{e}{(e+1)} \\
A^2 =&\frac{d^{2q+2}(e+1)^2}{e^4} + \frac{e^2}{(e+1)^2} = \frac{d^{q+1}}{e} + \frac{e^3}{(e+1)^2} \\
0 =&D = A^2 + Are + e^2 \\
=&\frac{d^{q+1}}{e} + \frac{e^3}{(e+1)^2} + \left(\frac{d^{q+1}(e+1)}{e^2} + \frac{e}{(e+1)}\right)\left(\frac{d^{q+1}(e+1)}{e^2} + \frac{1}{(e+1)}\right) + e^2 \\
=&\frac{d^{q+1}}{e} + \frac{e^3}{(e+1)^2} + \frac{d^{2q+2}(e+1)^2}{e^4} + \frac{d^{q+1}(e+1)}{e^2} + \frac{e}{(e+1)^2} + e^2 \\
=&\frac{d^{q+1}}{e} + \frac{e^3}{(e+1)^2} + \frac{d^{q+1}}{e} + \frac{e^2}{(e+1)} + \frac{d^{q+1}(e+1)}{e^2} + \frac{e}{(e+1)^2} + e^2 \\
=&d^{q+1}(\frac{e+1}{e^2}) + e + e^2 + \frac{e^2}{e+1} = d^{q+1} \cdot \frac{e+1}{e^2} + \frac{e(e^2+e+1)}{e+1} \\
d^{q+1} =&\frac{e^3(e^2+e+1)}{(e+1)^2}.
\end{aligned}$$

Therefore

$$r = \frac{e^2+e+1}{e+1} + \frac{1}{e(e+1)} = \frac{(e+1)^2}{e}$$

and $A = re+1 = e^2$. Then

$$0 = E = A^2r^2e^2 + Ar^2d^{q+1}e + Ar^2e^3 + re^3 = (e+1)^3 \cdot e^2.$$

This last result is not possible since $e \neq 0,1$. So, the system admits no solutions.

Therefore we have that when $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, (8.2) admits at most 5 distinct values. □

Proof of Theorem 8.1. Since F is a power function, from Proposition 2.2 we can consider $a = 1$, and thus $\beta_F = \max_{b \in \mathbb{F}_{q^4}^\star} S_{1,b}$. From Lemma 8.1 and Lemma 8.2 we have immediately that $\beta_F \leq 24$. □

From the proof of Lemma 8.1 and Lemma 8.2 we can distinguish five cases for the upper bound on the values $S_{1,b}$. In particular, we obtain the following.

Proposition 8.1. *Let $k > 1$ be odd and $q = 2^k$. The Bracken-Leander permutation $F(x) = x^{2^{2k}+2^k+1}$ defined over $\mathbb{F}_{q^4}$ is such that*

$$S_{1,b} \leq \begin{cases} 4 & \text{if } b \in \mathbb{F}_{q^2}^\star \text{ and } \mathrm{Tr}_1^{2k}(b) = 0 \\ 6 & \text{if } b \in \mathbb{F}_{q^2}^\star \text{ and } \mathrm{Tr}_1^{2k}(b) = 1 \\ 4 & \text{if } b \notin \mathbb{F}_{q^2}, \mathrm{Tr}_{2k}^{4k}(b) \in \mathbb{F}_q \text{ and } \mathrm{Tr}_1^k(\mathrm{Tr}_{2k}^{4k}(b)) = 1 \\ 12 & \text{if } b \notin \mathbb{F}_{q^2}, \mathrm{Tr}_{2k}^{4k}(b) \in \mathbb{F}_q \text{ and } \mathrm{Tr}_1^k(\mathrm{Tr}_{2k}^{4k}(b)) = 0 \\ 24 & \text{otherwise.} \end{cases}$$

Using Lemma 8.1 we evaluated (with the help of MAGMA) the boomerang uniformity for the Bracken-Leander permutation up to dimension $n = 60$. From Table 8.1 we can see that for the values $7 \leq k \leq 15$ the upper bound for the boomerang uniformity is attained.

Table 8.1: Boomerang uniformity of the function $x^{2^{2k}+2^k+1}$ over $\mathbb{F}_{2^{4k}}$

k :	3	5	7	9	11	13	15
β_F :	14	16	24	24	24	24	24

8.2 On the inverse function modified

In the past years, several constructions of differentially 4-uniform bijective functions, based on modifying the inverse function, have been proposed (see for instance [85, 95, 98, 108, 110]). In particular, in [85, 108], the authors modified the inverse functions composing it with some cycles, and studied when it could be possible to obtain a differentially 4-uniform permutation. In the following we study the boomerang uniformity of some of the functions obtained in [85] and in [108].

Given $m+1$ different elements of $\mathbb{F}_{2^n}$, α_i for $0 \leq i \leq m$, consider the cycle $\pi = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ over $\mathbb{F}_{2^n}$ defined as

$$F_\pi(x) = \begin{cases} \alpha_{i+1} & x = \alpha_i \\ x & x \notin \{\alpha_i \,:\, 0 \leq i \leq m\}, \end{cases}$$

where $\alpha_{m+1} = \alpha_0$.

In [108] the authors study the inverse function composed with cycles of length two (that is π a transposition), while in [85] they consider a more general case of functions of the type

$$\mathrm{Inv}_\pi(x) = \begin{cases} \alpha_{i+1}^{-1} & x = \alpha_i \\ x^{-1} & x \notin \{\alpha_i \,:\, 0 \leq i \leq m\}. \end{cases}$$

From [108] we have that:

Lemma 8.3. *Let $n = 2k$ be an even integer. Then the following statements hold.*

1. *Suppose $\pi = (0,1)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of Inv_π equals 4 if and only if k is odd.*
2. *Suppose $\pi = (1,c)$ is a transposition over $\mathbb{F}_{2^n}$. Then the differential uniformity of Inv_π equals 4 if and only if $\mathrm{Tr}(c) = \mathrm{Tr}(\frac{1}{c}) = 1$.*

In [85] it has been proved the following:

Lemma 8.4. *Suppose $\pi = (\alpha_0, \ldots, \alpha_m)$ is a cycle over $\mathbb{F}_{2^n}$. Then the following statements hold.*

1. *If $0 \in \pi$, then Inv_π is affine equivalent to Inv_{π_1}, where π_1 is a cycle over $\mathbb{F}_{2^n}$ of the type $(0, 1, \beta_1, \ldots, \beta_{m-1})$.*

2. *If* $0 \notin \pi$, *then* Inv_π *is affine equivalent to* Inv_{π_1}, *where* π_1 *is a cycle over* $\mathbb{F}_{2^n}$ *of the type* $(1, \beta_1, \ldots, \beta_m)$.

Recalling that the boomerang uniformity is invariant under affine equivalence, when $m = 1$ we need to consider, up to affine equivalence, only two types of permutations Inv_π:

- $\pi = (0,1)$,
- $\pi = (1,c)$, with $c \neq 0,1$.

In [84] Li et al. studied the boomerang uniformity of Inv_π with $\pi = (0,1)$. They obtained the following result.

Theorem 8.2. *Let* $F = \mathrm{Inv}_\pi$, *for* $\pi = (0,1)$, *and* $n \geq 3$. *Then the boomerang uniformity of* F *is*

$$\beta_F = \begin{cases} 10, & if\ n \equiv 0 \mod 6, \\ 8, & if\ n \equiv 3 \mod 6, \\ 6, & if\ n \not\equiv 0 \mod 3. \end{cases}$$

In the following we consider the case $\pi = (1,c)$.

Theorem 8.3. *Let* n *be even and* $F = \mathrm{Inv}_\pi$ *with* $\pi = (1,c)$ *be a differentially 4-uniform function over* $\mathbb{F}_{2^n}$. *Then,*

(i) if $c \notin \mathbb{F}_4$

$$\beta_F = \begin{cases} 10, & if\ n \equiv 0 \mod 4, \\ 8, & if\ n \equiv 2 \mod 4. \end{cases}$$

(ii) if $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ *(thus* $n \equiv 2 \mod 4$*)* $\beta_F = 6$.

Since the proof of Theorem 8.3 relies just on the study of all possible subcases that we can obtain from system (2.5), we omit it here. The proof is fully presented in Appendix B.

From Theorem 8.2 and Theorem 8.3 we obtain the following corollary.

Corollary 8.1. *Let* $n = 2k$ *and* $\pi = (\alpha_1, \alpha_2)$. *Consider the function* $F = \mathrm{Inv}_\pi$ *defined over* $\mathbb{F}_{2^n}$ *and suppose that* F *is differentially 4-uniform. Then,*

(i) if $0 \in \pi$, *then* k *is odd and*

$$\beta_F = \begin{cases} 10, & if\ n \equiv 0 \mod 6, \\ 6, & otherwise. \end{cases}$$

(ii) if $0 \notin \pi$, *then*

(a) if $\frac{\alpha_2}{\alpha_1} \notin \mathbb{F}_4^\star$, *then*

$$\beta_F = \begin{cases} 10 & if\ n \equiv 0 \mod 4 \\ 8 & if\ n \equiv 2 \mod 4. \end{cases}$$

(b) if $\frac{\alpha_2}{\alpha_1} \in \mathbb{F}_4^\star$, *then* k *is odd and* $\beta_F = 6$.

Proof. If $0 \in \pi$ then from Lemma 8.4 we have that $F = \mathrm{Inv}_\pi$ is affine equivalent to Inv_{π_0} where $\pi_0 = (0,1)$. So from Theorem 8.2 and since in the case $n \equiv 3 \mod 6$ F cannot be differentially 4-uniform, we have our claim.

Suppose now that $\alpha_1, \alpha_2 \neq 0$. From Lemma 8.4 we have that $\alpha_1^{-1}\pi(\alpha_1 x) = \pi_1(x)$ where $\pi_1(x) = (1, \beta_1)$ with $\beta_1 = \frac{\alpha_2}{\alpha_1}$, and thus $F = \mathrm{Inv}_\pi$ is affine equivalent to $\mathrm{Inv}_{\pi_1}(x) = \alpha_1 \mathrm{Inv}_\pi(\alpha_1 x)$. From Theorem 8.3 we obtain the claim. □

In [85], the authors extend the results obtained in [108] modifying the inverse function with cycles of order greater than two. In particular from their results we have the following differentially 4-uniform functions.

Lemma 8.5. *Let* $n = 2k$ *with* $k > 1$. *Let* $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, *then the functions* $F = \mathrm{Inv}_{\pi_1}$ *with* $\pi_1 = (0,1,c)$ *and* $G = \mathrm{Inv}_{\pi_2}$ *with* $\pi_2 = (1,c,c^2)$ *are differentially 4-uniform if and only if* k *is odd.*

Using a similar analysis as in Theorem 8.3 we can get the following results (we give some steps of the proof in Appendix B).

Theorem 8.4. *Let* $n = 2k$ *with* $k > 1$ *odd. Let* $F = \mathrm{Inv}_\pi$ *with* $\pi = (0,1,c)$ *and* $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, *be a differentially 4-uniform function over* $\mathbb{F}_{2^n}$. *Then,*

$$\beta_F = \begin{cases} 8 & if\ n \equiv 0 \mod 6 \\ 6 & otherwise. \end{cases}$$

Theorem 8.5. *Let* $n = 2k$ *with* $k > 1$ *odd. Let* $F = \mathrm{Inv}_\pi$ *with* $\pi = (1,c,c^2)$ *and* $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, *be a differentially 4-uniform function over* $\mathbb{F}_{2^n}$. *Then,*

$$\beta_F = \begin{cases} 8 & if\ n \equiv 0 \mod 6 \\ 6 & otherwise. \end{cases}$$

With same arguments as in Corollary 8.1 we have the following.

Corollary 8.2. *Let $n = 2k$ with k odd and $\pi = (\alpha_1, \alpha_2, \alpha_3)$ with $\alpha_1, \alpha_2, \alpha_3 \in \gamma\mathbb{F}_4$ for some $\gamma \in \mathbb{F}_{2^n}^\star$. Consider the function $F = \mathrm{Inv}_\pi$ defined over $\mathbb{F}_{2^n}$ and suppose that F is differentially 4-uniform. Then,*

$$\beta_F = \begin{cases} 8 & \text{if } n \equiv 0 \mod 6 \\ 6 & \text{otherwise.} \end{cases}$$

Chapter 9

Conclusions

This work is dedicated to three different problems in the area of cryptographically significant discrete functions. These problems concern respectively the APN property, the planar property and the boomerang uniformity. They are connected to each other and, to address them, we combined theoretical analysis with computational results.

The first problem relates to a study, construction and classification of infinite families of APN functions, in particular, quadratic APN functions. Here we first considered an already known construction of the form $L_1(x^3) + L_2(x^9)$ (see [30, 31]), for L_1 and L_2 linear, and derived more conditions for the APN property. Furthermore, we verified that many of the APN functions listed in [66] are of this particular form. We leave as a topic for future research to determine whether other known APN functions are CCZ-equivalent to a function of this type.

Then we considered the parallelism between APN and planar functions. Isotopic equivalence is a notion defined for quadratic planar functions in odd characteristic and it cannot be extended directly to APN functions in fields of even characteristic. It is an open problem whether, for the APN case, there exists an equivalence relation analogous to the isotopic equivalence. We investigated this problem and, from the analysis of isotopic equivalence, we introduce the concept of isotopic shift. We applied this concept to APN functions and obtained a useful construction method. In particular, applied to Gold maps, it provided theoretical conditions covering some known examples and producing one new case of an APN function. We conjectured that the obtained construction produces APN functions for an infinite number of dimensions. A generalisation of the isotopic shift construction led to further results. In particular, it yielded a family of quadratic APN functions covering some known

examples and producing several new cases of APN maps. Thanks to this result, all known APN functions in dimension 9 are now covered by an APN family. Furthermore, we proved that in odd dimensions the generalised isotopic shift connects every known APN power function (except the Dobbertin map) to a Gold function. Much is still to be studied regarding this construction method.

Further, we studied already known infinite families of APN functions and we proved that the two families introduced in [17, 26] (and their generalisations given in [62]) are EA-equivalent to each other. Besides, we showed that all these families are contained in another family of APN functions, the hexanomials introduced in [26]. This led to one of the main results of this work: we reduced the list of known infinite families of APN functions to families which are pairwise inequivalent in general.

As a second problem, we considered the isotopic shift construction applied to planar functions in odd characteristic. We proved that isotopic equivalence, between quadratic planar maps, is completely characterised by the isotopic shift construction and EA-equivalence transformation. Moreover, we showed that the isotopic shift transformation can connect isotopic inequivalent planar functions. It would be interesting to investigate further whether the isotopic shift construction can lead to new classes of planar mappings and, in particular, whether the functions given in Theorem 7.1 can be CCZ-inequivalent to the known ones.

The last problem concerns the recently introduced notion of boomerang uniformity. We studied its value for some known differentially 4-uniform permutations that are not quadratic: the Bracken-Leander map [18] and some modifications of the inverse map [85, 108]. The results obtained show that these functions are not optimal (i.e. $\delta_F \neq \beta_F$). In [16], it is proved that the inverse function is optimal ($\delta_F = \beta_F = 4$) if $n \equiv 2 \mod 4$. However, for the case $n \equiv 0 \mod 4$, which is widely used in cryptographic algorithms, from the results obtained here and in [16, 84, 91] we cannot find any permutation with boomerang uniformity 4. So, an interesting problem which remains open is to investigate the existence of a permutation having boomerang uniformity 4 over $\mathbb{F}_{2^n}$ with $n \equiv 0 \mod 4$.

Appendix A

Some computational results

We present here some computational results for the isotopic shift construction introduced in Chapter 4. In particular, these results (together with Corollary 4.1) prove Proposition 4.3.

In the following we consider the finite field $\mathbb{F}_{2^6}$ and set $\mathbb{F}_{2^6}^\star = \langle \zeta \rangle$. In Table 2.3 we have listed the thirteen CCZ-inequivalent quadratic APN maps defined over $\mathbb{F}_{2^6}$. An equivalent list of quadratic APN functions can be found in [57]. We recall the definition of isotopic shift, given in (4.1), that is $F_L(x) = F(x + L(x)) - F(x) - F(L(x))$. The following results are obtained restricting the search of possible linear 1-to-1 and 2-to-1 maps L thanks to Proposition 4.1. The starting function F is taken from the list of quadratic APN functions given in [57].

