CONTRIBUTIONS TO THE THEORY OF ALMOST PERFECT NONLINEAR FUNCTIONS

Dissertation

zu Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von M. Sc. Razi Arshad

geb. am 18.04.1979 in Lahore

genehmigt durch die Fakultät für Mathematik

der Otto-von-Guericke-Universität Magdeburg.

Gutachter: Prof. Dr. Alexander Pott

Prof.in Dr. Gohar Kyureghyan

eingereicht am: 06.06.2018

Verteidigung am: 04.09.2018

Zusammenfassung

In dieser Dissertation untersuchen wir fast perfekt nichtlineare (“almost perfect nonlinear”, APN) Funktionen. In der Kryptographie, insbesondere bei Blockchiffren, sind vektorielle Boolesche Funktionen von grundlegender Bedeutung. Es gibt zwei Hauptangriffe auf Blockchiffren: differentielle Angriffe [1] und lineare Angriffe [2]. Funktionen, die den Besten Schutz vor differentiellen Angriffen bieten, werden als APN Funktionen bezeichnet. Die Funktionen, die einen optimalen Schutz sowohl vor linearen als auch differentiellen Angriffen bieten, werden als “almost bent” (AB) Funktionen bezeichnet. Alle bekannten Konstruktionen von APN Funktionen verwenden endliche Köper, während in dieser Arbeit die Konstruktion von APN Funktionen unter Verwendung von im wesentlichen nur Vektorräumen studiert.

Zuerst schlagen wir einen neuen Ansatz zur Konstruktion von APN Funktionen unter Verwendung von Koordinatenfunktionen vor. Wir zeigen, dass “bent” Funktionen die besten Kandidaten für Koordinatenfunktionen von APN Funktionen sind. Wir untersuchen eine Variation der Maiorana-McFarland und der “partial spread” Klasse von Booleschen Funktionen. Wir zeigen, dass diese auch gute Kandidaten für Koordinatenfunktionen sind, insbesondere sind sie bessere Kandidaten als sogenannt plateaued Funktionen, die kürzlich vorgeschlagen wurden. Dann studieren wir die Klassen von vektoriellen “bent” Funktionen, die in den bekannten quadratischen APN Funktionen aus $\mathbb{F}_{2^6}$ enthalten sind.

Die vektoriellen booleschen Funktionen von $\mathbb{F}_2^n$ nach $\mathbb{F}_2^n$ können als ein Würfel der Dimension $n \times n \times n$ beschrieben werden. Wir zeigen, dass dieses Konzept auf vektorielle Boolesche Funktionen von $\mathbb{F}_2^n$ nach $\mathbb{F}_2^m$ erweitert werden kann.

Wir berechnen explizit verschiedene Invarianten der quadratischen APN Funktionen, die von Yu, Wang und Li [3] in $\mathbb{F}_{2^7}$ und $\mathbb{F}_{2^8}$ gefunden wurden. Wir präsentieren einige Ergebnisse zu Funktionen der Form $F(x) = x^3 + Tr_1^n(x)L(x)$, wobei $L(x)$ ein linearisiertes Polynom ist. Wir zeigen, dass $F(x) = x^3 + Tr_1^n(x)x$ niemals eine APN Funktion ist, indem wir Kloosterman-Summen verwenden.

Ferner schlagen wir auch einen neuen Ansatz für die Konstruktion von APN Funktionen vor, indem wir die Zerlegung von $\mathbb{F}_2^n$ in affine Unterräume verwenden. Wir haben mehrere Beispiele für APN Funktionen gefunden, indem wir diesen Ansatz in $\mathbb{F}_{2^6}$ und $\mathbb{F}_{2^8}$ verwenden. Schließlich zeigen wir die Äquivalenz der Göloğlu und der Gold APN Funktionen. Wir diskutieren einen Fehler in MAGMA [4] bezüglich der Code Äquivalenz.

Abstract

In this dissertation, we investigate almost perfect nonlinear (APN) functions.
In cryptography, particularly in block ciphers, vectorial Boolean functions are of fundamental importance. There are two main attacks on block ciphers, differential attacks [1] and linear attacks [2]. The functions which provide the best resistance against differential attacks are called APN functions. The functions which provide optimal resistance against both linear and differential attacks are called almost bent (AB) functions. All the known constructions of APN functions use finite fields. In this work, we study the construction of APN functions using vector space structure.
First, we propose a new approach for the construction of APN functions by using coordinate functions. We show that bent functions are the best candidates for coordinate functions of APN functions. We study a variation of the Maiorana-McFarland and the partial spread class of Boolean functions. We show that these are also good candidates for coordinate functions, in particular, they are better candidates than plateaued functions which have been proposed recently. Then we study classes of vectorial bent functions contained in the known quadratic APN functions on $\mathbb{F}_{2^6}$.
Vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ can be described in terms of a cube of dimension $n \times n \times n$. We show that this concept can be extended to vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.
We explicitly compute several invariants for quadratic APN functions found by Yu, Wang and Li [3] on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$. We present some results on functions of the form $F(x) = x^3 + Tr_1^n(x)L(x)$, where $L(x)$ is a linearized polynomial. We show that $F(x) = x^3 + Tr_1^n(x)x$ is never an APN function by using Kloosterman sums.
We also propose a new approach for the construction of APN functions by using the decomposition of $\mathbb{F}_2^n$ in affine subspaces. Using this construction on $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^8}$, we found several examples of APN functions.
Finally, we show the equivalence of the Göloğlu and the Gold APN functions.
We discuss a MAGMA [4] error about code equivalence.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my advisor Prof. Dr. Alexander Pott for the continuous support, encouragement and motivation throughout my Ph.D. studies. His insight, patience and scientific knowledge helped me to find new and interesting results. I am really very grateful for his availability, optimism and criticism while keeping a friendly working environment. His professional and editorial advice helped me in the completion of this thesis.

I am grateful to Prof.in Dr. Gohar Kyureghyan and Prof. Dr. Kai-Uwe Schmidt for helping me in the initial phase of my research. I am also grateful to Dr. Shuxing Li, Christian Kaspers, Daniel Gerike, for their kindness, friendship and valuable comments.

I shared an office with Alexandr Polujan for two and half year. I am grateful to him for many discussion on variety of topics, his friendship and valuable comments.

I am further grateful to Dr. Faruk Göloğlu and Dr. Yue Zhou for the mathematical discussions on the results of this thesis.

My deepest gratitude goes to my mother, mother-in-law, father-in-law and my brothers for all their endless love and encouragement.

I am grateful to my beloved wife for her endless support and patience in the completion of my Ph.D. studies. She bears all the direct and indirect tension of my Ph.D. studies. I am also grateful to her for unconditional and true love throughout my life.

I am further grateful to my sons Ayan Razi, Umair Razi and Ashar Razi for their inspiration and their love, otherwise, it would be much harder to keep the motivation to finish this thesis.

Finally, I would like to express my gratitude to the financial, academic and technical support from the Otto-von-Guericke University, Magdeburg and the financial support from HEC (*Higher Education Commission*) of Pakistan.

Contents

List of Tables

Overview

In cryptography, vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ can be used as building blocks in block ciphers, such as S-box in AES [5]. There are two main attacks on block ciphers: differential attacks and linear attacks. Nonlinearity and differential uniformity of vectorial Boolean functions provide resistance against linear attacks and differential attacks respectively.

The differential attack was presented by Biham and Shamir [1] in 1991. They study how differences in an input of a cryptosystem can affect the resultant difference at the output. The vectorial Boolean functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, being used as S-box in symmetric cryptosystem, provide the best resistance to differential attacks when the value

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

is small. These functions are called almost perfect nonlinear (APN) functions if $n = m$.

The linear attack was introduced by Matsui [2] in 1993. The linear attack is based on finding the affine approximation to the action of a cipher. The linear attack on the vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is successful if the value

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

is large. The functions achieving the maximum possible nonlinearity, that is,

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m \\ b\neq 0}} \mid \sum_{x\in\mathbb{F}_2^n} (-1)^{b\cdot F(x)+a\cdot x} \mid$$

provide the best resistance to linear attack. These functions are called almost bent (AB) or maximum nonlinear functions.

The classification of AB and APN functions is a hard problem. All the known constructions of APN functions use finite fields. In this thesis, we are interested in studying the APN property of vectorial Boolean functions by using the vector space structure.

Structure of the thesis

Chapter 1 contains all the necessary definitions related to Boolean and vectorial Boolean functions, AB and APN functions, equivalence relations among vectorial Boolean functions and infinite families of AB and APN functions.
In Chapter 2, we propose a new approach for the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ by using n coordinate functions. We study the coordinate function approach in terms of coding theory. Let $f_1(x), \ldots, f_m(x)$ be Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with $m \leq n$. We can define the $(n+m+1) \times 2^n$ matrix

$$H_{f_1,\ldots,f_m} = \begin{bmatrix} 1 \\ x \\ f_1(x) \\ \vdots \\ f_m(x) \end{bmatrix}_{x \in \mathbb{F}_2^n} .$$

Let $C_{f_1,\ldots,f_m} = \{x \in \mathbb{F}_2^{2^n} : H_{f_1,\ldots,f_m} \cdot x = 0\}$. This is the code that consists of all codewords (vectors) orthogonal to the rows of $H_{f_1,\ldots,f_m}$.
The function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}$$

is an APN function if and only if the minimum weight of $C_{f_1,\ldots,f_n}$ is 6, see Corollary 2.4. This means there is no weight 4 vector in the linear code $C_{f_1,\ldots,f_n}$.
In order to construct an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ by using n coordinate functions $f_1, \ldots, f_n$, we need to look at the pattern of reduction of the number of weight 4 vectors in the linear code $C_{f_1,\ldots,f_n}$. We compute the formula for the number of weight 4 vector in the linear code $C_{f_1,\ldots,f_m}$, given in the following theorem

Theorem 2.5. *Assume that F is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$. The number $\lambda(f_1, \ldots, f_m)$ of weight 4 vectors in the linear code $C_{f_1,\ldots,f_m}$ is*

$$\lambda(f_1, \ldots, f_m) = \frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a \in \mathbb{F}_2^n,\, b \in \mathbb{F}_2^m, \\ b \neq 0}} (W_F(a,b))^4 + 2^{4n}\right) - 3 \cdot 2^{2n} + 2^{n+1}\right],$$

where $W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}$.

From Corollary 2.3, we can also compute the number of weight 4 vectors in the linear code C_f of Boolean functions f.
We study several known examples of APN functions by using the coordinate

function approach. We found that bent functions f have minimum number of weight 4 vectors in the linear code C_f. Therefore, bent functions are the best choice for the coordinate functions.

Bent functions can be constructed by using the Maiorana-McFarland and the partial spread construction method. We study Boolean functions belonging to the partial spread and Maiorana-McFarland class.

In the partial spread construction method, we consider two possible cases of m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$. In the first case, we consider m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ without 0. In this case, we compute the number of weight 4 vectors in the linear code C_f.

Corollary 2.14. *Assume that $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function with Walsh spectrum given in Theorem 2.13. The number $\lambda(f_k)$ of weight 4 vectors in the linear code C_{f_k} is*

$$\begin{aligned}\lambda(f_k) =& \frac{1}{24}(\frac{1}{2^{n+1}}[16((2^{n-1} - 2^m k + k - 1)^4 + (2^n k^4 - 2^m k^5 + k^5 - k^4) \\ &+ k(k - 2^m)^4(2^m - 1)) + 2^{4n}] - 3 \cdot 2^{2n} + 2^{n+1}).\end{aligned}$$

In the second case, we consider m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ with 0. In this case, we compute the number of weight 4 vectors in the linear code C_f.

Corollary 2.17. *Assume that $f_k^{'} : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function with Walsh spectrum given in Theorem 2.16. The number $\lambda(f_k^{'})$ of weight 4 vectors in the linear code $C_{f_k^{'}}$ is*

$$\begin{aligned}\lambda(f_k^{'}) =& \frac{1}{24}(\frac{1}{2^{n+1}}[16((2^{n-1} - 2^m k + k - 1)^4 + (k-1)^4(2^n - 2^m k + k - 1) \\ &+ k(k - 2^m - 1)^4(2^m - 1)) + 2^{4n}] - 3 \cdot 2^{2n} + 2^{n+1}).\end{aligned}$$

In both cases, the value of k is less than or equal to 2^{m+1}. We show that for $k = \{2^{m-1} - 1, 2^{m-1} + 1\}$ in the first case and $k = \{2^{m-1}, 2^{m-1} + 2\}$ in the second case, partial spread Boolean functions reduce more weight 4 vectors in their linear code as compared with the weight 4 vectors in the linear code of plateaued Boolean functions.

We also study Boolean functions with certain restrictions belonging to the Maiorana-McFarland class. We compute the number of weight 4 vectors in the linear code related to Maiorana-McFarland Boolean functions.

Corollary 2.21. *Assume that $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function belonging to the Maiorana-McFarland class with Walsh spectrum given in Theorem 2.20. The number $\lambda(f)$ of weight 4 vectors in the linear code C_f is*

$$\lambda(f) = \frac{1}{24}\left[\frac{1}{2^{n+1}}\left(2^{5m}t + 2^{5m+3}s + 2^{4n}\right) - 3 \cdot 2^{2n} + 2^{n+1}\right]$$

We show that for $s = 1$ and $t = 2^m - 2$, Maiorana-McFarland Boolean functions reduce more weight 4 vectors in their linear code as compared with the weight 4 vectors in the linear code of plateaued Boolean functions. The Boolean functions belonging to the Maiorana-McFarland class and partial spread class are good candidates for coordinate functions which can be used in the construction of APN functions by using our coordinate functions approach.
In our coordinate functions approach, we choose vectorial bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n/2}$ as the first $n/2$ coordinate functions with n even. The vectorial bent functions reduce the maximum number of weight 4 vectors in the linear code $C_{f_1,\ldots,f_{n/2}}$. We need to choose other $n/2$ coordinate functions in such a way that there is no weight 4 vectors in the linear code $C_{f_1,\ldots,f_n}$. Then, we obtain APN functions.
In Chapter 3, we consider known quadratic APN functions from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$. We analyze that how these APN functions are constructed by using our coordinate functions approach. So, we study the classes of quadratic vectorial bent functions contained in these APN functions. We completely classify the quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$.

Theorem 3.1. *There are only three (up to equivalence) quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$ and only one (up to equivalence) quadratic vectorial bent function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$.*

In Chapter 4, we study quadratic vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in terms of a cube of dimension $n \times n \times n$. We propose an extension of the cube for quadratic vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Theorem 4.2. *Let F be a quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ defined by*

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix} = \begin{pmatrix} xQ_1x^T \\ \vdots \\ xQ_mx^T \end{pmatrix},$$

where $f_1(x), \ldots, f_m(x)$ are quadratic Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then $D_aF(x)$ is

$$D_aF(x) = \left(\sum_{i=1}^n x_i (\sum_{j=1}^n C_{ij}^1 a_j), \ldots, \sum_{i=1}^n x_i (\sum_{j=1}^n C_{ij}^m a_j) \right),$$

where

$$C^1 = Q_1 + Q_1^T, \ldots, C^m = Q_m + Q_m^T,$$

$a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n \setminus \{0\}$. For $k = 1, \ldots, m$, the matrix C_{**}^k corresponds to the coordinate function f_k of F. For $j = 1, \ldots, n$, $D_aF(x)$ is given by the non-zero linear combinations of matrices C_{*j}^*.

The ranks of all possible non-zero linear combinations of the matrices C_{*j}^*, $j = 1, \ldots, n$ determine the number of solutions of $F(x + a) + F(x) = b$. The matrices C_{**}^k, $k = 1, \ldots, m$ are symmetric matrices with zero diagonal entries. The ranks of all possible non-zero linear combinations of the matrices C^k_{**}, $k = 1, \dots, m$ determine the Walsh spectrum of F [6].

We study the local changes in the quadratic APN cube of dimension $n \times n \times n$. This has been proposed by Yu, Wang and Li [7] for the construction of quadratic APN functions. We extend the work of Yu, Wang and Li by applying different possible changes at different positions of quadratic APN cube of dimension $n \times n \times n$. Unfortunately, we are unable to find new APN functions.

We compute the following so called CCZ-invariants: Δ- and Γ-rank, order of the automorphism groups of $M(G_F)$ and Walsh spectrum for 471 quadratic APN function on $\mathbb{F}_{2^7}$ and 8157 quadratic APN functions on $\mathbb{F}_{2^8}$.

Yu, Wang and Li have constructed several CCZ-inequivalent quadratic APN functions but they were unable to find an infinite family of APN functions. In order to find an infinite family of APN function, it might be useful to have a representation in finite fields. The function

$$F(x) = x^3 + Tr^n_1(x)L(x),$$

where $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ can be obtained from a quadratic APN cube corresponding to the Gold APN function $F(x) = x^3$ by changing the entries $c^k_{i,j}$ with $1 \leq k \leq n$ and $i = n, j = n$ in the cube $C^k_{i,j}$, $1 \leq i, j, k \leq n$.

In Chapter 5, we study some conditions on the function F from $\mathbb{F}^n_2$ to $\mathbb{F}^n_2$ defined by

$$F(x) = x^3 + Tr^n_1(x)L(x),$$

where $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ such that F is an APN function. We prove a non-existence result by using Kloosterman sums:

Theorem 5.4. *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as*

$$F(x) = x^3 + Tr^n_1(x)x.$$

The function F is not an APN function for $n \geq 3$.

Yu, Wang and Li have used their approach for the construction of quadratic APN functions. We show that their approach can be extended to search for non-quadratic APN functions, in particular, if we add $Tr^n_1(x)Q(x)$ to quadratic APN functions F, where $Q(x)$ is an arbitrary polynomial then we could get a non-quadratic APN functions. This approach works for any APN functions from $\mathbb{F}^n_2$ to $\mathbb{F}^n_2$.

We also propose another new method for the construction of APN functions from $\mathbb{F}^n_2$ to $\mathbb{F}^n_2$. This method is based on the specific distribution of $n-2$ dimensional subspaces of $\mathbb{F}^n_2$. Up to our knowledge, this construction method is completely new.

Theorem 5.13. *Let F be an APN function from $\mathbb{F}^n_2$ to $\mathbb{F}^n_2$. Let U be a $n-2$ dimensional subspace of $\mathbb{F}^n_2$ and $U_0 = U$, $U_1 = U + v_1$, $U_2 = U + v_2$ and $U_3 = U + v_3$ are the* *four cosets of U such that $\mathbb{F}_2^n = U_0 \cup U_1 \cup U_2 \cup U_3$, where $v_1,\ v_2,\ v_3 \in \mathbb{F}_2^n$. Let $F^{'}$ be the function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined as*

$$F^{'}(x) = \begin{cases} F(x) + a_0, & \textit{for } x \in U_0, \\ F(x) + a_1, & \textit{for } x \in U_1, \\ F(x) + a_2, & \textit{for } x \in U_2, \\ F(x) + a_3, & \textit{for } x \in U_3, \end{cases}$$

with $a_i \in \mathbb{F}_2^n$, $i = 0, \ldots, 3$. The function $F^{'}$ is an APN function if and only if

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq a_0 + a_1 + a_2 + a_3$$

for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$ with $\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 1$ for all i.

We constructed several examples of APN functions by using Theorem 5.13. In Chapter 6, we study the Göloğlu infinite family of APN functions. We prove that Göloğlu family of APN functions is extended affine equivalent to the Gold family of APN functions.

Theorem 6.2. *Let $n = 2m = 4t$, where m is an even positive integer and $t > 0$. Let Tr_m^n be the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$: $Tr_m^n(x) = x + x^q$, where $q = 2^m$. The APN function*

$$F(x) = x^{2^k+1} + (Tr_m^n(x))^{2^k+1}$$

is EA equivalent to the Gold APN function

$$G(x) = x^{q^2/2^k+q}$$

with $gcd(k, n) = 1$.

We find a computational error in MAGMA which occurs during the testing of code equivalence between the Göloğlu and the Gold family of APN functions. Finally, it should be noted that the following material from this thesis has either been presented or is in preparation to be submitted for publication to international journals:

- ◇ Section 2.2, 2.6: R. Arshad and A. Pott. Almost perfect nonlinear function, KOLLOQUIUM ÜBER KOMBINATORIK, Paderborn, Germany, 24-25 November, 2017.
- ◇ Section 2.2, 2.6, 2.7: R. Arshad and A. Pott. On the variations of the Maiorana-McFarland and the (partial) spread class of Boolean functions, The 3rd International Workshop on Boolean Functions and their Applications (BFA), Leon, Norway 17-22 June, 2018.

◇ Section 4.5: R. Arshad and A. Pott. On the CCZ-invariants of Yu, Wang and Li quadratic APN functions. In preparation.

◇ Section 5.4: R. Arshad and A. Pott. A new construction method for almost perfect nonlinear function. In preparation.

Chapter 1

Preliminaries

Let $\mathbb{F}_2^n$ be the n dimensional vector space defined over the finite field $\mathbb{F}_2$. In this thesis, we are interested in the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$. These functions can be viewed as vectorial Boolean functions. If $m = 1$, they can be viewed as Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. In Section 1.1, we give necessary notions related to Boolean functions. In Section 1.2, we study the notions related to vectorial Boolean functions. Then, we discuss Almost Perfect Nonlinear (APN) and Almost Bent (AB) functions in Section 1.3. In Section 1.4, we study the equivalence between vectorial Boolean functions. Finally, we discuss infinite families of APN and AB functions in Section 1.5.

1.1 Boolean functions

A *Boolean function* f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. In cryptography and coding theory, we normally use two different representations of n variable Boolean functions. The first representation is a *truth table*, that is,

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

The second representation is by means of a polynomial in $\mathbb{F}_2[x_1,\ldots,x_n]/(x_1^2+x_1, \ldots, x_n^2+x_n)$. This representation is called *Algebraic Normal Form* (ANF) :

$$f(x_1,\ldots,x_n) = \sum_{u\in\mathbb{F}_2^n} a_u \left(\prod_{j=1}^{n} x_j^{u_j}\right),$$

where $a_u \in \mathbb{F}_2$ and $x^u = \prod_{j=1}^n x_j^{u_j}$ is called a *monomial*. The *algebraic degree* of f, denoted by $deg(f)$, is the maximal value of $wt(u)$ such that $a_u \neq 0$, where $wt(u)$ is the number of its nonzero coordinates.

A Boolean function f is called *affine* if $deg(f) \leq 1$ and f is called *linear* if $deg(f) \leq 1$ and $f(0) = 0$. Boolean functions of algebraic degree 2 are called *quadratic* functions. Quadratic Boolean functions without linear and constant

terms are called *quadratic homogeneous* Boolean functions. Every quadratic homogeneous Boolean function can be described in terms of a quadratic form.
Here, a *quadratic form* over $\mathbb{F}_2$ is a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$ such that all of its nonzero terms have degree 2. We can describe the quadratic form as

$$f(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j, \ a_{i,j} \in \mathbb{F}_2.$$

We can associate with f an upper triangular $n \times n$ matrix A whose (i, j) entries are denoted by a_{ij} and whose diagonal entries are zero. The matrix A is called the *coefficient matrix* of f. The function f can be written as

$$f(x_1, \ldots, x_n) = (x_1, \ldots, x_n) Q (x_1, \ldots, x_n)^T,$$

here $(x_1, \ldots, x_n)$ is a row vector in $\mathbb{F}_2^n$.

Example 1.1. Let f be a quadratic homogeneous Boolean function from $\mathbb{F}_2^4$ to $\mathbb{F}_2$ defined by

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4.$$

The coefficient matrix of f is

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

The *support* of f is defined as the set $\{x \in \mathbb{F}_2^n \mid f(x) \neq 0\}$. The *Hamming weight* $wt(f)$ of a Boolean function f is the size of the support of f. A Boolean function f is called *balanced* if its truth table contains the same number of zeros and ones, that is, if $wt(f) = 2^{n-1}$. The *Hamming distance* $d(f, g)$ between two Boolean functions f and g is the size of the support of $f + g$.
The minimum Hamming distance between a Boolean function f and all affine Boolean functions is called the *nonlinearity* of f and denoted by $NL(f)$. The nonlinearity of a Boolean function measures the level of confusion created by the Boolean function in a cryptographic system. In order to provide confusion in a cryptographic system, the cryptographic functions must be at large Hamming distance to all affine functions. It means the nonlinearity of a Boolean function must be high enough to resist the linear attacks which were introduced by Matsui [2].
The *Walsh transform* $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ of a Boolean function f is defined as

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

where $a \cdot x = \sum_{i=1}^n a_i x_i$ is the usual inner product in $\mathbb{F}_2^n$. For any element $a \in \mathbb{F}_2^n$, the value $W_f(a)$ is called the *Walsh coefficient* of f and the multi set $\Lambda_f = \{* \, W_f(a) : a \in \mathbb{F}_2^n \, *\}$ is called the *Walsh spectrum* of f (the notion {*. . . *} indicates multisets).

Table 1.1: Truth table of $f(x_1, x_2) = x_1x_2$

x_1, x_2	$f(x_1, x_2)$
$0,0$	0
$0,1$	0
$1,0$	0
$1,1$	1

Example 1.2. Let $f : \mathbb{F}_2^2 \to \mathbb{F}_2$ be a Boolean function defined by

$$f(x_1, x_2) = x_1x_2.$$

Table 1.1 is the truth table of f. From the definition of the Walsh transform, we have
$W_f(0,0) = (-1)^{0+(0,0)\cdot(0,0)} + (-1)^{0+(0,0)\cdot(0,1)} + (-1)^{0+(0,0)\cdot(1,0)} + (-1)^{1+(0,0)\cdot(1,1)} = 2.$
Similarly, $W_f(0,1) = 2, W_f(1,0) = 2, W_f(1,1) = -2$. Then

$$\Lambda_f = \{* \, 2, 2, 2, -2 \, *\}.$$

Proposition 1.3. *For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$,*

$$W_f(0) = 2^n - 2wt(f).$$

Proof. From the definition of the Walsh transform, we have

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

Now, consider $a = 0$, we have

$$\begin{aligned} W_f(0) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} \\ &= \#\{x \mid f(x) = 0\} - \#\{x \mid f(x) = 1\} \\ &= (2^n - \#\{x \mid f(x) = 1\}) - \#\{x \mid f(x) = 1\} \\ &= 2^n - 2\#\{x \mid f(x) = 1\} \\ &= 2^n - 2wt(f). \end{aligned}$$

□

From Proposition 1.3, one can see that for any Boolean function f and any element $a \in \mathbb{F}_2^n$, we have

$$W_f(a) = 2^n - 2wt(f(x) + a \cdot x) = 2^n - 2d(f(x), a \cdot x).$$

Then

$$d(f(x), a \cdot x) = 2^{n-1} - \frac{1}{2} W_f(a).$$

Similarly,

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

and

$$d(f(x)+1, a \cdot x) = 2^{n-1} - \frac{1}{2} W_{f+1}(a) = 2^{n-1} + \frac{1}{2} W_f(a).$$

Now, we can define the relationship between the nonlinearity of a Boolean function f and the values of its Walsh transform. We have the following Proposition.

Proposition 1.4. *[8] Let f be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, the nonlinearity of f is*

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \mid W_f(a) \mid .$$

The following are well known facts about the Walsh transform of a Boolean function f.

Proposition 1.5. *For any $a \in \mathbb{F}_2^n$, we have*

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

Proof. Assume that $a = 0$, then $a \cdot x = 0$, so

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n} 1 = 2^n.$$

Assume that $a \neq 0$, consider the sets $H_1 = \{x \in \mathbb{F}_2^n \mid a \cdot x = 0\}$ and $H_2 = \{x \in \mathbb{F}_2^n \mid a \cdot x = 1\}$. Obviously, H_1 and H_2 form a partition of $\mathbb{F}_2^n$. Moreover, for any $x \in H_1$, we have $(-1)^{a \cdot x} = 1$, and for any $y \in H_2$, we have $(-1)^{a \cdot y} = -1$. Since the cardinalities of H_1, H_2 are the same, that is, 2^{n-1}, we have

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} = 2^{n-1} - 2^{n-1} = 0.$$

□

Theorem 1.6 (Parseval's Identity). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then*

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

Proof. From the definition of the Walsh transform, we know that

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

hence

$$\begin{aligned}\sum_{a\in\mathbb{F}_2^n} W_f^2(a) &= \sum_{a\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}\sum_{y\in\mathbb{F}_2^n}(-1)^{f(y)+a\cdot y}\right)\\ &= \sum_{x,y\in\mathbb{F}_2^n}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}_2^n}(-1)^{a\cdot(x+y)}\\ &= 2^{2n},\end{aligned}$$

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

The Parseval's identity enables us to derive upper and lower bounds on the maximum values attained by the Walsh transform of a Boolean function.

Corollary 1.7. *For any Boolean function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ and for any value of $a\in\mathbb{F}_2^n$, we have*

$$2^{n/2}\leq\max_{a\in\mathbb{F}_2^n}\mid W_f(a)\mid\leq 2^n$$

Proof. If

$$\max_{a\in\mathbb{F}_2^n}\mid W_f(a)\mid< 2^{\frac{n}{2}}$$

then

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

which contradicts the Theorem 1.6. Therefore, we must have

$$\max_{a\in\mathbb{F}_2^n}\mid W_f(a)\mid\geq 2^{n/2}.$$

On the other hand, we have

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

therefore, it is clear that the maximal value of $\mid W_f(a)\mid$ is 2^n. □

Parsevals's identity gives the upper bound on the nonlinearity of a Boolean function f. We have the following Proposition.

Proposition 1.8. *[8] Let f be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, then the nonlinearity of f is bounded by $2^{n-1}-2^{\frac{n}{2}-1}$, that is*

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

This bound is valid for every Boolean function and it is tight for every even value of n. For odd values of n, the challenge is to get Boolean functions having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. In 1972 [9], it was shown that for $n = 5$, the maximum nonlinearity of n variable Boolean function is 12. In 1980, the case for $n = 7$ is solved and it was shown that the maximum nonlinearity of n variable Boolean function is 56. In 1983, Patterson and Wiedemann [10] showed that one can construct a 15 variable Boolean function f with nonlinearity 16276. In 2006 [11], the 9 variable Boolean function having nonlinearity 241 was identified and later it was improved to 242 in 2010 [12]. Recently, Kai-Uwe Schmidt [13] solved a conjecture of Patterson and Wiedemann [10] on the nonlinearity of Boolean functions from 1983.

The functions which achieve the nonlinearity bound with equality are called *bent functions* [14]. Bent functions exist with n even because $2^{n-1} - 2^{\frac{n}{2}-1}$ must be an integer. In other words, a function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called *bent* if and only if $\mid W_f(a) \mid = 2^{n/2}$, for all $a \in \mathbb{F}_2^n$.

Example 1.9. In Example 1.2, we have the Boolean function f from $\mathbb{F}_2^2$ to $\mathbb{F}_2$ defined as

$$f(x_1, x_2) = x_1x_2.$$

Note that

$$\Lambda_f = \{* \, 2, 2, 2, -2 \, *\},$$

hence the function f is a bent function.

The *derivative* of a Boolean function f with respect to $a \in \mathbb{F}_2^n$ is defined as

$$D_a f(x) = f(x + a) + f(x).$$

The derivative of a Boolean function may be used to determine many cryptographic properties, for instance, differential attack resistance [1]. Other cryptographic properties determined by using the derivative are the strict avalanche criteria (SAC) [15] and propagation criterion (PC) [16]. SAC and PC evaluates some kind of diffusion of Boolean functions.

If the derivative of Boolean function $D_a f(x)$ is constant at some point $a \in \mathbb{F}_2^n$, then a is called a *linear structure* of f. The set of all linear structures of f is a subspace of $\mathbb{F}_2^n$ [17]. Nonzero linear structures weakens the cryptographic property of Boolean functions [18].

Bent functions can also be described by using the derivative. We have the following characterization of bent functions.

Theorem 1.10. *[8] Let f be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The following statements are equivalent:*

(i) f is bent.

(ii) $W_f(a) = \pm 2^{n/2}$ *for all* $a \in \mathbb{F}_2^n$.

(iii) $D_a f(x) = f(x+a) + f(x)$ *is balanced for any* $a \neq 0$.

The function f is balanced if and only if $W_f(0) = 0$. From the definition of bent function, the Walsh coefficients of bent function are $\pm 2^{n/2}$, for all $a \in \mathbb{F}_2^n$. Therefore, bent functions are not balanced. In any cryptographic systems, we need Boolean functions which satisfy certain cryptographic properties, for instance, nonlinearity and balancedness. The bent functions are highly nonlinear but they are not balanced. So, we cannot use them directly in any cryptographic system.
A Boolean function f in n variables is called *plateaued* (or t-plateaued) if

$$W_f(a) \in \{0, \pm 2^{\frac{n+t}{2}}\}$$

for some fixed t, $0 \leq t \leq n$ with $n + t$ even and for any $a \in \mathbb{F}_2^n$. Plateaued functions include three significant classes of Boolean functions: *bent* functions, *near-bent* functions and *semi-bent* functions. Bent functions are 0-plateaued functions. Semi-bent functions are 1-plateaued functions. Near-bent functions are 2-plateaued functions.

1.2 Vectorial Boolean functions

Let n and m be positive integers. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is often called an (n, m) function or *vectorial Boolean function*. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, then the Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2, i = 1, \ldots, m$ defined by

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

are called *coordinate functions* of F. The *component functions* of F are $c \cdot F$, $c \in \mathbb{F}_2^m$. The component functions of F are the nonzero linear combinations of the coordinate functions of F.
The notion of the algebraic normal form of Boolean functions can be extended to vectorial Boolean functions. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Then, F can be uniquely represented as

$$F(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \left(\prod_{j=1}^{n} x_j^{u_j} \right),$$

where $a_u \in \mathbb{F}_2^m$. This representation is called *algebraic normal form* (ANF) of F. The algebraic degree of F is equal to the maximum algebraic degree of the coordinate functions of F, see [19].
If $n = m$, there is another representation of the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. If we

identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, then the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$:

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

In this representation, the component functions of F can be expressed as $\mathrm{Tr}_1^n(\alpha F)$, where $\alpha \in \mathbb{F}_{2^n}$, $\alpha \neq 0$ and $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. For any integer k, $0 \leq k \leq 2^n - 1$, its binary expansion is $\sum_{s=0}^{n-1} 2^s k_s,\ k_s \in \{0, 1\}$. The number $w_2(k)$ of nonzero coefficients k_s is called the 2-weight of k. We have the following proposition about the algebraic degree of F.

Proposition 1.11. *[20] Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as*

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

The algebraic degree of F is equal to the maximum 2-weight of the exponent i of the polynomial $F(x)$ such that $a_i \neq 0$.

A linearized polynomial F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is defined as

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

In cryptography, the balancedness of a vectorial Boolean function plays an important role. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called *balanced* if it takes every value of $\mathbb{F}_2^m$ equal number i.e, 2^{n-m} of times. Obviously, the balanced functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ are the permutations of $\mathbb{F}_2^n$. It is proved in [19] that a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is balanced if and only if all nonzero linear combinations of the coordinate functions of F are balanced, that is, $c \cdot F$ is balanced for every nonzero $c \in \mathbb{F}_2^n$. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. The function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ defined by

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

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

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

is called the *Walsh spectrum* of F. We define the *extended Walsh spectrum* of F as

$$\Lambda(F) = \{* \ \mid W_F(a, b) \mid : \ a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m,\ b \neq 0 \ *\}.$$

Nyberg [21] generalized the notion of nonlinearity of Boolean functions to the notion of nonlinearity of functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. This was further studied by

Chabaud and Vaudenay [22]. The *nonlinearity* $NL(F)$ of a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is the minimum nonlinearity of all the component functions $b \cdot F(x)$ with $b \neq 0$ of F.

In other words, $NL(F)$ equals the minimum Hamming distance between all component functions of F and all affine Boolean functions in n variables. The linear cryptanalysis, introduced by Matsui [2], is successful on those functions which have small value of nonlinearity.

From the equality relating the nonlinearity of a Boolean function with maximum absolute value of the Walsh transform, we obtain the nonlinearity of the vectorial Boolean functions.

Proposition 1.12. *[19] Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, then the nonlinearity of F is*

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m \\ b \neq 0}} \mid W_F(a,b) \mid .$$

We have discussed that the nonlinearity bound is valid for every n variable Boolean function. It is also valid for every vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Proposition 1.13. *[19] Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, the nonlinearity of F is bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$, that is*

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

This bound is called *universal bound* and the functions which achieve this bound have optimal nonlinearity and they are called *vectorial bent functions*.

Theorem 1.14. *[19] Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. The following statements are equivalent:*

(i) *F is a vectorial bent function.*

(ii) *For any nonzero $c \in \mathbb{F}_2^m$, the Boolean function $c \cdot F$ is bent.*

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

(iv) $\Lambda_F = \{\pm 2^{n/2}\}$.

A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called *perfect nonlinear (PN)* if for any nonzero $a \in \mathbb{F}_2^n$, the function $F(x+a) + F(x)$ is balanced. It follows from Theorem 1.14 that a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is a vectorial bent function if and only if it is a perfect nonlinear function.

Nyberg [21] gave a necessary condition on the existence of such a bent (perfect nonlinear) function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Theorem 1.15 (Nyberg Bound). *Let F be a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, then $m \leq n/2$.*

Since vectorial bent functions do not exist for $m > \frac{n}{2}$, it is a natural question whether a better upper bound than the universal bound can be found. Such a bound is given by Sidelnikov in the context of sequences and is further studied by Chabaud and Vaudenay [22] in the context of power functions. We call this bound the Sidelnikov-Chabaud-Vaudenay bound.

Theorem 1.16. *[19, 22] Let n and m are positive integers with $m \geq n-1$. Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Then*

$$NL(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n) - 2^{4n}}{(2^m-1)2^{2n}}}.$$

Proof. We know that

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m \\ b \neq 0}} \mid W_F(a,b) \mid .$$

From Theorem 4 [22], we have

$$\max_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m \\ b \neq 0}} (W_F(a,b))^2 \geq \frac{\sum_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m \\ b \neq 0}} (W_F(a,b))^4}{\sum_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m \\ b \neq 0}} (W_F(a,b))^2}. \tag{1.1}$$

Theorem 1.6 states that, for every $b \in \mathbb{F}_2^m$, we have

$$\sum_{a \in \mathbb{F}_2^n} (W_F(a,b))^2 = 2^{2n}. \tag{1.2}$$

Now, we consider the case

$$\sum_{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m} (W_F(a,b))^4 = \sum_{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m} \left(\sum_{x,y,z,w \in \mathbb{F}_2^n} (-1)^{a \cdot (x+y+z+w) + b \cdot (F(x)+F(y)+F(z)+F(w))} \right), \tag{1.3}$$

hence,

$$\sum_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m} (W_F(a,b))^4 = \sum_{x,y,z,w \in \mathbb{F}_2^n} \left[\sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot (x+y+z+w)} \right] \left[\sum_{b \in \mathbb{F}_2^m} (-1)^{b \cdot (F(x)+F(y)+F(z)+F(w))} \right]. \tag{1.4}$$

By using Proposition 1.5, we have

$$\sum_{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m} (W_F(a,b))^4 = 2^{n+m}\Gamma,$$

where

$$\Gamma = \#\left\{ (x,y,z,w) \in (\mathbb{F}_2^n)^4 \mid \left\{ \begin{array}{c} x+y+z+w=0 \\ F(x)+F(y)+F(z)+F(w)=0 \end{array} \right. \right\}.$$

This implies that

$$\Gamma = \#\left\{ (x,y,z) \in (\mathbb{F}_2^n)^3 \mid F(x)+F(y)+F(z)+F(x+y+z)=0 \right\}.$$

So,

$$\sum_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^m} (W_F(a,b))^4 \geq 2^{n+m} \left(\#\left\{ (x,y,z) \in (\mathbb{F}_2^n)^3 \mid x=y \text{ or } x=z \text{ or } y=z \right\} \right).$$

Clearly, we have
$\#\left\{ (x,y,z) \in (\mathbb{F}_2^n)^3 \mid x=y \text{ or } x=z \text{ or } y=z \right\} = 3(\#\{(x,x,y) \mid x,y \in \mathbb{F}_2^n\}) - 2(\#\{(x,x,x) \mid x \in \mathbb{F}_2^n\}) = 3\cdot 2^{2n} - 2\cdot 2^n$.
Hence,

$$\sum_{\substack{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^m \\ b\neq 0}} (W_F(a,b))^4 \geq 3\cdot 2^{2n} - 2\cdot 2^n - 2^{4n}, \tag{1.5}$$

we have used $W_F(a,0) = 2^n$, if $a=0$ and $W_F(a,0)=0$, if $a \neq 0$.
Now, we substitute equations (1.2) and (1.5) into equation (1.1) to get

$$\max_{\substack{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^m \\ b\neq 0}} (W_F(a,b))^2 \geq \frac{2^{n+m}(3\cdot 2^{2n} - 2\cdot 2^n) - 2^{4n}}{(2^m-1)2^{2n}},$$

which implies that

$$NL(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{n+m}(3\cdot 2^{2n} - 2\cdot 2^n) - 2^{4n}}{(2^m-1)2^{2n}}}.$$

□

The condition $m \geq n-1$ in Theorem 1.16 makes the expression located under the square root non-negative. Note that for $m = n-1$, the bound of the Theorem 1.16 coincides with the universal bound. For $m \geq n$, it strictly improves the universal bound and it is tight only if $n = m$ with n odd. We will consider this case in detail in the Section 1.3.

1.3 APN and AB functions

We have observed that the universal bound is attainable for functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with n even and $m \leq n/2$. The functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ which achieve the bound of Theorem 1.16 with equality, that is,

$$NL(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$$

are called *almost bent* (AB) function. Obviously, AB functions exist for n odd only.

Biham and Shamir [1] has proposed differential cryptanalysis on the DES block cipher. Differential cryptanalysis studies how the differences of input affect the resultant differences at the output. The following functions provide the best resistance to differential cryptanalysis.

Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let $\delta_F(a,b)$ denote the number of solutions of the equation $F(x+a)+F(x)=b$ for any element $a,b \in \mathbb{F}_2^n$, that is,

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

and we call the set

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

the *differential spectrum* of the function F. We can also describe the differential spectrum of F with the $(2^n-1)\times 2^n$ matrix

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

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

For any function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, we have

$$\max_{\substack{a,\ b\in\mathbb{F}_2^n,\\ a\neq 0}} \delta_F(a,b) \geq 2.$$

Indeed, for any $a,b \in \mathbb{F}_2^n$, the number $\delta_F(a,b)$ is even since if x_0 is the solution of $F(x_0+a)+F(x_0)=b$, then x_0+a is a solution too. If $\delta_F(a,b)=2$, the function F is called an *almost perfect nonlinear* (APN) function.

APN functions provide the best resistance to differential attacks. If the value of $\delta_F(a,b)$ is small then the resistance of the function F, when used as an S-box in a cipher to the differential attack is high. We have the following proposition.

Proposition 1.17. *A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is APN if and only if one of the following conditions are satisfied:*

(i) $\Delta_F = \{0,2\}$.

(ii) For every $a,\ b \in \mathbb{F}_2^n$ with $a \neq 0$, the system

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

has 0 *or* 2 *solutions.*

(iii) For any $a \in \mathbb{F}_2^n, a \neq 0$, the mapping $F(x+a)+F(x)$ is a two-to-one mapping.

Proof. The statements of the above proposition are obvious from the definition of APN functions. □

The APN property is related to 2-dimensional affine subspaces of $\mathbb{F}_2^n$. Let $A(\mathbb{F}_2^n)$ be the set of all 2-dimensional affine subspaces in $\mathbb{F}_2^n$. It means that $A(\mathbb{F}_2^n)$ consists of the sets $\{t,\ u,\ v,\ w\}$ of four pairwise different vectors with $t+u+v+w=0$.

Theorem 1.18. *[23, 24] Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then F is APN if and only if for all $\{t,\ u,\ v,\ w\} \in A(\mathbb{F}_2^n)$, it holds that*

$$F(t)+F(u)+F(v)+F(w) \neq 0.$$

According to Chabaud-Vaudenay proof of the Sidelnikov-Chabaud-Vaudenay bound, we have the following proposition.

Proposition 1.19. *[22] Let F be an AB function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, then F is an APN function.*

Remark 1.20. The converse of the Proposition 1.19 is not true. Not every APN function is an AB function. We have APN functions for odd values of n but they are not AB functions. We will dicuss them in Section 1.5. There are certain APN functions which are also AB functions.

We have the following proposition.

Proposition 1.21. *[20] Let F be a quadratic APN function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with n odd, then F is an AB function.*

A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is called *crooked* function if the sets $\{F(x)+F(x+a) \mid x \in \mathbb{F}_2^n\}$ are (affine) hyperplanes for any nonzero $a \in \mathbb{F}_2^n$.
Now, we discuss the equivalence of vectorial Boolean functions.

1.4 Equivalence of functions

Two vectorial Boolean functions are said to be equivalent if one vectorial Boolean function can be obtained from the other vectorial Boolean function under some simple transformation which does not change APN and AB properties.
There are mainly three notions of equivalence: affine equivalence, extented affine equivalence (EA) and Carlet-Charpin-Zinoviev (CCZ) equivalence respectively.
Let F and $F^{'}$ be two functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. F and $F^{'}$ are called *affine equivalent (or linear equivalent)* if $F^{'} = A_1 \circ F \circ A_2$, where A_1 and A_2 are affine (respectively linear) permutations of $\mathbb{F}_2^n$.
The functions F and $F^{'}$ are called *extended affine equivalent* (EA-equivalent) if $F^{'} = A_1 \circ F \circ A_2 + A$, where A_1 and A_2 are affine permutations of $\mathbb{F}_2^n$ and A is

any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ which is affine or constant.
Functions F and $F^{'}$ are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if their graphs are affine equivalent, that means there exists an affine permutation L of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $L(G_F) = G_{F^{'}}$, where $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$ and $G_{F^{'}} = \{(x, F^{'}(x)) \mid x \in \mathbb{F}_2^n\}$. Now, we discuss CCZ-equivalence in detail.
Let F and $F^{'}$ be vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ which are CCZ-equivalent. Then there exist a linear permutation L from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to $\mathbb{F}_2^n \times \mathbb{F}_2^n$ of the form $L = (L_1, L_2)$, where L_1 and L_2 are two linear functions from $\mathbb{F}_2^n \times \mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $L(G_F) = G_{F^{'}}$. We observe that

$$L(G_F) = L(x, F(x)) = (L_1(x, F(x)), L_2(x, F(x))).$$

We define two functions F_1 and F_2 as

$$F_1(x) = L_1(x, F(x)) \tag{1.6}$$

and

$$F_2(x) = L_2(x, F(x)). \tag{1.7}$$

So, we can write

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

For a given linear permutation of L, the set $L(G_F)$ is the graph of a function if and only if the function F_1 is a permutation. Define $F^{'} = F_2 \circ F_1^{-1}$, we have $L(G_F) = G_{F^{'}}$.
The equivalence relations defined above are related to each other. Linear equivalence is a particular case of affine equivalence and affine equivalence is a particular case of EA-equivalence.
Let F and $F^{'}$ be the EA-equivalent functions then Δ_F and Λ_F is equal to $\Delta_{F^{'}}$ and $\Lambda_{F^{'}}$ respectively. If F is a permutation then Δ_F is equal to $\Delta_{F^{-1}}$ and Λ_F is equal to $\Lambda_{F^{-1}}$.
This means if we have an APN function F (respectively AB function) and $F^{'}$ is EA-equivalent to either F or F^{-1} (if F is a permutation), then $F^{'}$ is also an APN function (respectively AB function). Carlet, Charpin and Zinoviev [20] showed that EA-equivalence is a particular case of CCZ-equivalence and any permutation F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is CCZ-equivalent to its inverse F^{-1} from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.
The algebraic degree of a function F (if it is not affine) from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is EA-invariant but, in general, it is not preserved by CCZ-equivalence. The composition by the inverse of F_1 modifies in general the algebraic degree of $F^{'}$ except for the case when $L_1(x, y)$ depends only on x. This corresponds to EA-equivalence of F and $F^{'}$.
It was proven in [25] that CCZ-equivalence is more general than EA-equivalence. However, there are some particular cases of functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ for

which CCZ-equivalence can be reduced to EA-equivalence. For instance, CCZ-equivalence coincides with EA-equivalence for all Boolean functions [26] and vectorial bent functions. CCZ-equivalence also coincides with EA-equivalence for two quadratic APN functions (conjectured by Edel, proven by Yoshiara [27]). There are some properties of vectorial Boolean functions which are invariant under CCZ-equivalence, for instance, the Walsh spectrum.

Proposition 1.22. *[25] Let F and $F^{'}$ be the CCZ-equivalent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then $\Lambda_F = \Lambda_{F'}$.*

Proof. Let F and $F^{'}$ be CCZ-equivalent functions, then $F^{'} = F_2 \circ F_1^{-1}$ for certain linear permutation $L = (L_1, L_2)$, where F_1, F_2 are defined by equation (1.6) and (1.7). For any $a,\ b \in \mathbb{F}_2^n,\ b \neq 0$, we have

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

so,

$$W_F(a,b) = W_{F'}(L^{-1*}(a,b))$$

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

We discussed in Section 1.2 that the nonlinearity is directly related with the Walsh spectrum. It follows that the nonlinearity is CCZ-invariant as well. For the differential spectrum, we have a similar observation.

Proposition 1.23. *[25] Let F and $F^{'}$ be CCZ-equivalent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then*

$$\Delta_{F'} = \Delta_F.$$

Proof. Let F and $F^{'}$ be the CCZ-equivalent functions with $L(G_F) = G_{F'}$. For any $a, b \in \mathbb{F}_2^n,\ b \neq 0$, we have

$$\begin{aligned} \delta_{F'}(a,b) &=\mid \{F^{'}(x) + F^{'}(x+a) = b\} \mid \\ &=\mid \{(x,F^{'}(x)) + (y,F^{'}(y)) = (a,b)\} \mid \\ &=\mid \{L(x,F(x)) + L(y,F(y)) = (a,b)\} \mid \\ &=\mid \{(x,F(x)) + (y,F(y)) = L^{-1}(a,b)\} \mid \\ &= \delta_F(L^{-1}(a,b)). \end{aligned}$$

Since L is a permutation, L^{-1} is a permutation as well and the differential spectrum of F and $F^{'}$ is equal up to a permutation. Hence, $\Delta_{F'} = \Delta_F$. □

Since the Walsh spectrum and the differential spectrum are CCZ-invariants, the resistance of a function to linear and differential attacks is also CCZ-invariant. In order to check the CCZ-equivalence between two arbitrary functions, a nice connection with coding theory is given in [28]. Note that codes are just linear subspaces in $\mathbb{F}_2^v$. We will discuss about codes in detail in Section 2.1.
Two functions F and H from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ are CCZ-equivalent if and only if the binary linear codes generated by the row space of the matrices

$$M_F = \begin{bmatrix} 1 \\ x \\ F(x) \end{bmatrix}_{(2n+1)\times 2^n}, \quad M_H = \begin{bmatrix} 1 \\ x \\ H(x) \end{bmatrix}_{(2n+1)\times 2^n} \quad x \in \mathbb{F}_2^n$$

are equivalent over $\mathbb{F}_2$. Here, two binary linear codes C_1 and C_2 (subspaces in $\mathbb{F}_2^v$) are equivalent if there is a bijective linear mapping L from $\mathbb{F}_2^v$ to $\mathbb{F}_2^v$ and a permutation π of the integers $\{1, 2, \dots, v\}$ such that for all $x \in \mathbb{F}_2^v$, the following result holds:

$$L(x_{\pi(1)}, \dots, x_{\pi(v)}) \in C_1 \text{ if and only if } (x_1, \dots, x_v) \in C_2.$$

In general, it seems difficult to establish CCZ-equivalence between two functions F and H from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. However, there are some CCZ-invariant parameters that can be proved to be different for two functions F and H. Before introducing these CCZ-invariant parameters, we need to introduce the group ring notation. Let $\mathbb{F}$ be an arbitrary field and $(G, +)$ be an additively written abelian group. The group algebra $\mathbb{F}[G]$ consist of all formal sums

$$\sum_{g \in G} a_g g, \; a_g \in \mathbb{F}.$$

We define a component wise addition as

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

and a multiplication

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

With these operations and a scalar multiplication

$$\lambda \sum_{g \in G} a_g g = \sum_{g \in G} (\lambda a_g) g,$$

$\mathbb{F}[G]$ becomes an algebra, the so called *group algebra*. The dimension of this algebra as a $\mathbb{F}$ vector space is $\mid G \mid$.

Let $\kappa = \mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^m]$ be the so called group algebra of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ defined over $\mathbb{F}_2$, consisting of the formal sums

$$\sum_{k \in \mathbb{F}_2^n \times \mathbb{F}_2^m} a_k k, \ a_k \in \mathbb{F}_2.$$

If T is a subset of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, it can be identified with the element $\sum_{t \in T} t$ of κ. The dimension of the ideal of κ generated by the graph

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

of F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called the Γ-*rank* of F. The dimension of the ideal of κ generated by the set

$$D_F = \{(a, F(x) + F(x+a)) : a, x \in \mathbb{F}_2^n, \ a \neq 0\}$$

of F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called the Δ-*rank* of F.

There are certain design or incidence structures associated with APN functions which can be used to distinguish two APN functions. We take the following definition from [29].

An *incidence structure* is a triple $D = (p, B, I)$, where p is a set of elements called *points* and B is a set of elements called *blocks (lines)* and $I \subseteq (p \times B)$ is a binary relation which is called *incidence relation*.

Any incidence structure is associated with an *incidence matrix*: rows and columns of the incidence matrix are indexed by points and blocks. The (p, B) entry is 1 if a point from p is incident with the block from B, otherwise 0.

Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with $n = m$. We define two incidence structures (designs) on the point set $\mathbb{F}_2^n \times \mathbb{F}_2^n$. In the first case, the blocks are the sets

$$G_F + (u, v) = \{(x + u, F(x) + v) : x \ \in \mathbb{F}_2^n\}$$

for $u, v \in \mathbb{F}_2^n$, i.e. the translates of G_F. We call this design the development of G_F and denote it by $dev(G_F)$. Similarly, the design whose blocks are the translates

$$D_F + (u, v) = \{(a + u, (F(x) + F(x+a)) + v) : \ a, \ x \in \mathbb{F}_2^n, \ a \neq 0\}$$

of D_F is called the development of D_F and denoted by $dev(D_F)$. The Γ-*rank* defined earlier is nothing but the $\mathbb{F}_2$ rank of the incidence matrix of $dev(G_F)$. Similarly, the Δ-*rank* is the $\mathbb{F}_2$ rank of the incidence matrix of $dev(D_F)$.

It is not difficult to determine the automorphism groups of these designs for small values of n with the help of MAGMA [4]. There is another group associated with the designs $dev(G_F)$ (respectively $dev(D_F)$): The sets G_F (respectively D_F) are subsets of $\mathbb{F}_2^{2n}$. Then, there may exist automorphisms φ of $\mathbb{F}_2^{2n}$ such that $\varphi(G_F) = G_F + (u, v)$ (respectively $\varphi(D_F) = D_F + (u, v)$) for some $u, v \in \mathbb{F}_2^n$. These automorphisms form a group contained in the automorphism group of

the designs $dev(G_F)$ (respectively $dev(D_F)$). We call the group of these automorphisms the so called *multiplier group* $M(G_F)$ (respectively $M(D_F)$) of $dev(G_F)$ (respectively $dev(D_F)$).
It is shown in [30] that $M(G_F)$ is much easier to compute with MAGMA than the full automorphism group of the design $dev(G_F)$. $M(G_F)$ is the automorphism group of the code generated by the row space of M_F. We have the following Theorem.

Theorem 1.24. *Let F_1 and F_2 be the CCZ-equivalent APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then Δ-rank, Γ-rank, $Aut(dev(D_{F_1})), Aut(dev(G_{F_1}))$ and $Aut(M(G_{F_1}))$ of the function F_1 are the same as Δ-rank, Γ-rank, $Aut(dev(D_{F_2})), Aut(dev(G_{F_2}))$ and $Aut(M(G_{F_2}))$ of the function F_2 respectively, where Aut is the automorphism group.*

1.5 Infinite families of AB and APN functions

The first classes of functions that have been checked for almost bentness and almost perfect nonlinearity were power functions $F(x) = x^d$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ (which are also called monomials). The checking of AB and APN properties of an arbitrary polynomial is more difficult but it is relatively easy in case of power function. Assume that we have a power function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by

$$F(x) = x^d,$$

then F is APN if and only if the mapping

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

is a two-to-one. In fact, since for any $a \in \mathbb{F}_{2^n},\ a \neq 0$

$$D_aF(x) = F(x+a) + F(x) = (x+a)^d + x^d = a^d\left(\left(\frac{x}{a}+1\right)^d + \left(\frac{x}{a}\right)^d\right) = a^d D_1F\left(\frac{x}{a}\right),$$

$D_aF(x)$ is a two-to-one mapping if and only if $D_1F(x)$ is a two-to-one. The function

$$F(x) = x^d$$

is AB if and only if

$$W_F(a,b) \in \{0, \pm 2^{\frac{n+1}{2}}\}$$

for $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}, b \neq 0$. Table 1.2 gives a complete list, up to CCZ-equivalence, of known power mappings which are APN and Table 1.3 gives a complete list, up to CCZ-equivalence, of known power mappings which are AB.

Gold [31] considered the power functions with the exponent $d = 2^i + 1$ in the context of maximum linear sequences. The proof of the APN and AB properties of the Gold functions is not difficult. We need the following lemma to prove the APN property of Gold functions.

Table 1.2: Known APN power functions x^d on $\mathbb{F}_{2^n}$

Functions	Exponent d	Conditions	References
Gold	$2^i + 1$	$gcd(i,n) = 1$	[31, 32]
Kasami	$2^{2i} - 2^i + 1$	$gcd(i,n) = 1$	[33, 34]
Welch	$2^k + 3$	$n = 2k + 1$	[35]
Niho	$2^k + 2^{\frac{k}{2}} - 1$, k even $2^k + 2^{\frac{3k+1}{2}} - 1$, k odd	$n = 2k + 1$	[36]
Inverse	$2^{2k} - 1$	$n = 2k + 1$	[32, 37]
Dobbertin	$2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$	$n = 5k$	[38]

Lemma 1.25. *[39] For any positive integers n and m, we have*

- $gcd(2^n - 1, 2^m - 1) = 2^{gcd(n,m)} - 1.$
- $gcd(2^n - 1, 2^m + 1) = \begin{cases} 1 & \textit{if} \;\; n/gcd(n,m) \textit{ is odd.} \\ 2^{gcd(n,m)} + 1 & \textit{if} \;\; n/gcd(n,m) \textit{ is even.} \end{cases}$

Theorem 1.26. *Let i and n be positive integers satisfying $gcd(i,n) = 1$. The function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x) = x^{2^i+1}$ is APN. If n is odd, then F is a permutation and if n is even, then F is a three-to-one mapping on $\mathbb{F}_{2^n}^*$.*

Proof. As, $F(x)$ is a quadratic function, then $F(x + a) + F(x) + F(a)$ is a linear function in x whose kernel has the same size as any of its translates, such as the solution set of $F(x + a) + F(x) = b$ in $\mathbb{F}_{2^n}$, for any $b \in \mathbb{F}_{2^n}$. We show that for every a, $b \in \mathbb{F}_{2^n}$, $a \neq 0$, the equation

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

has at most two solutions by counting the number of solutions of the equation

$$F(x + a) + F(x) + F(a) = 0.$$

This gives

$$F(x + a) + F(x) + F(a) = x^{2^i} a + a^{2^i} x.$$

We have

$$\mid \{x : F(x + a) + F(x) + F(a) = 0\} \mid = \mid \{x : x^{2^i} a = a^{2^i} x\} \mid$$

$$= \mid \{0\} \cup \{x : (x/a)^{2^i - 1} = 1\} \mid .$$

From Lemma 1.25, it follows that $gcd(2^n - 1, 2^i - 1) = 1$. Therefore, $\mid \{x : (x/a)^{2^i-1} = 1\} \mid = 1$ and F is an APN function. On the other hand, from Lemma 1.25, it follows that $gcd(2^i + 1, 2^n - 1) = 1$ if n is odd and $gcd(2^i + 1, 2^n - 1)$ $= 3$ if n is even. We see that F is a permutation if n is odd and F is a three-to-one mapping on $\mathbb{F}_{2^n}^*$ if n is even. □

Table 1.3: Known AB power functions x^d on $\mathbb{F}_{2^n}$, n odd

Functions	Exponent d	Conditions	References
Gold	2^i+1	$gcd(i,n)=1$	[31, 32]
Kasami	$2^{2i}-2^i+1$	$gcd(i,n)=1$	[33, 34]
Welch	2^k+3	$n=2k+1$	[35]
Niho	$2^k+2^{\frac{k}{2}}-1$, k even $2^k+2^{\frac{3k+1}{2}}-1$, k odd	$n=2k+1$	[36]

Theorem 1.27. *[19] Let i and n be positive integers satisfying $gcd(i,n)=1$ and n is odd. Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by*

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

Then

$$W_F(a,b)\in\{0,\pm 2^{\frac{n+1}{2}}\},\ \ a,b\in\mathbb{F}_{2^n},\ b\neq 0.$$

Proof. From Theorem 1.26, we know that if n is odd, then F is a permutation. We only need to consider $W_F(a,1)$, $a\in\mathbb{F}_{2^n}$, to determine the Walsh Spectrum of F. We have

$$W_F(a,1)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(x^{2^i+1})+Tr_1^n(ax)}.$$

Squaring both sides of the above equation, we get

$$\begin{aligned}
W_F^2(a,1)&=\sum_{x,y\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(x^{2^i+1})+Tr_1^n(y^{2^i+1})+Tr_1^n(a(x+y))}\\
&=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(ay)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(x^{2^i+1})+Tr_1^n((x+y)^{2^i+1})}\\
&=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(y^{2^i+1})+Tr_1^n(ay)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(x^{2^i}y+xy^{2^i})}\\
&=\sum_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(y^{2^i+1})+Tr_1^n(ay)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n((y^{2^i}+y^{2^{-i}})x)}\\
&=2^m\sum_{y\in\mathbb{F}_2}(-1)^{Tr_1^n(y^{2^i+1})+Tr_1^n(ay)}.
\end{aligned}$$

Since $y^{2^i}+y^{2^{-i}}=0$ means $y^{2^{2i}-1}=1$ and $y^{2^{gcd(2i,n)}}=1$, we have $y\in\mathbb{F}_2$. The function y^{2^i+1} is linear on $\mathbb{F}_2$, hence

$$Tr_1^n(y^{2^i+1}+ay)=Tr_1^n(y(1+a))=yTr_1^n(1+a)).$$

Since n is odd, it follows that

$$W_F^2(a,1)=\begin{cases}2^{n+1} & \text{if } \ Tr_1^n(1+a)=0\\ 0 & \text{otherwise}\end{cases}=\begin{cases}2^{n+1} & \text{if } \ Tr_1^n(a)=1\\ 0 & \text{otherwise}\end{cases}$$

Table 1.4: Two APN binomials

Dimension n	Polynomial	Conditions
10	$x^3 + \beta x^{36}$	$\beta \in \{\omega \mathbb{F}_{2^5}\} \cup \{\omega^2 \mathbb{F}_{2^5}\}$ where $\omega \in \mathbb{F}_{2^{10}}$ has order 3.
12	$x^3 + \beta x^{528}$	The order of β is a multiple of 45 and divides 585 or the order of β is a multiple of 7 and divides 273

This completes the proof that if n is odd then $W_F(a,b) = \{0, \pm 2^{\frac{n+1}{2}}\}$. □

Remark 1.28. It is difficult to determine the Walsh spectrum of $F(x) = x^{2^i+1}$ with $gcd(i,n) > 1$. Budaghyan and Pott [40] investigate the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, where

$$W_F(a,b) \in \{0, \pm 2^{\frac{n+s}{2}}\}, \;\; a, b \in \mathbb{F}_{2^n}, \; b \neq 0$$

and $gcd(i,n) = s$.

The power functions

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

were first studied in the context of coding theory. In 1971, Kasami showed that when $gcd(i,n) = 1$ and n is odd, the Walsh spectrum of F is $\{0, \pm 2^{\frac{n+1}{2}}\}$ (this is the result of Welch (1969) but he never published it). If n is odd and $gcd(i,n) = 1$, the function F is AB function and therefore F is also APN function. For n even and $gcd(i,n) = 1$, Janwa and Wilson [34] proved the APN property of F by using methods of algebraic geometry.

Note that the Gold and Kasami power functions in Table 1.2 are the only known exceptional APN functions [41]. Exceptional APN functions mean that the functions are APN for infinite many values of n.

Welch conjectured that the power function

$$F(x) = x^{2^{(n-1)/2}+3}$$

is an AB function in the context of maximum length sequences. In 1968, Golomb [42] mentioned this conjecture in his paper. In 2000, Canteaut, Charpin and Dobbertin [43] proved this conjecture .

In 1972, Niho conjectured in his PhD thesis that the power function

$$F(x) = x^{2^{2i}+2^i-1},$$

where $4i + 1 \equiv 0 \bmod n$, is AB. In 1999, Dobbertin [36] proved the APN property of Niho function. Note that the proofs of the APN property of Kasami, Welch and Niho functions are complicated and very technical.

In 1999, Canteaut and Dobbertin found the APN power function

$$F(x) = x^{2^{4k}+2^{3k}+2^{2k}+2^k-1}$$

with $n = 5k$. In 2000, Dobbertin proved its APN property by using multivariate equation method. It is proved in the paper [44] that the Dobbertin function is not an AB function.
Let F be the inverse mapping on $\mathbb{F}_{2^n}$, i.e.

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

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

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

If we square the equation $x^2 + x + 1 = 0$ and substitute $x^2 = x + 1$ in it, then we have the equation $x^4 = x$, which is only satisfied for $x \in \mathbb{F}_{2^2}$. The inverse function is an APN function for odd values of n and has the differential spectrum $\Delta_F = \{0,2,4\}$ for even values of n. This means the inverse function F opposes a good (but not optimal) resistance against differential cryptanalysis. The inverse APN function is not AB. It has the algebraic degree $n-1$ while the algebraic degree of any AB function is not greater than $(n+1)/2$, see [20]. The Walsh coefficients of the inverse function were determined by Lachaud and Wolfmann [45]. The nonlinearity of the inverse function is greater than or equal to $2^{n-1} - 2^{\frac{n}{2}}$, when n is even [32].