Table A.1: Linear functions L for which F_L (with $F(x) = x^3$, no. 1.1) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1

L 1-to-1	L 2-to-1	no. in Table 2.3
ζx (or $x^{16} + \zeta^3 x^4 + \zeta^{17} x$)	$x^{32} + x^{16} + x^8 + x^4 + x^2 + \zeta^{21} x$	F_L EA-eq to 1.1
$\zeta x^{16} + \zeta^{21} x$	$x^{32} + \zeta x^{16} + \zeta^{27} x^8 + \zeta^{46} x^4 + \zeta^{18} x^2 + \zeta^{33} x$	F_L EA-eq to 1.2
$x^8 + \zeta^5 x$	$x^{32} + \zeta x^{16} + \zeta^9 x^8 + \zeta^{39} x^4 + \zeta^7 x^2 + \zeta^{31} x$	F_L EA-eq to 2.1
$x^{32} + \zeta x^{16} + \zeta^{25} x^8 + \zeta^8 x^4 + \zeta^{42} x^2 + \zeta^{31} x$	$x^{32} + \zeta x^{16} + \zeta^{41} x^8 + \zeta^{49} x^4 + \zeta^5 x^2 + \zeta^5 x$	F_L EA-eq to 2.2
$x^{32} + \zeta^{23} x^8 + \zeta^{31} x^4 + \zeta^{46} x^2 + \zeta^{50} x$	$x^{32} + x^{16} + \zeta^{15} x^8 + \zeta^{42} x^4 + \zeta^{15} x^2 + \zeta^{16} x$	F_L EA-eq to 2.3
$x^{32} + \zeta x^{16} + \zeta^{42} x^8 + \zeta^3 x^4 + \zeta^{14} x^2 + \zeta^{22} x$	$x^{32} + \zeta x^{16} + \zeta^7 x^8 + \zeta^{51} x^4 + \zeta^{33} x^2 + \zeta^{14} x$	F_L EA-eq to 2.4
$x^{32} + \zeta^{13} x^{16} + x^8 + \zeta^{30} x^4 + \zeta x^2 + \zeta^{20} x$	$x^{32} + \zeta^9 x^{16} + \zeta^{31} x^8 + \zeta^{16} x^4 + \zeta^{57} x^2 + \zeta^{29} x$	F_L EA-eq to 2.5
$\zeta x^{16} + x^8 + \zeta^{50} x^4 + x^2 + \zeta^{47} x$	$x^{32} + \zeta x^{16} + \zeta^{16} x^8 + \zeta^{26} x^4 + \zeta^{14} x^2 + \zeta^{14} x$	F_L EA-eq to 2.6
$x^{32} + \zeta x^{16} + \zeta^{23} x^8 + \zeta^{53} x^4 + \zeta^{52} x^2 + \zeta x$	$x^{32} + \zeta x^{16} + \zeta^{23} x^8 + \zeta^{53} x^4 + \zeta^{52} x^2 + \zeta^{56} x$	F_L EA-eq to 2.7
$x^{32} + \zeta x^{16} + \zeta^{26} x^8 + \zeta^{50} x^4 + \zeta^{57} x^2 + \zeta^{34} x$	$x^{32} + \zeta^{13} x^8 + \zeta^{57} x^4 + \zeta^{36} x^2 + \zeta^{31} x$	F_L EA-eq to 2.8
$x^{16} + \zeta^9 x^8 + \zeta^9 x^4 + \zeta^{47} x^2 + \zeta^{50} x$	$x^{32} + x^{16} + \zeta^5 x^8 + \zeta^{50} x^4 + \zeta^8 x^2 + \zeta^{60} x$	F_L EA-eq to 2.9
$x^{32} + \zeta x^{16} + \zeta^{20} x^8 + \zeta^{28} x^4 + \zeta^{23} x^2 + \zeta^{36} x$	$x^{32} + \zeta x^{16} + \zeta^6 x^8 + \zeta^8 x^4 + \zeta^{26} x^2 + \zeta^{21} x$	F_L EA-eq to 2.10
$x^{16} + \zeta^5 x^8 + \zeta^8 x^4 + \zeta^{34} x^2 + \zeta^{57} x$	$x^{16} + \zeta^5 x^8 + \zeta^8 x^4 + \zeta^{34} x^2 + \zeta^{20} x$	F_L EA-eq to 2.12

Table A.2: Linear functions L for which F_L (with $F(x) = x^3 + \zeta^{-1}\mathrm{Tr}(\zeta^3 x^9)$ EA-eq. to no. 1.2) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^9 x$	$x^{32} + \zeta^{12}x^{16} + \zeta^{24}x^8 + \zeta^{24}x^4 + \zeta^{30}x^2 + \zeta^{47}x$	F_L EA-eq to 1.1
$\zeta^{21} x$	$\zeta^{31}x^{16} + \zeta^{60}x^4 + \zeta^{11}x^2 + \zeta^{30}x$	F_L EA-eq to 1.2
$x^8 + \zeta^9 x$	$\zeta^{11}x^8 + \zeta^{61}x^4 + \zeta^{51}x^2 + \zeta^{33}x$	F_L EA-eq to 2.1
$\zeta^{15}x^{16} + \zeta^6 x^8 + \zeta^{47}x^4 + \zeta^{21}x^2 + \zeta^{48}x$	$x^{16} + \zeta^{14}x^8 + \zeta^{49}x^4 + \zeta^{13}x^2 + \zeta^4 x$	F_L EA-eq to 2.2
$\zeta^3 x^8 + \zeta^{43}x^4 + \zeta^{23}x^2 + \zeta^9 x$	$\zeta x^{16} + \zeta x^8 + \zeta^4 x^4 + \zeta^{46}x$	F_L EA-eq to 2.3
$\zeta^{11}x^8 + \zeta^{22}x^4 + \zeta^{22}x^2 + \zeta^{50}x$	$\zeta^3 x^{16} + \zeta^{15}x^8 + \zeta^{15}x^4 + \zeta^{40}x^2 + \zeta^{11}x$	F_L EA-eq to 2.4
$\zeta^{10}x^{16} + \zeta^{11}x^8 + \zeta^{35}x^4 + \zeta^{27}x^2 + \zeta^{26}x$	$\zeta^{10}x^{16} + \zeta^{11}x^8 + \zeta^{35}x^4 + \zeta^{27}x^2 + \zeta^6 x$	F_L EA-eq to 2.5
$x^{32} + \zeta^{19}x^{16} + \zeta^{23}x^8 + \zeta^{38}x^4 + \zeta^{16}x^2 + \zeta^{58}x$	$x^{32} + \zeta^{19}x^{16} + \zeta^{23}x^8 + \zeta^{38}x^4 + \zeta^{16}x^2 + \zeta^{25}x$	F_L EA-eq to 2.6
$x^{16} + \zeta^7 x^8 + \zeta^{52}x^4 + \zeta^7 x^2 + \zeta^{25}x$	$\zeta^2 x^{16} + \zeta^8 x^8 + \zeta^{40}x^4 + \zeta^{38}x^2 + \zeta^5 x$	F_L EA-eq to 2.7
$x^{16} + \zeta^8 x^8 + \zeta^7 x^4 + \zeta^{49}x^2 + \zeta^{46}x$	$x^{16} + \zeta^8 x^8 + \zeta^7 x^4 + \zeta^{49}x^2 + \zeta^{22}x$	F_L EA-eq to 2.8
$\zeta x^8 + \zeta^{14}x^4 + \zeta^{13}x^2 + \zeta^{43}x$	$\zeta x^8 + \zeta^{14}x^4 + \zeta^{13}x^2 + \zeta^{37}x$	F_L EA-eq to 2.9
$\zeta^6 x^{16} + \zeta^{16}x^8 + \zeta^{52}x^4 + \zeta^{20}x^2 + \zeta^{52}x$	$\zeta x^{16} + \zeta^{16}x^8 + \zeta^{36}x^4 + \zeta^{61}x^2 + \zeta^{36}x$	F_L EA-eq to 2.10
$\zeta^{19}x^{16} + \zeta^3 x^8 + \zeta^{29}x^4 + \zeta^{39}x^2 + \zeta^{24}x$	$\zeta^{28}x^{16} + \zeta x^8 + \zeta^{31}x^4 + \zeta^{51}x^2 + \zeta^4 x$	F_L EA-eq to 2.12

Table A.3: Linear functions L for which F_L (with $F(x) = \zeta x^{24} + x^{10} + x^3$, no 2.1) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^5 x$	$x^{32} + \zeta^{22}x^{16} + \zeta^{54}x^8 + \zeta^{62}x^4 + \zeta^{11}x^2 + \zeta^{31}x$	F_L EA-eq to 1.1
$\zeta^3 x^{16} + \zeta^{37}x^8 + \zeta^{56}x^4 + \zeta^6 x^2 + \zeta^{12}x$	$\zeta^3 x^{16} + \zeta^{37}x^8 + \zeta^{56}x^4 + \zeta^6 x^2 + \zeta^{52}x$	F_L EA-eq to 1.2
$\zeta^6 x$	$x^{32} + \zeta^2 x^{16} + \zeta^{39}x^8 + \zeta^{12}x^4 + \zeta^7 x^2 + \zeta^{20}x$	F_L EA-eq to 2.1
$x^{16} + \zeta^9 x^8 + \zeta^{44}x^4 + \zeta^{22}x^2 + \zeta^{18}x$	$x^{16} + \zeta^9 x^8 + \zeta^{44}x^4 + \zeta^{22}x^2 + \zeta^{54}x$	F_L EA-eq to 2.2
$x^{16} + \zeta^{49}x^8 + \zeta^{22}x^4 + \zeta^{19}x^2 + \zeta x$	$\zeta^{52}x^8 + \zeta^4 x^4 + \zeta^{37}x^2 + \zeta^{19}x$	F_L EA-eq to 2.3
$\zeta^{18}x^8 + \zeta^5 x^4 + \zeta^{36}x^2 + \zeta^{33}x$	$x^{16} + \zeta^{25}x^8 + \zeta^{38}x^4 + \zeta^{56}x^2 + \zeta^{28}x$	F_L EA-eq to 2.4
$\zeta^5 x^{16} + \zeta^{50}x^8 + \zeta^{50}x^4 + \zeta^4 x^2 + \zeta^{52}x$	$x^{16} + \zeta^{60}x^8 + \zeta^{28}x^4 + \zeta^{44}x^2 + \zeta^{55}x$	F_L EA-eq to 2.5
$\zeta^3 x^{16} + \zeta^{52}x^8 + \zeta^{42}x^4 + \zeta^{56}x^2 + \zeta^{49}x$	$\zeta^3 x^{16} + \zeta^{52}x^8 + \zeta^{42}x^4 + \zeta^{56}x^2 + \zeta^2 x$	F_L EA-eq to 2.6
$x^{16} + x^8 + \zeta^{28}x^4 + \zeta^{51}x^2 + \zeta^4 x$	$x^{16} + \zeta^{12}x^8 + \zeta^{12}x^4 + \zeta^{25}x$	F_L EA-eq to 2.7
$x^{16} + \zeta^{44}x^8 + \zeta^{29}x^4 + \zeta^{27}x^2 + \zeta^2 x$	$x^{16} + \zeta^{44}x^8 + \zeta^{29}x^4 + \zeta^{27}x^2 + \zeta^{49}x$	F_L EA-eq to 2.8
$x^{16} + \zeta^{44}x^8 + \zeta^{43}x^4 + \zeta^{58}x^2 + \zeta^{15}x$	$x^{16} + \zeta^{48}x^8 + \zeta^{40}x^4 + \zeta^3 x^2 + \zeta^{25}x$	F_L EA-eq to 2.9
$\zeta x^{16} + \zeta^{36}x^8 + \zeta^{27}x^4 + \zeta^3 x^2 + \zeta^{37}x$	$x^{16} + \zeta^{23}x^8 + \zeta^{19}x^4 + \zeta^9 x^2 + \zeta x$	F_L EA-eq to 2.10
$\zeta^3 x^{16} + \zeta^7 x^8 + \zeta^{44}x^4 + \zeta^2 x^2 + \zeta^{14}x$	$\zeta^3 x^{16} + \zeta^7 x^8 + \zeta^{44}x^4 + \zeta^2 x^2 + \zeta^{16}x$	F_L EA-eq to 2.12

Table A.4: Linear functions L for which F_L (with $F(x) = \zeta^{17}x^{24} + \zeta^{17}x^{20} + \zeta^{17}x^{18} + \zeta^{17}x^{17} + x^3$ EA-eq. to no. 2.2) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^2x^{16} + \zeta^{36}x^8 + \zeta^{61}x^4 + x^2 + \zeta^{19}x$	$x^{32} + \zeta^{10}x^{16} + \zeta^{58}x^8 + \zeta^{50}x^4 + \zeta^{38}x^2 + \zeta^{21}x$	F_L EA-eq to 1.1
$\zeta^3x^{16} + \zeta^{11}x^8 + \zeta^{40}x^4 + \zeta^{14}x^2 + \zeta^{35}x$	$\zeta^3x^{16} + \zeta^{11}x^8 + \zeta^{40}x^4 + \zeta^{14}x^2 + \zeta^4x$	F_L EA-eq to 1.2
$\zeta^7x^{16} + \zeta^{39}x^8 + \zeta^{24}x^4 + \zeta^7x^2 + \zeta^3x$	$\zeta^{14}x^8 + x^4 + \zeta^{47}x^2 + \zeta^{15}x$	F_L EA-eq to 2.1
$\zeta^{21}x^8 + \zeta^{51}x^4 + \zeta^{25}x^2 + \zeta^{31}x$	$\zeta^{35}x^8 + \zeta^{31}x^4 + \zeta^{25}x^2 + \zeta^6x$	F_L EA-eq to 2.2
$\zeta^{58}x^8 + \zeta^{18}x^4 + \zeta^{47}x^2 + \zeta^{27}x$	$\zeta^{58}x^8 + \zeta^{18}x^4 + \zeta^{47}x^2 + \zeta^9x$	F_L EA-eq to 2.3
$\zeta^{32}x^8 + \zeta^{33}x^4 + \zeta^{60}x^2 + \zeta^{58}x$	$\zeta^{32}x^8 + \zeta^{33}x^4 + \zeta^{60}x^2 + \zeta^{25}x$	F_L EA-eq to 2.4
$x^{16} + \zeta^{38}x^8 + \zeta^{29}x^4 + \zeta^{52}x^2 + \zeta^{24}x$	$x^{16} + \zeta^{38}x^8 + \zeta^{29}x^4 + \zeta^{52}x^2 + \zeta^{41}x$	F_L EA-eq to 2.5
$\zeta^{14}x^{16} + \zeta^{58}x^8 + \zeta^{53}x^4 + \zeta^9x^2 + \zeta^{11}x$	$\zeta^{14}x^{16} + \zeta^{58}x^8 + \zeta^{53}x^4 + \zeta^9x^2 + \zeta^{23}x$	F_L EA-eq to 2.6
$x^{16} + \zeta^{19}x^8 + \zeta^4x^4 + \zeta^{52}x^2 + \zeta^{27}x$	$\zeta^6x^8 + \zeta^{50}x^4 + \zeta^{34}x^2 + \zeta^{50}x$	F_L EA-eq to 2.7
$\zeta^{62}x^8 + \zeta^{43}x^4 + \zeta^3x^2 + \zeta^{31}x$	$\zeta^{62}x^8 + \zeta^{43}x^4 + \zeta^3x^2 + \zeta^{59}x$	F_L EA-eq to 2.8
$\zeta^{22}x^8 + \zeta^{31}x^4 + \zeta^{36}x^2 + \zeta^{47}x$	$\zeta^{23}x^8 + \zeta^{39}x^4 + \zeta^{38}x^2 + \zeta^{10}x$	F_L EA-eq to 2.9
$\zeta^{38}x^8 + \zeta^{44}x^4 + \zeta^{22}x^2 + \zeta^{44}x$	$\zeta^{38}x^8 + \zeta^{44}x^4 + \zeta^{22}x^2 + \zeta^{29}x$	F_L EA-eq to 2.10
$\zeta x^{16} + \zeta^2x^8 + \zeta^{20}x^4 + \zeta^{52}x^2 + \zeta^{32}x$	$\zeta x^{16} + \zeta^2x^8 + \zeta^{20}x^4 + \zeta^{52}x^2 + \zeta^{28}x$	F_L EA-eq to 2.12

Table A.5: Linear functions L for which F_L (with $F(x) = \zeta^{29}x^{48} + \zeta^{15}x^{34} + \zeta^{35}x^{33} + \zeta^{62}x^{20} + \zeta^{10}x^6 + \zeta^{40}x^5$ EA-eq. to no. 2.3) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{21}x$	$\zeta^{16}x^{32} + \zeta^{61}x^{16} + \zeta^{20}x^8 + \zeta^{19}x^4 + \zeta^{15}x^2 + \zeta^{47}x$	F_L EA-eq to 1.1
$\zeta^{10}x^{16} + \zeta^{58}x^8 + \zeta^{60}x^4 + \zeta^5x^2 + \zeta^4x$	$\zeta^{10}x^{16} + \zeta^{58}x^8 + \zeta^{60}x^4 + \zeta^5x^2 + \zeta^{35}x$	F_L EA-eq to 1.2
$\zeta^{10}x^{16} + \zeta^{54}x^8 + \zeta x^4 + \zeta^{45}x^2 + \zeta^{50}x$	$\zeta^{10}x^{16} + \zeta^{54}x^8 + \zeta x^4 + \zeta^{45}x^2 + \zeta^{53}x$	F_L EA-eq to 2.1
$\zeta^{45}x^8 + \zeta^{12}x^4 + \zeta^{52}x^2 + \zeta^{25}x$	$\zeta^{27}x^8 + \zeta^{16}x^4 + \zeta^{19}x^2 + \zeta^{40}x$	F_L EA-eq to 2.2
ζ^9x	$\zeta^{59}x^8 + \zeta^{30}x^4 + \zeta^{32}x^2 + x$	F_L EA-eq to 2.3
$x^{16} + x^8 + \zeta^{39}x^4 + \zeta^{57}x^2 + \zeta^6x$	$x^{16} + \zeta^5x^8 + \zeta^{56}x^4 + \zeta^6x^2 + \zeta^{12}x$	F_L EA-eq to 2.4
$x^{16} + \zeta^9x^8 + \zeta^3x^4 + \zeta^{24}x^2 + \zeta^{44}x$	$x^{16} + \zeta^9x^8 + \zeta^3x^4 + \zeta^{24}x^2 + \zeta^{29}x$	F_L EA-eq to 2.5
$\zeta x^{16} + \zeta^{20}x^8 + \zeta^{45}x^4 + \zeta^8x^2 + \zeta^{48}x$	$\zeta x^{16} + \zeta^{20}x^8 + \zeta^{45}x^4 + \zeta^8x^2 + \zeta^{19}x$	F_L EA-eq to 2.6
$x^{16} + \zeta^2x^8 + \zeta^{22}x^4 + \zeta^{39}x^2 + \zeta^{30}x$	$\zeta^{55}x^8 + \zeta^{60}x^4 + \zeta^{15}x^2 + \zeta^{36}x$	F_L EA-eq to 2.7
$\zeta^{62}x^8 + \zeta^{51}x^4 + \zeta^{42}x^2 + \zeta^{57}x$	$\zeta^{62}x^8 + \zeta^{51}x^4 + \zeta^{42}x^2 + \zeta^{20}x$	F_L EA-eq to 2.8
$\zeta^{25}x^8 + \zeta^{41}x^4 + \zeta^{42}x^2 + \zeta^{16}x$	$\zeta^6x^8 + x^4 + \zeta^{42}x^2 + \zeta^{47}x$	F_L EA-eq to 2.9
$\zeta^{36}x^8 + \zeta^{10}x^4 + \zeta^6x^2 + \zeta^6x$	$\zeta^{61}x^8 + \zeta^{57}x^4 + \zeta^{35}x^2 + \zeta^{16}x$	F_L EA-eq to 2.10
$\zeta^2x^{16} + \zeta^2x^8 + \zeta^{30}x^4 + \zeta^{44}x^2 + \zeta^{47}x$	$\zeta x^{16} + \zeta^7x^8 + \zeta^{40}x^4 + \zeta^{39}x^2 + \zeta^{20}x$	F_L EA-eq to 2.12