Remark 1.29. It is still an open problem to find functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with n even having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n}{2}}$.

It was conjectured by Dobbertin that the list of APN functions given in Table 1.2 is complete. In 2006, two examples of APN functions on $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{12}}$ were found [54] which disprove the Dobbertin conjecture. These new APN functions are binomial and it has been shown that they are not equivalent to the known APN functions. Around the same time, John Dillon [55] gave several new APN functions on $\mathbb{F}_{2^6}$. He also showed that his examples are pairwise inequivalent and also inequivalent to the known power functions. So in 2006, the examples in Table 1.4 for $n = 10$ and 12 and Table 1.5 with $n = 6$ were known. In Table 1.5, α is the root of the irreducible polynomial $x^6 + x^4 + x^3 + x + 1$.
Since these "sporadic" examples have been found, many researchers tried to find infinite families of APN functions. A first infinite family generalized the example in dimension 12 listed in Table 1.4. Some more families have been found since then, and they will be summarized in Table 1.6. All of these families are different from each other in such a way that there are certain examples in each family which are not contained in any of the other known families. New APN functions

Table 1.5: Dillon APN functions on $\mathbb{F}_{2^6}$

No.	Polynomial, α is the root of $x^6 + x^4 + x^3 + x + 1$
D. 1	x^3
D. 2	$x^3 + \alpha^{11}x^6 + \alpha x^9$
D. 3	$\alpha x^5 + x^9 + \alpha^4 x^{17} + \alpha x^{18} + \alpha^4 x^{20} + \alpha x^{24} + \alpha^4 x^{34} + \alpha x^{40}$
D. 4	$\alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$
D. 5	$x^3 + \alpha x^{24} + x^{10}$
D. 6	$x^3 + \alpha^{17}(x^{17} + x^{18} + x^{20} + x^{24})$
D. 7	$x^3 + \alpha^{11}x^5 + \alpha^{13}x^9 + x^{17} + \alpha^{11}x^{33} + x^{48}$
D. 8	$\alpha^{25}x^5 + x^9 + \alpha^{38}x^{12} + \alpha^{25}x^{18} + \alpha^{25}x^{36}$
D. 9	$\alpha^{40}x^5 + \alpha^{10}x^6 + \alpha^{62}x^{20} + \alpha^{35}x^{33} + \alpha^{15}x^{34} + \alpha^{29}x^{48}$
D. 10	$\alpha^{34}x^6 + \alpha^{52}x^9 + \alpha^{48}x^{12} + \alpha^6 x^{20} + \alpha^9 x^{33} + \alpha^{23}x^{34} + \alpha^{25}x^{40}$
D. 11	$x^9 + \alpha^4(x^{10} + x^{18}) + \alpha^9(x^{12} + x^{20} + x^{40})$
D. 12	$\alpha^{52}x^3 + \alpha^{47}x^5 + \alpha x^6 + \alpha^9 x^9 + \alpha^{44}x^{12} + \alpha^{47}x^{33} + \alpha^{10}x^{34} + \alpha^{33}x^{40}$
D. 13	$\alpha(x^6 + x^{10} + x^{24} + x^{33}) + x^9 + \alpha^4 x^{17}$

were also found by using the switching method [50]. The switching method was further explored in [30] and more sporadic quadratic and nonquadratic APN functions were discovered. We will discuss the switching method in detail in Section 4.3.

For $n \leq 5$, the classification of APN functions is complete [23]. That list contains one "sporadic" example in addition to the known power mappings. This is a nonquadratic APN function which is also contained in [30]. By mistake in [23], the authors claimed that their example is quadratic.

For $n = 6$, the classification of quadratic APN functions is complete. There are only 13 CCZ-inequivalent quadratic APN functions as proven in [56].

It is shown in a recent work [7] that there are more than 470 ($n = 7$) and more than 8000 ($n = 8$) CCZ-inequivalent quadratic APN functions. Now, it is computationally intensive to check the CCZ-equivalence of new APN functions found on $\mathbb{F}_{2^8}$.

Hans Dobbertin proved that for n odd, all power APN functions are permutations. This result was also mentioned by Leander [57]. For n even, it was conjectured that no APN permutation exist on $\mathbb{F}_2^n$. In 2009, Dillon [58] constructed the first APN permutation for $n = 6$ and it is the only known APN permutation if n is even.

Remark 1.30. The existence of APN permutations for even $n \geq 8$ is still an open problem and considered a big open problem in the study of APN functions.

Table 1.6: Known infinite families of APN multinomials on $\mathbb{F}_{2^n}$

Number	Polynomial	Conditions	Reference
M.1	$x^{2^s+1} + A^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 3t, gcd(t,3) = gcd(s,3t) = 1,$ $t \geq 3, i = st(\text{mod } 3), r = 3 - i,$ $A \in \mathbb{F}_{2^n}$	[46]
M.2	$x^{2^s+1} + A^{2^t-1}x^{2^{it}+2^{rt+s}}$	$n = 4t, gcd(t,2) = gcd(s,2t) = 1,$ $t \geq 3, i = st(\text{mod } 4), r = 4 - i,$ $A \in \mathbb{F}_{2^n}$	[47]
M.3	$Ax^{2^s+1} + A^{2^m}x^{2^{m+s}+2^m}+$ $Bx^{2^m+1} + \sum_{i=1}^{m-1} c_i x^{2^{m+i}+2^i}$	$n = 2m, m$ odd, $c_i \in \mathbb{F}_{2^n},$ $gcd(s,m) = 1, s$ odd, $A, B \in \mathbb{F}_{2^n}$ primitive	[28]
M.4	$Ax^{2^{n-t}+2^{t+s}} + A^{2^t}x^{2^s+1} + bx^{2^{t+s}+2^s}$	$n = 3t, gcd(s,3t) = gcd(3,t) = 1,$ $3 \mid (t+s), A \in \mathbb{F}_{2^n}$ primitive, $b \in \mathbb{F}_{2^t}$	[28]
M.5	$A^{2^t}x^{2^{n-t}+2^{t+s}} + Ax^{2^s+1} + bx^{2^{n-t}+1}$	$n = 3t, gcd(s,3t) = gcd(3,t) = 1,$ $3 \mid (t+s), A \in \mathbb{F}_{2^n}$ primitive, $b \in \mathbb{F}_{2^t}$	[48]
M.6	$A^{2^t}x^{2^{n-t}+2^{t+s}} + Ax^{2^s+1}+$ $bx^{2^{n-t}+1} + cA^{2^t+1}x^{2^{t+s}+s^s}$	$n = 3t, gcd(s,3t) = gcd(3,t) = 1,$ $3 \mid (t+s), A \in \mathbb{F}_{2^n}$ primitive, $b, c \in \mathbb{F}_{2^t},\ bc \neq 1$	[48]
M.7	$x^{2^{2k}+2^k} + Bx^{2^m+1} + Cx^{2^m(2^{2k}+2^k)}$	$n = 2m, m$ odd, C *is a* $(2^m-1)st$ power but not a $(2^m-1)(2^i+1)st$ power, $CB^{2^m} + B \neq 0$	[49]
M.8	$x(x^{2^k} + x^{2^m} + Cx^{2^{k+m}})+$ $x^{2^k}(C^{2^m}x^{2^m} + Ax^{2^{k+m}}) + x^{(2^k+1)2^m}$	$n = 2m,\ gcd(n,k) = 1,\ C$ satisfies Theorem 11, $A \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$	[49]
M.9	$x^3 + Tr_1^n(x^9)$		[50]
M.10	$x^3 + A^{-1}Tr_3^n(A^3x^9 + A^6x^{18})$	$3 \mid n,\ A \neq 0$	[51]
M.11	$x^3 + A^{-1}Tr_3^n(A^6x^{18} + A^{12}x^{36})$	$3 \mid n,\ A \neq 0$	[51]
M.12	Bivariate construction of Theorem 1 [52]	$n = 2m$	[52]
M.13	Bivariate construction of Theorem 9 [53]	$n = 4m$	[53]

Chapter 2

On the number of weight 4 codewords

In this chapter, we study the pattern of reduction of weight 4 codewords in the linear code related with vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$. In Section 2.1, we discuss the connection between vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$ and coding theory. In Section 2.2, we compute an explicit formula to determine the number of weight 4 code words in the linear codes of vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$. We study the pattern of reduction of weight 4 codewords in the linear code of AB functions, APN power functions, vectorial bent functions and the Dillon APN permutation in Sections 2.3, 2.4, 2.9 and 2.10 respectively. In Section 2.5 and 2.8, we discuss the reduction of weight 4 codewords in the linear codes of quadratic Boolean functions, Dobbertin APN functions and Kavut et. al. Boolean functions respectively. We also discuss variations of the partial spread and the Maiorana-McFarland class of Boolean functions in Section 2.6 and 2.7. We study the reduction of weight 4 codewords in the linear code of the partial spread and the Maiorana-McFarland class of Boolean functions.

2.1 Connection between vectorial Boolean functions and coding theory

In this section, we discuss the connection between vectorial Boolean functions, in particular AB and APN functions and coding theory. We have discussed in Section 1.3 that the APN property of a vectorial Boolean function uses vector space structure. In order to study the vector space structure of APN functions, we need an interpretation of APN functions in terms of coding theory. First, we discuss the basics of coding theory.

A *binary linear code* C of length n and dimension k is a linear subspace of $\mathbb{F}_2^n$. Its parameters are $[n,\ k]$. The elements of the code C are called *codewords*. If a code C consists of only one codeword, then C is called a *trivial code*. i.e., $C = \{(0, \ldots, 0)\}$. To any binary linear code, we associate its dual code

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

The dual code has parameters $[n, n-k]$. The *(Hamming) weight* of any codeword $c \in C$ is denoted by $wt(c)$. The *(Hamming) distance* between any two codewords c_1 and c_2 of C is denoted by $d(c_1, c_2)$. The number $d = \min\{wt(c) \mid c \in C,\ c \neq 0\}$ is called the *minimum distance* of the binary linear code C. A binary linear code C of length n, dimension k and minimum distance d is called an $[n,\ k,\ d]$ code. Let a_i denote the number of codewords of C of weight i. The vector $(a_0, \ldots, a_{n-1})$ is called the *weight enumerator* of C and the polynomial $W_C(x) = \sum_{i=0}^{n-1} a_i x^i$ is called the *weight polynomial* of C. Let H be an $k \times n$ matrix defined over $\mathbb{F}_2$. A binary linear code C of length n is defined by the *parity check* matrix H if $C = \{c \in \mathbb{F}_2^n \mid H \cdot c = 0\}$.

Let $h_1, h_2, \ldots, h_n$ denote the columns of the parity check matrix H and $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, then $H \cdot v$ equals $v_1 h_1 + v_2 h_2 + \ldots + v_n h_n$. If there exist $v \neq 0$ such that $v_1 h_1 + \ldots + v_n h_n = 0$ then h_i, $1 \leq i \leq n$ are linearly dependent. Using the above observation, we say that the minimum number of dependent columns of H is equal to

$$\min_{\substack{v \in \mathbb{F}_2^n, \\ v \neq 0}} \{wt(v) \mid v_1 h_1 + \ldots + v_n h_n = 0\}.$$

Lemma 2.1. *Let H be a parity check matrix of an $[n,\ k,\ d]$ code C. The minimum distance d is equal to the minimum number of linearly dependent columns of H.*

Proof. We know that $c \in C$ if and only if $H \cdot c = 0$. It follows that each codeword with Hamming weight t corresponds to t linear dependent columns of H. We know that the minimum weight of codewords is equal to d. Hence, d equals the minimum number of linear dependent columns of H. □

There is a connection between the Walsh coefficient of a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ and the weights of codewords of $C_F^{\perp}$ which can be described in the following way.

Proposition 2.2. *Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Let $C_F^{\perp}$ be the code generated by the row space of the parity check matrix*

$$H_F = \begin{bmatrix} x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_2^n}$$

of dimension $(n+m) \times 2^n$. Note that $C_F = \{x \in \mathbb{F}_2^{2^n} : H_F \cdot x = 0\}$. The code words in $C_F^{\perp}$ are the vectors denoted by $C_{a,b} = a \cdot x + b \cdot F(x)$, where $x \in \mathbb{F}_2^n, a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m$. The weight of $C_{a,b}$ is

$$\lambda_{a,b} = 2^{n-1} - \frac{1}{2} W_F(a,b).$$

Proof. Assume that $s(x) = a \cdot x + b \cdot F(x)$. Note that the function $s(x)$ is actually a linear combination of the rows of H_F. Hence, the number $\lambda_{a,b} = \#\{x \in \mathbb{F}_2^n \mid s(x) = 1\}$ is the weight of the codewords $C_{a,b}$ in $C_F^{\perp}$.
As we know that

$$W_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x}, a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m, b \neq 0, \tag{2.1}$$

we can write the equation (2.1) as

$$\begin{aligned} W_F(a,b) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{s(x)} \\ &= \#\{x \in \mathbb{F}_2^n \mid s(x) = 0\} - \#\{x \in \mathbb{F}_2^n \mid s(x) = 1\} \\ &= (2^n - \#\{x \in \mathbb{F}_2^n \mid s(x) = 1\}) - \{x \in \mathbb{F}_2^n \mid s(x) = 1\} \\ &= 2^n - 2\#\{x \in \mathbb{F}_2^n \mid s(x) = 1\} \\ &= 2^n - 2\lambda_{a,b}, \end{aligned}$$

so,

$$\lambda_{a,b} = 2^{n-1} - \frac{1}{2} W_F(a,b).$$

□

We have introduced the basics of binary linear codes. The AB and APN properties can be described in terms of binary linear codes.

Theorem 2.3. *[20] Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $F(0) = 0$. Let C_F be the $[2^n - 1, k, d]$ code defined by the parity check matrix of dimension $2n \times 2^n - 1$*

$$H_F = \begin{bmatrix} x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_2^n \setminus \{0\}}.$$

Then

(i) F is APN if and only if $d = 5$.

(ii) F is AB if and only if the weight of every codeword of $C_F^{\perp}$ belongs to $\Omega = \{2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}\}$.

Proof. (i) Let $c = (c_1, \ldots, c_{2^n-1})$ be a binary vector. By the definition of H_F, c belong to C_F if and only if

$$H_F \cdot c = 0.$$

Since H_F has no zero column, it means that C_F has no codewords of Hamming weight 1. All the columns of H_F are distinct vectors then C_F has no codewords of Hamming weight 2. The C_F has minimum weight 3 if and only if there exist three distinct elements, say $x_1, x_2, x_3 \in \mathbb{F}_2^n$, such that

$$x_1 + x_2 + x_3 = 0 \text{ and } F(x_1) + F(x_2) + F(x_3) = 0.$$

The non-existence of codewords of weight 3 follows from the proof of Theorem 1.18. The 2-dimensional affine subspaces of $\mathbb{F}_2^n$ are the translates of 2-dimensional linear subspaces of $\mathbb{F}_2^n$ by some vector of $\mathbb{F}_2^n$ and F is an APN function.

The C_F has minimum weight 4 if and only if there exist four distinct elements, say $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n$, such that

$$x_1 + x_2 + x_3 + x_4 = 0 \text{ and } F(x_1) + F(x_2) + F(x_3) + F(x_4) = 0.$$

The non-existence of codewords of weight 4 also follows from the proof of Theorem 1.18. So, F is APN if and only if C_F has minimum distance $d \geq 5$. It is difficult to prove that $d \leq 5$, we refer to the proof from original paper [59]. Hence, F is APN if and only if $d = 5$.

(ii) From Proposition 2.2, we know that the codewords in $C_F^\perp$ are the vectors denoted by $C_{a,b} = a \cdot x + b \cdot F(x)$, where $x \in \mathbb{F}_2^n, a, b \in \mathbb{F}_2^n$. The weight of $C_{a,b}$ is denoted by

$$\lambda_{a,b} = 2^{n-1} - \frac{1}{2} W_F(a,b).$$

Assume that F is AB, i.e. $W_F(a,b) = 0$ or $\pm 2^{\frac{n+1}{2}}$. First consider $W_F(a,b) = 0$, it means that $\lambda_{a,b} = 2^{n-1}$. Therefore, $2^{n-1} \in \Omega$.

Similarly, consider $W_F(a,b) = \pm 2^{\frac{n+1}{2}}$, it means that

$$\lambda_{a,b} = 2^{n-1} \pm 2^{\frac{n-1}{2}} \in \Omega.$$

Thus, we have proved (ii). □

We may extend the matrix H_F by adding the vector $\mathbf{1} = (1, \ldots, 1)$ as a row to H_F to obtain the matrix H_F^{ext}. This means the row space of the matrix H_F^{ext} contains all the row vectors of the matrix H_F along with one additional coordinate 0 in the beginning, and with all codewords c also $c + \mathbf{1}$. We have the following characterization of APN functions.

Corollary 2.4. *[19] Let F be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with $F(0) = 0$. Let C_F be the $[2^n, k, d]$ code defined by the parity check matrix of dimension $(2n + 1 \times 2^n)$*

$$H_F^{ext} = \begin{bmatrix} \mathbf{1} \\ x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_2^n}$$

Then F is APN if and only if $d = 6$.

2.2 Formula for weight 4 codewords

In this section, we compute an explicit formula to determine the exact number of weight 4 codewords in a linear code of vectorial Boolean functions from $\mathbb{F}_2^n$ to

$\mathbb{F}_2^m$ with $m \leq n$. Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq n$ defined by

$$F(x) = \left(\begin{array}{c} f_1(x) \\ \vdots \\ f_m(x) \end{array} \right),$$

where $f_1(x), \ldots, f_m(x)$ are the coordinate functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. From Theorem 1.18, we known that a function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is APN if and only if F is not affine on any 2-dimensional affine subspaces of $\mathbb{F}_2^n$. This means an APN function "wipes out" all 2-dimensional affine subspaces of $\mathbb{F}_2^n$.

Here, we use the informal term "wipes out" which means that from the given set of all 2-dimensional affine subspaces of $\mathbb{F}_2^n$, we remove (wipe out) some particular 2-dimensional affine subspaces of $\mathbb{F}_2^n$. We will use the term "wipes out" frequently in the subsequent section.

We are interested in the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ by using coordinate functions. This means we need to find n Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ in such a way that these n Boolean functions wipe out all the 2-dimensional affine subspaces of $\mathbb{F}_2^n$. We name this approach as coordinate functions approach.

Coordinate functions approach

In this approach, we first need to find a Boolean function $f_1(x)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and determine the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by $f_1(x)$, that is,

$$f_1(x) + f_1(x+a) + f_1(y) + f_1(y+a) = 0.$$

Then, we try to find a Boolean function $f_2(x)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ that wipes out many of the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by the Boolean function $f_1(x)$. We can continue in the same way and finally we need to find a Boolean function $f_n(x)$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ that wipes out all the 2-dimensional affine subspaces of $\mathbb{F}_2^n$ which are not wiped out by the Boolean functions $f_1(x), \ldots, f_{n-1}(x)$.

We can also describe the coordinate functions approach for the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in terms of coding theory. Assume that $f_1(x), \ldots,$ $f_m(x)$ are Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with $m \leq n$. We can define the $(n+m+1) \times (2^n)$ matrix

$$H_{f_1,\ldots,f_m} = \left[\begin{array}{c} 1 \\ x \\ f_1(x) \\ \vdots \\ f_m(x) \end{array} \right]_{x \in \mathbb{F}_2^n} .$$

Let $C_{f_1,\dots,f_m} = \{x \in \mathbb{F}_2^{2^n} : H_{f_1,\dots,f_m} \cdot x = 0\}$. This is the code that consists of all codewords (vectors) orthogonal to the rows of $H_{f_1,\dots,f_m}$. In the subsequent section, we use the word vectors instead of codewords.

Assume that $\{x, x+a, y, y+a\}$ is a 2-dimensional affine subspaces of $\mathbb{F}_2^n$. The corresponding indicator function (which is 1 for $x,\ x+a,\ y,\ y+a$ and 0 otherwise) is a vector of weight 4. The function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}$$

is an APN function if and only if the minimum weight of $C_{f_1,\dots,f_n}$ is 6, see Corollary 2.4. In order to construct an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ using n coordinate functions $f_1, \dots, f_n$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, we need to look at the pattern of reduction of the number of weight 4 vectors in the linear code of $f_1, \dots, f_n$. A good strategy would be to find a chain of functions $f_1, \dots, f_n$ such that $\lambda(f_1, \dots, f_m)/\lambda(f_1, \dots, f_{m+1})$ is always quite large, where $m \le n$ and $\lambda(f_1, \dots, f_m)$ is the number of weight 4 vectors in $C_{f_1,\dots,f_m}$.

Note that $\lambda(0)$ is the total number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$. The total number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$ can be calculated using Gaussian Binomial. In general, the Gaussian Binomials are

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}.$$

In our case, we have $q = 2,\ k = 2$, then

$$\begin{bmatrix} n \\ 2 \end{bmatrix}_2 = \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} = \frac{(2^n-1)(2^n-2)}{6}.$$

The total number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$ are

$$\begin{bmatrix} n \\ 2 \end{bmatrix}_2 \cdot 2^{n-2} = \frac{(2^n-1)(2^n-2)}{6} \cdot 2^{n-2} = \frac{2^{3n-3} - 3 \cdot 2^{2n-3} + 2^{n-2}}{3},$$

here, 2^{n-2} is the number of all possible cosets of 2-dimensional linear subspaces. We observe that if $C_{f_1,\dots,f_m} = C_{g_1,\dots,g_m}$, then it is possible that $\lambda(f_1, \dots, f_i) \neq \lambda(g_1, \dots, g_i)$ for $i < m$. In other words, the pattern of reduction of $\lambda(f_1, \dots, f_m)$ or $\lambda(g_1, \dots, g_m)$ may depend upon the choice of the coordinate functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The number of weight 4 vectors can be computed in the following way.

Theorem 2.5. *Assume that F is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \le n$. The number $\lambda(f_1, \dots, f_m)$ of weight 4 vectors in the linear code $C_{f_1,\dots,f_m}$ are*

$$\lambda(f_1, \dots, f_m) = \frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{\substack{a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m, \\ b \neq 0}} (W_F(a,b))^4 + 2^{4n}\right) - 3 \cdot 2^{2n} + 2^{n+1}\right],$$

where $W_F(a,b) = \sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+b\cdot F(x)}$.

Proof. We have

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

Taking the fourth power on both sides, we get

$$(W_F(a,b))^4 = \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{a\cdot x+b\cdot F(x)}\right)^4, a \in \mathbb{F}_2^n,\ b \in \mathbb{F}_2^m,$$

From equations (1.3) and (1.4) of Theorem 1.16 and Proposition 1.5, we have

$$\sum_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^m}(W_F(a,b))^4 = 2^{n+m}\Gamma,$$

where

$$\Gamma = \#\left\{\ (x,y,z,w) \in (\mathbb{F}_2^n)^4 \mid \left\{\begin{array}{c} x+y+z+w=0 \\ F(x)+F(y)+F(z)+F(w)=0 \end{array}\right.\right\}. \tag{2.2}$$

Now, we discuss different cases for the possible values of the quadruple $(x,y,z,w) \in (\mathbb{F}_2^n)^4$ which satisfy the conditions of (2.2).

Case 1: Assume that $x = y = z = w$ and $F(x) = F(y) = F(z) = F(w)$. We have precisely 2^n possibilities for this type of occurrences.

Case 2: Assume that all the values in the quadruple $(x,y,z,w) \in (\mathbb{F}_2^n)^4$ are different: precisely these quadruples describe the weight 4 vectors in the linear code $C_{f_1,\ldots,f_m}$. Moreover, one vector of weight 4 gives exactly $4! = 24$ such quadruples, hence, we have precisely $24\lambda(f_1,\ldots,f_m)$ possibilities for this type of occurrences.

Case 3: Assume that any two of the values in the quadruple $(x,y,z,w) \in (\mathbb{F}_2^n)^4$ are the same, that is, either $x = y$ or $x = z$ or $x = w$ or $y = z$ or $y = w$ or $z = w$. Then, in order to have $x+y+z+w = 0$ in each of these 6 cases, the other two values must also be the same. There are $\left(\begin{array}{c} 2^n \\ 2 \end{array}\right)$ possibilities to choose these two values, which must be different from each other, since, we would be in case 1 otherwise. In total, we have $6\left(\begin{array}{c} 2^n \\ 2 \end{array}\right) = 3(2^{2n}-2^n)$ possibilities for this type of occurrences.

Cases 1, 2 and 3 altogether gives

$$\sum_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^m}(W_F(a,b))^4 = 2^{n+m}\left[2^n + 24\lambda(f_1,\ldots,f_m) + 3(2^{2n}-2^n)\right].$$

This leads to the desired result

$$\lambda(f_1,\ldots,f_m) = \frac{1}{24}\left[\frac{1}{2^{n+m}}\left(\sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m, b\neq 0}(W_F(a,b))^4 + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right],$$

where we have used $W_F(a,0) = 2^n$, if $a = 0$ and $W_F(a,0) = 0$, if $a \neq 0$. □

The following result is well known result about the 4th power of Walsh spectrum of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ [19, 60]. We can also derive this result from Theorem 2.5.

Corollary 2.6. *Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Then*

$$\sum_{\substack{a,b\in\mathbb{F}_2^n,\\ b\neq 0}} (W_F(a,b))^4 = 2^{3n+1}(2^n-1).$$

Proof. From Theorem 2.5, we know that

$$\lambda(f_1,\dots,f_n) = \frac{1}{24}\left[\frac{1}{2^{2n}}\left(\sum_{\substack{a,b\in\mathbb{F}_2^n,\\ b\neq 0}} (W_F(a,b))^4 + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right]. \tag{2.3}$$

Since, F is an APN function, we have $\lambda(f_1,\dots,f_n)=0$. Substitute $\lambda(f_1,\dots,f_n)=0$ in equation (2.3), we get

$$\frac{1}{24}\left[\frac{1}{2^{2n}}\left(\sum_{\substack{a,b\in\mathbb{F}_2^n,\\ b\neq 0}} (W_F(a,b))^4 + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right] = 0.$$

After simplification, we have

$$\sum_{\substack{a,b\in\mathbb{F}_2^n,\\ b\neq 0}} (W_F(a,b))^4 = 2^{3n+1}(2^n-1).$$

□

Corollary 2.7. *Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The number $\lambda(f_1)$ of weight 4 vectors in the linear code C_{f_1} is*

$$\lambda(f_1) = \frac{1}{24}\left[\frac{1}{2^{n+1}}\left(\sum_{a\in\mathbb{F}_2^n} (W_f(a,1))^4 + 2^{4n}\right) - 3\cdot 2^{2n} + 2^{n+1}\right].$$

Now, we discuss the pattern of reduction of weight 4 vectors in the linear code of AB functions.

2.3 AB Functions

In this section, we consider the AB functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with n odd. We want to observe the pattern of reduction of weight 4 vectors in the linear code of AB functions. The Gold, Kasami, Welch and Niho power functions from $\mathbb{F}_{2^n}$

Table 2.1: Walsh spectrum of AB functions on $\mathbb{F}_{2^n}$ with $n = 2m + 1$ odd

Walsh coefficient	Multiplicity
2^{m+1}	$(2^n - 1)(2^{n-2} + 2^{(n-3)/2})$
0	$(2^n - 1)(2^{n-1})$
-2^{m+1}	$(2^n - 1)(2^{n-2} - 2^{(n-3)/2})$

Table 2.2: Weight 4 vectors in the linear codes of AB functions $F : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$

No.	Value
$\lambda(0)$	1240
$\lambda(f_1)$	600
$\lambda(f_1, f_2)$	280
$\lambda(f_1, f_2, f_3)$	120
$\lambda(f_1, f_2, f_3, f_4)$	40
$\lambda(f_1, f_2, f_3, f_4, f_5)$	0

to $\mathbb{F}_{2^n}$ listed in Table 1.3 are AB functions. Carlet, Charpin and Zinoviev [20] showed that if $F(0) = 0$, then the Walsh spectrum of the AB functions F along with their multiplicities are given in Table 2.1. The values $\lambda(f_1), \ldots, \lambda(f_1, \ldots, f_m)$ can be computed from Theorem 2.5 in the following way.

Corollary 2.8. *Assume that F is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ such that all non-trivial component functions are semi-bent. Then, the number $\lambda(f_1, \ldots, f_m)$ of weight 4 vectors in the linear code $C_{f_1,\ldots,f_m}$ is*

$$\lambda(f_1, \ldots, f_m) = \frac{1}{3}\left[2^{3n-m-3} - 2^{2n-3} - 2^{2n-m-2} + 2^{n-2}\right].$$

Proof. The corollary follows from Theorem 2.5 and the definition of semi-bent Boolean functions. □

We have computed the number of weight 4 vectors in the linear code $C_{f_1,\ldots,f_n}$ of AB functions for small values of n. These values are explicitly listed in Tables 2.2, 2.3, 2.4 and 2.5. We observe that all the component functions of AB functions have the same Walsh spectrum. Therefore, the values $\lambda(f_1, \ldots, f_i)$, $2 \leq i \leq n$ do not depend upon the choice of the component functions f_i that we choose to represent $F(x)$.

Table 2.3: Weight 4 vectors in the linear codes of AB functions $F : \mathbb{F}_{2^7} \to \mathbb{F}_{2^7}$

No.	Value
$\lambda(0)$	85344
$\lambda(f_1)$	42336
$\lambda(f_1, f_2)$	20832
$\lambda(f_1, f_2, f_3)$	10080
$\lambda(f_1, f_2, f_3, f_4)$	4704
$\lambda(f_1, f_2, f_3, f_4, f_5)$	2016
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6)$	672
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7)$	0

Table 2.4: Weight 4 vectors in the linear codes of AB functions $F : \mathbb{F}_{2^9} \to \mathbb{F}_{2^9}$

No.	Value
$\lambda(0)$	5559680
$\lambda(f_1)$	2774400
$\lambda(f_1, f_2)$	1381760
$\lambda(f_1, f_2, f_3)$	685440
$\lambda(f_1, f_2, f_3, f_4)$	337280
$\lambda(f_1, f_2, f_3, f_4, f_5)$	163200
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6)$	76160
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7)$	32640
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8)$	10880
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9)$	0

Table 2.5: Weight 4 vectors in the linear code of AB functions $F : \mathbb{F}_{2^{11}} \to \mathbb{F}_{2^{11}}$

No.	Value
$\lambda(0)$	357389824
$\lambda(f_1)$	178607616
$\lambda(f_1, f_2)$	89216512
$\lambda(f_1, f_2, f_3)$	44520960
$\lambda(f_1, f_2, f_3, f_4)$	22173184
$\lambda(f_1, f_2, f_3, f_4, f_5)$	10999296
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6)$	5412352
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7)$	2618880
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8)$	1222144
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9)$	523776
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10})$	174592
$\lambda(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11})$	0

2.4 APN Power Functions

Now, we discuss the case of APN power functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with n odd. We have the following Theorem.

Theorem 2.9. *[57] Let $F(x) = x^d$ be a power APN function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ with n odd. Then the function F is a permutation.*

Proof. Assume that the mapping $x \to x^d$ is not a permutation. This means that there exist some $x \in \mathbb{F}_{2^n}$ such that $x^d = 1$, where $x \notin \mathbb{F}_2$. Divide $(x+1)^d$ on both sides of the equation $x^d = 1$. We get

$$\frac{x^d}{(x+1)^d} = \frac{1}{(x+1)^d},$$

it implies that

$$\frac{x^d}{(x+1)^d} + \frac{1}{(x+1)^d} = 0.$$

We can write the above equation as

$$\frac{x^d}{(x+1)^d} + \frac{1}{(x+1)^d} = 0 = \frac{(x^2)^d}{(x^2+1)^d} + \frac{1}{(x^2+1)^d},$$

hence, we have

$$\left(\frac{x}{x+1}\right)^d + \frac{1}{(x+1)^d} = 0 = \left(\frac{x^2}{x^2+1}\right)^d + \frac{1}{(x^2+1)^d}.$$

Since F is an APN power function, then we must either have

$$\frac{x}{x+1} = \frac{x^2}{x^2+1},$$

or

$$\frac{x}{x+1} = \frac{1}{x^2+1}.$$

Assume that

$$\frac{x}{x+1} = \frac{1}{x^2+1},$$

it implies that

$$x(x^2+1) = x+1,$$

hence, we have

$$x^3 + x = x + 1,$$

$$x^3 = 1.$$

which is impossible since $3 \nmid 2^n - 1$, if n is odd. This means that $F(x) = x^d$ is a permutation if n is odd. □

We have discussed that the reduction in the number of weight 4 vectors in the linear code related with vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ depends on the choice of coordinate functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. This is not true in case of APN power permutations from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. This was also observed by Berger, Canteaut, Charpin and Laigle Chapuy [60] in context of sum of square indicators.