Table A.6: Linear functions L for which F_L (with $F(x) = \zeta^{33}x^{40} + \zeta^{10}x^{34} + \zeta^{47}x^{33} + \zeta^{44}x^{12} + \zeta^{9}x^{9} + \zeta x^{6} + \zeta^{47}x^{5} + \zeta^{52}x^{3}$ EA-eq. to no. 2.4) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^4x^{32} + \zeta^2x^{16} + \zeta^{39}x^8 + \zeta^{21}x^4 + \zeta^{14}x^2 + \zeta^{14}x$	$\zeta^2x^{32} + \zeta^{52}x^{16} + \zeta^{39}x^8 + \zeta^7x^4 + \zeta^{19}x^2 + \zeta^{18}x$	F_L EA-eq to 1.1
$\zeta^3x^{16} + \zeta^{60}x^4 + \zeta^{47}x$	$\zeta^{48}x^{16} + \zeta^{37}x^8 + \zeta^{20}x^4 + \zeta^{12}x^2 + \zeta^{31}x$	F_L EA-eq to 1.2
$\zeta^{16}x^{16} + \zeta^2x^8 + \zeta^{22}x^4 + \zeta^{47}x^2 + \zeta^{32}x$	$x^8 + \zeta^{44}x^4 + \zeta^{25}x^2 + \zeta^{36}x$	F_L EA-eq to 2.1
$\zeta^{40}x^8 + \zeta^{18}x^4 + \zeta^{42}x^2 + \zeta^{49}x$	$\zeta^{40}x^8 + \zeta^{18}x^4 + \zeta^{42}x^2 + \zeta^2x$	F_L EA-eq to 2.2
$\zeta^{13}x^8 + \zeta^{55}x^4 + \zeta^{46}x^2 + \zeta^{22}x$	$x^{16} + \zeta^{11}x^8 + \zeta^{32}x^4 + \zeta^3x^2 + \zeta^{33}x$	F_L EA-eq to 2.3
$x^{16} + \zeta^{12}x^8 + \zeta^{61}x^4 + \zeta^{14}x$	$\zeta^{44}x^4 + \zeta^{61}x^2 + \zeta^{19}x$	F_L EA-eq to 2.4
$\zeta^7x^{16} + \zeta^{61}x^8 + \zeta^{21}x^4 + \zeta^{39}x^2 + \zeta^7x$	$\zeta^{18}x^8 + \zeta^{14}x^4 + \zeta^9x^2 + \zeta^6x$	F_L EA-eq to 2.5
$\zeta^7x^{16} + \zeta^{45}x^8 + \zeta^{53}x^4 + \zeta^{14}x^2 + \zeta^{56}x$	$x^{16} + \zeta^{52}x^8 + \zeta^{28}x^4 + \zeta^{19}x^2 + \zeta^{28}x$	F_L EA-eq to 2.6
$\zeta^{51}x^8 + \zeta^{55}x^4 + \zeta^{22}x^2 + \zeta^{50}x$	$\zeta x^8 + \zeta^{38}x^4 + \zeta^3x^2 + \zeta^{19}x$	F_L EA-eq to 2.7
$x^{16} + \zeta^{62}x^8 + \zeta^{55}x^4 + \zeta^8x^2 + \zeta^{22}x$	$x^{16} + \zeta^{62}x^8 + \zeta^{55}x^4 + \zeta^8x^2 + \zeta^{46}x$	F_L EA-eq to 2.8
$\zeta^{10}x^8 + \zeta^{19}x^4 + \zeta^{28}x^2 + \zeta^{25}x$	$x^{16} + \zeta^2x^8 + \zeta^2x^4 + \zeta^{25}x^2 + \zeta^{20}x$	F_L EA-eq to 2.9
$\zeta^{39}x^8 + \zeta^{47}x^4 + \zeta^{23}x^2 + \zeta^{53}x$	$\zeta^{39}x^8 + \zeta^{47}x^4 + \zeta^{23}x^2 + \zeta^{50}x$	F_L EA-eq to 2.10
$\zeta^{11}x^{16} + \zeta^{24}x^8 + \zeta^2x^4 + \zeta^{48}x^2 + \zeta^{50}x$	$\zeta^{11}x^{16} + \zeta^{60}x^8 + \zeta^{14}x^4 + \zeta^8x^2 + \zeta^{39}x$	F_L EA-eq to 2.12

Table A.7: Linear functions L for which F_L (with $F(x) = \zeta x^{40} + \zeta^4x^{34} + \zeta x^{24} + \zeta^4x^{20} + \zeta x^{18} + \zeta^4x^{17} + x^9 + \zeta x^5$ EA-eq. to no. 2.5) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{19}x^{16} + \zeta^8x^8 + \zeta^{35}x^4 + \zeta^{59}x^2 + \zeta^6x$	$\zeta^8x^{16} + \zeta^{25}x^8 + \zeta^{14}x^4 + \zeta^{18}x^2 + \zeta^4x$	F_L EA-eq to 1.1
$\zeta x^{16} + \zeta^{44}x^8 + \zeta^{61}x^4 + \zeta^{33}x^2 + \zeta^{22}x$	$\zeta^{32}x^{16} + \zeta^{51}x^8 + \zeta^{10}x^4 + \zeta^{62}x^2 + \zeta^{21}x$	F_L EA-eq to 1.2
$\zeta^{13}x^{16} + \zeta^9x^8 + \zeta^{21}x^4 + \zeta^{51}x^2 + \zeta^{37}x$	$x^{16} + \zeta^{46}x^8 + \zeta^{19}x^4 + \zeta^{32}x^2 + \zeta^{11}x$	F_L EA-eq to 2.1
$\zeta^9x^8 + \zeta^{24}x^2 + \zeta^{24}x$	$\zeta^{30}x^8 + \zeta^{29}x^4 + \zeta^{24}x^2 + \zeta^{46}x$	F_L EA-eq to 2.2
$\zeta^{20}x^8 + \zeta^5x^4 + \zeta^{11}x^2 + \zeta^{59}x$	$\zeta^{20}x^8 + \zeta^5x^4 + \zeta^{11}x^2 + \zeta^{31}x$	F_L EA-eq to 2.3
$\zeta^{62}x^8 + \zeta^{23}x^4 + \zeta^{32}x^2 + \zeta^{40}x$	$\zeta^{62}x^8 + \zeta^{23}x^4 + \zeta^{32}x^2 + \zeta^{51}x$	F_L EA-eq to 2.4
$x^{16} + \zeta^{34}x^8 + \zeta^{60}x^4 + \zeta^6x^2 + \zeta^{16}x$	$x^{16} + \zeta^{34}x^8 + \zeta^{60}x^4 + \zeta^6x^2 + \zeta^{14}x$	F_L EA-eq to 2.5
$\zeta^{40}x^8 + \zeta^{25}x^4 + \zeta^{18}x^2 + \zeta^{28}x$	$\zeta^{40}x^8 + \zeta^{25}x^4 + \zeta^{18}x^2 + \zeta^{32}x$	F_L EA-eq to 2.6
$\zeta^{32}x^8 + \zeta^{47}x^4 + \zeta^{48}x^2 + \zeta^{34}x$	$\zeta^{16}x^8 + \zeta^{62}x^4 + \zeta^{17}x^2 + \zeta^{17}x$	F_L EA-eq to 2.7
$\zeta^{31}x^8 + \zeta x^4 + \zeta^{11}x^2 + \zeta^{47}x$	$\zeta^{31}x^8 + \zeta x^4 + \zeta^{11}x^2 + \zeta^{61}x$	F_L EA-eq to 2.8
$\zeta^2x^{16} + \zeta^{23}x^8 + \zeta^{28}x^4 + \zeta^{40}x^2 + \zeta^{48}x$	$\zeta x^{16} + \zeta^4x^8 + \zeta^{33}x^4 + \zeta^5x^2 + \zeta^{50}x$	F_L EA-eq to 2.9
$\zeta^9x^8 + \zeta^{49}x^4 + \zeta^{43}x^2 + \zeta^{52}x$	$\zeta^{56}x^4 + \zeta^{34}x^2 + \zeta^2x$	F_L EA-eq to 2.10
$\zeta^7x^{16} + \zeta^6x^8 + \zeta^{52}x^4 + \zeta^{33}x^2 + \zeta^{19}x$	$\zeta^7x^{16} + \zeta^6x^8 + \zeta^{52}x^4 + \zeta^{33}x^2 + \zeta^{48}x$	F_L EA-eq to 2.12

Table A.8: Linear functions L for which F_L (with $F(x) = x^{48} + \zeta^{11}x^{33} + x^{17} + \zeta^{13}x^9 + \zeta^{11}x^5 + x^3$ EA-eq. to no. 2.6) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{32}x^{16} + \zeta^9x^8 + \zeta^{31}x^4 + x^2 + \zeta^{12}x$	$\zeta^2x^{32} + \zeta^4x^{16} + \zeta^{11}x^8 + \zeta^{35}x^4 + \zeta^{16}x^2 + \zeta^{29}x$	F_L EA-eq to 1.1
$\zeta^2x^{16} + \zeta^{32}x^4 + \zeta^{11}x$	$\zeta^{57}x^{16} + \zeta^{27}x^8 + \zeta^{46}x^4 + \zeta^{45}x^2 + \zeta^{27}x$	F_L EA-eq to 1.2
$\zeta^9x^{16} + \zeta^{50}x^8 + \zeta^{15}x^4 + \zeta^2x^2 + \zeta^9x$	$\zeta^9x^{16} + \zeta^{50}x^8 + \zeta^{15}x^4 + \zeta^2x^2 + \zeta^{27}x$	F_L EA-eq to 2.1
$\zeta^2x^{16} + \zeta^{38}x^8 + \zeta^{25}x^4 + \zeta^{20}x^2 + \zeta^7x$	$\zeta x^{16} + \zeta x^8 + \zeta^{13}x^4 + \zeta^{34}x^2 + \zeta^{24}x$	F_L EA-eq to 2.2
$x^{16} + \zeta^{18}x^8 + \zeta^{61}x^4 + \zeta^{13}x^2 + \zeta^{14}x$	$\zeta^2x^{16} + \zeta^4x^8 + \zeta^{53}x^4 + \zeta^{50}x^2$	F_L EA-eq to 2.3
$\zeta^2x^{16} + \zeta^{54}x^8 + \zeta^{25}x^4 + \zeta^7x^2 + \zeta^{62}x$	$\zeta^{41}x^8 + \zeta^6x^4 + \zeta^{38}x^2 + \zeta^{55}x$	F_L EA-eq to 2.4
$\zeta^4x^8 + \zeta^{59}x^4 + \zeta^{24}x^2 + \zeta^{33}x$	$\zeta^4x^8 + \zeta^{59}x^4 + \zeta^{24}x^2 + \zeta^{38}x$	F_L EA-eq to 2.5
$\zeta^{22}x^{16} + \zeta^{55}x^8 + \zeta^{49}x^4 + \zeta^{24}x^2 + \zeta^{11}x$	$\zeta^{12}x^{16} + \zeta^{41}x^8 + \zeta^{22}x^4 + \zeta^{31}x^2 + \zeta^{47}x$	F_L EA-eq to 2.6
$\zeta^{24}x^8 + \zeta^{18}x^4 + \zeta^{32}x^2 + \zeta^5x$	$\zeta^{24}x^8 + \zeta^{18}x^4 + \zeta^{32}x^2 + \zeta^{30}x$	F_L EA-eq to 2.7
$x^{16} + \zeta^{62}x^8 + \zeta^{15}x^4 + \zeta^{56}x^2 + \zeta^{10}x$	$x^{16} + \zeta^{62}x^8 + \zeta^{15}x^4 + \zeta^{56}x^2 + \zeta^{60}x$	F_L EA-eq to 2.8
$x^{16} + \zeta^{42}x^8 + \zeta^9x^4 + \zeta^{62}x^2 + \zeta^{18}x$	$x^{16} + \zeta^{42}x^8 + \zeta^9x^4 + \zeta^{62}x^2 + \zeta^{54}x$	F_L EA-eq to 2.9
$\zeta^{45}x^8 + \zeta^{43}x^4 + \zeta^{16}x^2 + \zeta^{41}x$	$\zeta^{45}x^8 + \zeta^{43}x^4 + \zeta^{16}x^2 + \zeta^{24}x$	F_L EA-eq to 2.10
$\zeta^5x^{16} + \zeta^{46}x^8 + \zeta^{20}x^4 + \zeta^{40}x^2 + \zeta^{17}x$	$\zeta^5x^{16} + \zeta^{46}x^8 + \zeta^{20}x^4 + \zeta^{40}x^2 + \zeta^{39}x$	F_L EA-eq to 2.12

Table A.9: Linear functions L for which F_L (with $F(x) = \zeta^{25}x^{36} + \zeta^{25}x^{18} + \zeta^{38}x^{12} + x^9 + \zeta^{25}x^5$ EA-eq. to no. 2.7) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{18}x^{16} + \zeta^9x^4 + \zeta^{31}x$	$\zeta^3x^{32} + \zeta^3x^{16} + \zeta^5x^8 + \zeta^{50}x^4 + \zeta^{50}x^2 + \zeta^{10}x$	F_L EA-eq to 1.1
$\zeta^{37}x^8 + \zeta^{55}x$	$\zeta^{11}x^{16} + \zeta^{56}x^8 + \zeta^{55}x^4 + \zeta^{57}x^2 + \zeta^{33}x$	F_L EA-eq to 1.2
$x^8 + \zeta^{36}x$	$\zeta x^{16} + \zeta^{23}x^8 + \zeta^6x^4 + \zeta^5x^2 + \zeta^9x$	F_L EA-eq to 2.1
$\zeta x^{16} + \zeta^{38}x^8 + \zeta^6x^4 + \zeta^{22}x^2 + \zeta^{17}x$	$x^{16} + \zeta^{51}x^8 + \zeta^{21}x^4 + \zeta^{46}x^2 + \zeta^{11}x$	F_L EA-eq to 2.2
$\zeta^{23}x^8 + \zeta^{13}x^4 + \zeta^{55}x^2 + \zeta^{13}x$	$\zeta^{23}x^8 + \zeta^{13}x^4 + \zeta^{55}x^2 + \zeta^3x$	F_L EA-eq to 2.3
$x^{16} + \zeta^{24}x^8 + \zeta^{50}x^4 + \zeta^{28}x^2 + \zeta^7x$	$\zeta^{39}x^8 + \zeta^{54}x^2 + \zeta^{11}x$	F_L EA-eq to 2.4
$\zeta x^{16} + \zeta^{28}x^8 + \zeta^{47}x^4 + \zeta^{42}x^2 + \zeta^{61}x$	$\zeta x^{16} + \zeta^{28}x^8 + \zeta^{47}x^4 + \zeta^{42}x^2 + \zeta^{47}x$	F_L EA-eq to 2.5
$\zeta x^{16} + \zeta^{34}x^8 + \zeta^{27}x^4 + \zeta^{18}x^2 + \zeta^{26}x$	$\zeta x^{16} + \zeta^{34}x^8 + \zeta^{27}x^4 + \zeta^{18}x^2 + \zeta^6x$	F_L EA-eq to 2.6
$\zeta^{60}x^8 + \zeta^{11}x^4 + \zeta^{44}x^2 + \zeta^{56}x$	$\zeta^{60}x^8 + \zeta^{11}x^4 + \zeta^{44}x^2 + \zeta x$	F_L EA-eq to 2.7
$\zeta^{43}x^8 + \zeta^{49}x^4 + \zeta^{41}x^2 + \zeta^{36}x$	$\zeta^{50}x^8 + \zeta^9x^4 + \zeta^{55}x^2 + \zeta^{51}x$	F_L EA-eq to 2.8
$x^8 + \zeta^{48}x^4 + \zeta^{56}x^2 + \zeta^{19}x$	$x^8 + \zeta^{48}x^4 + \zeta^{56}x^2 + \zeta^{48}x$	F_L EA-eq to 2.9
$x^8 + \zeta^{51}x^4 + \zeta^{47}x^2 + \zeta^9x$	$x^8 + \zeta^{51}x^4 + \zeta^{47}x^2 + \zeta^{27}x$	F_L EA-eq to 2.10
$\zeta^5x^{16} + \zeta^{52}x^8 + \zeta^{40}x^4 + \zeta^4x^2 + \zeta^{11}x$	$\zeta^{16}x^{16} + \zeta^{28}x^8 + \zeta^{51}x^4 + \zeta^{20}x$	F_L EA-eq to 2.12

Table A.10: Linear functions L for which F_L (with $F(x) = \zeta^{25}x^{40} + \zeta^{23}x^{34} + \zeta^9x^{33} + \zeta^6x^{20} + \zeta^{48}x^{12} + \zeta^{52}x^9 + \zeta^{34}x^6$ EA-eq. to no. 2.8) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{31}x^{16} + \zeta^{50}x^8 + \zeta^{10}x^4 + \zeta^{33}x^2 + \zeta^{25}x$	$\zeta^{14}x^{32} + \zeta^{12}x^{16} + \zeta^{41}x^8 + \zeta^{36}x^4 + \zeta^{27}x^2 + \zeta^{50}x$	F_L EA-eq to 1.1
$\zeta^7x^{16} + \zeta^{55}x^4 + \zeta^{37}x$	$\zeta x^{32} + \zeta^{40}x^{16} + \zeta^{12}x^8 + \zeta^{47}x^4 + \zeta^{26}x^2$	F_L EA-eq to 1.2
$\zeta^{16}x^{16} + \zeta^{21}x^8 + \zeta^{20}x^4 + \zeta^{46}x^2 + \zeta^{28}x$	$\zeta^3x^{16} + \zeta^{62}x^8 + \zeta^{41}x^4 + \zeta^{54}x^2 + \zeta^{19}x$	F_L EA-eq to 2.1
$\zeta x^{16} + \zeta^{46}x^8 + \zeta^{12}x^4 + \zeta^{60}x^2 + \zeta^{47}x$	$\zeta^3x^8 + \zeta^{50}x^4 + \zeta^{21}x^2$	F_L EA-eq to 2.2
$\zeta^{53}x^8 + \zeta^{29}x^4 + \zeta^3x^2 + \zeta^{21}x$	$\zeta^{54}x^8 + \zeta^{29}x^4 + \zeta^{55}x^2 + \zeta^{43}x$	F_L EA-eq to 2.3
$\zeta^4x^8 + \zeta x^4 + \zeta^{16}x^2 + \zeta^{33}x$	$\zeta^4x^8 + \zeta x^4 + \zeta^{16}x^2 + \zeta^{38}x$	F_L EA-eq to 2.4
$\zeta x^{16} + \zeta^{25}x^8 + \zeta^{12}x^4 + \zeta^{15}x^2 + \zeta^{28}x$	$\zeta^2x^{16} + \zeta^{24}x^8 + \zeta^6x^4 + \zeta^{12}x$	F_L EA-eq to 2.5
$\zeta^{10}x^{16} + \zeta^{30}x^8 + \zeta^{21}x^4 + \zeta^6x^2 + \zeta^{18}x$	$\zeta^5x^{16} + \zeta^{13}x^8 + \zeta^2x^4 + \zeta^{31}x^2 + \zeta^{14}x$	F_L EA-eq to 2.6
$\zeta^3x^{16} + \zeta^2x^8 + \zeta^{53}x^4 + \zeta^2x^2 + \zeta^{31}x$	$\zeta x^{16} + \zeta^{54}x^8 + \zeta x^4 + \zeta^{46}x^2 + \zeta^3x$	F_L EA-eq to 2.7
$\zeta^{40}x^4 + \zeta^{19}x^2 + \zeta^8x$	$\zeta^{40}x^4 + \zeta^{19}x^2 + \zeta^7x$	F_L EA-eq to 2.8
$\zeta^{28}x^8 + \zeta^{21}x^4 + \zeta^{48}x^2 + \zeta^{35}x$	$\zeta^{25}x^8 + \zeta^{16}x^4 + \zeta^{37}x^2 + \zeta^{37}x$	F_L EA-eq to 2.9
$\zeta^{39}x^8 + \zeta^{35}x^4 + \zeta^{37}x^2 + \zeta^3x$	$\zeta^{39}x^8 + \zeta^{35}x^4 + \zeta^{37}x^2 + \zeta^{13}x$	F_L EA-eq to 2.10
$\zeta^9x^8 + \zeta^{23}x^4 + \zeta^{31}x^2 + \zeta^{23}x$	$\zeta^9x^8 + \zeta^{23}x^4 + \zeta^{31}x^2 + \zeta^{11}x$	F_L EA-eq to 2.12

Table A.11: Linear functions L for which F_L (with $F(x) = \zeta^9x^{40} + \zeta^9x^{20} + \zeta^4x^{18} + \zeta^9x^{12} + \zeta^4x^{10} + x^9$ EA-eq. to no. 2.9) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^2x^{32} + \zeta^{12}x^{16} + \zeta^{11}x^8 + \zeta^{40}x^4 + \zeta^{36}x^2 + \zeta^{26}x$	$x^{32} + \zeta^{12}x^{16} + \zeta^{30}x^8 + \zeta^{42}x^4 + \zeta^{45}x^2 + \zeta^{20}x$	F_L EA-eq to 1.1
$\zeta^3x^{16} + \zeta^{17}x^8 + \zeta^{13}x^4 + \zeta^{29}x^2 + \zeta^{31}x$	$x^{32} + \zeta^2x^{16} + \zeta^{36}x^8 + \zeta^{33}x^4 + \zeta x^2 + \zeta^3x$	F_L EA-eq to 1.2
$\zeta^{13}x^{16} + \zeta^{50}x^8 + \zeta^{41}x^4 + \zeta^{42}x^2 + \zeta^{47}x$	$\zeta^{13}x^{16} + \zeta^{50}x^8 + \zeta^{41}x^4 + \zeta^{42}x^2 + \zeta^{61}x$	F_L EA-eq to 2.1
$x^{16} + \zeta^{32}x^8 + \zeta^{43}x^4 + \zeta^2x^2 + \zeta^{59}x$	$\zeta^7x^8 + \zeta^{25}x^4 + \zeta^{47}x^2 + \zeta^{50}x$	F_L EA-eq to 2.2
$\zeta^2x^{16} + \zeta^{12}x^8 + \zeta^{10}x^4 + \zeta^{39}x^2 + \zeta^{37}x$	$\zeta^{30}x^8 + \zeta^{53}x^2 + \zeta^{17}x$	F_L EA-eq to 2.3
$x^{16} + \zeta^4x^8 + \zeta^{49}x^4 + \zeta^{55}x^2 + \zeta^{39}x$	$\zeta^{51}x^8 + \zeta^{23}x^4 + \zeta^3x^2 + \zeta^{15}x$	F_L EA-eq to 2.4
$\zeta^6x^{16} + \zeta^{58}x^8 + \zeta^{19}x^4 + \zeta^{45}x^2 + \zeta^{12}x$	$\zeta^9x^8 + \zeta^{27}x^4 + \zeta^2x^2 + \zeta^{15}x$	F_L EA-eq to 2.5
$\zeta^3x^{16} + \zeta^9x^8 + x^4 + \zeta^{24}x$	$\zeta^3x^{16} + \zeta^9x^8 + x^4 + \zeta^{41}x$	F_L EA-eq to 2.6
$\zeta^{28}x^8 + \zeta^{41}x^4 + \zeta^{30}x^2 + \zeta^{52}x$	$\zeta^{28}x^8 + \zeta^{41}x^4 + \zeta^{30}x^2 + \zeta^{12}x$	F_L EA-eq to 2.7
$\zeta^{14}x^8 + \zeta^{42}x^4 + \zeta^{57}x^2 + \zeta^{23}x$	$\zeta^{14}x^8 + \zeta^{42}x^4 + \zeta^{57}x^2 + \zeta^{11}x$	F_L EA-eq to 2.8
$\zeta^{46}x^8 + \zeta^{30}x^4 + \zeta^{32}x^2 + \zeta^6x$	$\zeta^{46}x^4 + \zeta^{10}x^2 + \zeta^3x$	F_L EA-eq to 2.9
$\zeta^2x^8 + \zeta^8x^4 + \zeta^{59}x^2 + \zeta^{62}x$	$\zeta^2x^8 + \zeta^8x^4 + \zeta^{59}x^2 + \zeta^{55}x$	F_L EA-eq to 2.10
$\zeta^{15}x^{16} + \zeta^{20}x^8 + \zeta^{61}x^4 + x^2 + x$	$\zeta^{15}x^{16} + \zeta^{20}x^8 + \zeta^{61}x^4 + x^2$	F_L EA-eq to 2.12

Table A.12: Linear functions L for which F_L (with $F(x) = \zeta x^{33} + \zeta x^{24} + \zeta^4 x^{17} + \zeta x^{10} + x^9 + \zeta x^6$ EA-eq. to no. 2.10) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^7 x^{16} + \zeta^2 x^8 + \zeta^{47} x^4 + \zeta^{17} x^2 + \zeta^{33} x$	$\zeta^2 x^{32} + \zeta^{11} x^{16} + \zeta^{16} x^8 + \zeta^{45} x^4 + \zeta^5 x^2 + \zeta^{62} x$	F_L EA-eq to 1.1
$\zeta^4 x^{16} + \zeta x^8 + \zeta^{32} x^4 + \zeta^{58} x^2 + \zeta^6 x$	$\zeta^{60} x^{16} + \zeta^{29} x^8 + \zeta^{49} x^4 + \zeta^{39} x^2 + \zeta^{11} x$	F_L EA-eq to 1.2
$\zeta^7 x^{16} + \zeta^{54} x^8 + \zeta^{54} x^4 + \zeta^{43} x^2 + \zeta^{15} x$	$\zeta^6 x^{16} + \zeta^{20} x^8 + \zeta^{54} x^4 + \zeta^{42} x^2 + \zeta^{22} x$	F_L EA-eq to 2.1
$\zeta^{24} x^8 + \zeta^7 x^4 + \zeta^{61} x^2$	$\zeta^{24} x^8 + \zeta^7 x^4 + \zeta^{61} x^2 + x$	F_L EA-eq to 2.2
$\zeta x^{16} + \zeta^{12} x^8 + \zeta^{50} x^4 + \zeta^{27} x^2 + \zeta^4 x$	$\zeta^{31} x^8 + \zeta^{44} x^4 + \zeta^{10} x^2 + \zeta^{50} x$	F_L EA-eq to 2.3
$x^{16} + \zeta x^8 + \zeta^{29} x^4 + \zeta^{41} x^2 + \zeta^{42} x$	$\zeta^3 x^8 + \zeta^{31} x^4 + \zeta^{38} x^2 + \zeta^{55} x$	F_L EA-eq to 2.4
$x^{16} + \zeta^{26} x^8 + \zeta^{33} x^4 + \zeta^{57} x^2 + \zeta^2 x$	$x^{16} + \zeta^{26} x^8 + \zeta^{33} x^4 + \zeta^{57} x^2 + \zeta^{49} x$	F_L EA-eq to 2.5
$\zeta^{11} x^8 + \zeta^{34} x^4 + \zeta^4 x^2 + \zeta^{21} x$	$\zeta^{57} x^8 + \zeta^{13} x^4 + \zeta^{23} x^2 + \zeta^{17} x$	F_L EA-eq to 2.6
$\zeta^{46} x^8 + \zeta^{24} x^4 + \zeta^{55} x^2 + \zeta^{16} x$	$\zeta^{46} x^8 + \zeta^{24} x^4 + \zeta^{55} x^2 + \zeta^{14} x$	F_L EA-eq to 2.7
$\zeta^{37} x^8 + \zeta^4 x^4 + \zeta^{52} x^2 + \zeta^{22} x$	$\zeta^{37} x^8 + \zeta^4 x^4 + \zeta^{52} x^2 + \zeta^{46} x$	F_L EA-eq to 2.8
$x^{16} + \zeta^6 x^8 + \zeta^{39} x^4 + \zeta^{18} x^2 + \zeta^{31} x$	$x^{16} + \zeta^{28} x^8 + \zeta^{24} x^4 + \zeta^{17} x^2 + \zeta^{34} x$	F_L EA-eq to 2.9
$\zeta^{35} x^8 + \zeta^{15} x^4 + \zeta^{20} x$	$\zeta^{26} x^8 + \zeta^{60} x^4 + \zeta^{43} x^2 + \zeta^5 x$	F_L EA-eq to 2.10
$\zeta^{10} x^{16} + \zeta^4 x^8 + \zeta^{57} x^4 + \zeta^{13} x^2 + \zeta^6 x$	$\zeta^9 x^{16} + \zeta^{16} x^8 + \zeta^{41} x^4 + \zeta^9 x^2 + \zeta^{15} x$	F_L EA-eq to 2.12

Table A.13: Linear functions L for which F_L (with $F(x) = \zeta^6 x^{18} + x^{17} + \zeta^4 x^{10} + \zeta^3 x^9 + x^5 + \zeta^7 x^3$ EA-eq. to no. 2.12) is APN over $\mathbb{F}_{2^6}$, up to CCZ-equivalence, and their comparison with Table 2.3. We also specify if L is 1-to-1 or 2-to-1.

L 1-to-1	L 2-to-1	no. in Table 2.3
$\zeta^{17} x^{16} + \zeta^{21} x^8 + x^2 + \zeta^{37} x$	$\zeta^{17} x^{16} + \zeta^{21} x^8 + x^2 + \zeta^{43} x$	F_L EA-eq to 1.1
$\zeta^{39} x^8 + \zeta^{39} x^4 + \zeta^{51} x^2 + \zeta^3 x$	$\zeta^{39} x^8 + \zeta^{39} x^4 + \zeta^{51} x^2 + \zeta^{13} x$	F_L EA-eq to 1.2
$\zeta^{50} x^{16} + \zeta^{38} x^8 + \zeta^{15} x^4 + \zeta^{57} x^2 + \zeta^{51} x$	$\zeta^{38} x^{16} + \zeta^3 x^8 + \zeta^{46} x^4 + \zeta^{20} x^2 + \zeta^{31} x$	F_L EA-eq to 2.1
$x^{16} + \zeta^{18} x^8 + \zeta^{23} x^4 + \zeta^{59} x^2 + \zeta^{38} x$	$\zeta^{41} x^8 + \zeta x^4 + \zeta^{13} x^2 + \zeta^{19} x$	F_L EA-eq to 2.2
$\zeta^6 x^8 + \zeta^{37} x^4 + \zeta^{12} x^2 + \zeta^6 x$	$\zeta^6 x^8 + \zeta^{37} x^4 + \zeta^{12} x^2 + \zeta^{26} x$	F_L EA-eq to 2.3
$\zeta x^{16} + \zeta^8 x^8 + \zeta^{36} x^4 + \zeta^{36} x^2 + \zeta^{59} x$	$x^{16} + \zeta^{26} x^8 + \zeta^{16} x^4 + \zeta^{30} x^2 + \zeta^{21} x$	F_L EA-eq to 2.4
$x^{16} + \zeta^{37} x^8 + \zeta^{61} x^4 + \zeta^{51} x^2 + \zeta^{11} x$	$x^{16} + \zeta^{37} x^8 + \zeta^{61} x^4 + \zeta^{51} x^2 + \zeta^{23} x$	F_L EA-eq to 2.5
$\zeta^2 x^{16} + \zeta^{56} x^8 + \zeta^{51} x^4 + \zeta^{57} x^2 + \zeta^{14} x$	$\zeta^4 x^{16} + \zeta^{19} x^8 + \zeta^{62} x^4 + \zeta^{32} x^2 + \zeta^7 x$	F_L EA-eq to 2.6
$\zeta^{49} x^8 + \zeta^{61} x^4 + \zeta^{19} x^2 + \zeta^{27} x$	$\zeta^{49} x^8 + \zeta^{61} x^4 + \zeta^{19} x^2 + \zeta^9 x$	F_L EA-eq to 2.7
$x^{16} + \zeta^8 x^8 + \zeta^{17} x^4 + \zeta^{22} x^2 + \zeta^{12} x$	$x^{16} + \zeta^8 x^8 + \zeta^{17} x^4 + \zeta^{22} x^2 + \zeta^{52} x$	F_L EA-eq to 2.8
$x^{16} + \zeta^{15} x^8 + \zeta^{54} x^4 + \zeta^{20} x^2 + \zeta^{20} x$	$x^{16} + \zeta^{36} x^8 + \zeta^2 x^4 + \zeta^{45} x^2 + \zeta^{55} x$	F_L EA-eq to 2.9
$\zeta^{37} x^8 + \zeta^{50} x^4 + \zeta^{59} x^2 + \zeta^{27} x$	$\zeta^{37} x^8 + \zeta^{50} x^4 + \zeta^{59} x^2 + \zeta^9 x$	F_L EA-eq to 2.10
$\zeta^4 x^{16} + \zeta^{32} x^8 + \zeta x^4 + \zeta^{39} x^2 + \zeta^{40} x$	$\zeta^{20} x^{16} + \zeta^{46} x^8 + \zeta^9 x^4 + \zeta^{43} x^2 + \zeta^7 x$	F_L EA-eq to 2.12

Appendix B

Some proofs from Chapter 8

In the coming proofs we use the following well-known result.

Lemma B.1 ([92]). *Let $n = 2k$ be an even integer. Then for any $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_{2^n}$, the following statements hold.*

1. *$x^{-1} + (x+a)^{-1} = b$ has no roots in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\frac{1}{ab}) = 1$.*
2. *$x^{-1} + (x+a)^{-1} = b$ has 2 roots in $\mathbb{F}_{2^n}$ if and only if $ab \neq 1$ and $\mathrm{Tr}(\frac{1}{ab}) = 0$.*
3. *$x^{-1} + (x+a)^{-1} = b$ has 4 roots in $\mathbb{F}_{2^n}$ if and only if $b = a^{-1}$. Furthermore, when $b = a^{-1}$ the 4 roots of the above equation in $\mathbb{F}_{2^n}$ are $\{0, a, a\omega, a\omega^2\}$, where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$.*

Proof of Theorem 8.3. Our function is given by

$$F(x) = \begin{cases} 1 & x = c \\ c^{-1} & x = 1 \\ x^{-1} & x \neq 1, c \end{cases}$$

Since F is differentially 4-uniform we have that $\mathrm{Tr}(c) = \mathrm{Tr}\left(\frac{1}{c}\right) = 1$. Note that, if $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then $n \equiv 2 \mod 4$. In the following ω will denote a primitive element of $\mathbb{F}_4$. Let us study the solutions of System (2.4) for any $a, b \in \mathbb{F}_{2^n}^\star$. First of all, notice that $x \neq y$, otherwise $b = 0$. Moreover, due to the fact that if (x, y) is a solution, also $(y, x), (x + a, y + a), (y + a, x + a)$ are solutions, we just need to consider one of them for analysing the solutions.

When $x = 0$ then we have:

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

- If $y = 1$, then $b = c^{-1}$ and $F(a) + F(a + 1) = c^{-1}$. This is true if and only if $a = 1$ or $a = c, c + 1$ if $c \in \mathbb{F}_4$. The solution $a = 1$ is straightforward. Instead, if $a = c$ or $a = c + 1$ we obtain the equation $(c + 1)^{-1} + c^{-1} = 1$, that implies $c \in \mathbb{F}_4$. For the other values of a we have $a^{-1} + (a + 1)^{-1} = c^{-1}$, which does not admit solutions since $\mathrm{Tr}(c^{-1}) = 1$.
- If $y = c$, then $b = 1$ and $F(a) + F(a + c) = 1$. Similarly, this is true if and only if $a = c$ or $a = 1, c + 1$ if $c \in \mathbb{F}_4$.
- If $y = a$, then $b = a^{-1}$ is a possible solution for any $a \neq 0, 1, c$.
- If $y = a + 1$, with $a \neq 1, c + 1$, then $b = (a + 1)^{-1}$. Moreover, if $a = c$ then $c \in \mathbb{F}_4$. Otherwise $a^{-1} + c^{-1} = (a + 1)^{-1}$ does not admit solutions since $\mathrm{Tr}(c) = 1$.

- If $y = a + c$, with $a \neq c, c+1$, then $b = (a+c)^{-1}$ and $a^{-1} + 1 = (a+c)^{-1}$. Moreover, if $a = 1$ we have $c \in \mathbb{F}_4$. But if $a \neq 0, 1, c, c+1$ it does not admit solutions since $\mathrm{Tr}(c^{-1}) = 1$.

- If $y \neq 0, 1, c, a, a+1, a+c$, then $b = y^{-1}$. Thus, if $a = 1$ the equation $c^{-1} + (y+1)^{-1} = y^{-1}$ has no solutions. Also if $a = c$, then $1 + (y+c)^{-1} = y^{-1}$ has no solutions.
  If $a \neq 1, c$, the equation $a^{-1} + (y+a)^{-1} = y^{-1}$ admits 4 possible solutions for y which are $0, a, a\omega, a\omega^2$. From the cases above, only the last two can be considered.
  In particular, if $y = a\omega$ then $b = \omega^2 a^{-1}$ and $a \neq 0, \omega, \omega^2, c\omega, c\omega^2, 1, c$. While, if $y = a\omega^2$ then $b = \omega a^{-1}$ and $a \neq 0, \omega, \omega^2, c\omega, c\omega^2, 1, c$.

When $x = 1$ we have:

$$\begin{cases} F(a+1) + F(y+a) = b \\ F(y) + c^{-1} = b. \end{cases}$$

- If $y = c$, then $b = 1 + c^{-1}$ and $F(a+1) + F(a+c) = 1 + c^{-1}$. If $a = 1$ or $a = c$ then $c \in \mathbb{F}_4$. If $a = c+1$, then the equation is satisfied.
  For the other values we have $(a+1)^{-1} + (a+c)^{-1} = 1 + c^{-1}$. Let $z = a+1$, then we have $z^{-1} + (z+1+c)^{-1} = c^{-1}(c+1)$. Since $\frac{(1+c)^2}{c} = 1$ if and only if $c \in \mathbb{F}_4$, then the equation admits four solutions if $c \in \mathbb{F}_4$, which are $\{0, c, c\omega, c\omega^2\} = \{0, 1, c, c+1\}$, none of them is admissible. Otherwise it admits two solutions which are $a = 0$ and $a = c+1$, both not admissible.

- If $y = a$, with $a \neq 0, 1, c$, then $b = c^{-1} + a^{-1}$ and $F(a+1) = c^{-1} + a^{-1}$. When $a = c+1$ we have $1 = c^{-1} + (c+1)^{-1}$, implying $c \in \mathbb{F}_4$.
  If $a \neq 0, 1, c, c+1$, then $(a+1)^{-1} = c^{-1} + a^{-1}$ has no solutions.

- If $y = a+1$, then $b = (a+1)^{-1} + c^{-1}$ is a possible solution for any $a \neq 0, 1, c+1$.