Theorem 2.10. *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x) = x^d$ with n odd. Assume that F is a power permutation, that is, with $gcd(d, 2^n - 1) = 1$, then*

$$\sum_{a \in \mathbb{F}_{2^n}} (W_F(a,b))^4 = \Gamma,$$

where

$$\Gamma = \sum_{c \in \mathbb{F}_{2^n}} \left(\sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(y^d + cy)} \right)^4 .$$

In particular, if F is APN then $\Gamma = 2^{3n+1}$.

Proof. Let $F(x) = x^d$ be a power permutation from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We know that

$$\begin{aligned} W_F(a,b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(bF(x)) + Tr_1^n(ax)}, \ {}_{\substack{a,b \in \mathbb{F}_{2^n}, \\ b \neq 0}} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(bF(x) + ax)} \end{aligned}$$

Taking the fourth power on both sides, we get

$$\begin{aligned} (W_F(a,b))^4 &= \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(bF(x)+ax)} \right)^4 \\ &= \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(bx^d+ax)} \right)^4 \end{aligned}$$

Assume that $b = \beta^d$ for some $\beta \in \mathbb{F}_{2^n}$, then we have

$$\begin{aligned} (W_F(a,b))^4 &= \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\beta^d x^d+ax)} \right)^4 \\ &= \left(\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n((\beta x)^d+ax)} \right)^4 . \end{aligned}$$

Let $\beta x = y$, then $x = \beta^{-1} y$ and

$$\sum_{a \in \mathbb{F}_{2^n}} (W_F(a,b))^4 = \sum_{a \in \mathbb{F}_{2^n}} \left(\sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(y^d + \beta^{-1} ay)} \right)^4$$

Let $\beta^{-1}a = c$, where $c \in \mathbb{F}_{2^n}$, then

$$\sum_{a \in \mathbb{F}_{2^n}} (W_F(a,b))^4 = \Gamma,$$

where

$$\Gamma = \sum_{c \in \mathbb{F}_{2^n}} \left(\sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(y^d + cy)} \right)^4 .$$

Now, we take the sum over all $b \in \mathbb{F}_{2^n}$ with $b \neq 0$, then we have

$$\sum_{\substack{a,b \in \mathbb{F}_{2^n}, \\ b \neq 0}} (W_F(a,b))^4 = (2^n - 1)\Gamma \tag{2.4}$$

From Corollary 2.6 , we know that

$$\sum_{\substack{a,b \in \mathbb{F}_2^n, \\ b \neq 0}} (W_F(a,b))^4 = 2^{3n+1}(2^n - 1). \tag{2.5}$$

After comparing equation (2.4) and (2.5), we get

$$\Gamma = 2^{3n+1}.$$

□

Corollary 2.11. *Let $F^{'}$ be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ defined as*

$$F^{'}(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$$

If $F^{'}$ is a power APN permutation then the number of weight 4 vectors in the linear code of $F^{'}$ is independent of the choice of coordinate functions of $F^{'}$.

Proof. From Theorem 2.5, we know that the number of weight 4 vectors $\lambda(f_1, \ldots, f_m)$ in the linear code of $F^{'}$ depends upon the value of

$$\sum_{\substack{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m \\ b \neq 0}} \left(W_{F'}(a,b)\right)^4 .$$

For any value of $b \in \mathbb{F}_2^m$ with $b \neq 0$, we have one component function of $F^{'}$. If $F^{'}$ is an APN permutation then the value of $\Gamma = 2^{3n+1}$ is fixed for each component function of $F^{'}$. It means no matter in which order we choose component functions, the number of weight 4 vectors in the linear code of $F^{'}$ is independent of the choice of coordinate functions of $F^{'}$.

□

Table 2.6: Walsh spectrum of quadratic Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$

Walsh coefficient	Multiplicity
$2^{(n+e)/2}$	$2^{(n-e-1)} + 2^{(n-e-2)/2}$
0	$2^n - 2^{n-e}$
$-2^{(n+e)/2}$	$2^{(n-e-1)} - 2^{(n-e-2)/2}$

2.5 Plateaued Boolean functions

The notion of plateaued Boolean functions were introduced in [61]. It is a generalization of quadratic Boolean functions. All recently discovered infinite families of AB and APN functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ listed in Table 1.6 are quadratic. This means all of their component functions are quadratic. In this section, we consider the case of quadratic Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We are interested in observing the number of weight 4 vectors in the linear code related with quadratic Boolean functions.

Recall that a quadratic homogeneous Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is defined as

$$f(x_1, \ldots, x_n) = \sum_{1 \le i < j \le n} a_{i,j} x_i x_j,\ a_{i,j} \in \mathbb{F}_2.$$

The Walsh coefficients of a quadratic Boolean functions along with their multiplicities are given in Table 2.6, (see McEliece, 1987, Chapter 11 [62]), for instance. In Table 2.6, $e = n - r$ with

$$r = Rank(a_{i,j} + a_{j,i}).$$

If the value of n is even and $r = n$, then we have bent functions. We can compute the number of weight 4 vectors in the linear code C_f related with a quadratic Boolean functions f.

Corollary 2.12. *Assume that $f_{n,e} : \mathbb{F}_2^n \to \mathbb{F}_2$ is a quadratic Boolean function with a Walsh spectrum given in Table 2.6. The number $\lambda(f_{n,e})$ of weight 4 vectors in the linear code C_f is*

$$\lambda(f_{(n,e)}) = \frac{1}{3}\left[2^{2n+e-4} + 2^{3n-4} - 3 \cdot 2^{2n-3} + 2^{n-2}\right],$$

where e is defined as above.

Proof. The corollary follows from Theorem 2.5 and Table 2.6. □

In Table 2.7, we explicitly give the values of $\lambda(f_{n,e})$ for small values of n and e. From Corollary 2.12, we observe that bent functions wipe out

$$\frac{2^{3n-4} - 2^{2n-4}}{3}$$

Table 2.7: Weight 4 vectors in the linear code of quadratic Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$

n	e	$\lambda(f_{n,e})$
4	4	140
	2	76
	0	60
6	6	10416
	4	6320
	2	5296
	0	5040
8	8	690880
	6	428736
	4	363200
	2	346816
	0	342720
10	10	44608256
	8	27831040
	6	23636736
	4	22588160
	2	22326016
	0	22260480

(a) n even

n	e	$\lambda(f_{n,e})$
5	5	1240
	3	728
	1	600
7	7	85344
	5	52576
	3	44384
	1	42336
9	9	5559680
	7	3462528
	5	2938240
	3	2807168
	1	2774400
11	11	357389824
	9	223172096
	7	189617664
	5	181229056
	3	179131904
	1	178607616

(b) n odd

of the

$$\frac{2^{3n-3} - 3 \cdot 2^{2n-3} + 2^{n-2}}{3}$$

2-dimensional affine subspaces of $\mathbb{F}_2^n$, i.e., approximately half of them. Quadratic functions of rank $n - e$ wipe out

$$\frac{2^{3n-4} - 2^{2n+e-4}}{3}$$

of all (approximately $\frac{2^{3n-4}}{3}$) 2-dimensional affine subspaces of $\mathbb{F}_2^n$. This shows that bent functions are the best candidates of coordinate functions to construct APN functions. From Tables 1.2 and 1.6, we know that many APN functions consist of bent and plateaued coordinate functions. It has been proposed to search for more (nonquadratic) plateaued functions and somehow replace the quadratic functions by a nonquadratic plateaued functions. In our approach, we want to replace the plateaued Boolean functions by nonquadratic Boolean functions which are actually better than plateaued Boolean functions with respect to wiping out 2-dimensional affine subspaces of $\mathbb{F}_2^n$.

The bent functions can be constructed by using the Maiorana-McFarland and the partial spread construction method. We have discussed that the bent functions wipe out the maximum number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$. It may be a promising idea to look for Boolean functions which belong to the partial spread and Maiorana-McFarland class and which wipe out a large number of 2-dimensional affine subspaces of $\mathbb{F}_2^n$. First, we discuss the partial spread class and then we discuss the Maiorana-McFarland class.

2.6 Partial spread class

The partial spread class of bent functions was introduced by Dillon [63]. This class of bent function is defined corresponding to partial spreads, a classical geometric object. We consider the case of partial spread Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $n = 2m$. A partial spread of order k (k-spread) in $\mathbb{F}_2^n$ is a set of m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ such that $H_i \cap H_j = \{0\}$ for all $i \neq j$. A partial spread is a spread if the union of its elements equals $\mathbb{F}_2^n$ and in this case $k = 2^m + 1$.

We have two possible cases of m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$. In the first case, we consider m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ without 0 and in the second case, we consider m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ with 0. Now we consider the first case, where we have the following theorem.

Theorem 2.13. *Let $n = 2m$ and $H_1, ..., H_k$ be m-dimensional subspaces of $\mathbb{F}_2^n$ of a partial spread. The Boolean function f_k from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is the indicator function of*

$D = \cup_{i=1}^{k} H_i \setminus \{0\}$ such that $f_k(x) = 1$, if $x \in D$ and 0, otherwise. The Walsh spectrum of f_k is as follows.

Walsh coefficient	*Multiplicity*
$2^n - 2^{m+1}k + 2k$	1
$2k$	$2^n - 2^m k + k - 1$
$2k - 2^{m+1}$	$2^m k - k$

Proof. Let $H_1, \ldots, H_k$ be the m-dimensional subspaces of $\mathbb{F}_2^n$. Let $H_i^* = H_i \setminus \{0\}$ and $D = \cup_{i=1}^{k} H_i^*$. We know that

$$\begin{aligned} W_{f_k}(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f_k(x)+a\cdot x} \\ &= \sum_{x \in D} (-1)^{f_k(x)} \cdot (-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{f_k(x)} \cdot (-1)^{a\cdot x} \\ &= \sum_{x \in D} -(-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{a\cdot x} \\ &= -\sum_{x \in D} (-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{a\cdot x}. \end{aligned}$$

Assume that $a = 0$, then the above equation becomes

$$\begin{aligned} W_{f_k}(a) &= -\sum_{x \in D} (-1)^0 + \sum_{x \notin D} (-1)^0 \\ &= -\sum_{x \in D} (1) + \sum_{x \notin D} (1) \\ &= - \mid D \mid + (\mid \mathbb{F}_2^n \mid - \mid D \mid) \\ &= 2^n - 2((2^m - 1)k) \\ &= 2^n - 2^{m+1}k + 2k. \end{aligned}$$

The above value has multiplicity 1. Now, consider $a \neq 0$, then we have

$$W_{f_k}(a) = -\sum_{x \in D} (-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{a\cdot x}$$

From Proposition 1.5, we know that

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

Now, we have

$$\begin{aligned} W_{f_k}(a) &= -\sum_{x \in D} (-1)^{a\cdot x} - \sum_{x \in \mathbb{F}_2^n} (-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{a\cdot x} \\ &= -\sum_{x \in D} (-1)^{a\cdot x} - \sum_{x \in D} (-1)^{a\cdot x} - \sum_{x \notin D} (-1)^{a\cdot x} + \sum_{x \notin D} (-1)^{a\cdot x} \\ &= -2 \sum_{x \in D} (-1)^{a\cdot x}. \end{aligned}$$

Now, consider $\sum_{x\in D}(-1)^{a\cdot x}$, we have

$$\sum_{x\in D}(-1)^{a\cdot x} = \begin{cases} -1(\#H_i^*) & \text{if } a\cdot x \neq 0 \text{ on all } H_i, \quad 1\leq i\leq k, \\ \mid H_i^* \mid -(\#H_i^*-1) & \text{if } a\cdot x = 0 \text{ on exactly one } H_i,\ 1\leq i\leq k. \end{cases}$$

Now, we have

$$W_{f_k}(a) = -2\sum_{x\in D}(-1)^{a\cdot x} = \begin{cases} 2k & \text{if } a\cdot x \neq 0 \text{ on all } H_i, \quad 1\leq i\leq k, \\ -2(2^m-k) & \text{if } a\cdot x = 0 \text{ on exactly one } H_i,\ 1\leq i\leq k. \end{cases}$$

The multiplicity of $-2(2^m-k)$ is $(2^m-1)k$ and the multiplicity of $2k$ is $2^n-((2^m-1)k+1)$. □

Now, we can compute the number of weight 4 vectors in the linear code C_{f_k} of Boolean functions f_k.

Corollary 2.14. *Assume that $f_k:\mathbb{F}_2^n\to\mathbb{F}_2$ is a Boolean function with Walsh spectrum given in Theorem 2.13. The number $\lambda(f_k)$ of weight 4 vectors in the linear code C_{f_k} is*

$$\begin{aligned}\lambda(f_k) =&\frac{1}{24}(\frac{1}{2^{n+1}}[16((2^{n-1}-2^mk+k-1)^4+(2^nk^4-2^mk^5+k^5-k^4)\\ &+k(k-2^m)^4(2^m-1))+2^{4n}]-3\cdot 2^{2n}+2^{n+1}).\end{aligned} \tag{2.6}$$

Proof. The corollary follows from Theorem 2.5 and Theorem 2.13. □

Remark 2.15. Note that for $k=2^{m-1}$, we have a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For $k=2^{m-1}-1$, the number of weight 4 vectors in the linear code C_f of partial spread Boolean functions are

$$\lambda(f_{2^{m-1}-1}) = \frac{1}{3}\left[2^{6m-4}-5\cdot 2^{4m-4}+21\cdot 2^{2m-2}-3\cdot 2^{m+2}+7\right].$$

Similarly, for $k=2^{m-1}+1$, the number of weight 4 vectors in the linear code C_f of partial spread Boolean function are

$$\lambda(f_{2^{m-1}+1}) = \frac{1}{3}\left[2^{6m-4}-5\cdot 2^{4m-4}+5\cdot 2^{2m-2}-1\right].$$

The number of weight 4 vectors in the linear code C_f of quadratic Boolean function $f_{n,2}$ are

$$\lambda(f_{n,2}) = \frac{1}{3}\left[2^{6m-4}-2^{4m-3}+2^{2m-2}\right].$$

We observe that $\lambda(f_{2^{m-1}-1}) < \lambda(f_{n,2})$ and $\lambda(f_{2^{m-1}+1}) < \lambda(f_{n,2})$, this means that for some values of k, the partial spread Boolean functions reduce more weight 4 vectors in their linear code as compared with weight 4 vectors in the linear code of plateaued Boolean functions.

In the second case, we consider m-dimensional subspaces $H_1,...,H_k$ of $\mathbb{F}_2^n$ with 0. We have the following theorem.

Theorem 2.16. *Let $n = 2m$ and $H_1, ..., H_k$ be the m-dimensional subspaces of $\mathbb{F}_2^n$. The Boolean function f_k from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is the indicator function of $D = \cup_{i=1}^k H_i$ such that $f_k(x) = 1$, if $x \in D$ and 0, otherwise. The Walsh spectrum of f_k is as follows.*

Walsh coefficient	*Multiplicity*
$2^n - 2^{m+1}k + 2k - 2$	1
$2k - 2$	$2^n - 2^m k + k - 1$
$2k - 2^{m+1} - 2$	$2^m k - k$

Proof. The proof follows the same lines of proof given in Theorem 2.13. We consider m-dimensional subspaces $H_1, ..., H_k$ of $\mathbb{F}_2^n$ with 0, so we subtract the value 2 from each of the Walsh coefficients. □

We can compute the number of weight 4 vectors in the linear code $C_{f_k'}$ of Boolean functions f_k' in the following way.

Corollary 2.17. *Assume that $f_k' : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function with Walsh spectrum as in Theorem 2.16. The number $\lambda(f_k')$ of weight 4 vectors in the linear code $C_{f_k'}$ is*

$$\begin{aligned}\lambda(f_k') =& \frac{1}{24}\Big(\frac{1}{2^{n+1}}[16((2^{n-1} - 2^m k + k - 1)^4 + (k-1)^4(2^n - 2^m k + k - 1)\\ &+ k(k - 2^m - 1)^4(2^m - 1)) + 2^{4n}] - 3 \cdot 2^{2n} + 2^{n+1}\Big).\end{aligned} \tag{2.7}$$

Proof. The corollary follows from Theorem 2.5 and Theorem 2.16. □

Remark 2.18. Note that for $k = 2^{m-1} + 1$, we have a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For $k = 2^{m-1}$, the number of weight 4 vectors in the linear code $C_{f'}$ of partial spread Boolean functions is

$$\lambda(f_{2^{m-1}}') = \frac{1}{3}\left[2^{6m-4} - 5 \cdot 2^{4m-4} + 5 \cdot 2^{2m-2} - 1\right].$$

Similarly, for $k = 2^{m-1} + 2$, the number of weight 4 vectors in the linear code C_f of partial spread Boolean functions is

$$\lambda(f_{2^{m-1}+2}') = \frac{1}{3}\left[2^{6m-4} - 5 \cdot 2^{4m-4} + 21 \cdot 2^{2m-2} - 3 \cdot 2^{m+2} + 7\right].$$

The number of weight 4 vectors in the linear code C_f of quadratic Boolean functions $f_{n,2}$ is

$$\lambda(f_{n,2}) = \frac{1}{3}\left[2^{6m-4} - 2^{4m-3} + 2^{2m-2}\right].$$

We observe that $\lambda(f_{2^{m-1}}') < \lambda(f_{n,2})$ and $\lambda(f_{2^{m-1}+2}') < \lambda(f_{n,2})$, this means that for some values of k, the partial spread Boolean functions reduce more weight 4 vectors in their linear code as compared with weight 4 vectors in the linear code of plateaued Boolean functions.

Table 2.8: Weight 4 vectors in the linear code of the partial spread Boolean functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2$

$\lambda(0) = 10416$			
k	$\lambda(f_k)$	$\lambda(f_k^{'})$	$f_{(6,2)}$
3	5117	5152	5296
4	5040	5061	5296
5	5061	5040	5296
6	5152	5117	5296

Table 2.9: Weight 4 vectors in the linear code of the partial spread Boolean functions from $\mathbb{F}_2^8$ to $\mathbb{F}_2$

$\lambda(0) = 690880$			
k	$\lambda(f_k)$	$\lambda(f_k^{'})$	$f_{(8,2)}$
6	345520	345645	346816
7	343085	343280	346816
8	342720	342805	346816
9	342805	342720	346816
10	343280	343085	346816
11	345645	345520	346816

Table 2.10: Weight 4 vectors in the linear code of the partial spread Boolean functions from $\mathbb{F}_2^{10}$ to $\mathbb{F}_2$

$\lambda(0) = 44608256$			
k	$\lambda(f_k)$	$\lambda(f_k^{'})$	$f_{(10,2)}$
13	22307445	22308096	22326016
14	22272880	22273965	22326016
15	22262061	22262960	22326016
16	22260480	22260821	22326016
17	22260821	22260480	22326016
18	22262960	22262061	22326016
19	22273965	22272880	22326016
20	22308096	22307445	22326016

Remark 2.19. The Boolean functions belong to partial spread class are good candidates for coordinate functions which can be used in the construction of APN functions using our coordinate functions approach.

In Tables 2.8, 2.9 and 2.10, we explicitly give the values of $\lambda(f_k)$ and $\lambda(f_k^{'})$ for $n = 6, 8$ and 10 respectively.

2.7 Maiorana-McFarland class

Another well known construction of bent functions is obtained by using Maiorana-McFarland class. The Maiorana-McFarland class is as follows. Let $n = 2m$ and let f be a function from $\mathbb{F}_2^m \times \mathbb{F}_2^m$ to $\mathbb{F}_2$ defined by

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

Here, π is a mapping from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$ and $h(y) : \mathbb{F}_2^m \to \mathbb{F}_2$ is any Boolean function. If $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a permutation then the function f is a bent function.
We are interested in studying the reduction in the number of weight 4 vectors in the linear code of some of the Boolean functions that belong to the Maiorana-McFarland class. The Walsh spectrum of the Maiorana-McFarland class of Boolean functions is as follows.

Theorem 2.20. *Let $n = 2m$ and f be a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ belongs to the Maiorana-McFarland class. Assume that π is not a permutation and the image of π has s elements having 2 preimages and t elements having 1 preimage. We also assume that $\mid \pi^{-1}(0) \mid = 1$ and $h(y) : \mathbb{F}_2^m \to \mathbb{F}_2$ is the zero function. The Walsh spectrum of f is as follows:*

Walsh coefficient	*Multiplicity*
0	$(2^m + 2^{m-1})s$
2^m	$2^{m-1}t + 2^{m-1}$
-2^m	$2^{m-1}t - 2^{m-1}$
2^{m+1}	$2^{m-2}s$
-2^{m+1}	$2^{m-2}s.$

Proof. We know that

$$W_f(a,b) = \sum_{x,y \in \mathbb{F}_2^m} (-1)^{x \cdot \pi(y) + a \cdot x + b \cdot y},$$

$$W_f(a,b) = \sum_{y \in \mathbb{F}_2^m} (-1)^{b \cdot y} \cdot \sum_{x \in \mathbb{F}_2^m} (-1)^{x \cdot (\pi(y) + a)}. \tag{2.8}$$

Now, we discuss different cases for the possible values of Equation (2.8).
Case 1: Assume that $\pi(y) \neq a$. This means a is not contained in the image set of

π. From Proposition 1.5, we know that

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

The equation (2.8) becomes

$$W_f(a,b)=0.$$

Now, we want to determine the multiplicity of the value $W_f(a,b)=0$. We know that the size of the image of π is $s+t$. The number of a that are not contained in the image of π is $2^m-(s+t)=2s+t-(s+t)=s$. The multiplicity of the value $\sum_{a,b\in\mathbb{F}_2^m}W_f(a,b)=0$ is $2^m s$.

Case 2: Assume that $\pi(y)=a$, which means that a is contained in the image of π. We have two different subcases. In the first subcase, a has one preimage and in the second subcase, a has two preimages. We discuss these subcases in detail.

Case 2.a: Assume that $\pi(y)=a$ with the condition $\mid\pi^{-1}(a)\mid=1$, then Equation (2.8) becomes

$$W_f(a,b)=\sum_{y\in\mathbb{F}_2^m}(-1)^{b\cdot y}\cdot\sum_{x\in\mathbb{F}_2^m}(-1)^{x\cdot(\pi(y)+a)}=2^m\left(\sum_{\pi^{-1}(a)\in\mathbb{F}_2^m}(-1)^{b\cdot\pi^{-1}(a)}\right).$$

For a fixed value of a, we assume that $\pi^{-1}(a)=0$, then the above equation becomes

$$W_f(a,b)=2^m.$$

This value has multiplicity 1. Now, we assume that $\pi^{-1}(a)\neq 0$, then $b\cdot\pi^{-1}(a)=0$ for 2^{m-1} values of b and $b\cdot\pi^{-1}(a)=1$ for 2^{m-1} values of b. Then

$$W_f(a,b)=\begin{cases}2^m & \text{if } b\cdot\pi^{-1}(a)=0,\\ -2^m & \text{if } b\cdot\pi^{-1}(a)\neq 0.\end{cases}$$

The value 2^m occurs $2^{m-1}(t+1)$ times and -2^m occurs $2^{m-1}(t-1)$ times.

Case 2.b: Now, we consider that $\pi(y)=a$ and $\mid\pi^{-1}(a)\mid=2$. This means $\pi^{-1}(a)=\{y_1,\ y_2\}$ with $y_1\neq y_2$ and $y_1,y_2\neq 0$ because $\mid\pi^{-1}(0)\mid=1$. Then Equation (2.8) becomes

$$W_f(a,b)=2^m\left(\sum_{y_1\in\mathbb{F}_2^m}(-1)^{b\cdot y_1}+\sum_{y_2\in\mathbb{F}_2^m}(-1)^{b\cdot y_2}\right). \tag{2.9}$$

Assume that $y_1,y_2\neq 0$, then we have

$$(-1)^{b\cdot y_1}+(-1)^{b\cdot y_2}=\begin{cases}2 & \text{if } b\cdot y_1=0=b\cdot y_2,\\ 0 & \text{if } b\cdot y_1\neq b\cdot y_2,\\ -2 & \text{if } b\cdot y_1=1=b\cdot y_2.\end{cases}$$

So, the equation (2.9) becomes

$$W_f(a,b) = \begin{cases} 2^{m+1} & \text{if } b \cdot y_1 = 0 = b \cdot y_2, \\ 0 & \text{if } b \cdot y_1 \neq b \cdot y_2, \\ -2^{m+1} & \text{if } b \cdot y_1 = 1 = b \cdot y_2. \end{cases}$$

The value 2^{m+1} occurs $2^{m-2}s$ times, the value 0 occurs $2^{m-1}s$ times and the value 2^{m+1} occurs $2^{m-2}s$ times. □

Now, we can compute the number of weight 4 vectors in the linear code C_f of Boolean functions belong to the Maiorana-McFarland class.

Corollary 2.21. *Assume that $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function that belongs to the Maiorana-McFarland class with Walsh spectrum given in Theorem 2.20. The number $\lambda(f)$ of weight 4 vectors in the linear code C_f is*

$$\lambda(f) = \frac{1}{24}\left[\frac{1}{2^{n+1}}\left(2^{5m}t + 2^{5m+3}s + 2^{4n}\right) - 3 \cdot 2^{2n} + 2^{n+1}\right]. \qquad (2.10)$$

Proof. The corollary follows from Theorem 2.5 and Theorem 2.20. □

Remark 2.22. Note that for $s = 0,\ t = 2^m$, we have a bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. For $s = 1,\ t = 2^m - 2$, the number of weight 4 vectors in the linear code C_f related to the Maiorana-McFarland Boolean functions is

$$\lambda(f) = \frac{1}{3}\left[2^{6m-4} - 5 \cdot 2^{4m-4} + 3 \cdot 2^{3m-3} + 2^{2m-2}\right].$$

The number of weight 4 vectors in the linear code C_f related to quadratic Boolean functions $f_{n,2}$ is

$$\lambda(f_{n,2}) = \frac{1}{3}\left[2^{6m-4} - 2^{4m-3} + 2^{2m-2}\right].$$

We observe that $\lambda(f) < \lambda(f_{n,2})$, this means that for some values of s and t, the Maiorana-McFarland Boolean functions reduce more weight 4 vectors in their linear code as compared with weight 4 vectors in the linear code of plateaued Boolean functions. The Boolean functions belong to the Maiorana-McFarland class are good candidates for coordinate functions which can be used in the construction of APN functions using our coordinate functions approach.

For small values of n, we have computed $\lambda(f)$ for Maiorana-McFarland Boolean functions which is Tables 2.11, 2.12 and 2.13.

2.8 Dobbertin APN function and Kavut et. al. Boolean function

In this section, first we consider the Dobbertin APN functions from $\mathbb{F}_{2^{10}}$ to $\mathbb{F}_{2^{10}}$. For odd values of n, the Dobbertin APN function is an APN permutation and

Table 2.11: Weight 4 vectors in the linear code of the Maiorana-McFarland Boolean functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2$

$\lambda(0) = 10416$			
s	t	$\lambda(f)$	$f_{(6,2)}$
0	8	5040	5296
1	6	5104	5296
2	4	5168	5296
3	2	5232	5296

Table 2.12: Weight 4 vectors in the linear code of the Maiorana-McFarland Boolean functions from $\mathbb{F}_2^8$ to $\mathbb{F}_2$

$\lambda(0) = 690880$			
s	t	$\lambda(f)$	$f_{(8,2)}$
0	16	342720	346816
1	14	343232	346816
2	12	343744	346816
3	10	344256	346816
4	8	344768	346816
5	6	245280	346816
6	4	345792	346816
7	2	346304	346816

Table 2.13: Weight 4 vectors in the linear code of the Maiorana-McFarland Boolean functions from $\mathbb{F}_2^{10}$ to $\mathbb{F}_2$

$\lambda(0) = 44608256$			
s	t	$\lambda(f)$	$f_{(10,2)}$
0	32	22260480	22326016
1	30	22264576	22326016
2	28	22268672	22326016
3	26	22272768	22326016
4	24	22276864	22326016
5	22	22280960	22326016
6	20	22285056	22326016
7	18	22289152	22326016
8	16	22293248	22326016
9	14	22297344	22326016
10	12	22301440	22326016
11	10	22305536	22326016
12	8	22309632	22326016
13	6	22313728	22326016
14	4	22317824	22326016
15	2	22321920	22326016

each of its component functions has the same number of weight 4 vectors in their linear codes.

For even values of n, we are interested in comparing the reduction of weight 4 vectors in the linear codes of component functions of the Dobbertin APN function, the partial spread Boolean functions as well as the Maiorana-McFarland Boolean functions.

Using MAGMA, we have computed the complete Walsh spectrum of component functions of Dobbertin function on $\mathbb{F}_{2^{10}}$. The values in brackets in Table 2.14 give the multiplicities of the Walsh coefficients and the notion $\{* \dots *\}$ denote the multiset. The numbers of weight 4 vectors in the linear code of component functions of Dobbertin function are given in Table 2.14.

We compare the reduction in the numbers of weight 4 vectors in the linear code of component functions of the Dobbertin function and the partial spread Boolean functions for $k = 14, 15, 17, 18, 19$ as well as the Maiorana-McFarland Boolean functions for $s = 1, 2, 3$. For given values of k and s, we found that the partial spread and the Maiorana-McFarland Boolean functions reduce more weight 4 vectors in their linear codes as compared with the weight 4 vectors in the linear codes of component functions of the Dobbertin APN functions.

This gives us another indication that just by looking at the reduction in the number of weight 4 vectors in the linear code, the partial spread and the Maiorana-McFarland Boolean function may serve as good candidates of coordinate functions for the construction of APN functions by using our coordinate functions approach.

In 2006, Kavut, Maitra, Sarker and Yücel [64] counted the Boolean functions from $\mathbb{F}_2^9$ to $\mathbb{F}_2$ having nonlinearity greater than 240. They found that there are 1512 Boolean functions having nonlinearity 241. All of these Boolean functions have the same Walsh Spectrum which is $\{* -30(127), -22(27), -14(36), -6(18), 2(55), 10(39), 18(15), 26(156) *\}$, here the values in the bracket denote the multiplicities and $\{* \dots *\}$ denote the multiset. We have computed the number of weight 4 vectors in linear code C_f of their boolean functions which is 2771125. We have compared it with the number of weight 4 vectors in linear code C_f of component functions of AB functions which is 2774400.

We found that the Kavut et al. Boolean functions reduces more weight 4 vectors in their linear code as compared with the weight 4 vectors in the linear code of AB component functions. So, just by looking at the reduction in the number of weight 4 vectors in their linear codes, Kavut et al. Boolean functions may be good candidates for coordinate functions which can be used in the construction of AB functions from $\mathbb{F}_{2^9}$ to $\mathbb{F}_{2^9}$ using our coordinate functions approach.

Table 2.14: Weight 4 vectors in the linear codes of the component functions of the Dobbertin function from $\mathbb{F}_{2^{10}}$ to $\mathbb{F}_2$

No. of component functions	Walsh spectrum	Weight 4 vectors
682	$\{* -48(138), -32(136), -16(210), 16(270), 32(120), 48(150)*\}$	22275840
341	$\{* - 80(3), -64(30), -48(210), -16(270), 0(180), 16(240), 48(135), 64(46)*\}$	22295296

2.9 Vectorial bent functions

In this section, we consider vectorial bent functions F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq \frac{n}{2}$ and n is even. We are interested in observing the pattern of reduction of weight 4 vectors in the linear code of vectorial bent functions.

We have discussed that bent functions are the best candidates for coordinate functions which can be used in the construction of APN functions by using our coordinate functions approach. We can compute the number of weight 4 vectors in the linear code C_F related with vectorial bent functions.

Corollary 2.23. *Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a vectorial Boolean function with n even and $m \leq \frac{n}{2}$. Let $f_1, \ldots, f_m$ be the coordinate functions of F. The function F is a vectorial bent function if and only if the number $\lambda(f_1, \ldots, f_m)$ of weight 4 vectors in the linear code $C_{f_1,\ldots,f_m}$ is*

$$\lambda(f_1, \ldots, f_m) = \frac{1}{3}\left[(2^n - 1)(2^n - 2^{m+1})2^{n-m-3}\right]. \tag{2.11}$$

Proof. This follows from Theorem 2.5 using

$$\mid W_F(a, b) \mid = 2^{n/2}$$

for all $b \neq 0$. □

We have computed the values of $\lambda(f_1, \ldots, f_{n/2})$ of vectorial bent functions for $n = 4, 6, \ldots, 20$ which are listed in Table 2.15. We compare the values of $\lambda(f_1, \ldots, f_{n/2})$ with $\lambda(0)$. We observe that for the increasing values of n, the value

$$\frac{\lambda(f_1, \ldots, f_{n/2})}{\lambda(0)} = \frac{2^{3n/2} - 2^{n+1} - 2^{n/2} + 2}{2^{2n} - 2^{n+1} - 2^n + 2}$$

tends to 0.

We observe that vectorial bent functions reduce maximum number of weight 4 vectors in their linear codes. The vectorial bent functions are the best choice for $n/2$ coordinate functions which can be used for the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with n even by using coordinate functions approach.