- If $y = a+c$, with $a \neq 0, c, c+1$, then $b = (a+c)^{-1} + c^{-1}$ and $F(a+1) + 1 = (a+c)^{-1} + c^{-1}$.
  If $a = 1$, then $(1+c)^{-1} + c^{-1} = 1$ implies $c \in \mathbb{F}_4$. For the other values we have $(a+1)^{-1} + 1 = (a+c)^{-1} + c^{-1}$. Let $z = a+1$, then we have $z^{-1} + (z+1+c)^{-1} = c^{-1}(c+1)$. As explained before the equation admits at most four solutions that are $\{0, 1, c, c+1\}$, none of which admissible.

- If $y \neq 0, 1, c, a, a+1, a+c$, then $b = y^{-1} + c^{-1}$ and $F(a+1) + (y+a)^{-1} = y^{-1} + c^{-1}$.
  If $a = 1$, then the equation does not admit solutions. For $a = c+1$, the equation $1 + (y+c+1)^{-1} = y^{-1} + c^{-1}$ admits at most four solutions: $\{0, 1, c, c+1\}$, none of which admissible.
  For the other values we have $(a+1)^{-1} + (y+a)^{-1} = y^{-1} + c^{-1}$. Since $\frac{c(a+1)}{a(c+a+1)} = 1$ does not admit solutions, the equation has two solutions (for y) if $\mathrm{Tr}\left(\frac{c(a+1)}{a(c+a+1)}\right) = 0$. Otherwise none. In particular, one solution is $y = \frac{c}{bc+1}$ which implies $b^2ac(a+1) + ba(a+c+1) + c + 1 = 0$.

When $x = c$ we have:

$$\begin{cases} F(a+c) + F(y+a) = b \\ F(y) + 1 = b. \end{cases}$$

Since $y \neq 0, 1, c$ we have $b = y^{-1} + 1$.

- If $y = a$, with $a \neq 0, 1, c$, then $b = a^{-1} + 1$ and $F(a+c) = a^{-1} + 1$. If $a = c+1$ then $c \in \mathbb{F}_4$. In the other cases the equation has no solutions.

- If $y = a+1$, with $a \neq 0,1,c+1$, then $b = (a+1)^{-1}+1$ and $F(a+c)+c^{-1} = (a+1)^{-1}+1$. If $a = c$ then $c \in \mathbb{F}_4$ and $b = c^{-1}$.
  In the other cases we have $(a+c)^{-1}+(a+1)^{-1} = c^{-1}+1$. The equation admits at most four solutions that are $\{0,1,c,c+1\}$, none of which admissible.
- If $y = a+c$, then $b = (a+c)^{-1}+1$ is a possible solution for any $a \neq 0,c,c+1$.
- If $y \neq 0,1,c,a,a+1,a+c$, then $y^{-1}+1 = F(a+c)+(y+a)^{-1}$.
  If $a = c$, then the equation has no solutions.
  If $a = c+1$, then $y^{-1}+1 = c^{-1}+(y+c+1)^{-1}$ admits at most four solutions $\{0,1,c,c+1\}$, none of which admissible.
  If $a \neq 0,c,c+1$, then $y^{-1}+1 = (a+c)^{-1}+(y+a)^{-1}$. Since $\frac{(a+c)}{a(1+a+c)} = 1$ does not admit solutions, the equation has two solutions (for y) if $\mathrm{Tr}\left(\frac{(a+c)}{a(1+a+c)}\right) = 0$. Otherwise none. In particular, one solution is $y = (b+1)^{-1}$ which implies $b^2a(a+c)+ba(a+c+1)+c+1 = 0$.

When $x \neq 0,1,c,a,a+1,a+c$ and $y \neq 0,1,c,a,a+1,a+c,x$ we have:

$$\begin{cases} (x+a)^{-1}+(y+a)^{-1} = b \\ x^{-1}+y^{-1} = b. \end{cases}$$

Hence we have $x = \frac{y}{by+1}$, $y \neq b^{-1}$. Therefore $x+a = \frac{y+aby+a}{by+1}$, $y \neq \frac{a}{ab+1}$, and

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

The equation admits two solutions if and only if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$. Moreover $b+ab+a \neq 0$ and $bc^2+abc+a \neq 0$, due to the restrictions on y. Assume that $\frac{1}{ab} = r^2+r$, then we have $\frac{y}{a} = r$ or $\frac{y}{a} = r+1$. If $y = ra$ then $\frac{y}{by+1} = a(r+1)$. If $y = (r+1)a$ then $\frac{y}{by+1} = ra$. Since we consider pairs (x,y) up to a swap or the addition of a, we have just one pair. Therefore we have the following possible solution:

- $(\frac{y}{by+1}, y)$ if $\frac{1}{ab} = r^2+r$, $b+ab+a \neq 0$, $bc^2+abc+a \neq 0$ and $y = ra$. Moreover $ra, (r+1)a \neq 0,1,c,a,a+1,a+c$

Considering the case $c \notin \mathbb{F}_4$, from the analysis above (swapping the pairs (x,y) and adding a) we have the following list:

(1) for $a = 1$ and $b = c^{-1}$, we have the solutions $\{(0,1),(1,0)\}$,

(2) with $a = c$ and $b = 1$, we have the solutions $\{(0,c),(c,0)\}$,

(3) with $b = a^{-1}$ and $a \neq 0,1,c$, we have $\{(0,a),(a,0)\}$,

(4) with $b=\omega^2a^{-1}$ and $a\neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$, we have $\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}$,

(5) with $b=\omega a^{-1}$ and $a\neq 0,\omega,\omega^2,c\omega,c\omega^2,1,c$, we have $\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}$,

(6) with $a=c+1$ and $b=c^{-1}+1$, we have $\{(1,c),(c,1)\}$,

(7) with $b=(a+1)^{-1}+c^{-1}$ and $a\neq 0,1,c+1$, we have $\{(1,a+1),(a+1,1)\}$,

(8) if $\mathrm{Tr}\left(\frac{c(a+1)}{a(c+a+1)}\right)=0$, $a\neq 0,1,c+1$ and $b^2ac(a+1)+ba(a+c+1)+c+1=0$, we have $\{(1,\frac{c}{bc+1}),(\frac{c}{bc+1},1),(a+1,a+\frac{c}{bc+1}),(a+\frac{c}{bc+1},a+1)\}$,

(9) with $b=(a+c)^{-1}+1$ and $a\neq 0,c,c+1$, we have $\{(c,c+a),(c+a,c)\}$,

(10) if $\mathrm{Tr}\left(\frac{a+c}{a(c+a+1)}\right)=0$, $a\neq 0,c,c+1$ and $b^2a(a+c)+ba(a+c+1)+c+1=0$, we have $\{(c,\frac{1}{b+1}),(\frac{1}{b+1},c),(c+a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,c+a)\}$,

(11) if $\frac{1}{ab}=r^2+r$ (that is $\mathrm{Tr}(\frac{1}{ab})=0$), $b+ab+a\neq 0$, $bc^2+abc+a\neq 0$ and $y=ra$, we have $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ (moreover $ra,(r+1)a\neq 0,1,c,a,a+1,a+c$).

We want to study now, for different possible fixed pairs $a,b\in\mathbb{F}_{2^n}^\star$ how many solutions (x,y) are possible.

- If $a=1$ the possible cases are

  case (1) with $b=c^{-1}$,
  case (9) with $b=(c+1)^{-1}+1$,
  case (11) if $\mathrm{Tr}(b^{-1})=0$, $b\neq(c^2+c)^{-1}$.

  Obviously cases (1) and (9) cannot coexist, since $c\notin\mathbb{F}_4$. Cases (1) and (11) cannot either, since $\mathrm{Tr}(c)=1$. The same for (9) and (11). Therefore if $a=1$ there can be at most 2 solutions.

  We do not have to consider case (1) any more.

- If $a=c$ we have

  case (2) with $b=1$,
  case (7) with $b=(c+1)^{-1}+c^{-1}$,
  case (11) if $\mathrm{Tr}((bc)^{-1})=0$, $b^{-1}\neq 1+c^{-1}$.

  Cases (2) and (7) cannot coexist since $c\notin\mathbb{F}_4$. Also cases (2) and (11) and cases (7) and (11) cannot since $\mathrm{Tr}(c)=\mathrm{Tr}(c^{-1})=1$. Therefore if $a=c$ there can be at most 2 solutions.

  We do not have to consider case (2) any more.

- If $a=c+1$ we have

  case (3) with $b=(c+1)^{-1}$,
  case (4) with $b=(c+1)^{-1}\omega^2$,
  case (5) with $b=(c+1)^{-1}\omega$,
  case (6) with $b=c^{-1}+1$,
  case (11) if $\mathrm{Tr}((bc+b)^{-1})=0$, $b\neq 1+c^{-1}$ (we assume $\frac{1}{b(c+1)}=r+r^2$, with $r\neq 0,1,(c+1)^{-1},(c+1)^{-1}+1$).

Therefore we have:

- if $b = (c+1)^{-1}$, then the only possible cases are (3) and (11) with $r = \omega$.
- if $b = (c+1)^{-1}\omega^2$, then we have case (4). For (6) we need $c^2 + \omega^2 c + 1 = 0$, that has 2 values only if $\mathrm{Tr}(\omega) = 0$. For case (11) we need also that $\mathrm{Tr}(\omega) = 0$ but $b \neq c^{-1} + 1$ (hence no condition (6)).
- if $b = (c+1)^{-1}\omega$, then we have case (5). For (6) we need $c^2 + \omega c + 1 = 0$, that has 2 values only if $\mathrm{Tr}(\omega) = 0$. For case (11) we need also that $\mathrm{Tr}(\omega) = 0$ but $b \neq c^{-1} + 1$ (hence no (6)).
- if b is different from the cases already analysed, it is clear that it cannot satisfy more than one pair of cases.

Therefore if $a = c + 1$ there can be at most 6 solutions. Moreover, if $\mathrm{Tr}(\omega) = 1$ there can be at most 4 solutions.

We do not have to consider case (6) any more.

- If $a = b^{-1} \neq 1, c, c+1$ we can have

  case (3) since the condition is satisfied,

  case (11) is possible if $b \neq \omega, \omega^2$, $bc \neq \omega, \omega^2$ and $by = \omega$ or $by = \omega^2$.

  Therefore if $a = b^{-1}$ we have at most 4 solutions.

  We do not have to consider case (3) any more.

- If $a = b^{-1}\omega$ we have

  case (5) with $b \neq 0, 1, \omega, \omega^2, c^{-1}, c^{-1}\omega, c^{-1}\omega^2$,

  case (7) is possible if $b^2 c + b(c\omega^2 + 1) + \omega = 0$, hence if $\mathrm{Tr}\left(\frac{c\omega}{c^2\omega+1}\right) = 0$,

  case (8) is possible if $\mathrm{Tr}(c\omega^2) = 0$ (hence $\mathrm{Tr}(c\omega) = 1$), moreover we have $b^2 c + b\omega + \omega = 0$ and for $c\omega^2 = r^2 + r$ we have $b = r^{-1}$ or $b = (r+1)^{-1}$,

  case (9) is possible if $b^2 c + b(c + \omega^2) + \omega = 0$, hence if $\mathrm{Tr}\left(\frac{c\omega}{c^2+\omega}\right) = 0$,

  case (10) is possible if $\mathrm{Tr}(\frac{1}{c\omega}) = 0$, hence for $\frac{1}{c\omega} = r^2 + r$ we have $b = r\omega$ or $b = (r+1)\omega$,

  case (11) is possible if $\mathrm{Tr}(\omega) = 0$.

  Hence we have

  - case (7) has to satisfy $cb^2 + b(c\omega^2 + 1) + \omega = 0$,
  - case (8) has to satisfy $cb^2 + b\omega + \omega = 0$,
  - case (9) has to satisfy $cb^2 + b(\omega^2 + c) + \omega = 0$,
  - case (10) has to satisfy $cb^2 + bc\omega + \omega = 0$.

  We can satisfy at most one condition of the above plus the condition of case (5) and case (11). Therefore if $ab = \omega$ we have at most 10 solutions. Moreover if $\mathrm{Tr}(\omega) = 1$ we have at most 8 solutions. While, if $\mathrm{Tr}(c\omega^2) = \mathrm{Tr}(\frac{1}{c\omega}) = \mathrm{Tr}(\omega) = 1$ we have at most 6 solutions, and if $\mathrm{Tr}(\frac{c\omega}{c^2\omega+1}) = \mathrm{Tr}(c\omega^2) = \mathrm{Tr}(\frac{c\omega}{c^2+\omega}) = \mathrm{Tr}(\frac{1}{c\omega}) = \mathrm{Tr}(\omega) = 1$ we have at most 4 solutions.

  We do not have to consider case (5) any more.

- If $a = b^{-1}\omega^2$ we have a symmetric set of solutions with the previous case.

  In particular we obtain

  - case (7) has to satisfy $cb^2 + b(c\omega + 1) + \omega^2 = 0$ and $\mathrm{Tr}(\frac{c\omega^2}{c^2\omega^2+1}) = 0$,
  - case (8) has to satisfy $cb^2 + b\omega^2 + \omega^2 = 0$ and $\mathrm{Tr}(c\omega) = 0$,
  - case (9) has to satisfy $cb^2 + b(\omega + c) + \omega^2 = 0$ and $\mathrm{Tr}(\frac{c\omega^2}{c^2+\omega^2}) = 0$,
  - case (10) has to satisfy $cb^2 + bc\omega^2 + \omega^2 = 0$ and $\mathrm{Tr}(\frac{1}{c\omega^2}) = 0$.

  Moreover we have the following relations:

$$\mathrm{Tr}\Big(\frac{1}{c\omega}\Big) = 1 + \mathrm{Tr}\Big(\frac{1}{c\omega^2}\Big), \qquad \mathrm{Tr}(c\omega^2) = 1 + \mathrm{Tr}(c\omega),$$
$$\mathrm{Tr}\Big(\frac{c\omega}{c^2+\omega}\Big) = \mathrm{Tr}\Big(\frac{c\omega^2}{c^2\omega^2+1}\Big), \qquad \mathrm{Tr}\Big(\frac{c\omega}{c^2\omega+1}\Big) = \mathrm{Tr}\Big(\frac{c\omega^2}{c^2+\omega^2}\Big).$$

  We can satisfy at most one condition of the above plus the condition of case (4) and case (11). Therefore if $ab = \omega^2$ we have at most 10 solutions. Moreover, if $\mathrm{Tr}(\omega) = 1$ we have at most 8 solutions.
  While, if $\mathrm{Tr}(c\omega) = \mathrm{Tr}(\frac{1}{c\omega^2}) = \mathrm{Tr}(\omega) = 1$ we have at most 6 solutions, and if $\mathrm{Tr}(\frac{c\omega^2}{c^2\omega^2+1}) = \mathrm{Tr}(c\omega) = \mathrm{Tr}(\frac{c\omega^2}{c^2+\omega^2}) = \mathrm{Tr}(\frac{1}{c\omega^2}) = \mathrm{Tr}(\omega) = 1$ we have at most 4 solutions.

  We do not have to consider case (4) any more.

- If case (7) is satisfied, that is if $b = (a+1)^{-1} + c^{-1}$, we have

  case (7) for $a \neq 0, 1, c+1$,

  case (11) is possible if $\mathrm{Tr}\Big(\frac{c(a+1)}{a(a+1+c)}\Big) = 0$.

  Therefore if $b = (a+1)^{-1} + c^{-1}$ we have at most 4 solutions.

  We do not have to consider case (7) any more.

- If case (9) is satisfied, that is if $b = (a+c)^{-1} + 1$, we have

  case (9) with $a \neq 0, c, c+1$,

  case (11) is possible if $\mathrm{Tr}\Big(\frac{a+c}{a(1+a+c)}\Big) = 0$.

  Therefore if $b = (a+c)^{-1} + 1$ we have at most 4 solutions.

  We do not have to consider case (9) any more.

- If case (8) is satisfied, that is $b^2ac(a+1) + ba(a+1+c) + 1 + c = 0$, we have

  case (8) if $\mathrm{Tr}\Big(\frac{c(a+1)}{a(c+a+1)}\Big) = 0$,

  case (11) if $\mathrm{Tr}(\frac{1}{ab}) = 0$.

  Therefore if $b^2ac(a+1) + ba(a+1+c) + 1 + c = 0$ we have at most 6 solutions.

  We do not have to consider case (8) any more.

- If case (10) is satisfied, that is $b^2a(a+c) + ba(a+1+c) + 1 + c = 0$, we have

  case (10) if $\mathrm{Tr}\Big(\frac{a+c}{a(c+a+1)}\Big) = 0$,

case (11) if $\mathrm{Tr}(\frac{1}{ab})=0$.

Therefore if $b^2a(a+c)+ba(a+1+c)+1+c=0$ we have at most 6 solutions.

We do not have to consider case (10) any more.

- For the other possible values for a and b we have at most 2 possible solutions coming from case (11).

Therefore we have that for $c\notin\mathbb{F}_4$ $\beta_F\leq 10$. Moreover, if $\mathbb{F}_{2^n}=\mathbb{F}_{2^{2k}}$ with k an odd integer, we have $\mathrm{Tr}(\omega)=1$ and, in this case, we have $\beta_F=8$. Indeed, since $\mathrm{Tr}(c\omega^2)=1+\mathrm{Tr}(c\omega)$ we have that one of them is equal to zero, hence in the case $ab=\omega$ or $ab=\omega^2$ it is possible to reach 8 solutions for k odd. Otherwise, for k even, $\beta_F=10$.

Now, let us consider the case $c\in\mathbb{F}_4\setminus\mathbb{F}_2$. Since we need the restriction $\mathrm{Tr}(c)=\mathrm{Tr}(c^{-1})=1$ then we consider $c=\omega$ or $c=\omega^2$ only over $\mathbb{F}_{2^{2k}}$ for k odd. Let us assume, without loss of generality, that $c=\omega$. Hence we have the following list of possible solutions.