Table 2.15: Weight 4 vectors in the linear code of vectorial bent functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{n/2}}$

No.	n	$\lambda(0)$	$\lambda(f_1, \cdots, f_{n/2})$	Reduction Percentage = $(1 - \lambda(f_1, \cdots, f_{n/2})/\lambda(0)) * 100$
1	4	140	20	85.741
2	6	10416	1008	90.323
3	8	690880	38080	94.488
4	10	44608250	1309440	97.065
5	12	2861214720	43330560	98.486
6	14	183218384896	1409200128	99.231
7	16	11727587164160	45454376960	99.612
8	18	750591347982336	1460283310080	99.805
9	20	48038258586419200	46820825497600	99.903

Table 2.16: Walsh Spectrum of component functions of the Dillon APN Permutation

No.	Walsh Spectrum	Number of Component functions
1	$\{* -16(6),\ 0(48),\ 16(10)*\}$	7
2	$\{* -16(2),\ -8(20), 0(12),\ 8(28), 16(2)*\}$	21
3	$\{* -8(24),\ 0(12),\ 8(24),\ 16(4)*\}$	7
4	$\{* -16,\ -8(22),\ 0(12),\ 8(28),\ 16(3)*\}$	21
5	$\{* -16(3),\ -8(18),\ 0(12),\ 8(30),\ 16*\}$	7

2.10 APN Permutation

In 2009, Dillon [58] introduced the first APN permutation F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ defined by
$F(x) = a^{45}x^{60} + a^{41}x^{58} + a^{43}x^{57} + a^{4}x^{56} + a^{50}x^{54} + a^{20}x^{53} + a^{45}x^{52} + a^{20}x^{51} + a^{23}x^{50} + a^{36}x^{49} + a^{56}x^{48} + a^{21}x^{46} + a^{5}x^{45} + a^{21}x^{44} + a^{28}x^{43} + a^{3}x^{42} + a^{59}x^{41} + a^{58}x^{40} + a^{57}x^{39} + a^{53}x^{38} + a^{37}x^{37} + a^{40}x^{36} + a^{18}x^{35} + a^{41}x^{34} + a^{54}x^{33} + a^{3}x^{32} + a^{49}x^{30} + a^{41}x^{29} + a^{42}x^{28} + a^{50}x^{27} + a^{53}x^{26} + a^{58}x^{25} + a^{9}x^{24} + x^{23} + a^{28}x^{22} + a^{3}x^{21} + a^{21}x^{20} + a^{52}x^{19} + a^{60}x^{17} + a^{59}x^{16} + a^{10}x^{15} + a^{42}x^{13} + a^{8}x^{12} + a^{35}x^{11} + a^{44}x^{10} + a^{45}x^{8} + a^{8}x^{7} + a^{61}x^{6} + a^{59}x^{5} + a^{20}x^{4} + a^{12}x^{3} + a^{37}x^{2} + a^{2}x,$
where a is a primitive element of $\mathbb{F}_{2^6}$.
We are interested in observing the pattern of reduction of number of weight 4 vectors in the linear code C_f of component functions of the Dillon APN permutation. We computed the Walsh coefficients along with the multiplicities of component functions of Dillon APN permutation using MAGMA. These values are given in Table 2.16. The values in the brackets in Table 2.16 give the multiplicities of Walsh coefficients and the notion $\{* \ldots *\}$ denote the multiset. We made several random choices for the selection of component functions of F. We

observed that after the choice of the first component function, approximately half (i.e. 5312) of the weight 4 vectors out of the total (i.e. 10416) weight 4 vectors are reduced. Similarly, after the choice of second component function, approximately half of the remaining weight 4 vectors are reduced. This reduction pattern continues until the choice of the fifth component function. After the choice of the sixth component function, we have no weight 4 vectors in the linear code C_F. It is interesting to observe that approximately half of the weight 4 vectors are reduced in each steps. This reduction pattern is the same for all our random choices of component functions.

Chapter 3

Classes of vectorial bent functions contained in known quadratic APN functions

We discussed in Section 2.9 that vectorial bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq \frac{n}{2}$ reduce the maximum number of weight 4 vectors in their linear code. In our coordinate function approach, we can choose vectorial bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ with $m \leq \frac{n}{2}$ as the first m coordinate functions out of n coordinate functions. We need to choose other m coordinate functions in such a way that there are no weight 4 vectors in the linear code $C_{f_1,\ldots,f_n}$. Then, we can construct APN functions. Note that the first m coordinate functions generate a subspace which is contained in the vectorspace generated by the n coordinate functions.
In this Chapter, we are interested in studying the construction of known APN functions by using our proposed coordinate function approach. So, we study the classes of vectorial bent functions contained in the known APN functions. The Dobbertin function is an example of an APN function which has no bent components. We consider the known classes of quadratic APN functions from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$. In Section 3.1, we completely classify the quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$. In Section 3.2, we discuss one problem.

3.1 *Case $n = 6$*

In this Section, we investigate the vectorial bent functions contained in the APN functions listed in Table 1.5.
First, we discuss the known classes of quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$ and $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$. Then, we discuss the algebraic representation of these classes. Finally, we discuss which vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$ and $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$ are contained in Dillon APN functions from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$.
In 2009, Budaghyan and Carlet [26] published a paper about the equivalence of

vectorial bent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ with $m \leq \frac{n}{2}$. They proved that the CCZ-equivalence of vectorial bent functions is the same as their EA-equivalence. In the subsequent section, we use the term equivalence for the CCZ-equivalence. Up to equivalence there is only one quadratic bent function from $\mathbb{F}_2^6$ to $\mathbb{F}_2$, see [8]. The interesting cases are quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$ and $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$. Using MAGMA, it is not difficult to show the following theorem.

Theorem 3.1. *There are only three (up to equivalence) quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$ and only one (up to equivalence) quadratic vectorial bent function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$.*

We have no nice algebraic representation of the quadratic vectorial bent function F from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$ but the matrices associated with the quadratic forms of each bent function are as follows.

$$Q_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad Q_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The matrices Q_1 and Q_2 generate a vectorspace of matrices over $\mathbb{F}_2$. We have

$$F(x) = \begin{pmatrix} xQ_1x^T \\ xQ_2x^T \end{pmatrix} = \begin{pmatrix} x_1x_2 + x_1x_6 + x_2x_4 + x_3x_4 + x_4x_5 + x_5x_6 \\ x_1x_3 + x_1x_6 + x_2x_4 + x_2x_5 + x_3x_5 \end{pmatrix}$$

where $x = (x_1, \ldots, x_6) \in \mathbb{F}_2^6$ is a row vector.

We have identified the algebraic representation of two out of three quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$. The first quadratic vectorial bent function F_1 belongs to the following class of quadratic vectorial bent functions expressed in trace representation [52]: Let $n = 2m, n \equiv 2 \mod 4, d = 2^i + 1$ with $gcd(i,n) = 1$ and $w \notin (\mathbb{F}_{2^n})^3$. The function

$$G_1(x) = Tr_m^n(wx^d)$$

is a vectorial bent function, where $Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{im}}$. In our case, we have $i = 1, d = 3, n = 6$ and $m = 3$.

The second quadratic vectorial bent function F_2 belongs to the following class of quadratic vectorial bent function: if $n = 2m$, the function

$$G_2(x,y) = xy$$

is a vectorial bent function from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.

We have no nice algebraic representation for the third quadratic vectorial bent

Table 3.1: Occurrence of 3 dimensional vectorial bent functions in the Dillon APN functions

No.	D.1	D.2	D.3	D.4	D.5	D.6	D.7	D.8	D.9	D.10	D.11	D.12	D.13
F_1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
F_2		✓			✓				✓				
F_3			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

function F_3 but the matrices associated with the quadratic forms of each bent function are listed below:

$$Q_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, Q_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, Q_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The matrices Q_1, Q_2 and Q_3 generate a vectorspace of matrices over $\mathbb{F}_2$. We have

$$F_3(x) = \begin{pmatrix} F(x) \\ xQ_3x^T \end{pmatrix} = \begin{pmatrix} F(x) \\ x_1x_4 + x_1x_6 + x_2x_5 + x_3x_5 + x_3x_6 + x_4x_5 + x_5x_6 \end{pmatrix},$$

Note that quadratic vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$ contain the (unique) quadratic vectorial bent function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$. Now, we want to analyse in which Dillon APN functions these three vectorial bent functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2^3$ are contained.

From Table 3.1, it is interesting to observe that F_1 is contained in all Dillon APN functions listed in Table 1.5, while F_2 has minimum number of occurrences in these functions. We also computed the order of automorphism groups of linear codes of F_1, F_2 and F_3. The order of automorphism groups of the function F_1 is 4032, F_2 is 677376 and F_3 is 10752.

In 2009, Edel and Pott [30] found a sporadic example of a nonquadratic APN function F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ defined as $F(x) = x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + u^{14}(Tr_1^6(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + u^{18}x^9 + u^{36}x^{18} + u^{72}x^{36} + x^{21} + x^{42})$, where u is a primitive root of $\mathbb{F}_{2^6}$. We observe that the quadratic vectorial bent functions F_1 and F_3 are also contained in this nonquadratic APN function.

Remark 3.2. There are 23 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$ which are listed in Table 9 [30]. Recently, Yu, Wang and Li [7] have constructed 8157 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$. In total, we have 8180 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$. It is computationally very intensive to investigate the classes of quadratic vectorial bent functions contained in 8180 quadratic APN function.

3.2 Open problem

In this section, we discuss an open problem that arises from our computational results of Section 3.1. First, we want to prove that the quadratic vectorial bent function defined in [52] is contained in the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x) = x^3$. In order to prove this result, we need the following preliminary result. This preliminary result is also mentioned in Theorem 2.2.10 [65].

Theorem 3.3. *[65, 66] Let $\alpha \in \mathbb{F}_{2^n}$, $i \in \mathbb{N}$, $d = 2^i + 1$. The function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ with $f(x) = Tr_1^n(\alpha x^d)$ is bent if and only if $\alpha \notin \{x^d : x \in \mathbb{F}_{2^n}\}$.*

Proof. Assume that $\alpha \notin \{x^d : x \in \mathbb{F}_{2^n}\}$. For any $x, w \in \mathbb{F}_{2^n}$ we have

$$(x+w)^{2^i+1} = (x+w)^{2^i}(x+w) = (x^{2^i}+w^{2^i})(x+w) = x^{2^i+1}+x^{2^i}w+xw^{2^i}+w^{2^i+1}.$$

Now, for any $a, w \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}
W_f(a) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha x^d)+Tr_1^n(ax)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha((x+w)^{2^i+1}+x^{2^i}w+xw^{2^i}+w^{2^i+1}))+Tr_1^n(ax)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha((x+w)^d+x^{2^i}w+xw^{2^i}+w^d))+Tr_1^n(ax)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha(x+w)^d+\alpha x^{2^i}w+\alpha xw^{2^i}+\alpha w^d+ax)}
\end{aligned}$$

Assume that we can choose w independent of a such that for all $x \in \mathbb{F}_{2^n}$, we have

$$Tr_1^n(\alpha x^{2^i}w + \alpha xw^{2^i} + ax) = 0. \tag{3.1}$$

Then, we have

$$\begin{aligned}
W_f(a) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha(x+w)^d+\alpha w^d)} \\
&= (-1)^{Tr_1^n(\alpha w^d)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha(x+w)^d} \\
&= (-1)^{Tr_1^n(\alpha w^d)} \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha(x)^d} \\
&= (-1)^{Tr_1^n(\alpha w^d)} W_f(0).
\end{aligned}$$

Thus, the Walsh coefficients of f would have constant absolute value. By Theorem 1.6, the Walsh spectrum of f would therefore consist entirely of the values

$\pm 2^{\frac{n}{2}}$, hence f would be bent. Therefore, we consider the linear equation (3.1),

$$\begin{aligned} Tr_1^n(\alpha x^{2^i} w + \alpha x w^{2^i} + ax) &= 0 \\ Tr_1^n(\alpha x^{2^i} w + (\alpha x w^{2^i})^{2^i} + (ax)^{2^i}) &= 0 \\ Tr_1^n(\alpha x^{2^i} w + \alpha^{2^i} x^{2^i} w^{2^{2i}} + a^{2^i} x^{2^i}) &= 0 \\ Tr_1^n(x^{2^i}(\alpha w + \alpha^{2^i} w^{2^{2i}} + a^{2^i})) &= 0 \end{aligned}$$

This can be true for all $x \in \mathbb{F}_{2^n}$ if

$$\alpha w + \alpha^{2^i} w^{2^{2i}} + a^{2^i} = 0$$

In order to choose w properly, we have to prove that the mapping

$$w \rightarrow \alpha w + \alpha^{2^i} w^{2^{2i}}$$

must be bijective, that means the mapping has a trivial kernel if $\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^n}\}$. For $w \neq 0$, we have

$$\alpha w + \alpha^{2^i} w^{2^{2i}} = 0,$$

this impies that

$$\begin{aligned} \alpha^{2^i} w^{2^{2i}} &= \alpha w \\ w^{2^{2i}-1} &= \alpha^{1-2^i}, \end{aligned}$$

hence, we have

$$(w^{2^i+1})^{2^i-1} = (\alpha^{-1})^{2^i-1}.$$

As $gcd(2^i+1, 2^i-1) = 1$, the left hand side of the above equation is a d-th power while the right hand side of the above equation is a d-th power if and only if α is a d-th power which is a contradiction. Thus, whenever α is not a d-th power, the function f is bent.

Now, let us consider $\alpha \in \{x^d : x \in \mathbb{F}_{2^n}\}$. Suppose furthermore that f is bent. Clearly, f must be non-zero, therefore we may write $\alpha = \beta^d$ for some $\beta \in \mathbb{F}_{2^n}^*$. Then

$$f(x) = Tr_1^n(\alpha x^d) = Tr_1^n((\beta x)^d).$$

The above equation shows that the function f is bent for any choice of $\alpha \in \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Since we have proved earlier that f is bent for all $\alpha \notin \{x^d : x \in \mathbb{F}_{2^n}\}$, we conclude that f is bent for all $\alpha \in \mathbb{F}_{2^n}^*$, which is impossible. Assume that f is bent for every $\alpha \in \mathbb{F}_{2^n}^*$, this would allow the construction of a vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ which contradicts the Nyberg bound. □

Corollary 3.4. *Let $\alpha \in \mathbb{F}_{2^n}$, $d = 3$. The function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by*

$$f(x) = Tr_1^n(\alpha x^3)$$

is bent if and only if $\alpha \notin \{x^3 : x \in \mathbb{F}_{2^n}\}$.

Proof. For $i = 1$, the corollary follows the same line of proof given in Theorem 3.3. □

Theorem 3.5. *[19] Let $n = 2m$ and G be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$ defined as*

$$G(x) = (Tr_1^n(\beta_1 w x^3), \dots, Tr_1^n(\beta_m w x^3)),$$

where $(\beta_1, \dots, \beta_m)$ is a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and $w \notin (\mathbb{F}_{2^n})^3$. If $n \equiv 0$ mod 4, then G is not a vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$. If $n \equiv 2$ mod 4, then G is a vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$.

Proof. Assume that $n \equiv 0$ mod 4, in this case $gcd(3, 2^m - 1) = 3$. $\mathbb{F}_{2^m}$ consists of cube and non-cubes. If we choose $w \in \mathbb{F}_{2^n}$ which is not a cube, then nonzero elements of the vectorspace $A = w\mathbb{F}_{2^m}$ which are cubes turn into non-cubes and non-cubes turns into cubes. From Corollary 3.4, we note that some of the component functions $Tr_1^n(\alpha x^3)$ are bent, where $\alpha \in A \setminus \{0\}$ is not a cube and some of the component functions $Tr_1^n(\alpha x^3)$ are non-bent, where $\alpha \in A \setminus \{0\}$ is a cube. It means that the vectorspace A does not lead to the construction of vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$.
On the other hand, assume that $n \equiv 2 \; mod \; 4$, in this case $gcd(3, 2^m - 1) = 1$. $\mathbb{F}_{2^m}$ consists of cubes only. If we choose $w \in \mathbb{F}_{2^n}$ which is not a cube then all the nonzero elements of the vectorspace $A = w\mathbb{F}_{2^m}$ are non-cubes. From Corollary 3.4, all the component functions $Tr_1^n(\alpha x^3), \alpha \in A \setminus \{0\}$ are bent. This leads to a vectorial bent function $G(x) = (Tr_1^n(\alpha_1 x^3), \dots, Tr_1^n(\alpha_m x^3)) = (Tr_1^n(\beta_1 w x^3), \dots, Tr_1^n(\beta_m w x^3)) \in \mathbb{F}_2^m$, where $(\beta_1, \dots, \beta_m)$ is a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. □

From Table 1.6, we have an APN function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by

$$F(x) = x^3 + Tr_1^n(x^9).$$

It is CCZ-inequivalent with Gold APN function $F(x) = x^3$ for $n \geq 7$. The function $F(x) = x^3 + Tr_1^n(x^9)$ is obtained by applying the switching approach on Gold APN function $F(x) = x^3$. We have proved in Theorem 3.5 that the vectorial bent function G is contained in the Gold APN function $F(x) = x^3$ if $n \equiv 2$ mod 4. We leave the following problem as an open problem.

Problem 3.1. Is the vectorial bent function G defined in Theorem 3.5 is also contained in the function $F(x) = x^3 + Tr_1^n(x^9)$ for $n \geq 8$ with $n \equiv 2$ mod 4?

Chapter 4

Local changes in the quadratic APN cube

In this chapter, we describe the derivative of quadratic homogeneous vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ in terms of a cube of dimension $n \times n \times m$ in Section 4.1. In Section 4.2, we discuss the Yu, Wang and Li [7] approach. Yu, Wang and Li constructed several new quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$. We give a different point of view of the Yu, Wang and Li approach using a cube over $\mathbb{F}_2$ of dimension $n \times n \times n$. Another possible approach for the construction of new APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ was introduced by John Dillon [55]. Dillon named this approach *Switching Approach*. In Section 4.3, we study the switching approach in detail. In Section 4.4, we also discuss the local changes in the quadratic APN cube. In Section 4.5, we give our computational results.

4.1 Cube of dimension $n \times n \times m$

First, we discuss the basics of cubical array of dimension n. A *cube* C is defined over $\mathbb{F}_2$ as an $n \times n \times n$ ordered set of elements of $\mathbb{F}_2$. The (i, j, k)-th entry of C is denoted by C_{ij}^k, where $1 \le i, j, k \le n$.
We use the notation similar to C_{ij}^k for matrices. Given a matrix M, let M_{ij} denote the (i, j)-th entry of M. It is quite often useful to construct matrices from the entries of a cube. Given a cube C, we define the following matrices by fixing an index of C, here $*$ denote the variable index :

$$C_{**}^k = M \;\Leftrightarrow\; C_{ij}^k = M_{ij},$$

in this case, k is the fixed index and i, j are variable indices.

$$C_{i*}^* = M \;\Leftrightarrow\; C_{ij}^k = M_{kj},$$

in this case, i is the fixed index and k, j are variable indices.

$$C_{*j}^* = M \;\Leftrightarrow\; C_{ij}^k = M_{ik},$$

in this case, j is the fixed index and i, k are variable indices.
We are interested in interpreting the derivative of a quadratic homogeneous vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ in terms of a cube of dimension $n \times n \times m$. We may abuse the word cube in order to describe the derivative of quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ because a cube has always dimension $n \times n \times n$.
Let F be a quadratic homogeneous vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. The function F is defined as

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix} = \begin{pmatrix} xQ_1x^T \\ \vdots \\ xQ_mx^T \end{pmatrix}$$

where $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $Q_1, \ldots, Q_m$ are the corresponding coefficient matrices of quadratic homogeneous Boolean functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \ldots, m$. A nice property of a quadratic function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is that the mapping

$$x \mapsto F(x+a) + F(x) + F(a)$$

is always linear. If we want to find the number of solutions of $F(x+a) + F(x) = b$, then we just need to check the dimension of the kernel of the linear mapping $x \mapsto F(x+a) + F(x) + F(a)$.
First, we compute the derivative of the Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with respect to $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n \setminus \{0\}$. In this chapter, we assume that $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is a row vector.

Lemma 4.1. *Let f be a quadratic homogeneous Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ defined by the quadratic form $f(x) = xQx^T$, where Q is the upper right triangular matrix with zero diagonal and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is a row vector. Then*

$$D_af(x) = xCa^T, \text{ where } C = Q + Q^T,$$

or

$$D_af(x) = \sum_{j=1}^{n} x_j (\sum_{k=1}^{n} c_{jk} a_k).$$

Proof. Let $f(x) = xQx^T$ be a quadratic function. The mapping $D_af(x) = f(x+a) + f(x) + f(a)$ is linear mapping. We have

$$\begin{aligned}
D_a f(x) &= f(x+a) + f(x) + f(a) \\
&= (x+a)Q(x+a)^T + xQx^T + aQa^T \\
&= (x+a)Q(x^T + a^T) + xQx^T + aQa^T \\
&= xQx^T + xQa^T + aQx^T + aQa^T + xQx^T + aQa^T \\
&= xQa^T + aQx^T \\
&= xQa^T + (aQx^T)^T \\
&= xQa^T + xQ^T a^T \\
&= x(Q + Q^T)a^T \\
&= xCa^T, \text{where } C = Q + Q^T \\
&= (x_1, \ldots, x_n) \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.
\end{aligned}$$

In other words,

$$\begin{aligned}
D_a f(x) &= (x_1, \ldots, x_n)(c_{11}a_1 + \ldots + c_{1n}a_n, \ldots, c_{n1}a_1 + \ldots + c_{nn}a_n) \\
&= (x_1, \ldots, x_n)(\sum_{k=1}^{n} c_{1k}a_k, \sum_{k=1}^{n} c_{2k}a_k, \ldots, \sum_{k=1}^{n} c_{nk}a_k) \\
D_a f(x) &= \sum_{j=1}^{n} x_j (\sum_{k=1}^{n} c_{jk}a_k).
\end{aligned}$$

□

Now, it is meaningful to describe the derivative of quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ in terms of cube of dimension $n \times n \times m$.

Theorem 4.2. *Let F be a quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ defined by*

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix} = \begin{pmatrix} xQ_1x^T \\ \vdots \\ xQ_mx^T \end{pmatrix},$$

where $f_1(x), \ldots, f_m(x)$ are quadratic Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then $D_aF(x)$ is

$$D_aF(x) = \left(\sum_{i=1}^n x_i(\sum_{j=1}^n C_{ij}^1 a_j), \ldots, \sum_{i=1}^n x_i(\sum_{j=1}^n C_{ij}^m a_j)\right),$$

where

$$C^1 = Q_1 + Q_1^T, \ldots, C^m = Q_m + Q_m^T,$$

$a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n \setminus \{0\}$. For $k = 1, \ldots, m$, the matrix C_{**}^k corresponds to the coordinate function f_k of F. For $j = 1, \ldots, n$, $D_aF(x)$ is given by the non-zero linear combinations of matrices C_{*j}^*.

Proof. From lemma 4.1, we have

$$D_aF(x) = \left(\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^1 a_j), \ldots, \sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^m a_j)\right), \tag{4.1}$$

where $x \in \mathbb{F}_2^n$, $a \in \mathbb{F}_2^n \setminus \{0\}$. We observe that for $1 \leq k \leq m,\ 1 \leq i,j \leq n$, C_{ij}^k is a symmetric matrix with zero diagonal.
We can view these m matrices each having dimension $n \times n$ as a cube C of dimension $n \times n \times m$.
For $k = 1, \ldots, m$, the matrix C_{**}^k corresponds to the coordinate function f_k of F.
Consider $\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^1 a_j)$ from equation (4.1) which can be described as

$$\begin{aligned}
\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^1 a_j) &= (x_1, \ldots, x_n) \begin{pmatrix} c_{11}^1 & c_{12}^1 & \ldots & c_{1n}^1 \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1}^1 & c_{n2}^1 & \ldots & c_{nn}^1 \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \\
&= (x_1, \ldots, x_n) \begin{pmatrix} c_{11}^1 a_1 + c_{12}^1 a_2 + \ldots + c_{1n}^1 a_n \\ \vdots \\ c_{n1}^1 a_1 + c_{n2}^1 a_2 + \ldots + c_{nn}^1 a_n \end{pmatrix} \\
&= (x_1, \ldots, x_n) \left(a_1 \begin{pmatrix} c_{11}^1 \\ c_{21}^1 \\ \vdots \\ c_{n1}^1 \end{pmatrix} + a_2 \begin{pmatrix} c_{12}^1 \\ c_{22}^1 \\ \vdots \\ c_{n2}^1 \end{pmatrix} + \ldots + a_n \begin{pmatrix} c_{1n}^1 \\ c_{2n}^1 \\ \vdots \\ c_{nn}^1 \end{pmatrix} \right).
\end{aligned}$$

Now, consider $\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^2 a_j)$ from equation (4.1) which can also be described as

$$\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^2 a_j) = (x_1, \ldots, x_n) \left(a_1 \begin{pmatrix} c_{11}^2 \\ c_{21}^2 \\ \vdots \\ c_{n1}^2 \end{pmatrix} + a_2 \begin{pmatrix} c_{12}^2 \\ c_{22}^2 \\ \vdots \\ c_{2n}^2 \end{pmatrix} + \ldots + a_n \begin{pmatrix} c_{1n}^2 \\ c_{2n}^2 \\ \vdots \\ c_{nn}^2 \end{pmatrix} \right).$$

Similarly, consider $\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^m a_j)$ from equation (4.1) which can also be described as

$$\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^m a_j) = (x_1, \ldots, x_n) \left(a_1 \begin{pmatrix} c_{11}^m \\ c_{21}^m \\ \vdots \\ c_{n1}^m \end{pmatrix} + a_2 \begin{pmatrix} c_{12}^m \\ c_{22}^m \\ \vdots \\ c_{n2}^m \end{pmatrix} + \ldots + a_n \begin{pmatrix} c_{1n}^m \\ c_{2n}^m \\ \vdots \\ c_{nn}^m \end{pmatrix} \right).$$

Combining all these equations, we get

$$D_aF(x) = (x_1, \ldots, x_n) \left(a_1 \begin{pmatrix} c_{11}^1 & c_{11}^2 & \ldots & c_{11}^m \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1}^1 & c_{n1}^2 & \ldots & c_{n1}^m \end{pmatrix} + a_2 \begin{pmatrix} c_{12}^1 & c_{12}^2 & \ldots & c_{12}^m \\ \vdots & \vdots & \vdots & \vdots \\ c_{n2}^1 & c_{n2}^2 & \ldots & c_{n2}^m \end{pmatrix} + \ldots \right.$$

$$+a_n \begin{pmatrix} c_{1n}^1 & c_{1n}^2 & \dots & c_{1n}^m \\ \vdots & \vdots & \vdots & \vdots \\ c_{nn}^1 & c_{nn}^2 & \dots & c_{nn}^m \end{pmatrix}.$$

Since $(a_1, \dots, a_n) \in \mathbb{F}_2^n \setminus \{0\}$, the $D_aF(x)$ of F with respect to a is given by nonzero linear combinations of matrices C_{*j}^* for $j = 1, \dots, n$. □

Remark 4.3. The matrices C_{**}^k, $k = 1, \dots, m$ are symmetric matrices with diagonal entries zero. The rank distribution of all possible nonzero linear combinations of the matrices C_{**}^k, $k = 1, \dots, m$ determine the Walsh spectrum of F [6].
The rank distribution of all possible nonzero linear combinations of the matrices $C_{*j}^*, j = 1, \dots, n$ determine the number of solutions of $F(x+a) + F(x) + F(a) = 0$.

Example 4.4. Let F be a quadratic homogeneous Boolean function from $\mathbb{F}_2^4$ to $\mathbb{F}_2^3$ defined by

$$F(x_1, x_2, x_3, x_4) = \begin{pmatrix} f_1(x_1, x_2, x_3, x_4) \\ f_2(x_1, x_2, x_3, x_4) \\ f_3(x_1, x_2, x_3, x_4) \end{pmatrix},$$

where $f_1(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_3 + x_2x_4$, $f_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_3x_4$, $f_3(x_1, x_2, x_3, x_4) = x_2x_4 + x_3x_4$. As, f_1, f_2, f_3 are quadratic homogeneous Boolean functions from $\mathbb{F}_2^4$ to $\mathbb{F}_2$. We can write them in terms of quadratic forms.

$$f_1(x) = xQ_1x^T = (x_1, x_2, x_3, x_4) \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_2(x) = xQ_2x^T = (x_1, x_2, x_3, x_4) \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_3(x) = xQ_3x^T = (x_1, x_2, x_3, x_4) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Then $D_aF(x)$ with $a \in \mathbb{F}_2^n \setminus \{0\}$ is

$$D_aF(x) = \left(\sum_{i=1}^4 x_i \left(\sum_{j=1}^4 c_{ij}^1 a_j \right), \sum_{i=1}^4 x_i \left(\sum_{j=1}^4 c_{ij}^2 a_j \right), \sum_{i=1}^4 x_i \left(\sum_{j=1}^4 c_{ij}^3 a_j \right) \right) \quad (4.2)$$

Note that

$$C_{**}^1 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; C_{**}^2 = Q_2 + Q_2^T = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$C^3_{**} = Q_3 + Q_3^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Here, $C^k_{**},\ k = 1,2,3$ are symmetric matrices of dimension 4×4 with main diagonal entries zero. If we consider matrices in the cube $C^k_{**},\ k = 1,2,3$, then these matrices correspond exactly to the coordinate functions $f_1,\ f_2,\ f_3$.

We consider the equation $\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^1_{ij} a_j)$ from equation (4.2), which can be described as

$$\sum_{i=1}^{4} x_i(\sum_{j=1}^{4} c^1_{ij} a_j) = (x_1, x_2, x_3, x_4) \left(a_1 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + a_3 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_4 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right).$$

Consider the equation $\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^2_{ij} a_j)$ from equation (4.2), which can be described as

$$\sum_{i=1}^{4} x_i(\sum_{j=1}^{4} c^2_{ij} a_j) = (x_1, x_2, x_3, x_4) \left(a_1 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_3 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} + a_4 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right).$$

Finally, consider the equation $\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^3_{ij} a_j)$ from equation (4.2), which can be described as

$$\sum_{i=1}^{4} x_i(\sum_{j=1}^{4} c^3_{ij} a_j) = (x_1, x_2, x_3, x_4) \left(a_1 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + a_4 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right).$$

After combining $\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^1_{ij} a_j)$,$\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^2_{ij} a_j)$ and $\sum_{i=1}^4 x_i(\sum_{j=1}^4 c^3_{ij} a_j)$, we get

$$D_a F(x) = (x_1, x_2, x_3, x_4) \left(a_1 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \cdots + a_4 \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \right).$$

Since $(a_1, a_2, a_3, a_4) \in \mathbb{F}_2^4 \setminus \{0\}$, the $D_a F(x)$ is given by the nonzero linear combinations of the matrices C^*_{*j} for $j = 1, \ldots, 4$.

Quadratic APN cube (QAC)

Now, we consider quadratic homogeneous vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We are interested in studying the APN property of quadratic homogeneous vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in terms of a cube of dimension

$n \times n \times n$.

Let F be a quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}, \ x \in \mathbb{F}_2^n.$$

Then, C_{ij}^k, $1 \le i,j,k \le n$ is called *Quadratic APN Cube* (QAC) if and only if it satisfies the following two conditions.

- For $k = 1, \ldots, n$, each matrix C_{**}^k is symmetric with main diagonal entries are zero.

- For $j = 1, \ldots, n$, every nonzero linear combination of matrices C_{*j}^* has rank $n-1$.

Theorem 4.5. *Let F be a quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by*

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix},$$

where $f_1(x), \ldots, f_n(x)$ are quadratic homogeneous Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then

$$\Lambda_F = \max_{\substack{a,b \in \mathbb{F}_2^n \\ a \neq 0}} \mid \{x \in \mathbb{F}_2^n : F(x+a) + F(x) = b\} \mid = 2^k$$

if and only if the smallest rank of any nonzero linear combination of n matrices C_{*j}^*, $j = 1, \ldots, n$, is $n-k$. In particular, F is APN on $\mathbb{F}_2^n$ if and only if $C_{ij}^k, 1 \le i,j,k \le n$ is a quadratic APN cube.

Proof. Let

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}.$$

We define

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

Note that $D_aF(x)$ is a linear function. In order to find the maximum number of solutions of $D_aF(x) = 0$, we need to find the maximum dimension of the kernel of $D_aF(x)$ for all $a \in \mathbb{F}_2^n \setminus \{0\}$.

It means that $\Lambda_F = 2^k$ if and only if

$$\max\{dim(Ker(D_aF(x))) \mid a \in \mathbb{F}_2^n, a \neq 0\} = k.$$

From Theorem 4.2, we know that

$$D_aF(x) = \left(\sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^1 a_j), \dots, \sum_{i=1}^n x_i(\sum_{j=1}^n c_{ij}^m a_j)\right).$$

We can write the above equation as

$$D_aF(x) = (x_1, \dots, x_n)\left(a_1\begin{pmatrix} c_{11}^1 & c_{11}^2 & \dots & c_{11}^n \\ \vdots & \vdots & \vdots & \vdots \\ c_{1n}^1 & c_{1n}^2 & \dots & c_{1n}^n \end{pmatrix} + a_2\begin{pmatrix} c_{12}^1 & c_{12}^2 & \dots & c_{12}^n \\ \vdots & \vdots & \vdots & \vdots \\ c_{n2}^1 & c_{n2}^2 & \dots & c_{n2}^n \end{pmatrix} + \dots\right.$$
$$\left. + a_n\begin{pmatrix} c_{1n}^1 & c_{1n}^2 & \dots & c_{1n}^n \\ \vdots & \vdots & \vdots & \vdots \\ c_{nn}^1 & c_{nn}^2 & \dots & c_{nn}^n \end{pmatrix}\right).$$

Then $D_aF(x)$ is given by the nonzero linear combinations of the matrices C_{*j}^* for $j = 1, \dots, n$. The rank of the matrix obtained from the nonzero linear combinations of matrices C_{*j}^* for $j = 1, \dots, n$ actually determine the number of solutions of $D_aF(x) = 0$.