(1) with $a=1$ and $b=\omega^2$, we have the solutions $\{(0,1),(1,0)\}$,

(2) with $a=\omega$ and $b=\omega^2$, we have the solutions $\{(0,1),(1,0),(\omega,\omega^2),(\omega^2,\omega)\}$,

(3) with $a=\omega^2$ and $b=\omega^2$, we have the solutions $\{(0,1),(1,0),(\omega^2,\omega),(\omega,\omega^2)\}$,

(4) with $a=1$ and $b=1$, we have the solutions $\{(0,\omega),(\omega,0),(1,\omega^2),(\omega^2,1)\}$,

(5) with $a=\omega$ and $b=1$, we have the solutions $\{(0,\omega),(\omega,0)\}$,

(6) with $a=\omega^2$ and $b=1$, we have the solutions $\{(0,\omega),(\omega,0),(\omega^2,1),(1,\omega^2)\}$,

(7) with $b=a^{-1}$ and $a\neq 0,1,\omega$, we have the solutions $\{(0,a),(a,0)\}$,

(8) with $a=\omega$ and $b=\omega$, we have the solutions $\{(0,\omega^2),(\omega^2,0),(\omega,1),(1,\omega)\}$,

(9) with $a=1$ and $b=\omega$, we have the solutions $\{(0,\omega^2),(\omega^2,0),(1,\omega),(\omega,1)\}$,

(10) with $b=\omega^2a^{-1}$ and $a\neq 0,1,\omega,\omega^2$, we have $\{(0,a\omega),(a\omega,0),(a,a\omega^2),(a\omega^2,a)\}$,

(11) with $b=\omega a^{-1}$ and $a\neq 0,1,\omega,\omega^2$, we have $\{(0,a\omega^2),(a\omega^2,0),(a,a\omega),(a\omega,a)\}$,

(12) with $a=\omega^2$ and $b=\omega$, we have the solutions $\{(1,\omega),(\omega,1)\}$,

(13) with $b=(a+1)^{-1}+\omega^2$ and $a\neq 0,1,\omega^2$, we have the solutions $\{(1,a+1),(a+1,1)\}$,

(14) if $\mathrm{Tr}\left(\frac{\omega(a+1)}{a(\omega^2+a)}\right)=0$, $a\neq 0,1,\omega^2$ and $b^2a\omega(a+1)+ba(a+\omega^2)+\omega^2=0$, we have $\{(1,\frac{\omega}{b\omega+1}),(\frac{\omega}{b\omega+1},1),(a+1,a+\frac{\omega}{b\omega+1}),(a+\frac{\omega}{b\omega+1},a+1)\}$,

(15) with $b=(a+\omega)^{-1}+1$ and $a\neq 0,\omega,\omega^2$, we have $\{(\omega,\omega+a),(\omega+a,\omega)\}$,

(16) if $\mathrm{Tr}\left(\frac{a+\omega}{a(\omega^2+a)}\right)=0$, $a\neq 0,\omega,\omega^2$ and $b^2a(a+\omega)+ba(a+\omega^2)+\omega^2=0$, we have $\{(\omega,\frac{1}{b+1}),(\frac{1}{b+1},\omega),(\omega+a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,\omega+a)\}$,

(17) if $\frac{1}{ab}=r^2+r$ (that is $\mathrm{Tr}(\frac{1}{ab})=0$), $b+ab+a\neq 0$, $b\omega^2+ab\omega+a\neq 0$ and $y=ra$, we have $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ (moreover $ra,(r+1)a\neq 0,1,\omega,a,a+1,a+\omega$).

Now we start analysing the possible solutions for different values of a and b in $\mathbb{F}_{2^n}^\star$.

- If $a=1$ we have

case (1) with $b=\omega^2$,

case (4) with $b = 1$,

case (9) with $b = \omega$,

case (15) with $b = \omega^2$,

case (17) if $\mathrm{Tr}(b^{-1}) = 0$, $b \neq 1$.

Therefore if $a = 1$ we have at most 4 solutions. We do not have to consider cases (1), (4) and (9) any more.

- If $a = \omega$ we have

  case (2) with $b = \omega^2$,

  case (5) with $b = 1$,

  case (8) with $b = \omega$,

  case (13) with $b = 1$,

  case (17) if $\mathrm{Tr}((\omega b)^{-1}) = 0$, $b \neq \omega + 1$.

  Therefore for $a = \omega$ we have at most 4 solutions. We do not have to consider cases (2), (5) and (8) any more.

- If $a = \omega^2$ we have

  case (3) with $b = \omega^2$,

  case (6) with $b = 1$,

  case (7) with $b = \omega$,

  case (12) with $b = \omega$,

  case (17) if $\mathrm{Tr}(\omega b^{-1}) = 0$, $b \neq \omega$.

  Therefore for $a = \omega^2$ we have at most 4 solutions. We do not have to consider cases (3), (6) and (12) any more.

- If $ab = 1$ and $a \notin \mathbb{F}_4$ we have

  case (7) since the condition is satisfied,

  case (17) with $r = \omega$ is satisfied.

  Therefore for $ab = 1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (7) any more.

- If $ab = \omega$ and $a \notin \mathbb{F}_4$ we have

  case (11) since the condition is satisfied.

  Therefore for $ab = \omega$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not need to consider case (11) any more.

- If $ab = \omega^2$ and $a \notin \mathbb{F}_4$ we have

  case (10) since the condition is satisfied.

  Therefore for $ab = \omega^2$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (10) any more.

- If $b = (a + 1)^{-1} + \omega^2$ and $a \notin \mathbb{F}_4$ we have

case (13) since the condition is satisfied,

case (17) if $\mathrm{Tr}((ab)^{-1}) = 0$.

Therefore for $b = (a+1)^{-1} + \omega + 1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (13) any more.

- If $b = (a+\omega)^{-1} + 1$ and $a \notin \mathbb{F}_4$ we have

  case (15) since the condition is satisfied,

  case (17) if $\mathrm{Tr}((ab)^{-1}) = 0$.

  Therefore for $b = (a+\omega)^{-1} + 1$, $a \notin \mathbb{F}_4$, we have at most 4 solutions. We do not have to consider case (15) any more.

  The last cases that we have to consider are

  case (14) if $b^2 a\omega(a+1) + ba(a+\omega^2) + \omega^2 = 0$,

  case (16) if $b^2 a(a+\omega) + ba(a+\omega^2) + \omega^2 = 0$,

  case (17) if $\mathrm{Tr}((ab)^{-1}) = 0$.

  Note that, considering $a \notin \mathbb{F}_4$, the trace conditions in (14) and (16) are equivalent to having solutions for the above equations. We analyse in the following if these equations can be satisfied.

  We have that cases (14) and (16) cannot happen at the same time since $b^2 a\omega(a+1) = b^2 a(a+\omega)$ cannot be satisfied.

  Therefore if $b^2 a\omega(a+1) + ba(a+\omega^2) + \omega^2 = 0$ or $b^2 a(a+\omega) + ba(a+\omega^2) + \omega^2 = 0$ we have at most 6 solutions. We will show that there exist a, b satisfying condition (17) and one between (14) and (16).

  Let $Tr_0 = \{x : \mathrm{Tr}(x) = 0\}$ and $k = \frac{1}{ab}$. From cases (14) and (16) we can obtain the relations:

  (a) $a^2 k\omega + a(k^2 + k + \omega) + \omega^2 = 0$;

  (b) $a^2 k\omega + a(k^2 + k + \omega^2) + \omega^2 = 0$.

  For any fixed k the equations (a) and (b) admits solutions if and only if

$$\begin{aligned} 0 =& \mathrm{Tr}\left(\frac{k}{(k^2+k+\omega)^2}\right) = \mathrm{Tr}\left(\frac{k^2+\omega}{(k^2+k+\omega)^2} + \frac{1}{k^2+k+\omega}\right) \\ =& \mathrm{Tr}\left(\frac{k+\omega^2}{k^2+k+\omega} + \frac{1}{k^2+k+\omega}\right) = \mathrm{Tr}\left(\frac{k+\omega}{k^2+k+\omega}\right) \\ =& \mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega} + 1\right) = \mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega}\right) \end{aligned} \tag{B.1}$$

  and

$$\begin{aligned} 0 =& \mathrm{Tr}\left(\frac{k}{(k^2+k+\omega^2)^2}\right) = \mathrm{Tr}\left(\frac{k^2+\omega^2}{(k^2+k+\omega^2)^2} + \frac{1}{k^2+k+\omega^2}\right) \\ =& \mathrm{Tr}\left(\frac{k+\omega}{k^2+k+\omega^2} + \frac{1}{k^2+k+\omega^2}\right) = \mathrm{Tr}\left(\frac{k+\omega^2}{k^2+k+\omega^2}\right) \\ =& \mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega^2} + 1\right) = \mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega^2}\right) \end{aligned} \tag{B.2}$$

Since we want to exclude the cases already studied, we have $k \neq 0,1$ (so $b \neq a^{-1}$). Hence, from (a) and (b) we obtain $a \notin \mathbb{F}_4$.

Suppose that for any $k \in Tr_0 \setminus \{0,1\}$ the conditions (B.1) and (B.2) are not satisfied. Thus, since $k+1 \in Tr_0 \setminus \{0,1\}$ for any $k \in Tr_0 \setminus \{0,1\}$ we have that

$$1 = \mathrm{Tr}\left(\frac{k^2+1}{k^2+k+\omega}\right) = \mathrm{Tr}\left(\frac{k^2}{k^2+k+\omega}\right) + \mathrm{Tr}\left(\frac{1}{k^2+k+\omega}\right) = 1 + \mathrm{Tr}\left(\frac{1}{k^2+k+\omega}\right)$$

and

$$1 = \mathrm{Tr}\left(\frac{k^2+1}{k^2+k+\omega^2}\right) = 1 + \mathrm{Tr}\left(\frac{1}{k^2+k+\omega^2}\right).$$

So, denoting by $S = \{k^2+k : k \in Tr_0\}$ we have that for all $s \in S \setminus \{0\}$

$$\mathrm{Tr}\left(\frac{1}{s+\omega}\right) = \mathrm{Tr}\left(\frac{1}{s+\omega^2}\right) = 0.$$

Now, since $\mathrm{Tr}(\omega) = \mathrm{Tr}(\omega^2) = 1$ and $1 \notin S$, we have that $Tr_1 = \{x : \mathrm{Tr}(x) = 1\} = (\omega + S) \cup (\omega^2 + S)$, where $\omega^i + S = \{\omega^i + s : s \in S\}$.

This means that the inverse function $\mathrm{Inv}(x) = x^{-1}$ maps $Tr_1 \setminus \{\omega, \omega^2\}$ onto $Tr_0 \setminus \{0,1\}$, and thus $\mathrm{Inv}(Tr_1 \setminus \{\omega,\omega^2\}) = Tr_0 \setminus \{0,1\}$.

Define the map

$$G(x) = \begin{cases} x+\omega & \text{if } x \in \mathbb{F}_4 \\ x^{-1} & \text{if } x \notin \mathbb{F}_4. \end{cases}$$

Then, $G(Tr_1) = Tr_0$, so considering $H(x) = G^{-1}(x) + \omega$ we would obtain $H(Tr_0) = Tr_0$ and also $H(0) = 0$. Thus, H is such that there exists a vector space of dimension $n-1$ which is sent to another vector space of dimension $n-1$. From Proposition 5.3 in [3] we have that this is equivalent to $\mathcal{NL}(H) = 0$. However, H is CCZ-equivalent to the function G which coincides with the inverse function except over the set $U = \mathbb{F}_4$. Then, it is easy to check that for any $\alpha, \beta \in \mathbb{F}_{2^n}$ we have

$$|\mathcal{W}_G(\alpha,\beta)| \leq |\mathcal{W}_{\mathrm{Inv}}(\alpha,\beta)| + 2 \cdot |U|,$$

implying that $\mathcal{NL}(G) \geq \mathcal{NL}(\mathrm{Inv}) - |U| = 2^{n-1} - 2^{n/2} - 4 > 0$ since $n \geq 6$. So we obtain a contradiction. Therefore, there should exist a, b with $b \neq a^{-1}$, $a \notin \mathbb{F}_4$ such that case (17) and one between case (14) and case (16) are satisfied.

For all the other cases we have at most 2 solutions. □

Proof of Theorem 8.4. Performing a similar analysis as in Theorem 8.3 we obtain that, up to swap x and y, and adding $+a$ to both terms, we have the following list of possible solutions:

(1) $\{(0,1),(1,0),(a,a+1),(a+1,a)\}$ with $a = 1, c, c^2$ and $b = c$,

(2) $\{(0,c),(c,0),(a,a+c),(a+c,a)\}$ with $a = 1, c, c^2$ and $b = 1$,

(3) $\{(0,a),(a,0)\}$ with $a \neq 1, c$ and $b = a^{-1} + 1$,

(4) $\{(0,c^2),(c^2,0),(1,c),(c,1)\}$ with $a = 1, c, c^2$ and $b = c^2$,

(5) $\{(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)\}$ with $a^2b^2 + ab(a+1) + 1 = 0$ and $a \neq 1, c, c^2$,

(6) $\{(1,a+1),(a+1,1)\}$ with $a \neq 1, c^2$ and $b = (a+1)^{-1} + c^2$,

(7) $\{(1,\frac{1}{b+c^2}),(\frac{1}{b+c^2},1),(1+a,\frac{1}{b+c^2}+a),(\frac{1}{b+c^2}+a,1+a)\}$ with $ab^2(a+1)+ab(ac^2+c)+c=0$ and $a\neq 1,c,c^2$,

(8) $\{(c,a+c),(a+c,c)\}$ with $a\neq c,c^2$ and $b=(a+c)^{-1}$,

(9) $\{(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)\}$ with $ab^2(a+c)+ab+1$ and $a\neq 1,c,c^2$,

(10) $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ with $by^2+aby+a=0$ and $\mathrm{Tr}(\frac{1}{ab})=0$.

It is easy to verify that if $a=1,c,c^2$ then for any fixed b there are at most 4 different solutions. For example for $a=1$ we consider cases (1), (2), (4), (8), (10). When $b=1$ we have $(0,c),(c,0),(1,c^2),(c^2,1)$ from case (2). When $b=c$ we have $(0,1),(1,0)$ from case (1) and $(c,c^2),(c^2,c)$ from case (8). When $b=c^2$ we have $(0,c^2),(c^2,0)(1,c),(c,1)$ from case (4). Otherwise when $\mathrm{Tr}(\frac{1}{b})=0$ we have two solutions from case (10).

Hence we just need to focus on cases (3), (5), (6), (7), (8), (9) and (10) for $a\neq 1,c,c^2$.

(I) If $b=a^{-1}+1$ then we have

case (3) we have 2 solutions: $(0,a),(a,0)$.

case (7) leads to $a^3c=a+1$, and we have 4 solutions: $(1,\frac{1}{b+c^2}),(\frac{1}{b+c^2},1),(1+a,\frac{1}{b+c^2}+a),(\frac{1}{b+c^2}+a,1+a)$

case (9) leads to $a^3=a^2c^2+a+c$, and we have 4 solutions: $(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)$

case (10) is possible if $\mathrm{Tr}(\frac{1}{a+1})=0$, and we have 2 solutions: $(\frac{y}{by+1},y),(y,\frac{y}{by+1})$.

For case (7), we have $a^3c+a+1=(a+c^2)(a^2c+a+c)=0$. Hence no proper solution is possible. For case (9), considering $a^3=a^2c^2+a+c$, we obtain $a^{2^6}=a$. Since $a\neq 0,1$, it admits solution only if $3|k$. Therefore if $3\nmid k$ we have at most 4 solutions. In the other cases we can have exactly 8 solutions. Indeed, let $k=3m$ and $\mathbb{F}_{2^6}^\star=\langle w\rangle$, then $a=w^{13}$ satisfies the relation in (9). Moreover, we have $a+1=w^3$ and $\frac{1}{a+1}=w^{60}$. Therefore, $\mathrm{Tr}(\frac{1}{a+1})=\mathrm{Tr}(w^{60})=\mathrm{Tr}(w^{15})=\mathrm{Tr}(w^7+w^{14})=0$. We have exactly 6 solutions from (9) and (10) and two solutions from (3), hence we have in total 8 solutions.

(II) If $b=(a+1)^{-1}+c^2$ then we have

case (5) leads to $a^4+a^3c+a^2+ac^2=0$, and we have 4 solutions: $(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)$,

case (6) we have 2 solutions: $(1,a+1),(a+1,1)$,

case (9) leads to $a^4c+a^2(c^2)+a(c^2)+1=0$ and we have 4 solutions: $(c,\frac{1}{b}),(\frac{1}{b},c),(c+a,\frac{1}{b}+a),(\frac{1}{b}+a,c+a)$,

case (10) is possible if $\mathrm{Tr}(\frac{1}{ab})=0$, and we have 2 solutions: $(\frac{y}{by+1},y),(y,\frac{y}{by+1})$.

For case (5), we have that if $a^4=a^3c+a^2+ac+1$ then $a^{2^8}=a$. Since $a\neq 0,1$ then we do not have possible solutions. The same for case (9). Indeed, if $a^4c=a^2c^2+ac^2+1$ then $a^{2^8}=a$. Therefore we have at most 4 solutions.

(III) If $b=(a+c)^{-1}$ then we have

case (5) leads to $a^3+a^2(c^2)+ac+c^2$, and we have 4 solutions: $(0,\frac{1}{b+1}),(\frac{1}{b+1},0),(a,\frac{1}{b+1}+a),(\frac{1}{b+1}+a,a)$,

case (8) we have 2 solutions: $(c,a+c),(a+c,c)$,

case (10) is possible if $\mathrm{Tr}(\frac{1}{ab}) = 0$, and we have 2 solutions: $(\frac{y}{by+1}, y), (y, \frac{y}{by+1})$.

For case (5) we have that if $a^3 = a^2c^2 + ac + c^2$ then $a^{2^6} = a$. Therefore we have solutions only if $3|k$. In this case we have at most 8 solutions.

Now we are left with cases (5), (7), (9) and (10).

- If cases (5) and (7) are both satisfied, then we have the following constrain on a:

$$a^4 = a^3 + a^2c + c^2.$$

Computing the 2-powers of a, we notice that $a^{2^8} = a$, hence $a \in \mathbb{F}_{2^8}$. This is not possible since $a \in \mathbb{F}_{2^{2k}}$ with k odd and $a \notin \mathbb{F}_{2^2}$.

- If cases (5) and (9) are both satisfied, then we obtain

$$bc = a \text{ and } b^4 = b^3 + b^2(c^2) + c.$$

Using the same technique we can verify that $b^{2^8} = b$, hence we get a contradiction.

- If cases (7) and (9) are both satisfied, then we obtain

$$a^4 = a^3(c^2) + a^2c + c.$$

Again $a^{2^8} = a$, hence a contradiction.

Therefore at most we can have 4 solutions coming from one of these three cases, plus two solutions from (12). Thus, at most 6 solutions.

Assume now case (5). Therefore we have the condition $\mathrm{Tr}(\frac{1}{a+1}) = 0$. Assume then, $\frac{1}{a+1} = r^2 + r$ for some r. Hence, $b = r^2\frac{a+1}{a}$ or $b = (r^2+1)\frac{a+1}{a}$. Let us consider $b = r^2\frac{a+1}{a}$, for case (10) we should have:

$$\frac{1}{ab} = \frac{1}{r^2(a+1)} = \frac{1}{r^2}(r^2+r) = 1 + \frac{1}{r}$$
$$\mathrm{Tr}\left(\frac{1}{ab}\right) = \mathrm{Tr}\left(1 + \frac{1}{r^2}\right) = \mathrm{Tr}\left(\frac{1}{r}\right).$$

Then, we need to consider an element $r \neq 0$ with inverse of null trace and set $a = \frac{1}{r^2+r} + 1$ and $b = r^2\frac{a+1}{a}$. So, we obtain 6 possible solutions. In order to avoid the three cases previously analysed, we only need to consider $r \neq 1$, $r^4 + r^2c + rc + c^2 \neq 0$ and $r^3c + r^2c^2 + r + 1 \neq 0$. Moreover, due to the restrictions on a, we have $r^2 + r \neq 1, c, c^2$. Since $n \geq 6$ there exists such an element r in $\mathbb{F}_{2^n}$. □

Proof of Theorem 8.5. Consider now $\pi = (1, c, c^2)$ with $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and the function

$$F(x) = \begin{cases} c^2 & \text{if } x = 1, \\ c & \text{if } x = c, \\ 1 & \text{if } x = c^2, \\ x^{-1} & \text{otherwise.} \end{cases}$$

Performing a similar analysis as in Theorem 8.3 we obtain that, up to swap and adding a to both terms, we have the following list of possible solutions:

(1) $\{(0,1),(1,0),(c,c^2),(c^2,c)\}$ with $a = 1, c, c^2$ and $b = c^2$,

(2) $\{(0,c),(c,0),(1,c^2),(c^2,1)\}$ with $a = 1, c, c^2$ and $b = c$,

(3) $\{(0,c^2),(c^2,0),(1,c),(c,1)\}$ with $a=1,c,c^2$ and $b=1$,

(4) $\{(0,a),(a,0)\}$ with $a\notin\mathbb{F}_4$ and $b=a^{-1}$,

(5) $\{(0,ac),(ac,0),(a,ac+a),(ac+a,a)\}$ with $a\notin\mathbb{F}_4$ and $b=a^{-1}c^2$,

(6) $\{(0,ac+a),(ac+a,0),(a,ac),(ac,a)\}$ with $a\notin\mathbb{F}_4$ and $b=a^{-1}c$,

(7) $\{(1,a+1),(a+1,1)\}$ with $a\notin\mathbb{F}_4$ and $b=c^2+(a+1)^{-1}$,

(8) $\{(1,(b+c^2)^{-1}),((b+c^2)^{-1},1),(1+a,(b+c^2)^{-1}+a),((b+c^2)^{-1}+a,1+a)\}$ with $a\notin\mathbb{F}_4$ and $b^2(a^2+a)+b(ac+a^2c^2)+c=0$,

(9) $\{(c,a+c),(a+c,c)\}$ with $a\notin\mathbb{F}_4$ and $b=c+(a+c)^{-1}$,

(10) $\{(c,(b+c)^{-1}),((b+c)^{-1},c),(c+a,(b+c)^{-1})+a,((b+c)^{-1}+a,c+a)\}$ with $a\notin\mathbb{F}_4$ and $b^2(a^2+ac)+b(ac+a^2c)+c=0$,

(11) $\{(c^2,a+c^2),(a+c^2,c^2)\}$ with $a\notin\mathbb{F}_4$ and $b=1+(a+c^2)^{-1}$,

(12) $\{(c^2,(b+1)^{-1}),((b+1)^{-1},c^2),(a+c^2,a+(b+1)^{-1}),(a+(b+1)^{-1},a+c^2)\}$ with $a\notin\mathbb{F}_4$ and $b^2(a^2+ac^2)+b(a^2+ac)+c=0$,

(13) $\{(\frac{y}{by+1},y),(y,\frac{y}{by+1})\}$ with $by^2+aby+a=0$, $\frac{y}{by+1},y\notin\mathbb{F}_4, a+\mathbb{F}_4$, hence $\mathrm{Tr}\left(\frac{1}{ab}\right)=0$.

It is easy to verify that for $a=1,c,c^2$ and for any fixed b, we have at most 4 different solutions. For example for $a=1$ we consider solutions from (1),(2),(3),(13). When $b=1$ we have $(0,c^2),(c^2,0),(1,c),(c,1)$ from (3), and none from (13). When $b=c$ we have $(0,c),(c,0),(1,c^2),(c^2,1)$ from (2) and none from (13). When $b=c^2$ we have $(0,1),(1,0),(c,c^2),(c^2,c)$ from (1) and none from (13). When $b\notin\mathbb{F}_4$ and $\mathrm{Tr}\left(\frac{1}{b}\right)=0$ then we have at most 2 solutions from (13).

Hence we just need to focus on cases (4), (5), (6), (7), (8), (9), (10), (11), (12), (13).

- If $b=a^{-1}$ then we have

  case (4), $(0,a)$, $(a,0)$,

  case (13), $\left(\frac{y}{a^{-1}y+1},y\right)$, $\left(y,\frac{y}{a^{-1}y+1}\right)$,

  hence we have 4 solutions.

- If $b=a^{-1}c^2$ then we have

  case (5), $(0,ac)$, $(ac,0)$, (a,ac^2), (ac^2,a),

  hence 4 solutions.

- If $b=a^{-1}c$ then we have

  case (6), $(0,ac^2)$, $(ac^2,0)$, (a,ac), (ac,a),

  hence 4 solutions.

- If $b=c^2+(a+1)^{-1}$ then we have

  case (7), $(1,a+1)$, $(a+1,1)$,

  case (10) is possible if $a^3c+a^2c^2+a+c^2=0$ (it implies $a^{64}=a$, hence only possible when $3|k$ and in this case we have 4 solutions),

case (13), $\left(\frac{y}{by+1}, y\right)$, $\left(y, \frac{y}{by+1}\right)$ if $\mathrm{Tr}\left(\frac{1}{ab}\right)$=0,

hence at most 4 solutions.

- If $b = c + (a+c)^{-1}$ then we have

  case (9), $(c, a+c)$, $(a+c, c)$,

  case (8) is possible if $a^3 = a^2 + 1$ (it implies $a^8 = a$, hence only possible when $3|k$ and in this case we have 4 solutions),

  case (12) is possible if $a^3 = a^2c^2 + ac + c$ (it implies $a^{64} = a$, hence only possible when $3|k$ and in this case we have 4 solutions),

  case (13) is possible if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, 2 solutions.

  It is trivial that both cases (8) and (12) cannot be verified. Therefore if k is not a multiple of 3 we have at most 4 solutions. Otherwise we have at most 8 solutions.

- If $b = 1 + (a+c^2)^2$ we have

  case (11), $(c^2, a+c^2)$, $(a+c^2, c^2)$,

  case (8) is possible if $a^3 = a^2 + a + c$ (it implies $a^{64} = a$, hence only if $3|k$ and in this case we have at most 4 solutions),

  case (10) is possible if $a^4 = a^3c^2 + a^2c + a + 1$ (it implies $a^{64} = a$, hence only if $3|k$ and in this case we have at most 4 solutions),

  case (13) is possible if $\mathrm{Tr}\left(\frac{1}{ab}\right) = 0$, 2 solutions.

  Again, both (8) and (10) cannot be satisfied. Therefore when k is not a multiple of 3 we have at most 4 solutions, otherwise we have at most 8 solutions.
  We are now left to consider cases (8), (10), (12), (13).

- If (8) and (10) are satisfied, then we obtain $b = ac$ and $a^3 = a^2c + ac^2 + c^2$. Then $a^{64} = a$, and it is possible only if k is multiple of 3.

- If (8) and (12) are satisfied, then $b = a$ and $a^3 = a^2 + a + c$. This leads to $a^{64} = a$, hence it is possible only if k is multiple of 3.

- If (10) and (12) are satisfied, then $b = ac^2$ and $a^3 + c^2a^2 + ac + c^2 = 0$. So, $a^{64} = a$, and it is possible only if k is multiple of 3.

Therefore we have that if k is not a multiple of 3 we can have at most 6 solutions (4 from one among (8), (10), (12) and 2 from (13)). If k is a multiple of 3 that we can have at most 10 solutions.

Let $\mathbb{F}_{2^6}^\star = \langle w \rangle$. For the case when (8) and (10) are satisfied we have $b = ac$ and w^{46}, w^{58}, w^{43} are the solutions of $a^3 = a^2c + ac^2 + c^2$. However, for these values $\mathrm{Tr}(\frac{1}{ab}) = 1$, and so condition (13) is not satisfied.
Similar, when (8) and (12) are satisfied we have $b = a$ and w, w^4, w^{16} are solutions of $a^3 = a^2 + a + c$. Hence a must assume one of these values. But since $\mathrm{Tr}\left(\frac{1}{w}\right) = 1$ we have that case (13) is not possible.
Also for the last case we have $b = ac^2$ and the solutions of $a^3 + c^2a^2 + ac + c^2 = 0$ are w^{22}, w^{25}, w^{37}. For all these cases $\mathrm{Tr}(\frac{1}{ab}) = 1$, implying that (13) cannot happen.
Therefore for k multiple of 3 we have 8 solutions.

Now, as for the the last part of Theorem 8.3, we show that if $3 \nmid n$ we have exactly 6 solutions. Then, let $k = \frac{1}{ab}$ of null trace, as in Theorem 8.3 we consider $k \neq 0, 1$. From condition (8), (10) and (12) we obtain

(a) $a^2kc + a(k^2+k+c^2) + c^2 = 0$;

(b) $a^2kc^2 + a(k^2+k+c^2) + 1 = 0$;

(c) $a^2kc^2 + a(k^2+k+c^2) + c = 0$.

For (a) and (c) we can have solutions if and only if

$$\begin{aligned} 0 =& \mathrm{Tr}\left(\frac{k}{(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k^2+c^2}{(k^2+k+c^2)^2} + \frac{1}{k^2+k+c^2}\right) \\ =& \mathrm{Tr}\left(\frac{k+c}{k^2+k+c^2} + \frac{1}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{k+c^2}{k^2+k+c^2}\right) \\ =& \mathrm{Tr}\left(\frac{k^2}{k^2+k+c^2} + 1\right) = \mathrm{Tr}\left(\frac{k^2}{k^2+k+c^2}\right) \end{aligned} \tag{B.3}$$

and for (b)

$$\begin{aligned} 0 =& \mathrm{Tr}\left(\frac{kc^2}{(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k}{c(k^2+k+c^2)^2}\right) = \mathrm{Tr}\left(\frac{k^2+c^2}{c(k^2+k+c^2)^2} + \frac{1}{c(k^2+k+c^2)}\right) \\ =& \mathrm{Tr}\left(\frac{k+c}{c^2(k^2+k+c^2)} + \frac{1}{c(k^2+k+c^2)}\right) = \mathrm{Tr}\left(\frac{k}{c^2(k^2+k+c^2)}\right) \\ =& \mathrm{Tr}\left(\frac{kc}{k^2+k+c^2}\right) \end{aligned} \tag{B.4}$$

Suppose, by contradiction, that for any $k \in Tr_0 \setminus \{0,1\}$ (B.3) and (B.4) cannot happen. Then

$$\mathrm{Tr}\left(\frac{k}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{kc}{k^2+k+c^2}\right) = 1,$$

for any k. Since $k+1 \in Tr_0 \setminus \{0,1\}$ for all $k \in Tr_0 \setminus \{0,1\}$, we obtain

$$\mathrm{Tr}\left(\frac{1}{k^2+k+c^2}\right) = \mathrm{Tr}\left(\frac{c}{k^2+k+c^2}\right) = 0,$$

for any $k \in Tr_0 \setminus \{0,1\}$. Now, let $S = \{k^2+k : \mathrm{Tr}(k) = 0\}$. As above, $Tr_1 = (c+S) \cup (c^2+S)$. Now, $\frac{k^2+k+c^2}{c} = c^2s + c$, with $s \in S$, and we have that $c^2S = S$. Indeed, since any $k \in Tr_0$ can be written as $k = d^2 + d$ for some $d \in \mathbb{F}_{2^n}$ we have that $S = \{d^4 + d : d \in \mathbb{F}_{2^n}\}$. So,

$$c^2s = c^2(d^4+d) = (c^2d)^4 + c^2d = [(c^2d)^2 + c^2d]^2 + \underbrace{(c^2d)^2 + c^2d}_{\in Tr_0} \in S.$$

Therefore, $c + c^2S = c + S$ implying that all the elements in $Tr_1 \setminus \{c, c^2\}$ are mapped by the inverse function into $Tr_0 \setminus \{0,1\}$ So, as in Theorem 8.3 we obtain a contradiction and thus, for some $k \in Tr_0 \setminus \{0,1\}$, there exist a, b satisfying (13) and one among (8), (10) and (12). □

Bibliography

[1] ALBERT, A. A. On nonassociative division algebras. In *Transaction of the American Mathematical Society* (1952), vol. 72, pp. 296–309. 2.4.2, 2.4.3, 7.1, 7.1

[2] ALBERT, A. A. Finite division algebras and finite planes. In *Proceedings of the 10th Symposium in Applied Mathematics (Providence)* (1960), vol. 10, pp. 53–70. 2.4.1

[3] ARAGONA, R., CALDERINI, M., TORTORA, A., AND TOTA, M. Primitivity of PRESENT and other lightweight ciphers. *Journal of Algebra and Its Applications 17*, 06 (2018), 1850115. B

[4] AT, N., AND COHEN, S. D. A new tool for assurance of perfect nonlinearity. In *Sequences and Their Applications – SETA 2008, Lecture Notes in Computer Science* (2008), Springer Berlin Heidelberg, pp. 415–419. 7.3

[5] BARTOLI, D., AND BONINI, M. Planar polynomials arising from linearized polynomials. arXiv, abs/1903.02112, 2019. To appear in Journal of Algebra and its Applications. 7, 7.2.2, 7.3

[6] BERGER, T. P., CANTEAUT, A., CHARPIN, P., AND LAIGLE-CHAPUY, Y. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory 52*, 9 (2006), 4160–4170. 2.3.1, 3.2.3, 3.2.3

[7] BETH, T., AND DING, C. On almost perfect nonlinear permutations. In *Advances in Cryptology - EUROCRYPT 1993, Lecture Notes in Computer Science* (1994), vol. 765, Springer Berlin Heidelberg, pp. 65–76. 2.1, 5.3

[8] BIERBRAUER, J. New semifields, PN and APN functions. *Designs, Codes and Cryptography 54*, 3 (2010), 189–200. 2.4.2

[9] BIERBRAUER, J. Commutative semifields from projection mappings. *Designs, Codes and Cryptography 61*, 2 (2011), 187–196. 2.4.2

[10] BIHAM, E., ANDERSON, R., AND KNUDSEN, L. Serpent: A new block cipher proposal. In *Fast Software Encryption- FSE 1998, Lecture Notes in Computer Science* (1998), vol. 1372, Springer Berlin Heidelberg, pp. 222–238. 2.3.1

[11] BIHAM, E., DUNKELMAN, O., AND KELLER, N. New results on boomerang and rectangle attacks. In *Fast Software Encryption - FSE 2002, Lecture Notes in Computer Science* (2002), vol. 2365, Springer Berlin Heidelberg, pp. 1–16. 2.1.3

[12] BIHAM, E., AND SHAMIR, A. Differential cryptanalysis of DES-like cryptosystems. In *Advances in Cryptology – CRYPTO 1990, Lecture Notes in Computer Science* (1991), vol. 537, Springer Berlin Heidelberg, pp. 2–21. 1, 2.1.3

[13] BIRYUKOV, A., DE CANNIÈRE, C., AND DELLKRANTZ, G. Cryptanalysis of Safer++. In *Advances in Cryptology - CRYPTO 2003, Lecture Notes in Computer Science* (2003), vol. 2729, Springer Berlin Heidelberg, pp. 195–211. 2.1.3

[14] BLUHER, A. W. On existence of Budaghyan–Carlet APN hexanomials. *Finite Fields and Their Applications 24* (2013), 118–123. 6.2.4

[15] BOGDANOV, A., KNUDSEN, L. R., LEANDER, G., PAAR, C., POSCHMANN, A., ROBSHAW, M. J. B., SEURIN, Y., AND VIKKELSOE, C. Present: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science* (2007), vol. 4727, Springer, pp. 450–466. 2.3.1

[16] BOURA, C., AND CANTEAUT, A. On the boomerang uniformity of cryptographic Sboxes. *IACR Transactions on Symmetric Cryptology 2018*, 3 (2018), 290–310. 1, 2.1.3, 2.3.2, 2.3.2, 2.3.2, 8, 8.1, 9

[17] BRACKEN, C., BYRNE, E., MARKIN, N., AND MCGUIRE, G. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications 14*, 3 (2008), 703–714. 1, 2.2, 6, 6.1, 6.2, 6.2, 9

[18] BRACKEN, C., AND LEANDER, G. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications 16* (2009), 231–242. 1, 2.8, 8, 8.1, 9

[19] BRACKEN, C., TAN, C. H., AND TAN, Y. Binomial differentially 4 uniform permutations with high nonlinearity. *Finite Fields and Their Applications 18*, 3 (2012), 537–546. 2.8, 8

[20] BRINKMANN, M. Extended affine and CCZ equivalence up to dimension 4. *IACR Cryptology ePrint Archive 2019* (2019), 316. 1, 2.2.2

[21] BRINKMANN, M., AND LEANDER, G. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography 49*, 1 (2008), 273–288. 1, 2.3.1, 2.3.1, 4.4

[22] BROWNING, K., DILLON, J., KIBLER, R., AND MCQUISTAN, M. APN polynomials and related codes. *Journal of Combinatorics, Information & System Sciences 34* (2009), 135–159. 2.3.1, 2.3.1, 2.3.1, 2.3.1, 4, 4.2, 5.1.3

[23] BROWNING, K. A., DILLON, J. F., MCQUISTAN, M. T., AND WOLFE, A. J. An APN permutation in dimension six. In *9th International conference on Finite Fields and Applications; Fq'09* (2010), vol. 518, AMS, pp. 33–42. 1, 2.3.1

[24] BUDAGHYAN, L., CALDERINI, M., CARLET, C., COULTER, R., AND VILLA, I. Generalized isotopic shift construction for APN functions. Cryptology ePrint Archive, Report 2020/295, 2020. To appear in Designs, Codes and Cryptography. 6.1, 6.2

[25] BUDAGHYAN, L., CALDERINI, M., AND VILLA, I. On relations between CCZ- and EA-equivalences. *Cryptography and Communications 12*, 1 (2020), 85–100. 5.1.2

[26] BUDAGHYAN, L., AND CARLET, C. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory 54*, 5 (2008), 2354–2357. 1, 1, 2.2, 6, 6.1, 6.1, 6.1, 6.2.4, 6.2.4, 6.2, 9

[27] BUDAGHYAN, L., AND CARLET, C. CCZ-equivalence of single and multi output boolean functions. In *9th International conference on Finite Fields and Applications; Fq'09* (2010), vol. 518, AMS, pp. 43–54. 2.2.2

[28] BUDAGHYAN, L., CARLET, C., AND LEANDER, G. On inequivalence between known power APN functions. In *International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2008* (2008). 1, 2.3.1, 4.3.2

[29] BUDAGHYAN, L., CARLET, C., AND LEANDER, G. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory 54*, 9 (2008), 4218–4229. 1, 1, 2.3.1, 2.3.1, 2.2, 6.1, 6.2