For all $a \in \mathbb{F}_2^n \setminus \{0\}$, if the matrix obtained from the nonzero linear combination of the matrices C_{*j}^* for $j = 1, \dots, n$ has rank n, then $D_aF(x) = 0$ has a unique solution. This is impossible because if x is a solution of $D_aF(x) = 0$, then $x + a$ is another solution of $D_aF(x) = 0$. Similarly, for all $a \in \mathbb{F}_2^n \setminus \{0\}$, if the matrix obtained from the nonzero linear combinations of matrices C_{*j}^* for $j = 1, \dots, n$. has rank $n - k$ then $D_aF(x) = 0$ has 2^k solutions. Thus, $\Lambda_F = 2^k$ if and only if the maximum number of solutions of $D_aF(x) = 0$ is 2^k for $a \in \mathbb{F}_2^n \setminus \{0\}$.

Note that C_{**}^k, $k = 1, \dots, n$ are symmetric $n \times n$ matrices with main diagonal entries are zero. Consequently, a quadratic homogeneous vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is APN if and only if C_{ij}^k, $1 \le i, j, k \le n$ is a quadratic APN cube. □

Remark 4.6. We have discussed the derivative of a quadratic homogeneous vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ in terms of a cube of dimension $n \times n \times m$. Assume that $n = m$, the derivative of a quadratic homogeneous APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is described in terms of a cube of dimension $n \times n \times n$ which is called QAC.

On the other hand, assume that $m \le n/2$, then the derivative of a quadratic homogeneous vectorial bent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ can also be described in terms of a cube C_{ij}^k, $1 \le k \le m$, $1 \le i, j \le n$ of dimension $n \times n \times m$. The cube C_{ij}^k is called a *Quadratic Vectorial Bent Cube* (QVBC) if and only if it satisfies the following two conditions.

- For $k = 1, \dots, m$, each matrix C_{**}^k is symmetric with main diagonal entries are zero and every non-zero linear combination of the matrices C_{**}^k has rank n.

- For $j = 1, \ldots, n$, every non-zero linear combination of the matrices C^*_{*j} has rank m.

In 2013, Yu, Wang and Li [7] proposed a guess and determine approach which they used to construct several CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$. In their approach, they modified certain elements of QAC $C^k_{ij}, 1 \leq i, j,$ $k \leq n$ to obtain a new QAC $D^k_{ij},\ 1 \leq i, j, k \leq n$. Now, we discuss the Yu, Wang and Li approach in detail.

4.2 Yu, Wang and Li (YWL) approach

First, we discuss a very important property of QAC which is used by YWL in their guess and determine approach for the construction of new quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$.
Let $C^k_{ij}, k = 1, \ldots, n,\ i = 1, \ldots, r,\ j = 1, \ldots, s$ be a $r \times s \times n$ cube with $r = s$ and $r, s \leq n$. The cube C^k_{ij} is called a *proper cube* if every non-zero linear combination of $C^*_{*j},\ j = 1, \ldots, s$ of dimension $r \times n$ has rank $r - 1$. We explain this property with the help of the following example.

Example 4.7. Let F be the quadratic APN function from $\mathbb{F}_{2^4}$ to $\mathbb{F}_{2^4}$ defined by $F(x) = x^3$. We represent $\mathbb{F}_{2^4}$ as $\mathbb{F}_2[\alpha]$, where $\alpha^4 + \alpha + 1 = 0$. We choose the basis $\{1, \alpha, \alpha^2, \alpha^3\}$ both for input and output of F. We write $x = x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3$ and

$$x^3 = (x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3)^3$$

After simplification, we get
$x^3 = (x_1 + x_1x_3 + x_2x_3 + x_2x_4) \cdot 1 + (x_1x_2 + x_1x_3 + x_3x_4 + x_4) \cdot \alpha +$
$(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_3) \cdot \alpha^2 + (x_2 + x_2x_4 + x_3 + x_3x_4 + x_4) \cdot \alpha^3.$
Here,

$$\begin{aligned}
f_1(x_1, x_2, x_3, x_4) &= x_1 + x_1x_3 + x_2x_3 + x_2x_4. \\
f_2(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_3x_4 + x_4. \\
f_3(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_3. \\
f_4(x_1, x_2, x_3, x_4) &= x_2 + x_2x_4 + x_3 + x_3x_4 + x_4.
\end{aligned}$$

Ignoring the linear terms in the above functions, we get the following quadratic homogeneous Boolean functions

$$\begin{aligned}
f_1(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_3 + x_2x_4. \\
f_2(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_3x_4. \\
f_3(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4. \\
f_4(x_1, x_2, x_3, x_4) &= x_2x_4 + x_3x_4.
\end{aligned}$$

We write the quadratic homogeneous Boolean functions $f_1,\ f_2,\ f_3,\ f_4$ in terms of quadratic forms as

$$f_1(x) = xQ_1x^T = (x_1,\ldots,x_n)\begin{pmatrix}0&0&1&0\\0&0&1&1\\0&0&0&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

$$f_2(x) = xQ_2x^T = (x_1,\ldots,x_n)\begin{pmatrix}0&1&1&0\\0&0&0&0\\0&0&0&1\\0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

$$f_3(x) = xQ_3x^T = (x_1,\ldots,x_n)\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&0&0&1\\0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}$$

$$f_4(x) = xQ_4x^T = (x_1,\ldots,x_n)\begin{pmatrix}0&0&0&0\\0&0&0&1\\0&0&0&1\\0&0&0&0\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}.$$

Note that,

$$C^1_{**} = Q_1 + Q_1^T = \begin{pmatrix}0&0&1&0\\0&0&1&1\\1&1&0&0\\0&1&0&0\end{pmatrix},\ C^2_{**} = Q_2 + Q_2^T = \begin{pmatrix}0&1&1&0\\1&0&0&0\\1&0&0&1\\0&0&1&0\end{pmatrix},$$

$$C^3_{**} = Q_3 + Q_3^T = \begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix},\ C^4_{**} = Q_4 + Q_4^T = \begin{pmatrix}0&0&0&0\\0&0&0&1\\0&0&0&1\\0&1&1&0\end{pmatrix}.$$

Here, $C^k_{**},\ k = 1,\ldots,4$ are symmetric matrices with main diagonal entries are zero. Now, consider the subcube $\mathbf{C}^k_{ij},\ k = 1,\ldots,4$ and $i,j = 1,\ldots,3$ of dimension $3 \times 3 \times 4$. We have

$$\mathbf{C}^1_{**} = \begin{pmatrix}0&0&1\\0&0&1\\1&1&0\end{pmatrix},\ \mathbf{C}^2_{**} = \begin{pmatrix}0&1&1\\1&0&0\\1&0&0\end{pmatrix},$$

$$\mathbf{C}^3_{**} = \begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix},\ \mathbf{C}^4_{**} = \begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}.$$

Note that the bold letter **C** is used to represent the subcube. For $j = 1, \dots, 3$, we have the following matrices

$$\mathbf{C}^*_{*1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \mathbf{C}^*_{*2} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \mathbf{C}^*_{*3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

One can check that the $Rank(\mathbf{C}^*_{*j}) = 2$, $j = 1, \dots, 3$ and all possible non-zero linear combinations of these matrices also have rank equal to 2. So the cube $\mathbf{C}^k_{ij}$, $k = 1, \dots, 4$, $1 \leq i, j \leq 3$ is a proper subcube.

From the definition of QAC C^k_{ij}, $1 \leq i, j, k \leq n$, we know that the nonzero linear combinations of matrices C^*_{*j}, $j = 1, \dots, n$ has rank $n - 1$. We can choose a subcube $\mathbf{C}^k_{ij}$, $1 \leq k \leq n$, $1 \leq i, j \leq n - 1$ from the QAC C^k_{ij}, $1 \leq i, j, k \leq n$. The subcube $\mathbf{C}^k_{ij}$ has n matrices of dimension $(n - 1 \times n - 1)$. One can check that for $j = 1, \dots, n - 1$, every nonzero linear combination of the matrices $\mathbf{C}^*_{*j}$ of dimension $(n - 1 \times n)$ has rank $n - 2$.
In order to discuss the YWL approach, first, we need to look at the positions of the QAC where we want to change the values in order to get a new QAC.
First, we construct a QAC C^k_{ij}, $1 \leq i, j, k \leq n$ from the known quadratic APN function. For each $1 \leq k \leq n$, we have the following matrix

$$C^k_{ij} = \begin{pmatrix} 0 & c^k_{12} & \cdots & c^k_{1n-1} & c^k_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c^k_{n-11} & c^k_{n-12} & \cdots & 0 & c^k_{n-1n} \\ c^k_{n1} & c^k_{n2} & \cdots & c^k_{nn-1} & 0 \end{pmatrix}.$$

For each value of k, we want to reassign the values in the last column and the last row of each matrix. It means that we need to change the following values

$$C^k_{ij} = \begin{pmatrix} 0 & c^k_{12} & \cdots & c^k_{1n-1} & \mathbf{c^k_{1n}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c^k_{n-11} & c^k_{n-12} & \cdots & 0 & \mathbf{c^k_{n\text{-}1n}} \\ \mathbf{c^k_{n1}} & \mathbf{c^k_{n2}} & \cdots & \mathbf{c^k_{nn\text{-}1}} & 0 \end{pmatrix}.$$

For each value of k, the change in the last column and the last row of each corresponding matrix is reflected in the derivative matrix C^*_{*j}, $j = 1, \dots, n$ in the following way.
For $j = 1$, we have the following matrix

$$C^*_{*1} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ c^1_{21} & c^2_{21} & \cdots & c^n_{21} \\ \vdots & \vdots & \vdots & \vdots \\ c^1_{n-11} & c^2_{n-11} & \cdots & c^n_{n-11} \\ \mathbf{c^1_{n1}} & \mathbf{c^2_{n1}} & \cdots & \mathbf{c^n_{n1}} \end{pmatrix}.$$

For $j = 2$, we have the following matrix

$$C^*_{*2} = \begin{pmatrix} c^1_{12} & c^2_{12} & \dots & c^n_{12} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c^1_{n-12} & c^2_{n-12} & \dots & c^n_{n-12} \\ \mathbf{c^1_{n2}} & \mathbf{c^2_{n2}} & \dots & \mathbf{c^n_{n2}} \end{pmatrix}.$$

Similarly, for $j = n$, we have the following matrix

$$C^*_{*n} = \begin{pmatrix} \mathbf{c^1_{1n}} & \mathbf{c^2_{1n}} & \dots & \mathbf{c^n_{1n}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{c^1_{n\text{-}1n}} & \mathbf{c^2_{n\text{-}1n}} & \dots & \mathbf{c^n_{n\text{-}1n}} \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

The YWL approach is an elegant approach for the construction of new quadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. It works in the following way:
First choose a subcube $\mathbf{C}^k_{ij}$, $1 \le k \le n$, $1 \le i,j \le n-1$ from the QAC C^k_{ij}, $1 \le i,j,k \le n$. The subcube $\mathbf{C}^k_{ij}$ has n matrices of dimension $(n-1 \times n-1)$.
We want to construct a new cube D^k_{ij}, $1 \le i,j,k \le n$ using the subcube
$\mathbf{C}^k_{ij}$, $1 \le k \le n$, $1 \le i,j \le n-1$ in such a way that the new cube D^k_{ij} is again a QAC.
The procedure for the construction of the new cube D^k_{ij} is as follows:
For each $1 \le k \le n$, we have the following matrix

$$D^k_{**} = \begin{pmatrix} 0 & c^k_{12} & \dots & c^k_{1n-1} & \mathbf{d^k_{1n}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c^k_{n-11} & c^k_{n-12} & \dots & 0 & \mathbf{d^k_{n\text{-}1n}} \\ \mathbf{d^k_{n1}} & \mathbf{d^k_{n2}} & \dots & \mathbf{d^k_{nn\text{-}1}} & 0 \end{pmatrix}.$$

For each value of k, the change in the last column and the last row of each corresponding matrix is reflected in the derivative matrix D^*_{*j}, $j = 1, \dots, n$ in the following way.
For $j = 1$, we have the following matrix

$$D^*_{*1} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ c^1_{21} & c^2_{21} & \dots & c^n_{21} \\ \vdots & \vdots & \vdots & \vdots \\ c^1_{n-11} & c^2_{n-11} & \dots & c^n_{n-11} \\ \mathbf{d^1_{n1}} & \mathbf{d^2_{n1}} & \dots & \mathbf{d^n_{n1}} \end{pmatrix}$$

For $j = 2$, we have the following matrix

$$D^*_{*2} = \begin{pmatrix} c^1_{12} & c^2_{12} & \dots & c^n_{12} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c^1_{n-12} & c^2_{n-12} & \cdots & c^n_{n-12} \\ \mathbf{d^1_{n2}} & \mathbf{d^2_{n2}} & \dots & \mathbf{d^n_{n2}} \end{pmatrix}$$

Similarly, for $j = n$, we have the following matrix

$$D^*_{*n} = \begin{pmatrix} \mathbf{d^1_{1n}} & \mathbf{d^2_{1n}} & \dots & \mathbf{d^n_{1n}} \\ \vdots & \vdots & \vdots & \vdots \\ \mathbf{d^1_{n\text{-}1n}} & \mathbf{d^2_{n\text{-}1n}} & \cdots & \mathbf{d^n_{n\text{-}1n}} \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

For $j = 1$, we need to choose a vector $(d^1_{n1}, d^2_{n1}, \dots, d^n_{n1}) \in \mathbb{F}_2^n$ in such a way that it is not contained in the subspace generated by the row vectors $\{(c^1_{21}, c^2_{21}, \dots, c^n_{21}),$ $\dots, (c^1_{n-11}, c^2_{n-11}, \dots, c^n_{n-11})\}$ of D^*_{*1}. We use the vector $(d^1_{n1}, d^2_{n1}, \dots, d^n_{n1})$ as a row vector in the matrix D^*_{*1}. Then D^*_{*1} has $n-1$ linearly independent rows and one zero row. It means that the rank of the matrix D^*_{*1} is $n-1$.
For $j = 2$, we only choose a vector $(d^1_{n2}, d^2_{n2}, \dots, d^n_{n2}) \in \mathbb{F}_2^n$ which is not contained in the subspace generated by the row vectors $\{(c^1_{12}, c^2_{12}, \dots, c^n_{12}), \dots,$ $(c^1_{n-12}, c^2_{n-12}, \dots, c^n_{n-12})\}$ of D^*_{*2}. We use the vector $(d^1_{n2}, d^2_{n2}, \dots, d^n_{n2})$ as a row vector in the matrix D^*_{*2}. Then D^*_{*2} has $n-1$ linearly independent rows and one zero row. It means that the rank of the matrix D^*_{*2} is $n-1$.
The important condition is that the sum of the matrices D^*_{*1} and D^*_{*2} also has rank $n-1$. Assume that the sum of the matrices D^*_{*1} and D^*_{*2} does not have rank $n-1$, then we need to choose again a vector $(d^1_{n2}, d^2_{n2}, \dots, d^n_{n2}) \in \mathbb{F}_2^n$ and repeat the same procedure.
Similarly, for $j = 3, 4, \dots, n-1$, we use the new vectors in the matrices $D^*_{*3}, D^*_{*4}, \dots, D^*_{*n-1}$ respectively and check the ranks of each matrix. If the rank of each matrix for $j = 3, 4, \dots, n-1$ is $n-1$ and all possible non-zero linear combinations of these matrices also have rank $n-1$, then the cube $D^k_{ij}, 1 \le i, j, k \le n$ is a quadratic APN cube. Note that for $j = n$, the last row of D^*_{*n} is zero. So, we do not need to find a new row vector in this case.
Now, we explain the YWL approach with the help of an example.

Example 4.8. From Example 4.7 and for $j = 1, \dots, 4$, we have the following matrices.

$$C^*_{*1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; C^*_{*2} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

$$C^*_{*3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix},\ C^*_{*4} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

One can check that the $Rank(C^*_{*1}) = Rank(C^*_{*2}) = Rank(C^*_{*3}) = Rank(C^*_{*4}) = 3$ and all possible non-zero linear combinations of these matrices also have rank equal to 3.

Now, we want to apply the YWL approach to construct new quadratic APN function. We only need to change the last row and last column of each matrix C^k_{ij}, $1 \leq i, j, k \leq 4$ in such a way that the resulting cube also satisfies the properties of QAC.

First, consider the subcube $\mathbf{C}^k_{ij}$, $1 \leq k \leq 4$ and $1 \leq i, j \leq 3$ of dimension $3 \times 3 \times 4$. We have

$$\mathbf{C}^1_{**} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},\ \mathbf{C}^2_{**} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{C}^3_{**} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},\ \mathbf{C}^4_{**} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

We want to construct a cube D^k_{ij}, $1 \leq i, j, k \leq 4$, using the subcube $\mathbf{C}^k_{ij}$, $1 \leq k \leq 4$ and $1 \leq i, j \leq 3$. In the new cube D^k_{ij}, $1 \leq i, j, k \leq 4$, the values in the last row and column of D^k_{ij} are not known.

For $k = 1$, we have the following matrix

$$D^1_{**} = \begin{pmatrix} 0 & 0 & 1 & d^1_{14} \\ 0 & 0 & 1 & d^1_{24} \\ 1 & 1 & 0 & d^1_{34} \\ d^1_{41} & d^1_{42} & d^1_{43} & 0 \end{pmatrix}.$$

For $k = 2$, we have the following matrix

$$D^2_{**} = \begin{pmatrix} 0 & 1 & 1 & d^2_{14} \\ 1 & 0 & 0 & d^2_{24} \\ 1 & 0 & 0 & d^2_{34} \\ d^2_{41} & d^2_{42} & d^2_{43} & 0 \end{pmatrix}.$$

For $k = 3$, we have the following matrix

$$D^3_{**} = \begin{pmatrix} 0 & 1 & 1 & d^3_{14} \\ 1 & 0 & 1 & d^3_{24} \\ 1 & 1 & 0 & d^3_{34} \\ d^3_{41} & d^3_{42} & d^3_{43} & 0 \end{pmatrix}.$$

For $k = 4$, we have the following matrix

$$D^4_{**} = \begin{pmatrix} 0 & 0 & 0 & D^4_{14} \\ 0 & 0 & 0 & D^4_{24} \\ 0 & 0 & 0 & D^4_{34} \\ D^4_{41} & D^4_{42} & D^4_{43} & 0 \end{pmatrix}.$$

Now, we consider the matrices $D^*_{*j}, j = 1, 2, 3, 4$. These matrices are actually the derivative matrices of the function F from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$.
For $j = 1$, we have the following matrix

$$D^*_{*1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ d^1_{41} & d^2_{41} & d^3_{41} & d^4_{41} \end{pmatrix}.$$

For $j = 2$, we have the following matrix

$$D^*_{*2} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ d^1_{42} & d^2_{42} & d^3_{42} & d^4_{42} \end{pmatrix}.$$

For $j = 3$, we have the following matrix

$$D^*_{*3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ d^1_{43} & d^2_{43} & d^3_{43} & d^4_{43} \end{pmatrix}.$$

For $j = 4$, we have the following matrix

$$D^*_{*4} = \begin{pmatrix} d^1_{14} & d^2_{14} & d^3_{14} & d^4_{14} \\ d^1_{24} & d^2_{24} & d^3_{24} & d^4_{24} \\ d^1_{34} & d^2_{34} & d^3_{34} & d^4_{34} \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Now, choose the following vectors from $\mathbb{F}_2^4$ as

$$(d^1_{41}, d^2_{41}, d^3_{41}, d^4_{41}) = (1, 0, 0, 1) \in \mathbb{F}_2^4,$$

$$(d^1_{42}, d^2_{42}, d^3_{42}, d^4_{42}) = (0, 1, 1, 1) \in \mathbb{F}_2^4,$$

$$(d^1_{43}, d^2_{43}, d^3_{43}, d^4_{43}) = (0, 0, 1, 1) \in \mathbb{F}_2^4.$$

For $j = 1, 2, 3, 4$, the matrices D^*_{*j} become

$$D^*_{*1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \; D^*_{*2} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

$$D^*_{*3} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \; D^*_{*4} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

One can check that the $Rank(D^*_{*j}) = 3,\ j = 1, \ldots, 4$ and all possible non-zero linear combinations of these matrices have also rank equal to 3. It means that $D^k_{ij},\ 1 \leq i, j, k \leq 4$ is a new quadratic APN cube. For $k = 1, 2, 3, 4$, we have the following matrices

$$D^1_{**} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; D^2_{**} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$D^3_{**} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \; D^4_{**} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

As, we know that

$$D^1_{**} = Q_1 + Q_1^T,\ D^2_{**} = Q_2 + Q_2^T\ D^3_{**} = Q_3 + Q_3^T\ D^4_{**} = Q_4 + Q_4^T.$$

So, we have

$$f_1^{'}(X) = xQ_1x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_2^{'}(X) = xQ_2x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_3^{'}(X) = xQ_3x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_4^{'}(X) = xQ_4x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$f_1^{'}(x_1, x_2, x_3, x_4) = x_1x_3 + x_1x_4 + x_2x_3.$
$f_2^{'}(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4.$
$f_3^{'}(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 + x_3x_4.$
$f_4^{'}(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_4 + x_3x_4.$
Here, $F^{'} = (f_1^{'}, f_2^{'}, f_3^{'}, f_4^{'})$ is also a quadratic APN function from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$ and $F^{'}$ is CCZ-equivalent with F.

4.3 The switching approach

In this section, we discuss a different point of view for the construction of new APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$: the *Switching Approach*. The idea of switching is as follows.
Assume that we have an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined as

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix},$$

where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $f_1(x), \ldots, f_n(x)$ are the coordinate functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. If we replace or modify one coordinate function f_1 of F by some suitable Boolean function g_1 from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which more or less satisfies the same properties as satisfied by f_1, then the function G from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by

$$G(x) = \begin{pmatrix} g_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix},$$

is an APN function. The function G is obtained via switching of the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.
The following Theorem gives a necessary and sufficient condition for a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ to produce another (not necessarily equivalent) APN function.

Theorem 4.9. *[30] Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The function $F^{'}$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by*

$$F^{'}(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} + \begin{pmatrix} f(x) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

is an APN function if and only if

$$f(x) + f(x+a) + f(y) + f(y+a) = 0$$

for all $x,\ y,\ a \in \mathbb{F}_2^n$ *with*

$$F(x) + F(x+a) + F(y) + F(y+a) = 1,$$

where $1 = (1, 0, \ldots, 0) \in \mathbb{F}_2^n$.

Proof. Since F is an APN function, the equation

$$F(x+a) + F(x) = b,\ a, b \in \mathbb{F}_2^n,\ a \neq 0.$$

has at most 2 solutions. Now, we add a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ to the first coordinate function of the APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We obtain the function $F^{'}$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The derivative of the function $F^{'}$ in the direction of $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ with $a \neq 0$ is

$$F(x+a) + F(x) + \begin{pmatrix} f(x+a) + f(x) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

and we have the following equation

$$F(x+a) + F(x) + \begin{pmatrix} f(x+a) + f(x) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = b. \tag{4.3}$$

Now, we want to determine the number of solutions of the equation (4.3). Assume that $F(x+a) + F(x) = b$, then equation (4.3) becomes

$$f(x+a) + f(x) = 0.$$

Assume that $F(x+a) + F(x) = b + 1$, then equation (4.3) becomes

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

Therefore, equation (4.3) has at most 4 solutions. The solutions are for those values of x for which

$$F(x+a) + F(x) \in \{b,\ b+1\}.$$

Assume that there are 4 different solutions $x,\ y,\ x+a,\ y+a$, then we have

$$F(x+a) + F(x) + \begin{pmatrix} f(x+a) + f(x) \\ 0 \\ \vdots \\ 0 \end{pmatrix} = b,$$

$$F(y+a)+F(y)+\begin{pmatrix} f(y+a)+f(y) \\ 0 \\ \vdots \\ 0 \end{pmatrix}=b.$$

By the addition of above two equations, we get

$$F(x+a)+F(x)+F(y+a)+F(y)=\begin{pmatrix} f(x+a)+f(x)+f(y+a)+f(y) \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

This is possible if and only if

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

and

$$F(x+a)+F(x)+F(y+a)+F(y)=1,$$

holds which is a contradiction because we assume that

$$f(x+a)+f(x)+f(y+a)+f(y)=0.$$

□

The switching approach introduced by Dillon changes only one coordinate function of an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ to produce another APN function G from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The dimension of the image set of the mapping $F+G$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is always 1.

Theorem 4.10. *[67] Let F and G be functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. If F is the switching of G, then the image set of the mapping $F+G$ defined by $x \to F(x)+G(x)$ spans a 1-dimensional vector space.*

Proof. Let F and G be the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by

$$F(x)=\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}, \; G(x)=\begin{pmatrix} g_1(x) \\ \vdots \\ g_n(x) \end{pmatrix},$$

where $x=(x_1,\dots,x_n)\in\mathbb{F}_2^n$. Assume that $F(x)$ is the switching of $G(x)$, which means that $f_1(x)\neq g_1(x)$ and $f_i(x)=g_i(x)$, $2\leq i\leq n$. Hence,

$$F(x)+G(x)=\begin{pmatrix} f_1(x)+g_1(x) \\ \vdots \\ 0 \end{pmatrix}$$

shows that the dimension of the vectorspace generated by the image set of the mapping $F+G$ is equal to 1. □

In 2008, Budaghyan, Carlet and Leander [50] obtained an example of an APN function by using the switching approach which is as follows.

Theorem 4.11. *[50] Let F be the function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x) = x^3 + Tr_1^n(x^9)$. Then F is an APN function for any $n \geq 1$.*

Indeed, the function $F(x) = x^3 + Tr_1^n(x^9)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is a switching over $\mathbb{F}_2$ of the Gold APN function $G(x) = x^3$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$.
First, choose a basis $A = (1, \alpha_1, \alpha_2, \ldots, \alpha_{n-1})$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $(g_0(x), g_1(x), \ldots, g_{n-1}(x))$ be the coordinate functions of the function $G(x)$ with respect to the basis A. Then

$$G(x) = g_0(x) \cdot 1 + g_1(x) \cdot \alpha_1 + \ldots + g_{n-1}(x) \cdot \alpha_{n-1}$$

and consequently,

$$F(x) = (g_0(x) + Tr_1^n(x^9)) \cdot 1 + g_1(x) \cdot \alpha_1 + \ldots + g_{n-1} \cdot \alpha_{n-1}.$$

It shows that $F(x)$ is obtained from $G(x)$ by switching over $\mathbb{F}_2$.

Remark 4.12. In 2009, Budaghyan, Carlet and Leander [51] obtained two more infinite families of APN functions using switching approach which are $M.10$ and $M.11$ of Table 1.6.

In 2008, Edel and Pott [30] extensively studied the switching approach proposed by Dillon. They generalized the Dillon switching approach by replacing the Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ by cf, where $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$ with $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$. It is interesting to observe that the Edel and Pott switching approach can be iterated with the different values of $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$ with $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$.
The following Theorem gives a necessary and sufficient condition for a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ to produce another APN function.

Theorem 4.13. *[30] Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ and $c = (c_1, \ldots, c_n) \in \mathbb{F}_2^n$, $c \neq 0$. The function $F + cf$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by*

$$F(x) + cf(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_n(x) \end{pmatrix} + \begin{pmatrix} c_1 f(x) \\ c_2 f(x) \\ \vdots \\ c_n f(x) \end{pmatrix}$$

is an APN function if and only if

$$f(x) + f(x+a) + f(y) + f(y+a) = 0,$$

$$F(x) + F(x+a) + F(y) + F(y+a) = c,$$

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

Proof. Since, F is an APN function, then

$$F(x+a)+F(x)=b,\ a,b\in\mathbb{F}_2^n,\ a\neq 0.$$

has at most 2 solution.
Now, we add a Boolean function cf to the coordinate functions of an APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We obtain the function $F+cf$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The derivative of the function $F+cf$ in the direction of $a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n$ with $a\neq 0$ is

$$F(x+a)+F(x)+c(f(x+a)+f(x))$$

and we have the following equation

$$F(x+a)+F(x)+c(f(x+a)+f(x))=b. \tag{4.4}$$

We want to determine the number of solutions of equation (4.4). Assume that $F(x+a)+F(x)=b$, then the equation (4.4) becomes

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

hence

$$f(x+a)+f(x)=0.$$

So, if x is one solution then $x+a$ is another solution.
Assume that $F(x+a)+F(x)=b+c$, then the equation (4.4) becomes

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

hence

$$c+c(f(x+a)+f(x))=0,$$
$$f(x+a)+f(x)=1.$$

So, if x is one solution, then $x+a$ is another solution. The equation (4.4) has at most 4 solutions. The solutions are for those values of x for which

$$F(x+a)+F(x)\in\{b,\ b+c\}.$$

Assume that there are 4 different solutions $x,\ y,\ x+a,\ y+a$, then we have

$$F(x+a)+F(x)+c(f(x+a)+f(x))=b,$$

$$F(y+a)+F(y)+c(f(y+a)+f(y))=b.$$

By the addition of above two equations, we get

$$F(x+a)+F(x)+F(y+a)+F(y)=c(f(x+a)+f(x)+f(y+a)+f(y)).$$

This is possible if and only if

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

and

$$F(x+a)+F(x)+F(y+a)+F(y)=c$$

holds which is a contradiction because we assume that

$$f(x+a)+f(x)+f(y+a)+f(y)=0.$$

□

Remark 4.14. The Edel and Pott switching approach may change more than one coordinate function of the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The Dillon switching approach is a particular case of the Edel and Pott switching approach. The Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ depends on c, i.e. for different choices of c, we may get different f's.

Theorem 4.13 suggest a way to find a Boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ such that $F(x)+cf(x)$ is an APN function.
First, find all the 4-tuples $(x,y,x+a,y+a)\in(\mathbb{F}_2^n)^4$ such that the following equation holds:

$$F(x)+F(x+a)+F(y)+F(y+a)=c.$$

These 4-tuples give rise to constraints

$$f(x)+f(x+a)+f(y)+f(y+a)=0.$$

We may view f as a vector of length 2^n (coordinates are indexed by elements x in $\mathbb{F}_2^n$ and the entries of the vector are $f(x)$). The constraints are linear constraints, and we may find f by solving the system of linear equations.
Now, we explain the switching approach with the help of an example.

Example 4.15. Let F be the APN function from $\mathbb{F}_{2^5}$ to $\mathbb{F}_{2^5}$ defined by $F(x)=x^3$. We represent $\mathbb{F}_{32}$ as $\mathbb{F}_2[\alpha]$ where $\alpha^5+\alpha^2+1=0$. Choose a basis $\{1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4\}$ of $\mathbb{F}_{2^5}$ over $\mathbb{F}_2$. We write $x=x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4$ and obtain

$$x^3=(x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4)^3$$

After simplification, we get
$x^3=f_1(x_1,\dots,x_5)\cdot 1+f_2(x_1,\dots,x_5)\cdot\alpha+f_3(x_1,\dots,x_5)\cdot\alpha^2+f_4(x_1,\dots,x_5)\cdot\alpha^3+f_5(x_1,\dots,x_5)\cdot\alpha^4$
where,
$f_1(x_1,\dots,x_5)=x_4x_5+x_3x_5+x_4x_5+x_3x_4+x_1x_5+x_3x_5+x_2x_3+x_2x_4+x_1.$
$f_2(x_1,\dots,x_5)=x_5+x_4x_5+x_4+x_2x_5+x_3+x_1x_4+x_2x_5+x_1x_2.$
$f_3(x_1,\dots,x_5)=x_5+x_4x_5+x_3x_4+x_1x_5+x_3x_5+x_2x_4+x_3x_4+x_2x_3+x_2x_4+x_1x_3+x_1x_2.$
$f_4(x_1,\dots,x_5)=x_5+x_4+x_2x_5+x_3x_4+x_1x_5+x_3x_5+x_3+x_1x_4+x_2x_5+x_1x_4+x_2.$
$f_5(x_1,\dots,x_5)=x_3x_5+x_4x_5+x_4+x_2x_5+x_2x_4+x_3x_4+x_1x_5+x_2x_3+x_1x_3.$

Now, choose a vector $u = (1,0,0,1,0) \in \mathbb{F}_2^5$. We need to find $x,\ y,\ a \in \mathbb{F}_2^5$ such that

$$F(x) + F(x+a) + F(y) + F(y+a) = u$$

Using computer, we found 960 linear equations in 32 variables $x_1, x_2, \ldots, x_{32}$. After solving the system of linear equations, we have 21 linear equation in 32 variables $x_1, x_2, \ldots, x_{32}$. We describe these linear equations in a matrix A of dimension (21×32) as follows.

$$A = \left(\begin{array}{cccccccccccccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&1&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&1&1&1&1&0&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&1&0&0&0&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&1&1&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&1&1&1&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&1&1&0&0&1&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&1
\end{array}\right)_{(21\times 32)}$$

Now, we have a linear transformation $T : \mathbb{F}_2^{32} \longrightarrow \mathbb{F}_2^{21}$ defined as $x \longrightarrow A \cdot x$, where $x = (x_1, \ldots, x_{32}) \in \mathbb{F}_2^{32}$. We need to find the kernel of the linear map T to determine the Boolean function f from $\mathbb{F}_2^5$ to $\mathbb{F}_2$. The kernel of the linear map T is the set of solutions of the equation $A \cdot x = 0$, that is,

$$Ker(A) = \{x \in \mathbb{F}_2^{32} \mid A \cdot x = 0\}.$$

We have computed the basis of $Ker(A)$. We write the basis in terms of a matrix B of dimension (11×32) which is as follows.

$$B = \left(\begin{array}{cccccccccccccccccccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&0&1&1&1&1&1&0&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&1&1&0&1&1&0&1&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&1&1&1&1&0&0&1&0&0&1&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&1&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&1&0&0&0&0&1&0&0&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&1&1&0&0&0&1&1&0&0&1&0&1&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&1&1&0&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&1&0&1&1&1&1&1&1&0&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&1&0&1&1&1&0&1&0&0&0&1&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&1&0&0&0&0&1&1&0&0&0&0&0&1&0&1&0
\end{array}\right)_{(11\times 32)}$$

The dimension of the basis is 11. It means that there are 2^{11} possible candidates for the Boolean function f from $\mathbb{F}_2^5$ to $\mathbb{F}_2$ such that the function $G(x) = F(x) + cf(x)$ from $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$ is an APN function. We have 2^{11} possible APN functions. For simplicity, we choose one Boolean function f from $\mathbb{F}_2^5$ to $\mathbb{F}_2$ which is as follows.

$$f(x_1, x_2, x_3, x_4, x_5) = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_2 + x_3x_5 + x_4.$$

The function G from $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$ defined by

$$G(x_1, x_2, x_3, x_4, x_5) = \begin{pmatrix} g_1(x_1, x_2, x_3, x_4, x_5) \\ f_2(x_1, x_2, x_3, x_4, x_5) \\ f_3(x_1, x_2, x_3, x_4, x_5) \\ g_4(x_1, x_2, x_3, x_4, x_5) \\ f_5(x_1, x_2, x_3, x_4, x_5) \end{pmatrix}$$

where
$g_1(x_1, \ldots, x_5) = x_4x_5 + x_3x_5 + x_4x_5 + x_3x_4 + x_1x_5 + x_3x_5 + x_2x_3 + x_2x_4 + x_1 + (x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_2 + x_3x_5 + x_4)$.
$f_2(x_1, \ldots, x_5) = x_5 + x_4x_5 + x_4 + x_2x_5 + x_3 + x_1x_4 + x_2x_5 + x_1x_2$.
$f_3(x_1, \ldots, x_5) = x_5 + x_4x_5 + x_3x_4 + x_1x_5 + x_3x_5 + x_2x_4 + x_3x_4 + x_2x_3 + x_2x_4 + x_1x_3 + x_1x_2$.
$g_4(x_1, \ldots, x_5) = x_5 + x_4 + x_2x_5 + x_3x_4 + x_1x_5 + x_3x_5 + x_3 + x_1x_4 + x_2x_5 + x_1x_4 + x_2 + (x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_2 + x_3x_5 + x_4)$.
$f_5(x_1, \ldots, x_5) = x_3x_5 + x_4x_5 + x_4 + x_2x_5 + x_2x_4 + x_3x_4 + x_1x_5 + x_2x_3 + x_1x_3$.
is the switching of the function F from $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$.
Note that, we have changed two coordinate functions of the function F from $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$ to obtain the function G from $\mathbb{F}_2^5$ to $\mathbb{F}_2^5$.

It is interesting to observe that Edel and Pott found the first and currently the only known sporadic example of a nonquadratic APN function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^6$ by using the switching approach. The nonquadratic APN function is described as follows.

Theorem 4.16. *[30] Let F be a functions from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ defined as*
$F(x) = x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + u^{14}(Tr_1^6(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + u^{18}x^9 + u^{36}x^{18} + u^{72}x^{36} + x^{21} + x^{42})$,
where u is the primitive root of $\mathbb{F}_{2^6}$

The equivalent representation of this nonquadratic APN function F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ in $\mathbb{F}_2^6$ is as follows.
Let

$$F(x) = G(x) + u^{14}f(x),$$

where

$$G(x) = x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24})$$

and

$$f(x) = Tr_1^6(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + u^{18}x^9 + u^{36}x^{18} + u^{72}x^{36} + x^{21} + x^{42}.$$

We represent $\mathbb{F}_{2^6}$ as $\mathbb{F}_2[\alpha]$, where $\alpha^6+\alpha^4+\alpha^3+\alpha+1=0$. We choose the basis $\{1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5\}$ both for input and output of G. We write

$$x = x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3 + x_5\alpha^4 + x_6\alpha^5$$

and
$G(x) = (x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4+x_6\alpha^5)^{17} + u^{17}((x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4+x_6\alpha^5)^{17} + (x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4+x_6\alpha^5)^{18} + (x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4+x_6\alpha^5)^{20} + (x_1+x_2\alpha+x_3\alpha^2+x_4\alpha^3+x_5\alpha^4+x_6\alpha^5)^{24})$
After simplification, we get
$G(x) = g_1(x_1,\dots,x_6)\cdot 1 + g_2(x_1,\dots,x_6)\cdot\alpha + g_3(x_1,\dots,x_6)\cdot\alpha^2 + g_4(x_1,\dots,x_6)\cdot\alpha^3 + g_5(x_1,\dots,x_6)\cdot\alpha^4 + g_6(x_1,\dots,x_6)\cdot\alpha^5$,
where
$g_1(x_1,\dots,x_6) = x_1x_4+x_1+x_2x_5+x_2x_6+x_2+x_4x_5+x_4x_6+x_5x_6.$
$g_2(x_1,\dots,x_6) = x_1x_3+x_1x_4+x_1x_5+x_2x_3+x_2x_6+x_3x_4+x_3x_6+x_3+x_4x_5+x_4x_6+x_4.$
$g_3(x_1,\dots,x_6) = x_1x_2+x_1x_3+x_2x_4+x_2x_5+x_2x_6+x_3x_5+x_3+x_4x_6.$
$g_4(x_1,\dots,x_6) = x_1x_2+x_1x_4+x_1x_5+x_2+x_2+x_3x_5+x_3x_6+x_4+x_4x_5.$
$g_5(x_1,\dots,x_6) = x_1x_2+x_1x_4+x_1x_5+x_2x_5+x_2x_6+x_3x_5+x_4x_5+x_5x_6.$
$g_6(x_1,\dots,x_6) = x_1x_2+x_1x_4+x_1x_6+x_2x_5+x_3x_4+x_3x_5+x_4+x_4x_6.$
and
$f(x_1,x_2,x_3,x_4,x_5,x_6) = x_1x_2x_4+x_1x_2x_6+x_1x_5+x_1x_6+x_1+x_2x_3x_4+x_2x_3x_6+x_2x_4+x_2x_5+x_2+x_3x_4+x_3x_6+x_4x_5+x_4x_6+x_4+x_6.$
We observe that

$$F(x_1,\dots,x_6) = \begin{pmatrix} f_1(x_1,\dots,x_6)\\ f_2(x_1,\dots,x_6)\\ f_3(x_1,\dots,x_6)\\ f_4(x_1,\dots,x_6)\\ f_5(x_1,\dots,x_6)\\ f_6(x_1,\dots,x_6)\end{pmatrix} = \begin{pmatrix} g_1(x_1,\dots,x_6)\\ g_2(x_1,\dots,x_6)\\ g_3(x_1,\dots,x_6)\\ g_4(x_1,\dots,x_6)\\ g_5(x_1,\dots,x_6)\\ g_6(x_1,\dots,x_6)\end{pmatrix} + \begin{pmatrix} 0\\ f(x_1,\dots,x_6)\\ 0\\ 0\\ f(x_1,\dots,x_6)\\ 0\end{pmatrix}$$

In this example of a nonquadratic APN function F from $\mathbb{F}_2^6$ to $\mathbb{F}_2^6$, we add a cubic Boolean function f from $\mathbb{F}_2^6$ to $\mathbb{F}_2$ into two coordinate functions of the function G from $\mathbb{F}_2^6$ to $\mathbb{F}_2^6$.
Edel and Pott also proved that this example of a nonquadratic APN function is CCZ-inequivalent to a crooked function and it is also CCZ-inequivalent to known APN power mappings.

Remark 4.17. Finding new examples of nonquadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is still an open problem.

4.4 Local changes in the quadratic APN cube

In Section 4.2, we discussed the YWL approach for the construction of quadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. In Section 4.3, we discussed the switching approach for the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. In the switching approach, we made changes in one coordinate functions of the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We are interested in applying changes in more than one coordinate function of the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We introduce the concept of local change. Local change means that we make small changes in the coordinate matrices of a quadratic APN cube.

First, we apply the local changes in Quadratic APN cube of dimension $n \times n \times n$ defined over $\mathbb{F}_2$. After performing the local changes in a quadratic APN cube, we can use the YWL approach to construct a new quadratic APN functions.

Let F be a quadratic APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined as

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}, x \in \mathbb{F}_2^n,$$

where $f_1(x), \ldots, f_n(x)$ are quadratic homogeneous Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The function F can be describe in terms of the cube C_{ij}^k, $1 \leq i, j, k \leq n$ of dimension $n \times n \times n$ defined over $\mathbb{F}_2$. For $k = 1, \ldots, n$, the matrix C_{ij}^k, $1 \leq i, j \leq n$ corresponds to the coordinate function f_k of F. We can write the coordinate functions f_k, $k = 1, \ldots, n$ corresponding to C_{ij}^k, $1 \leq i, j \leq n$ as

$$f_k(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} c_{i,j}^k x_i x_j,\ c_{i,j}^k \in \mathbb{F}_2.$$

Single point local change

We discuss a very particular case of a local change. In this particular case, we make a small change at one point in the coordinate matrix corresponding to one coordinate function of F.

Assume that we can add $x_1 x_2$, where $x_1,\ x_2 \in \mathbb{F}_2 \setminus \{0\}$ in the first coordinate function $f_1(x_1, \ldots, x_n)$. The modified coordinate function $f_1^{'}$ corresponding to C_{ij}^1, $1 \leq i, j \leq n$ is

$$f_1^{'}(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} c_{i,j}^1 x_i x_j + x_1 x_2,\ c_{i,j}^1 \in \mathbb{F}_2.$$

The coordinate functions f_k, $k = 2, \ldots, n$ corresponding to C_{ij}^k, $1 \leq i, j \leq n$ are

$$f_k(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} c_{i,j}^k x_i x_j,\ c_{i,j}^k \in \mathbb{F}_2.$$

For $k = 1$, we have the following modified matrix

$$C_{ij}^1 = \begin{pmatrix} 0 & \mathbf{c_{12}^1 + 1} & \dots & c_{1n-1}^1 & c_{1n}^1 \\ \mathbf{c_{21}^1 + +1} & 0 & \dots & c_{2n-1}^1 & c_{2n}^1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{n-11}^1 & c_{n-12}^1 & \dots & 0 & c_{n-1n}^1 \\ c_{n1}^1 & c_{n2}^1 & \dots & c_{nn-1}^1 & 0 \end{pmatrix}.$$

As the matrix C_{ij}^1 is a symmetric matrix, so we add $x_1^{'}x_2^{'}$ in C_{21}^1 too.
For $k = 2, \dots, n$, we have the following unchanged matrices

$$C_{ij}^k = \begin{pmatrix} 0 & c_{12}^k & \dots & c_{1n-1}^k & c_{1n}^k \\ c_{21}^k & 0 & \dots & c_{2n-1}^k & c_{2n}^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ c_{n-11}^k & c_{n-12}^k & \dots & 0 & c_{n-1n}^k \\ c_{n1}^k & c_{n2}^k & \dots & c_{nn-1}^k & 0 \end{pmatrix}.$$

Note that this local change has changed the structure of the quadratic APN cube. It means that for $j = 1, \dots, n$, every nonzero linear combinations of matrices C_{*j}^* have not necessarily rank $n - 1$. In order to construct a new quadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. We use the following procedure.

Procedure:

First, we choose a subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq n, 1 \leq i, j \leq n-1$ from the modified cube C_{ij}^k, $1 \leq i, j, k \leq n$, here $\mathbf{C}$ denotes the subcube. The subcube $\mathbf{C}_{ij}^k$ has n matrices of dimension $(n - 1 \times n - 1)$. Now, we want to check that the subcube $\mathbf{C}_{ij}^k$ is proper or not. Assume that the subcube $\mathbf{C}_{ij}^k$ is proper, it means that for $j = 1, \dots, n-1$, every nonzero linear combination of the matrices $\mathbf{C}_{ij}^k$ of dimension $(n - 1 \times n)$ has rank $n - 2$. Now, we may apply the YWL approach for the construction of new QAC D_{ij}^k, $1 \leq i, j, k \leq n$.

On the other hand, assume that the subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq n$, $1 \leq i, j \leq n-1$ is not proper. We need to choose a subcube of smaller dimension, that is, a subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq n$, $1 \leq i, j \leq n-2$ from the modified cube C_{ij}^k, $1 \leq i, j, k \leq n$. The subcube $\mathbf{C}_{ij}^k$ has n matrices of dimension $(n - 2 \times n - 2)$. We check that the subcube $\mathbf{C}_{ij}^k$ is proper or not. Assume that the subcube $\mathbf{C}_{ij}^k$ is proper, it means that for $j = 1, \dots, n-2$, every non-zero linear combination of the matrices $\mathbf{C}_{ij}^k$ of dimension $(n - 2 \times n)$ has rank $n - 3$. Now, we may apply the YWL approach two times for the construction of new QAC D_{ij}^k, $1 \leq i, j, k \leq n$.

On the other hand, if the subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq n$, $1 \leq i, j \leq n-2$ is not proper. Then, we repeat the above procedure until we find the proper subcube and we apply the YWL approach appropriate number of times for the construction of new cube D_{ij}^k, $1 \leq i, j, k \leq n$. The new cube D_{ij}^k, $1 \leq i, j, k \leq n$ is a QAC. We explain this procedure with the help of an example.

Example 4.18. We use the same function F from $\mathbb{F}_{2^4}$ to $\mathbb{F}_{2^4}$ as we discussed in Example 4.7. For $k = 1, \dots, 4$, C_{**}^k are symmetric matrices with main diagonal entries are zero.

$$C_{**}^1 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; C_{**}^2 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$C_{**}^3 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \; C_{**}^4 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Now, we only change the entries C_{12}^1 and C_{21}^1 into 1. So, we have the modified cube M_{ij}^k, $1 \leq i, j, k \leq n$ which is as follows

$$M_{**}^1 = Q_1 + Q_1^T = \begin{pmatrix} 0 & \mathbf{1} & 1 & 0 \\ \mathbf{1} & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; M_{**}^2 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$M_{**}^3 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \; M_{**}^4 = Q_1 + Q_1^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Now, consider the subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq 4$ and $1 \leq i, j \leq 3$ of dimension $3 \times 3 \times 4$ from the modified cube M_{ij}^k, $1 \leq i, j, k \leq n$.

$$\mathbf{C}_{**}^1 = \begin{pmatrix} 0 & \mathbf{1} & 1 \\ \mathbf{1} & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; \mathbf{C}_{**}^2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{C}_{**}^3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; \mathbf{C}_{**}^4 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Note that $Rank(\mathbf{C}_{*1}^*) = 1$, the subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq 4$ and $1 \leq i, j \leq 3$ is not proper.

Now, we choose the subcube $\mathbf{C}_{ij}^k$, $1 \leq k \leq 4$ and $1 \leq i, j \leq 2$ of dimension $2 \times 2 \times 4$ from the modified cube M_{ij}^k, $1 \leq i, j, k \leq n$. Note that the subcube

$\mathbf{C}_{ij}^k$, $1 \leq k \leq 4$ and $1 \leq i,j \leq 2$ is proper.
We apply the YWL approach two times to get the new quadratic APN cube D_{ij}^k, $1 \leq i,j,k \leq 4$.
For $k = 1,2,3,4$, we have the following matrices

$$D_{**}^1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; D_{**}^2 = \begin{pmatrix} 0 & 1 & & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

$$D_{**}^3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; D_{**}^4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

As, we know that

$$D_{**}^1 = Q_1 + Q_1^T, \; D_{**}^2 = Q_2 + Q_2^T \; D_{**}^3 = Q_3 + Q_3^T \; D_{**}^4 = Q_4 + Q_4^T.$$

So, we have

$$f_1^{'}(X) = xQ_1x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_2^{'}(X) = xQ_2x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_3^{'}(X) = xQ_3x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$$f_4^{'}(X) = xQ_4x^T = (x_1, \ldots, x_4) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

$f_1^{'}(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3$.
$f_2^{'}(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_4 + x_2x_3$.
$f_3^{'}(x_1, x_2, x_3, x_4) = x_1x_2 + x_2x_4$.
$f_4^{'}(x_1, x_2, x_3, x_4) = x_3x_4$.
Here, $F^{'} = (f_1^{'}, f_2^{'}, f_3^{'}, f_4^{'})$ is also a quadratic APN function from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$ and $F^{'}$ is CCZ equivalent to F.

Remark 4.19. We have discussed a very particular case of local changes. In general, it is possible to change cube in more complicated way. If there exists a subcube in the modified cube which is proper then we can construct a new quadratic APN functions by using the YWL approach.

4.5 Computational results

In this section, we discuss several computational results which we performed on quadratic APN cube of dimension $n \times n \times n$.

Remark 4.20. Note that in all of our computational results, we use default primitive element of MAGMA $v2.23 - 9$ for $\mathbb{F}_{2^n}$.

Yu, Wang and Li have used their approach two times on the QAC $C^k_{i,j}$, $1 \leq i, j, k \leq n$ and constructed 471 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^7}$. They have also constructed 8157 CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^8}$. On $\mathbb{F}_{2^8}$, they have also checked that their CCZ-inequivalent quadratic APN functions are not equal to a permutation.
We extend the Yu, Wang and Li work by computing the following so called CCZ-invariants:

- Δ- and Γ- Rank.
- order of the automorphism groups of $M(G_F)$.
- Walsh spectrum.

of Yu, Wang and Li quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$. We have listed our computational results about these CCZ-invariants in Tables 4.1 and 4.2. We have the following observations.

Result 4.21. In Tables 4.1 and 4.2, we found that there are several CCZ-inequivalent quadratic APN functions which have same CCZ-invariants, that is, they have same Δ-rank, Γ-rank, order of the automorphism groups of $M(G_F)$ and Walsh spectrum.

Problem 4.1. It is an interesting problem to investigate that why so many CCZ-inequivalent quadratic APN functions having same CCZ-invariant parameters.

In 2017, Kai-Uwe Schmidt at the fifth irsee conference which was held in Germany has mentioned that there are few quadratic APN functions found by Yu, Wang and Li have 7 valued Walsh spectrum. We have explicitly computed the number of APN functions having 7 valued Walsh spectrum. We found that there are 487 quadratic APN function on $\mathbb{F}_{2^8}$ having Walsh spectrum

$$\{* - 64[6], -32[2240], -16[20880], 0[15600], 16[23664], 32[2880], 64[10]*\}$$

Table 4.1: Quadratic APN functions from $\mathbb{F}_{2^7}$ to $\mathbb{F}_{2^7}$

No	Δ-rank	Γ-rank	$\mid M(G_F) \mid$	Walsh spectrum	# of APN functions
1	212	4048	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	201
2	212	4046	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	172
3	210	4048	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	3
4	212	4050	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	60
5	212	4044	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	32
6	212	4042	128	$\{* -16[3556], 0[8128], 16[4572]*\}$	3

and 12 quadratic APN functions on $\mathbb{F}_{2^8}$ having Walsh spectrum

$$\{* -64[12], -32[2100], -16[21360], 0[14880], 16[24208], 32[2700], 64[20]*\}$$

(the values in brackets [ ] denote the multiplicities of the Walsh coefficients and the notion $\{* \ldots *\}$ indicates *multisets*).

Yu, Wang and Li have used Gold APN function $F(x) = x^3$ to construct QAC and generate several CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$.

In our computational results, we choose known quadratic APN functions other than Gold APN function and construct QAC corresponding to these quadratic APN functions. We tried to find new examples of quadratic APN functions by using Yu, Wang and Li approach. We discuss several cases for $n = 6,\ 7,\ 8$ in Appendix A.

Table 4.2: Quadratic APN functions from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$

No.	Δ-Rank	Γ-Rank	$\mid M(G_F) \mid$	Walsh Spectrum	# CCZ-inequivalent APN functions
1	454	14048	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	3168
2	454	14046	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	2696
3	454	14044	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	560
4	454	14050	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1116
5	454	14046	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	176
6	454	14044	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	42
7	454	14042	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	31
8	454	14048	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	204
9	454	14050	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	57
10	452	14048	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	32
11	452	14044	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	10
12	454	14042	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	3
13	452	14050	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	16
14	452	14048	256	{*-64[6],-32[2240],-16[20880],0[15600],16[23664],32[2880],64[10]*}	5
15	452	14046	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	22
16	454	14032	768	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
17	454	14048	256	{*-64[12],-32[2100],-16[21360],0[14880],16[24208],32[2700],64[20]*}	4
18	454	14040	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
19	454	14046	256	{*-64[12],-32[2100],-16[21360],0[14880],16[24208],32[2700],64[20]*}	6
20	452	14050	512	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
21	454	14050	512	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
22	446	14044	768	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
23	450	14048	256	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
24	454	14030	768	{*-64[12],-32[2100],-16[21360],0[14880],16[24208],32[2700],64[20]*}	1
25	446	14042	768	{*-32[2380],-16[20400],0[16320],16[23120],32[3060]*}	1
26	454	14038	768	{*-64[12],-32[2100],-16[21360],0[14880],16[24208],32[2700],64[20]*}	1

Chapter 5

Functions of the type $F(x) = x^3 + Tr_1^n(x)L(x)$

In this chapter, we are interested in studying some conditions on the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by

$$F(x) = x^d + Tr_1^n(x)L(x),$$

where $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ such that F is an APN function. First, we consider the particular case $d = 3$, then we discuss different cases of d listed in Table 1.2 such that F is an APN function.

5.1 Characterization of $F(x) = x^3 + Tr_1^n(x)L(x)$

In Section 4.2, we have discussed the Yu, Wang and Li approach for the construction of new quadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Recall that a quadratic APN function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ can be described in terms of cube C_{ij}^k, $1 \leq i, j, k \leq n$ of dimension $n \times n \times n$ defined over $\mathbb{F}_2$.
For $k = 1$, the matrix C_{ij}^1, $1 \leq i, j \leq n$ corresponds to the coordinate function f_1 of F. We can write the coordinate functions f_1 as

$$f_1(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n-1} c_{i,j}^1 x_i x_j + x_n L_1(x_1, \dots, x_{n-1}),\ c_{i,j}^1 \in \mathbb{F}_2.$$

Similarly, for $k = 2, \dots, n$, the matrices C_{ij}^k, $1 \leq i, j \leq n$ corresponds to the coordinate functions f_k of F. We can also write the coordinate functions f_k as

$$f_k(x_1, \dots, x_n) = \sum_{1 \leq i < j \leq n-1} c_{i,j}^k x_i x_j + x_n L_k(x_1, \dots, x_{n-1}),\ c_{i,j}^k \in \mathbb{F}_2,$$

here, $L_1, \dots, L_n$ are linear mappings from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$.
In Yu, Wang and Li approach, for $k = 1, \dots, n$, we change one row and column corresponds to x_n in the QAC C_{ij}^k with $1 \leq i, j \leq n$ to obtain a new QAC D_{ij}^k with

$1 \leq i, j, k \leq n$. This means we add x_n times a linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$ in each coordinate function of C_{ij}^k with $1 \leq i, j, k \leq n$.
For $k = 1$, the coordinate functions $f_1^{'}$ corresponds to D_{ij}^1, $1 \leq i, j \leq n$ is

$$f_1^{'}(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n-1} c_{i,j}^1 x_i x_j + x_n \left(L_1(x_1, \ldots, x_{n-1}) + L_1^{'}(x_1, \ldots, x_{n-1}) \right).$$

Similarly, for $k = 2, \ldots, n$, the coordinate functions $f_k^{'}$ corresponds to D_{ij}^k, $1 \leq i, j \leq n$ are

$$f_k^{'}(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n-1} c_{i,j}^k x_i x_j + x_n \left(L_k(x_1, \ldots, x_{n-1}) + L_k^{'}(x_1, \ldots, x_{n-1}) \right),$$

where, $c_{i,j}^k \in \mathbb{F}_2$.
Yu, Wang and Li have constructed several CCZ-inequivalent quadratic APN functions on $\mathbb{F}_{2^7}$ and $\mathbb{F}_{2^8}$ but they were unable to find an infinite family of APN functions. In order to find an infinite family of APN functions, it might be useful to have a representation in finite fields. The function

$$F(x) = x^3 + Tr_1^n(x)L(x),$$

where $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ can be obtained from a quadratic APN cube corresponding to the Gold APN function $F(x) = x^3$ by changing the entries $c_{i,j}^k$ with $1 \leq k \leq n$ and $i = n$ and $j = n$ in the cube $C_{i,j}^k$, $1 \leq i, j, k \leq n$.

Remark 5.1. The function

$$F(x) = x^3 + Tr_1^n(\alpha x)L_1(x) + Tr_1^n(\beta x)L_2(x), \ \alpha, \beta \in \mathbb{F}_{2^n}$$

where $L_1(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ and $L_2(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$, $b_i \in \mathbb{F}_{2^n}$ can be obtained from a quadratic APN cube corresponding to the Gold APN function $F(x) = x^3$ by changing the entries $c_{i,j}^k$ with $1 \leq k \leq n$, $i = n$, $i = n-1$ and $j = n$ and $j = n-1$ in the cube $C_{i,j}^k$, $1 \leq i, j, k \leq n$.

We are interested in studying the conditions such that F is an APN function. We can state the following lemma.

Lemma 5.2. *For any positive integer n and a linear function L from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^n}$ *defined by* $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, *the function*

$$F(x) = x^3 + Tr_1^n(x)L(x)$$

is APN if and only if for all $a \in \mathbb{F}_{2^n}$, $a \neq 0$,

$$x^2 a + a^2 x + Tr_1^n(x)L(a) + Tr_1^n(a)L(x) \neq 0 \ \textit{if } x \neq 0, \ a.$$

Proof. The function F is a quadratic function satisfying $F(0) = 0$. We can reformulate the APN condition in the following way: For any $a \in \mathbb{F}_{2^n}$, $a \neq 0$, we have

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

The above equation is equivalent to the following:

$$F(x+a) + F(x) + F(a) = (x+a)^3 + Tr_1^n(x+a)L(x+a) + (x)^3$$
$$+Tr_1^n(x)L(x) + a^3 + Tr_1^n(a)L(a).$$

After simplification, we have

$$F(x+a) + F(x) + F(a) = x^2a + a^2x + Tr_1^n(x)L(a) + Tr_1^n(a)L(x) = 0.$$

Therefore, we have

$$x^2a + a^2x + Tr_1^n(x)L(a) + Tr_1^n(a)L(x) \neq 0 \text{ if and only if } x \neq 0,\ a.$$

□

Now, we discuss further conditions on $L(x)$ such that the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $F(x) = x^3 + Tr_1^n(x)L(x)$ is APN or not.

Proposition 5.3. *Let n be a positive even integer. The functions F and G from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by $G(x) = x^3$ and $F(x) = x^3 + (x + x^2)Tr_1^n(x)$ are EA-equivalent.*

Proof. Let $L(x) = x + Tr_1^n(x)$. We claim that

$$G(L(x)) = F(x) + Tr_1^n(x).$$

Note that $L(x)$ is a permutation for any even n and $Tr_1^n(1) = 0$: Indeed,

$$x + Tr_1^n(x) = y + Tr_1^n(y),$$
$$x + y = Tr_1^n(x+y)$$

if and only if $x = y$.
Furthermore, we have

$$\begin{aligned} G(L(x)) &= (x + Tr_1^n(x))^3 \\ &= (x + Tr_1^n(x))^2(x + Tr_1^n(x)) \\ &= (x^2 + (Tr_1^n(x))^2)(x + Tr_1^n(x)) \end{aligned}$$

We use the fact $(Tr_1^n(x))^2 = Tr_1^n(x)$ to obtain

$$G(L(x)) = x^3 + (x + x^2)Tr_1^n(x) + Tr_1^n(x),$$

which implies that

$$G(L(x)) = F(x) + Tr_1^n(x).$$

□

In order to prove the Theorem 5.4, we need to define the following preliminary results. The Kloosterman sum of $a \in \mathbb{F}_{2^n}$ is defined as

$$K(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{Tr_1^n(x^{-1}+ax)},$$

where, we interpret $0^{-1} = 0$. For Kloosterman sums, the classical Weil inequality [68] is as follows:

$$\mid K(a) \mid \leq 2^{\frac{n}{2}+1}$$

Theorem 5.4. *Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as*

$$F(x) = x^3 + Tr_1^n(x)x.$$

The function F is not an APN function for $n \geq 3$.

Proof. We show that the equation

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

has more than two solutions for $a,\ b \in \mathbb{F}_{2^n}$ with $a \neq 0$. Note that $F(x)$ is a quadratic function, we can count the number of solutions of the equations

$$F(x+a) + F(x) + F(a) = 0.$$

This gives

$$F(x+a)+F(x)+F(a) = (x+a)^3 + Tr_1^n(x+a)(x+a) + x^3 + Tr_1^n(x)x + a^3 + Tr_1^n(a)a = 0.$$

After simplification, we have

$$x^2a + a^2x + Tr_1^n(x)a + Tr_1^n(a)x = 0. \tag{5.1}$$

Assume that if $Tr_1^n(a) = 0$, then equation (5.1) becomes

$$x^2a + a^2x + Tr_1^n(x)a = 0. \tag{5.2}$$

Case 1: Assume that $Tr_1^n(x) = 0$, then equation (5.2) becomes

$$x^2a + a^2x = 0.$$

The above equation has two solutions which are $\{0,\ a\}$.
Case 2: Assume that $Tr_1^n(x) = 1$, then equation (5.2) becomes

$$x^2a + a^2x + a = 0.$$

$$x^2 + ax + 1 = 0. \tag{5.3}$$

We want to prove that for some a with $Tr_1^n(a) = 0$, equation (5.3) has solutions with $Tr_1^n(x) = 1$. If we are able to show that there exist at least one a such that

equation (5.3) has solutions with $Tr_1^n(x) = 1$ and $Tr_1^n(a) = 0$, then the function F is not an APN function.
Let

$$x^2 + ax + 1 = (x+b)\left(x + \frac{1}{b}\right),$$

we will show that there exist b with $Tr_1^n(b) = 1$ and $Tr_1^n\left(b + \frac{1}{b}\right) = 0$. This implies that

$$x^2 + (b + \frac{1}{b})x + 1 = 0$$

has two solutions namely b and $\frac{1}{b}$ such that $Tr_1^n(b) = 1$. Therefore, the function F is not an APN function. Assume on the contrary that

$$\#\{b : Tr_1^n(b) = 1 \text{ and } Tr_1^n\left(b + \frac{1}{b}\right) = 0\} = 0$$

which implies that

$$\#\{b : Tr_1^n(b) = 1 \text{ and } Tr_1^n\left(\frac{1}{b}\right) = 1\} = 0.$$

This means

$$\sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} = 2^{n-1},$$

where $H = \{b \in \mathbb{F}_{2^n} : \; Tr_1^n(b) = 0\}$. We need to show that

$$\sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} \neq 2^{n-1},$$

We know that

$$\sum_{b \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(b^{-1})} = \sum_{b \in H} (-1)^{Tr_1^n(b^{-1})} + \sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} = 0.$$

From Kloosterman sum, we have

$$K(a) = \sum_{b \in \mathbb{F}_2^n} (-1)^{Tr_1^n(b^{-1} + ab)},$$

and

$$\begin{aligned}
K(1) &= \sum_{b \in \mathbb{F}_2^n} (-1)^{Tr_1^n(b^{-1} + b)} \\
&= \sum_{b \in H} (-1)^{Tr_1^n(b^{-1} + b)} + \sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1} + b)} \\
&= \sum_{b \in H} (-1)^{Tr_1^n(b^{-1})} - \sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} \\
&= -\sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} - \sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} \\
&= -2 \sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})}
\end{aligned}$$

which implies that

$$\sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} = -\frac{K(1)}{2}.$$

We know that the Weil inequality states that for any non-zero a,

$$\mid K(a) \mid \leq 2^{\frac{n}{2}+1},$$

which implies that

$$\sum_{b \in \mathbb{F}_{2^n} \setminus H} (-1)^{Tr_1^n(b^{-1})} =\mid \frac{K(1)}{2} \mid \leq 2^{\frac{n}{2}} < 2^{n-1}.$$

This shows that equation (5.3) has solutions and $Tr_1^n(a) = Tr_1^n(b + \frac{1}{b}) = 0$ implies that both solutions are either Trace 1 or Trace 0. This shows that the function F is not an APN function.