[30] BUDAGHYAN, L., CARLET, C., AND LEANDER, G. Constructing new APN functions from known ones. *Finite Fields and Their Applications 15*, 2 (2009), 150–159. 1, 2.2, 3, 3.1, 3.2.2, 4.1, 6.1, 6.2, 9

[31] BUDAGHYAN, L., CARLET, C., AND LEANDER, G. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop* (2009), pp. 374–378. 1, 2.2, 3, 3.1, 3.1, 3.2.1, 3.2.2, 4.1, 6.1, 6.2, 9

[32] BUDAGHYAN, L., CARLET, C., AND POTT, A. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory 52*, 3 (2006), 1141–1152. 1, 2.2.2, 2.3.1, 4.3.2

[33] BUDAGHYAN, L., AND HELLESETH, T. New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p. In *Sequences and Their Applications – SETA 2008, Lecture Notes in Computer Science* (2008), Springer Berlin Heidelberg, pp. 403–414. 1, 2.2.2, 2.4.1, 2.4.2, 2.4.3, 7.1

[34] BUDAGHYAN, L., HELLESETH, T., AND KALEYSKI, N. A new family of APN quadrinomials. *IEEE Transactions on Information Theory* (2020), 1–1. 2.2, 6.1, 6.2

[35] BUDAGHYAN, L., HELLESETH, T., LI, N., AND SUN, B. Some results on the known classes of quadratic APN functions. In *Codes, Cryptology and Information Security – C2SI 2017, Lecture Notes in Computer Science* (2017), vol. 10194, Springer International Publishing, pp. 3–16. 1, 1, 1, 4.3.2, 6, 6, 6.1, 6.2.1

[36] CALDERINI, M. On the EA-classes of known APN functions in small dimensions. *Cryptography and Communications 12*, 5 (2020), 821–840. 1

[37] CALDERINI, M., SALA, M., AND VILLA, I. A note on APN permutations in even dimension. *Finite Fields and Their Applications 46* (2017), 1–16. 2.3.1

[38] CANTEAUT, A., CHARPIN, P., AND KYUREGHYAN, G. M. A new class of monomial bent functions. *Finite Fields and Their Applications 14*, 1 (2008), 221–241. 3.2.3

[39] CANTEAUT, A., AND PERRIN, L. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications 56* (2019), 209–246. 5.5

[40] CARLET, C. Partially-bent functions. *Designs, Codes and Cryptography 3*, 2 (1993), 135–145. 5

[41] CARLET, C. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography 59*, 1-3 (2009), 89–109. 6.1

[42] CARLET, C. Vectorial boolean functions for cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010, pp. 398–470. 2.2, 2.2.1, 2.3.1, 6, 2.3.3, 3.2.3

[43] CARLET, C. More constructions of APN and differentially 4-uniform functions by concatenation. *Science China Mathematics 56*, 7 (2013), 1373–1384. 6.1

[44] CARLET, C., CHARPIN, P., AND ZINOVIEV, V. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography 15*, 2 (1998), 125–156. 1, 2.1.3, 2.2.2, 2.3.3

[45] CHABAUD, F., AND VAUDENAY, S. Links between differential and linear cryptanalysis. In *Advances in Cryptology – EUROCRYPT 1994, Lecture Notes in Computer Science* (1995), vol. 950, Springer Berlin Heidelberg, pp. 356–365. 2.3.3

[46] CID, C., HUANG, T., PEYRIN, T., SASAKI, Y., AND SONG, L. Boomerang Connectivity Table: A new cryptanalysis tool. In *Advances in Cryptology – EUROCRYPT 2018, Lecture Notes in Computer Science* (2018), vol. 10821, Springer International Publishing, pp. 683–714. 1, 2.1.3, 2.3.2, 2.3.2, 8

[47] COHEN, S. D. Primitive elements and polynomials with arbitrary trace. *Discrete Mathematics 83*, 1 (1990), 1–7. 3.2.1

[48] COHEN, S. D., AND GANLEY, M. J. Commutative semifields, two dimensional over their middle nuclei. *Journal of Algebra 75*, 2 (1982), 373–385. 2.4.2, 7.1

[49] COULTER, R., AND HENDERSON, M. Commutative presemifields and semifields. *Advances in Mathematics 217* (2008), 282–304. 1, 2.1.3, 2.4.1, 2.4.1

[50] COULTER, R., HENDERSON, M., HU, L., KOSICK, P., XIANG, Q., AND ZENG, X. Planar polynomials and commutative semifields two dimensional over their middle nucleus and four dimensional over their nucleus. Available online at https://sites.udel.edu/coulter/publications/. 7.1.3

[51] COULTER, R. S., AND MATTHEWS, R. W. Planar functions and planes of Lenz-Barlotti Class II. *Designs, Codes and Cryptography 10*, 2 (1997), 167–184. 2.4.2, 7.1

[52] DAEMEN, J., AND RIJMEN, V. *The design of Rijndael: AES - The Advanced Encryption Standard*, vol. 2. Springer, 2002. 2.1.2, 2.3.1

[53] DE CANNIÈRE, C. Analysis and design of symmetric encryption algorithms. *Doctoral Dissertaion, KULeuven* (2007). 1

[54] DEMPWOLFF, U. CCZ equivalence of power functions. *Designs, Codes and Cryptography 86*, 3 (2018), 665–692. 1, 2.3.1

[55] DICKSON, L. E. On commutative linear algebras in which division is always uniquely possible. In *Transaction of the American Mathematical Society* (1906), vol. 7, pp. 514–522. 2.4.1, 2.4.2, 2.4.3, 7.3, 7.1

[56] DICKSON, L. E. Linear algebras with associativity not assumed. *Duke Mathematical Journal 1*, 2 (1935), 113–125. 7.3

[57] DILLON, J. F. APN polynomials and related codes, 2006. Polynomials over Finite Fields and Applications, Banff International Research Station. 3.2.3, 4, 4.2, 4.4, A

[58] DING, C., AND YUAN, J. A family of skew Hadamard difference sets. *Journal of Combinatorial Theory, Series A 113*, 7 (2006), 1526–1535. 2.4.2, 7.3

[59] DOBBERTIN, H. Almost perfect nonlinear power functions on GF(2^n): The Niho case. *Information and Computation 151*, 1 (1999), 57–72. 1, 2.1, 2.3.1, 5.3

[60] DOBBERTIN, H. Almost perfect nonlinear power functions on GF(2^n): The Welch case. *IEEE Transactions on Information Theory 45*, 4 (1999), 1271–1275. 2.1, 5.3

[61] DOBBERTIN, H. Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5. In *Finite Fields and Applications* (2001), Springer Berlin Heidelberg, pp. 113–121. 1, 2.1, 2.3.1, 5.3

[62] DUAN, X. Y., AND DENG, Y. L. Two classes of quadratic crooked functions. *Applied Mechanics and Materials 513* (2014), 2734–2738. 1, 6, 6.1, 6.1, 6.1.1, 6.3, 9

[63] DUNKELMAN, O., KELLER, N., AND SHAMIR, A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology 27*, 4 (2014), 824–849. 2.1.3

[64] EDEL, Y. Quadratic APN functions as subspaces of alternating bilinear forms. In *Contact Forum Coding Theory and Cryptography III 2009* (Belgium, 2011), pp. 11–24. 2.3.1

[65] EDEL, Y., KYUREGHYAN, G., AND POTT, A. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory 52*, 2 (2006), 744–747. 2.3.1

[66] EDEL, Y., AND POTT, A. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications 3* (2009), 59–81. 1, 2.3, 2.3.1, 2.3.1, 2.3.1, 2.3.1, 2.3, 2.3.1, 2.4, 2.3.1, 2.5, 2.6, 3.3, 3.3, 4.4, 5, 5.1.3, 9

[67] FEISTEL, H. Cryptography and computer privacy. *Scientific American 228*, 5 (1973), 15–23. 2.1.2

[68] FEISTEL, H., NOTZ, W. A., AND SMITH, J. L. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE 63*, 11 (1975), 1545–1554. 2.1.2

[69] GANLEY, M. J. Central weak nucleus semifields. *European Journal of Combinatorics 2*, 4 (1981), 339–347. 2.4.2, 7.1

[70] GÖLOĞLU, F. Almost perfect nonlinear trinomials and hexanomials. *Finite Fields and Their Applications 33* (2015), 258–282. 6, 6.2.4

[71] GÖLOĞLU, F., AND LANGEVIN, P. Almost perfect nonlinear families which are not equivalent to permutations. *Finite Fields and Their Applications 67* (2020), 101707. 2.3.1

[72] GÖLOĞLU, F., AND PAVLU, J. Search for APN permutations among known APN functions, 2019. Presented at BFA 2019, 4th International Workshop on Boolean Functions and their Applications. 2.3.1, 5, 5.4

[73] GOLD, R. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory 14*, 1 (1968), 154–156. 2.1, 2.8, 4.3.2, 5.3

[74] HOU, X. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete Applied Mathematics 154*, 2 (2006), 313–325. Coding and Cryptography. 2.3.1

[75] JANWA, H., AND WILSON, R. M. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes – AAECC 1993, Lecture Notes in Computer Science* (1993), vol. 673, Springer Berlin Heidelberg, pp. 180–194. 2.1, 5.3

[76] KASAMI, T. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control 18*, 4 (1971), 369–394. 2.1, 2.8, 5.3

[77] KATZ, J., AND LINDELL, Y. *Introduction to Modern Cryptography*. CRC press, 2014. 2.1

[78] KELSEY, J., KOHNO, T., AND SCHNEIER, B. Amplified boomerang attacks against reduced-round MARS and Serpent. In *Fast Software En-*

cryption - FSE 2000, Lecture Notes in Computer Science (2001), vol. 1978, Springer Berlin Heidelberg, pp. 75–93. 2.1.3

[79] KERCKHOFFS, A. La cryptographic militaire. *Journal des Sciences Militaires IX* (1883), 5–38. 2.1

[80] KNUDSEN, L. R. Truncated and higher order differentials. In *Fast Software Encryption - FSE 1994, Lecture Notes in Computer Science* (1995), vol. 1008, Springer Berlin Heidelberg, pp. 196–211. 5

[81] KYUREGHYAN, G., AND ÖZBUDAK, F. Planarity of products of two linearized polynomials. *Finite Fields and Their Applications 18*, 6 (2012), 1076–1088. 7.2.2, 7.6, 7.3

[82] LACHAUD, G., AND WOLFMANN, J. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Transactions on Information Theory 36*, 3 (1990), 686–692. 2.1

[83] LAI, X. Higher order derivatives and differential cryptanalysis. In *Communications and Cryptography: Two Sides of One Tapestry. The Springer International Series in Engineering and Computer Science (Communications and Information Theory)*, vol. 276. Springer US, 1994, pp. 227–233. 5

[84] LI, K., QU, L., SUN, B., AND LI, C. New results about the boomerang uniformity of permutation polynomials. *IEEE Transactions on Information Theory 65* (2019), 7542–7553. 2.3.2, 2.2, 8, 8.2, 9

[85] LI, Y., WANG, M., AND YU, Y. Constructing differentially 4-uniform permutations over GF(2^{2k}) from the inverse function revisited. *IACR Cryptology ePrint Archive 2013* (2013), 731. 1, 8, 8.2, 8.2, 8.2, 9

[86] LUNARDON, G., MARINO, G., POLVERINO, O., AND TROMBETTI, R. Symplectic spreads and quadric veroneseans, 2009. Manuscript, also presented at Finite Fields 2009, Dublin, Ireland. 2.4.2, 7.1

[87] MARINO, G., AND POLVERINO, O. On isotopisms and strong isotopisms of commutative presemifields. *Journal of Algebraic Combinatorics 36*, 2 (2012), 247–261. 2.4.2

[88] MATSUI, M. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science* (1994), vol. 765, Springer Berlin Heidelberg, pp. 386–397. 2.1.3, 2.3.3

[89] MCELIECE, R. J. *Finite Fields for Computer Scientists and Engineers*, vol. 23. Springer US, Kluwer Academic Publishers, 1987. 6.1

[90] MENICHETTI, G. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *Journal of Algebra 47*, 2 (1977), 400–410. 7.3

[91] MESNAGER, S., TANG, C., AND XIONG, M. On the boomerang uniformity of quadratic permutations. *Designs, Codes and Cryptography* (2020). 1, 2.3.2, 8, 9

[92] NYBERG, K. Differentially uniform mappings for cryptography. In *Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science* (1994), vol. 765, Springer Berlin Heidelberg, pp. 55–64. 2.1.3, 2.1, 2.8, 4.3.2, 5.3, B.1

[93] NYBERG, K. S-boxes and round functions with controllable linearity and differential uniformity. In *Fast Software Encryption – FSE 1994, Lecture Notes in Computer Science* (1995), vol. 1008, Springer Berlin Heidelberg, pp. 111–130. 2.3.1, 3.2.3

[94] PIEPER-SEIER, I., AND SPILLE, B. Remarks on the paper on strong isotopy of Dickson semifields and geometric implications. *Results in Mathematics 35*, 3 (1999), 310–313. 2.4.1

[95] QU, L., TAN, Y., TAN, C. H., AND LI, C. Constructing differentially 4-uniform permutations over $F_{2^{2k}}$ via the Switching Method. *IEEE Transactions on Information Theory 59* (2013), 4675–4686. 8.2

[96] SHANNON, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal 28*, 4 (1949), 656–715. 1, 2.1.2

[97] STINSON, D. R. *Cryptography: theory and practice*. CRC press, 1995. 2.1

[98] TANG, D., CARLET, C., AND TANG, X. Differentially 4-uniform bijections by permuting the inverse function. *Designs, Codes and Cryptography 77*, 1 (2015), 117–141. 8.2

[99] TANIGUCHI, H. On some quadratic APN functions. *Designs, Codes and Cryptography 87*, 9 (2019), 1973–1983. 2.2, 6.1, 6.2

[100] VAN TILBORG, H. C., AND JAJODIA, S. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014. 2.1

[101] WAGNER, D. The boomerang attack. In *Fast Software Encryption – FSE 1999, Lecture Notes in Computer Science* (1999), vol. 1636, Springer Berlin Heidelberg, pp. 156–170. 1, 2.1.3

[102] WENG, G., TAN, Y., AND GONG, G. On quadratic almost perfect nonlinear functions and their related algebraic object. Available online at http://www.selmer.uib.no/WCC2013/pdfs/Weng.pdf. 1, 2.3.1, 2.7, 3.3, 4.4, 5, 5.1.1, 5.1, 5.1, 5.2

[103] YANG, M., ZHU, S., AND FENG, K. Planarity of mappings $x(\mathrm{Tr}(x) - \alpha 2x)$ on finite fields. *Finite Fields and Their Applications 23* (2013), 1–7. 7.2.2

[104] YOSHIARA, S. Notes on APN functions, semibiplanes and dimensional dual hyperovals. *Designs, Codes and Cryptography 56*, 2-3 (2010), 197–218. 1, 2.1.3

[105] YOSHIARA, S. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics 35*, 3 (2012), 461–475. 1, 2.2.2, 5.1, 6

[106] YOSHIARA, S. Equivalences of power APN functions with power or quadratic APN functions. *Journal of Algebraic Combinatorics 44* (2016), 561–585. 1, 2.3.1, 4.3.2, 4.4

[107] YU, Y., KALEYSKI, N., BUDAGHYAN, L., AND LI, Y. Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9. *Finite Fields and Their Applications 68* (2020), 101733. 2.3.1

[108] YU, Y., WANG, M., AND LI, Y. Constructing differentially 4 uniform permutations from known ones. *Chinese Journal of Electronics 22* (2013), 495–499. 1, 8, 8.2, 8.2, 9

[109] YU, Y., WANG, M., AND LI, Y. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography 73*, 2 (2014), 587–600. 1, 2.3.1, 2.3.1, 3.3, 4.4

[110] ZHA, Z., HU, L., AND SUN, S. Constructing new differentially 4-uniform permutations from the inverse function. *Finite Fields and Their Applications 25* (2014), 64–78. 8.2

[111] ZHA, Z., KYUREGHYAN, G. M., AND WANG, X. Perfect nonlinear binomials and their semifields. *Finite Fields and Their Applications 15*, 2 (2009), 125–133. 1, 2.4.2

[112] ZHOU, Y., AND POTT, A. A new family of semifields with 2 parameters. *Advances in Mathematics 234* (2013), 43–60. 1, 2.2, 2.3.1, 2.4.2, 2.4.3, 6.1, 6.2, 7.1

Errata for
Analysis, classification and construction of optimal cryptographic Boolean functions

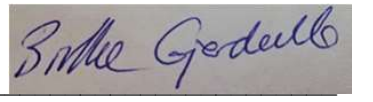
Irene Villa

Thesis for the degree philosophiae doctor (PhD)

at the University of Bergen

10/12/2020 Irene Villa

(date and sign. of candidate)



(date and sign. of faculty)

Errata

Page iii “infinite many” – corrected to “infinitely many”

Page 2 “APN function” – corrected to “APN functions”

Page 4 “over $\mathbb{F}_{2^6}$ F and G,” – corrected to “F and G over $\mathbb{F}_{2^6}$,”

Page 5 “of dimension i” – corrected to “of certain dimension”

Page 7 “The properties of the [..] are” – corrected to “Determining the [..] is”

Page 9 “any more” – corrected to “anymore”

Page 9 added the word “German”

Page 10 “The keys involved are” – corrected to “The decryption key involved is”

Page 13 “public-key” – corrected to “key”

Page 13 “itermediate” – corrected to “intermediate”

Page 13 “distinguisher attack” – corrected to “distinguishing attack”

Page 14 “black/grey/white box” – corrected to “black/grey/white-box”

Page 14 “difference in an input” – corrected to “difference between two inputs”

Page 19 “k=1” – corrected to “k=0” (in the definition of Trace function)

Page 21 “number of its classes” – corrected to “number of classes”

Page 24 “APN function” – corrected to “APN functions”

Page 24 “Vectorial” – corrected to “vectorial”

Page 25 “2006” – corrected to “2009” and removed reference [57]

Page 27 “$(2^n$-1)” – corrected to “2^n”

Page 31 “is given by” – corrected to “is”

Page 32 “number of solution” – corrected to “number of solutions”

Page 34 “Functions that achieve such bound” – corrected to “The functions that achieve this bound”

Page 35 “upper bound” – corrected to “maximum”

Page 35 removed “optimal”

Page 42 moved the footnote mark from “f” to “function”

Page 54 [42] – corrected to [93]

Page 61 “to study” – corrected to “to the study of”

Page 138 “$\pi(x) =$” – corrected to “$F_\pi(x) =$”

Page 144 “can not” – corrected to “cannot”

Bibliography

[34], [104], [107] “apn” – corrected to “APN”

[67] “american” – corrected to “American”

[77] “modern cryptography” – corrected to “Modern Cryptography”

Graphic design: Communication Division, UiB / Print: Skipnes Kommunikasjon AS

uib.no

ISBN: 9788230848036 (print)
9788230852217 (PDF)