□

Remark 5.5. Faruk Göloğlu [69] suggests the proof of Theorem 5.4 using Kloostermann sums.

Remark 5.6. Note that our computational results also shows that the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as

$$F(x) = x^3 + Tr_1^n(x)x^2$$

is not an APN function for small values of n.

Remark 5.7. One of the reviewer of the thesis mentioned that the similar results as of Theorem 5.4 and Remark 5.6 by using different methods has also been mentioned in [60].

Remark 5.8. After the submission of the thesis, we have proved a necessary and sufficient condition on $L(x)$ such that $F(x) = x^3 + Tr_1^n(x)L(x)$ is an APN function which is as follows:
Let F be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined as

$$F(x) = x^3 + Tr_1^n(x)L(x).$$

Then F is APN if and only if

$$\sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{Tr_1^n\left(\frac{x^2L(x^2+x)}{(x^2+x)^3}\right)} - \frac{1}{2} \sum_{x \in \mathbb{F}_{2^n} \setminus \{0,1\}} (-1)^{Tr_1^n\left(\frac{L(x^2+x)}{(x^2+x)^3}\right)} = 2^{n-1} - 1.$$

5.2 Computational results for $F(x) = x^d + Tr_1^n(x)L(x)$

In this section, we discuss several computational results which are obtained by using different values of the exponent d such that the function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ defined by

$$F(x) = x^d + Tr_1^n(x)L(x),$$

where $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$ is an APN function.
We have listed our computational results in Tables 5.1, 5.2 and 5.3. Note that in Tables 5.1, 5.2 and 5.3, we consider the particular case of $L(x)$ in which $a_i \in \mathbb{F}_2$.
We did some additional computation in case of the Gold APN function $F(x) = x^3$ which is as follows.

Linearized polynomial of the form $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^2}$

We consider linearized polynomial of the form $L(x) = \sum_{i=0}^{1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^2}$.
For $n = 6$, we found 7 APN functions. All of them are CCZ-equivalent with $F(x) = x^3$.
For $n = 8$, we found 63 APN functions. One APN function is

$$F(x) = x^3 + Tr_1^8(x)(\alpha Tr_2^8(x)).$$

It is CCZ-equivalent to the APN function

$$F(x) = x^3 + \beta^{245}x^{33} + \beta^{183}x^{66} + \beta^{21}x^{144}$$

listed in Appendix 2 of [3].
Rest of them, that is 62 APN functions are CCZ-equivalent with either $F(x) = x^3$ or $F(x) = x^3 + Tr_1^8(x^9)$, here α is the root of $x^2 + x + 1$ and β is the root of $x^8 + x^4 + x^3 + x^2 + 1$.
For $n = 10$, we found one APN functions $F(x) = x^3 + Tr_1^{10}(x)Tr_1^{10}(x)$. It is already listed in Table 5.1.

Linearized polynomial of the form $L(x) = \sum_{i=0}^{1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$

Now, we consider linearized polynomial of the form $L(x) = \sum_{i=0}^{1} a_i x^{2^i}$, $a_i \in \mathbb{F}_{2^n}$.
For $n = 6$, we found 31 APN functions. All of them are CCZ-equivalent with $F(x) = x^3$.
For $n = 8$, we found 127 APN functions. All of them are CCZ-equivalent with $F(x) = x^3$
Based on our computational results on Gold APN function $F(x) = x^3$, we have formulated the following conjecture.

Conjecture 5.9. *Let $F(x) = x^3$ be an APN function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Let $L = \{L_1(x), L_2(x), \ldots, L_n(x)\}$ be a set of linearized polynomials with coefficients in $\mathbb{F}_{2^n}$. If*

Table 5.1: Classification of $F(x) = x^3 + Tr_1^n(x)L(x),\ L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}, a_i \in \mathbb{F}_2$

n	No.	$L(x)$	CCZ-Equivalence
6	6.1	$x + x^2$	x^3
	6.2	$x^4 + x^8 + x^{16} + x^{32}$	
	6.3	$Tr_1^6(x)$	
7	7.1	$x^2 + x^4 + x^{16}$	x^3
	7.2	$x + x^8 + x^{32} + x^{64}$	
	7.3	$Tr_1^7(x)$	
8	8.1	$x + x^2$	x^3
	8.2	$x + x^8 + x^{32} + x^{128}$	Table 1.2: No. 9
	8.3	$x + x^4 + x^{16} + x^{64}$	
	8.4	$x^2 + x^8 + x^{32} + x^{128}$	
	8.5	$x^2 + x^4 + x^{16} + x^{64}$	
	8.6	$x^4 + x^8 + x^{16} + x^{32} + x^{64} + x^{128}$	x^3
	8.7	$Tr_1^8(x)$	
9	9.1	$Tr_1^8(x)$	x^3
10	10.1	$x + x^2$	x^3
	10.2	$x^4 + x^8 + x^{16} + x^{32} + x^{64} + x^{128} + x^{256} + x^{512}$	
	10.3	$Tr_1^{10}(x)$	
11	11.1	$Tr_1^{11}(x)$	x^3

$G(x) = x^3 + Trace(x)l(x)$ is APN function for each $l \in L$, then the set L is a vector space.

Remark 5.10. Note that we make this conjecture for Gold APN function $F(x) = x^3$ only, see for instance, Tables 5.2 and 5.3.

5.3 A possible approach for the construction of nonquadratic APN function

There is one possible approach for the construction of nonquadratic APN functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$.

Let F be a quadratic APN function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We can describe F in terms of cube C_{ij}^k, $1 \leq i, j, k \leq n$ of dimension $n \times n \times n$ defined over $\mathbb{F}_2$.

In Yu, Wang and Li approach, we add x_n times a linear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$ in each coordinate function of C_{ij}^k with $1 \leq i, j, k \leq n$ to obtain a new quadratic APN cube D_{ij}^k with $1 \leq i, j, k \leq n$.

Yu, Wang and Li has used their approach for the construction of quadratic APN functions. We can extend their approach to search for nonquadratic APN functions.

Table 5.2: Classification of $F(x) = x^d + Tr_1^n(x)L(x),\ L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}, a_i \in \mathbb{F}_2$, *n odd*

n	No.	x^d	Families from Table 1.1	$L(x)$	CCZ-Equivalence
7	7.1	x^5	Gold	x^2	Table 7:No.2.2 [30]
	7.2			$x+x^2+x^{32}$	Table 7:No.12.1[30]
	7.3			$x^4+x^8+x^{16}+x^{64}$	Table 7:No.12.1[30]
	7.4			$x+x^4+x^8+x^{16}+x^{32}+x^{64}$	Table 7:No.2.2 [30]
	7.5			$Tr_1^7(x)$	x^5
	7.6	x^9		$x+x^{16}+x^{32}$	Table7:No.10.1[30]
	7.7			$x^2+x^4+x^8+x^{64}$	Table 7:No.10.1[30]
	7.8			$x^2+x^4+x^{32}$	Table 7:No.2.1[30]
	7.9			$x+x^8+x^{16}+x^{64}$	Table 7:No.2.1[30]
	7.10			$Tr_1^7(x)$	x^9
	7.11	x^{13}	Kasami	$Tr_1^7(x)$	x^{13}
	7.12	x^{57}			x^{57}
	7.13	x^{63}	Inverse		x^{63}
9	9.1	x^5	Gold	$Tr_1^9(x)$	x^5
	9.2	x^{17}			x^{17}
	9.3	x^{13}	Kasami		x^{13}
	9.4	x^{241}			x^{241}
	9.5	x^{19}	Welch		x^{19}
	9.6	x^{255}	Niho		x^{255}
11	11.1	x^5	Gold	$Tr_1^{11}(x)$	x^5
	11.2	x^9			x^9
	11.3	x^{17}			x^{17}
	11.4	x^{33}			x^{33}
	11.5	x^{13}	Kasami		x^{13}
	11.6	x^{57}			x^{57}
	11.7	x^{241}			x^{241}
	11.8	x^{993}			x^{993}
	11.9	x^{35}	Welch		x^{35}
	11.10	x^{287}	Niho		x^{287}
	11.11	x^{1023}	Inverse		x^{1023}

Table 5.3: Classification of $F(x) = x^d + Tr_1^n(x)L(x),\ L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}, a_i \in \mathbb{F}_2$, *n even*

n	No.	x^d	Families from Table 1.1	$L(x)$	CCZ-Equivalence
8	8.1	x^9	Gold	$x+x^2+x^{32}+x^{128}$	$x^3+x^6+x^{44}$
	8.2			$x^4+x^8+x^{16}+x^{64}$	
	8.3			$x+x^4+x^{16}+x^{64}$	
	8.4			$x^2+x^8+x^{32}+x^{128}$	
	8.5			$x+x^8$	x^9
	8.6			$x^2+x^4+x^{16}+x^{32}+x^{64}+x^{128}$	
	8.7			$Tr_1^8(x)$	
	8.6	x^{57}	Kasami	$Tr_1^8(x)$	x^{57}
10	10.1	x^9	Gold	$x+x^8$	x^9
	10.2			$x^2+x^4+x^{16}+x^{32}+x^{64}+x^{128}+x^{256}+x^{512}$	
	10.3			$Tr_1^{10}(x)$	
	10.4	x^{57}	Kasami	$Tr_1^{10}(x)$	Kasami
	10.5	x^{339}	Dobbertin	$Tr_1^{10}(x)$	Dobbertin

If we add x_n times a nonlinear mapping from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2$ in coordinate function of C_{ij}^k with $1 \leq i, j, k \leq n$ then we can get nonquadratic APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.
In terms of finite fields, if we add $Tr_1^n(x)Q(x)$ to any quadratic APN function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, where $Q(x)$ is any arbitrary polynomial from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ then we can also get a nonquadratic APN function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$.

Remark 5.11. Note that this approach is true for any APN functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. If Q is a linear function, then it is a special case of YWL approach.

Computational results

In this section, we discuss some partial results for $n = 6, 7, 8, 9, 10$ and 11. In all of these cases, we consider the following polynomial

$$Q(x) = a_{i,j}x^{2^i+2^j},$$

with $i, j = 0, \ldots, n-1,\ i < j$ and $a_{i,j} \in \mathbb{F}_{2^n},\ a_{i,j} \neq 0$. In this computational results, we used all possible $Q(x)$.
1. For $n = 6$, we consider the quadratic APN functions listed in Table 1.5. We added $Tr_1^6(x)Q(x)$ in each of the quadratic APN functions.
2. For $n = 7$, we consider the APN functions listed in Tables 1.2, 1.6 and Appendix 1 of Yu, Wang and Li paper [3]. We added $Tr_1^7(x)Q(x)$ in each of the APN functions.
3. For $n = 8$, we consider the APN functions listed in Tables 1.2, 1.6 and Table 9 of Edel and Pott paper [30]. We added $Tr_1^8(x)Q(x)$ in each of the APN function.
4. For $n = 9, 10, 11$, we consider the APN functions listed in Tables 1.2 and 1.6. We added $Tr_1^9(x)Q(x)$,$Tr_1^{10}(x)Q(x)$ and $Tr_1^{11}(x)Q(x)$ in each of the APN functions respectively.
For $n = 6, 7, 8, 9, 10, 11$, we checked the APN property of the modified functions. Unfortunately, we are unable to find any APN function.

Remark 5.12. Our computational results shows that for this very particular case of the polynomial $Q(x)$, it is not possible to find any nonquadratic APN functions for $n = 6, 7, 8, 9, 10, 11$.

5.4 A new construction method for APN functions

In this section, we propose a new method for the construction of APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. This method is based on the specific distribution of $n-2$ dimensional subspaces of $\mathbb{F}_2^n$. Our proposed construction method is as follows.

Theorem 5.13. *Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let U be an $n-2$ dimensional subspace of $\mathbb{F}_2^n$ and $U_0 = U,\ U_1 = U + v_1,\ U_2 = U + v_2$ and $U_3 = U + v_3$ are the four cosets of U such that $\mathbb{F}_2^n = U_0 \cup U_1 \cup U_2 \cup U_3$, where $v_1,\ v_2,\ v_3 \in \mathbb{F}_2^n$. Let $F^{'}$ be the function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined as*

$$F^{'}(x) = \begin{cases} F(x) + a_0, & \textit{for } x \in U_0, \\ F(x) + a_1, & \textit{for } x \in U_1, \\ F(x) + a_2, & \textit{for } x \in U_2, \\ F(x) + a_3, & \textit{for } x \in U_3, \end{cases}$$

with $a_i \in \mathbb{F}_2^n,\ i = 0, \ldots, 3$. The function $F^{'}$ is an APN function if and only if

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq a_0 + a_1 + a_2 + a_3$$

for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$ with $\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 1$ for all i.

Proof. Let U be an $n-2$ dimensional subspace of $V = \mathbb{F}_2^n$. We decompose V into four cosets of U such that $V = U_0 \cup U_1 \cup U_2 \cup U_3$, where $U_0 = U,\ U_1 = U + v_1$, $U_2 = U + v_2$ and $U_3 = U + v_3$ and $v_1,\ v_2,\ v_3 \in \mathbb{F}_2^n$. Assume that F is an APN function, it means that

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 0$$

for all 2-dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$. Recall that if $\{x_1, x_2, x_3, x_4\}$ is an affine 2-dimensional subspace of $\mathbb{F}_2^n$, then x_1, x_2, x_3, x_4 are pairwise different and $x_1 + x_2 + x_3 + x_4 = 0$. Now, we discuss the distribution of affine 2-dimensional subspaces $\{x_1, x_2, x_3, x_4\}$ in $U_i,\ i = 0, \ldots, 3$.
Assume that if $x_1, x_2, x_3 \in U_i$, then $x_4 \in U_i,\ i = 0, \ldots, 3$. Now, assume that $x_1, x_2 \in U_i,\ x_3 \in U_j$ and $x_4 \in U_k$ with i, j, k are pairwise different. Then, $x_1 + x_2 \in U_0$ and $x_3 + x_4 \notin U_0$. Therefore, $x_1 + x_2 + x_3 + x_4 = 0 \in U_0$ is not possible. The only possible distributions of x_1, x_2, x_3, x_4 are either $x_1, x_2, x_3, x_4 \in U_i$ for some i or $x_1, x_2 \in U_i$ and $x_3,\ x_4 \in U_j$ with $(i \neq j)$ or $\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 1$ for $i = 0, 1, 2, 3$.
Assume that

$$F^{'}(x) = \begin{cases} F(x) + a_0, & \text{for } x \in U_0, \\ F(x) + a_1, & \text{for } x \in U_1, \\ F(x) + a_2, & \text{for } x \in U_2, \\ F(x) + a_3, & \text{for } x \in U_3, \end{cases}$$

with $a_i \in \mathbb{F}_2^n,\ i = 0, \ldots, 3$. Then

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4)$$

if $\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 0$ or 2 for all i.
Assume that $\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 1$ for $i = 0, 1, 2, 3$. Then, we have

$$F^{'}(x_1)+F^{'}(x_2)+F^{'}(x_3)+F^{'}(x_4) = F(x_1)+F(x_2)+F(x_3)+F(x_4)+(a_0+a_1+a_2+a_3).$$

Let $A = a_0 + a_1 + a_2 + a_3$. It means that

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4) + A.$$

So, the function $F^{'}$ is an APN function if and only if

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq A$$

for all 2 dimensional affine subspaces $\{x_1, x_2, x_3, x_4\}$ of $\mathbb{F}_2^n$ with
$\mid \{x_1, x_2, x_3, x_4\} \cap U_i \mid= 1$ for all i. □

Computational Results

We apply Theorem 5.13 on the known examples APN functions for $n = 6, 8$ and $n = 10$. First, we discuss the case $n = 6$.

Case $n = 6$

We choose quadratic APN function $D.1$ from Table 1.5. We apply Theorem 5.13 on $D.1$. We found the following example.

Example 5.14. Let F be an APN function from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ defined as $F(x) = x^3$. First, we decompose $\mathbb{F}_{2^6}$ into four set $U_0,\ U_1,\ U_2,\ U_3$ such that

$$U_0 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = 0\},$$
$$U_1 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = 1\},$$
$$U_2 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = \alpha\},$$
$$U_3 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = \alpha^2\},$$

where α is the root of $x^2 + x + 1$.
Now, we choose all $x_1 \in U_0,\ x_2 \in U_1,\ x_3 \in U_2$ and $x_4 \in U_3$ in such a way that

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Then, we compute

$$w = \{F(x_1) + F(x_2) + F(x_3) + F(x_4)\} \subseteq \mathbb{F}_{2^6},$$

where $x_1 + x_2 + x_3 + x_4 = 0$ and $x_i \in U_i,\ i = 0, \ldots, 3$.
We found that $T = \mathbb{F}_{2^6} \setminus w = \{0, \beta^7, \beta^{14}, \beta^{28}, \beta^{35}, \beta^{49}, \beta^{56}\}$, here β is the root of $x^6 + x^4 + x^3 + x + 1$.

We can choose $a_0,\ a_1,\ a_2,\ a_3 \in \mathbb{F}_{2^6}$ such that $a_0 + a_1 + a_2 + a_3 = \beta^7$. Assume that
if $x \in U_0$, then $F^{'}(x) = F(x) + a_0$,
if $x \in U_1$, then $F^{'}(x) = F(x) + a_1$,
if $x \in U_2$, then $F^{'}(x) = F(x) + a_2$,
if $x \in U_3$, then $F^{'}(x) = F(x) + a_3$.
Note that

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4) + \beta^7.$$

Since

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq \beta^7,$$

we have

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) \neq 0$$

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^6}$ with $x_1 + x_2 + x_3 + x_4 = 0$, as we know that $Tr_1^6(x) = Tr_1^2(Tr_2^6(x)) = Tr_2^6(x) + (Tr_2^6(x))^2$. If $Tr_2^6(x) = 0$, then $Tr_1^6(x) = 0$. Similarly, if $Tr_2^6(x) = 1, Tr_2^6(x) = \alpha, Tr_2^6(x) = \alpha^2$ then $Tr_1^6(x) = 0, Tr_1^6(x) = 1, Tr_1^6(x) = 1$ respectively. This means if $Tr_1^6(x) = 1$ then we add

$$\beta^7\alpha + \beta^7\alpha^2 = \beta^7(\alpha + \alpha^2) = \beta^7$$

to the function $F(x)$ to obtain the function $F^{'}(x)$. The function $F^{'}$ from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ is defined as

$$F^{'}(x) = x^3 + Tr_1^6(x)(\beta^7 Tr_2^6(x))$$

is an APN function.

Remark 5.15. We have checked the CCZ-equivalence of

$$F^{'}(x) = x^3 + Tr_1^6(x)(\beta^7 Tr_2^6(x))$$

with known examples of the APN functions. We found that $F^{'}(x)$ is CCZ-equivalent to APN function $D.2$ of Table 1.5.
Note that for other values of $T \setminus \{0\}$ in Example 5.14, we have CCZ-equivalent APN functions with $F^{'}(x)$.
In the subsequent examples, we have tried all possible values of $a_0, a_1, a_2$and a_3 and we found several APN functions but all of them are CCZ-equivalent with $F^{'}(x)$.
Also, note that checking CCZ-equivalence between $F(x)$ and $F^{'}(x)$ means that we are checking code equivalence between $F(x)$ and $F^{'}(x)$.

Next, we choose quadratic APN function $D.2$ from Table 1.5. We apply Theorem 5.13 on $D.2$. We found the following example.

Example 5.16. Let F be an APN function from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ defined as

$$F(x) = x^3 + \beta^{11}x^6 + \beta x^9,$$

here β is the root of $x^6 + x^4 + x^3 + x + 1$.
First, we decompose $\mathbb{F}_{2^6}$ into four set $U_0,\ U_1,\ U_2,\ U_3$ such that

$$U_0 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = 0\},$$

$$U_1 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = 1\},$$

$$U_2 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = \alpha\},$$

$$U_3 = \{x \in \mathbb{F}_{2^6} : Tr_2^6(x) = \alpha^2\},$$

α is the root of $x^2 + x + 1$.
Now, we choose all $x_1 \in U_0,\ x_2 \in U_1,\ x_3 \in U_2$ and $x_4 \in U_3$ in such a way that

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Then, we compute

$$w = \{F(x_1) + F(x_2) + F(x_3) + F(x_4)\} \subseteq \mathbb{F}_{2^6},$$

where $x_1 + x_2 + x_3 + x_4 = 0$ and $x_i \in U_i,\ i = 0, \ldots, 3$.
We found that $T = \mathbb{F}_{2^6} \setminus w = \{0, \beta^{12}, \beta^{21}, \beta^{24}, \beta^{27}, \beta^{46}, \beta^{58}\}$.
We can choose $a_0,\ a_1,\ a_2,\ a_3 \in \mathbb{F}_{2^8}$ such that $a_0 + a_1 + a_2 + a_3 = \beta^{12}$. Assume that
if $x \in U_0$, then $F^{'}(x) = F(x) + a_0$,
if $x \in U_1$, then $F^{'}(x) = F(x) + a_1$,
if $x \in U_2$, then $F^{'}(x) = F(x) + a_2$,
if $x \in U_3$, then $F^{'}(x) = F(x) + a_3$.
Note that

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4) + \beta^{12}.$$

Since

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq \beta^{12},$$

we have

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) \neq 0$$

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$ with $x_1 + x_2 + x_3 + x_4 = 0$,
as we know that $Tr_1^6(x) = Tr_1^2(Tr_2^6(x)) = Tr_2^6(x) + (Tr_2^6(x))^2$.
If $Tr_2^6(x) = 0$, then $Tr_1^6(x) = 0$. Similarly, if $Tr_2^6(x) = 1, Tr_2^6(x) = \alpha, Tr_2^6(x) = \alpha^2$ then $Tr_1^6(x) = 0, Tr_1^6(x) = 1, Tr_1^6(x) = 1$ respectively. This means if $Tr_1^6(x) = 1$ then we add

$$\beta^{12}\alpha + \beta^{12}\alpha^2 = \beta^{12}(\alpha + \alpha^2) = \beta^{12}$$

to the function $F(x)$ to obtain the function $F^{'}(x)$. The function $F^{'}$ from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ is defined as

$$F^{'}(x) = x^3 + \beta^{11}x^6 + \beta x^9 + Tr_1^6(x)(\beta^{12}Tr_2^6(x))$$

is an APN function.

Remark 5.17. We have checked the CCZ-equivalence of

$$F^{'}(x) = x^3 + \beta^{11}x^6 + \beta x^9 + Tr_1^6(x)(\beta^{12}Tr_2^6(x))$$

with known examples of APN functions. We found that $F^{'}(x)$ is CCZ-equivalent to APN function $D.2$ of Table 1.5.
Note that for other values of $T \setminus \{0\}$ in Example 5.16, we have CCZ-equivalent APN functions with $F^{'}(x)$.

Similary, We apply Theorem 5.13 on $D.3, \ldots, D.13$. We found the following examples. Note that we use the same procedure as we discussed in Examples 5.14 and 5.16.

Example 5.18. The function F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ is defined as

$$F(x) = x^3 + \beta^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + Tr_1^6(x)(\beta^9 Tr_2^6(x))$$

is an APN function, here β is the root of $x^6 + x^4 + x^3 + x + 1$.

Remark 5.19. We have checked the CCZ-equivalence of

$$F(x) = x^3 + \beta^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + Tr_1^6(x)(\beta^9 Tr_2^6(x))$$

with known examples of APN functions. We found that $F(x)$ is CCZ-equivalent to APN function $D.13$ of Table 1.5. In this example, we have $T = \{0, \beta^9\}$.

Example 5.20. The function F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ is defined as

$$F(x) = \beta^{25}x^5 + x^9 + \beta^{38}x^{12} + \beta^{25}x^{18} + \beta^{25}x^{36} + Tr_1^6(x)(\beta^{46}Tr_2^6(x))$$

is an APN function, here β is the root of $x^6 + x^4 + x^3 + x + 1$.

Remark 5.21. We have checked the CCZ-equivalence of

$$F(x) = \beta^{25}x^5 + x^9 + \beta^{38}x^{12} + \beta^{25}x^{18} + \beta^{25}x^{36} + Tr_1^6(x)(\beta^{46}Tr_2^6(x))$$

with known examples of APN functions. We found that $F(x)$ is CCZ-equivalent to APN function $D.10$ of Table 1.5. In this example, we have $T = \{0, \beta^{46}\}$.

Example 5.22. The function F from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$ is defined as

$$F(x) = \beta^{34}x^6 + \beta^{52}x^9 + \beta^{48}x^{12} + \beta^6x^{20} + \beta^9x^{33} + \beta^{23}x^{34} + \beta^{25}x^{40} + Tr_1^6(x)(\beta^{36}Tr_2^6(x))$$

is an APN function, here β is the root of $x^6 + x^4 + x^3 + x + 1$.

Remark 5.23. We have checked the CCZ-equivalence of

$$F(x) = \beta^{34}x^6 + \beta^{52}x^9 + \beta^{48}x^{12} + \beta^6x^{20} + \beta^9x^{33} + \beta^{23}x^{34} + \beta^{25}x^{40} + Tr_1^6(x)(\beta^{36}Tr_2^6(x))$$

with known examples of APN functions. We found that $F(x)$ is CCZ-equivalent to APN function $D.13$ of Table 1.5. In this example, we have $T = \{0, \beta^{36}\}$.

Case $n = 8$

There are 8180 quadratic APN functions listed in Appendix 2 of YWL paper [3]. It is computationally intensive to apply Theorem 5.13 to 8180 quadratic APN functions. We choose first 23 APN functions from Appendix 2 of YWL paper. These 23 APN functions are also listed in Table 9 of Edel and Pott paper [30]. We apply Theorem 5.13 on these 23 APN functions. We found the following examples.

Example 5.24. Let F be an APN function from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ defined as $F(x) = x^3$. First, we decompose $\mathbb{F}_{2^8}$ into four set $U_0,\ U_1,\ U_2,\ U_3$ such that

$$U_0 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = 0\},$$

$$U_1 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = 1\},$$

$$U_2 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = \alpha\},$$

$$U_3 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = \alpha^2\},$$

where α is the root of $x^2 + x + 1$.
Now, we choose all $x_1 \in U_0,\ x_2 \in U_1,\ x_3 \in U_2$ and $x_4 \in U_3$ in such a way that

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Then, we compute

$$w = \{F(x_1) + F(x_2) + F(x_3) + F(x_4)\} \subseteq \mathbb{F}_{2^8},$$

where $x_1 + x_2 + x_3 + x_4 = 0$ and $x_i \in U_i,\ i = 0, \ldots, 3$.
We found that $T = \mathbb{F}_{2^8} \setminus w = \{0,\ 1,\ \beta^{85},\ \beta^{170}\}$, here β is the root of $x^8 + x^4 + x^3 + x^2 + 1$. We can choose $a_0,\ a_1,\ a_2,\ a_3 \in \mathbb{F}_{2^8}$ such that $a_0 + a_1 + a_2 + a_3 = \beta^{85}$. Assume that
if $x \in U_0$, then $F'(x) = F(x) + a_0$,
if $x \in U_1$, then $F'(x) = F(x) + a_1$,
if $x \in U_2$, then $F'(x) = F(x) + a_2$,
if $x \in U_3$, then $F'(x) = F(x) + a_3$.
Note that

$$F'(x_1) + F'(x_2) + F'(x_3) + F'(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4) + \beta^{85}.$$

Since

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq \beta^{85},$$

we have

$$F'(x_1) + F'(x_2) + F'(x_3) + F'(x_4) \neq 0$$

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$ with $x_1 + x_2 + x_3 + x_4 = 0$, as we know that $Tr_1^8(x) = Tr_1^2(Tr_2^8(x)) = Tr_2^8(x) + (Tr_2^8(x))^2$. If $Tr_2^8(x) = 0$, then $Tr_1^8(x) = 0$. Similarly, if

$Tr_2^8(x) = 1, Tr_2^8(x) = \alpha, Tr_2^8(x) = \alpha^2$ then $Tr_1^8(x) = 0, Tr_1^8(x) = 1$, $Tr_1^8(x) = 1$ respectively. This means if $Tr_1^8(x) = 1$ then we add

$$\beta^{85}\alpha + \beta^{85}\alpha^2 = \beta^{85}(\alpha + \alpha^2) = \beta^{85}$$

to the function $F(x)$ to obtain the function $F^{'}(x)$.
The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as

$$F^{'}(x) = x^3 + Tr_1^8(x)(\beta^{85}Tr_2^8(x))$$

is an APN function.

Remark 5.25. We have checked the CCZ-equivalence of $F^{'}(x) = x^3 + Tr_1^8(x)(\beta^{85}Tr_2^8(x))$ with known examples of APN functions. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^3 + \beta^{245}x^{33} + \beta^{183}x^{66} + \beta^{21}x^{144}$$

listed in Appendix 2 of [3].

Now, we apply Theorem 5.13 on the function $F(x) = x^9$. We found the following example.

Example 5.26. Let F be an APN function from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ defined as $F(x) = x^9$. First, we decompose $\mathbb{F}_{2^8}$ into four set $U_0,\ U_1,\ U_2,\ U_3$ such that

$$U_0 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = 0\},$$

$$U_1 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = 1\},$$

$$U_2 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = \alpha\},$$

$$U_3 = \{x \in \mathbb{F}_{2^8} : Tr_2^8(x) = \alpha^2\},$$

where α is the root of $x^2 + x + 1$.
Now, we choose all $x_1 \in U_0,\ x_2 \in U_1,\ x_3 \in U_2$ and $x_4 \in U_3$ in such a way that

$$x_1 + x_2 + x_3 + x_4 = 0.$$

Then, we compute

$$w = \{F(x_1) + F(x_2) + F(x_3) + F(x_4)\} \subseteq \mathbb{F}_{2^8},$$

where $x_1 + x_2 + x_3 + x_4 = 0$ and $x_i \in U_i,\ i = 0, \ldots, 3$.
We found that $T = \mathbb{F}_{2^8} \setminus w = \{0,\ 1,\}$.
We can choose $a_0,\ a_1,\ a_2,\ a_3 \in \mathbb{F}_{2^8}$ such that $a_0 + a_1 + a_2 + a_3 = 1$. Assume that
if $x \in U_0$, then $F^{'}(x) = F(x) + a_0$,
if $x \in U_1$, then $F^{'}(x) = F(x) + a_1$,
if $x \in U_2$, then $F^{'}(x) = F(x) + a_2$,

if $x \in U_3$, then $F^{'}(x) = F(x) + a_3$.
Note that

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) = F(x_1) + F(x_2) + F(x_3) + F(x_4) + 1.$$

Since

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 1,$$

we have

$$F^{'}(x_1) + F^{'}(x_2) + F^{'}(x_3) + F^{'}(x_4) \neq 0$$

for all $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8}$ with $x_1 + x_2 + x_3 + x_4 = 0$, as we know that $Tr_1^8(x) = Tr_1^2(Tr_2^8(x)) = Tr_2^8(x) + (Tr_2^8(x))^2$. If $Tr_2^8(x) = 0$, then $Tr_1^8(x) = 0$. Similarly, if $Tr_2^8(x) = 1, Tr_2^8(x) = \alpha, Tr_2^8(x) = \alpha^2$ then $Tr_1^8(x) = 0, Tr_1^8(x) = 1, Tr_1^8(x) = 1$ respectively. This means if $Tr_1^8(x) = 1$ then we add

$$\alpha + \alpha^2 = 1$$

to the function $F(x)$ to obtain the function $F^{'}(x)$.
The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as

$$F^{'}(x) = x^9 + Tr_1^8(x)(Tr_2^8(x))$$

is an APN function.

Remark 5.27. We have checked the CCZ-equivalence of $F^{'}(x) = x^9 + Tr_1^8(x)(Tr_2^8(x))$ with known examples of APN functions. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^3 + x^6 + x^{44}$$

listed in Appendix 2 of [3].

Now, we apply Theorem 5.13 on remaining 21 APN functions listed in Appendix 2 of [3]. We found the following examples. Note that we use the same procedure as we discussed in Examples 5.24 and 5.26.

Example 5.28. The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as

$$F^{'}(x) = x^3 + x^6 + x^{72} + Tr_1^8(x)(\beta^{85} Tr_2^8(x))$$

is an APN function, here β is the root of $x^8 + x^4 + x^3 + x^2 + 1$.

Remark 5.29. We have checked the CCZ-equivalence of

$$F^{'}(x) = x^3 + x^6 + x^{72} + Tr_1^8(x)(\beta^{85} Tr_2^8(x))$$

with known examples of APN functions listed in Appendix 2 of [3]. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^3 + \beta^{245} x^{33} + \beta^{183} x^{66} + \beta^{21} x^{144}.$$

In this example, we have $T = \{0, 1, \beta^{85}, \beta^{170}\}$. Note that for other values of $T \setminus \{0\}$, we have CCZ-equivalent APN functions with $F^{'}(x)$.

Example 5.30. The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as

$$F^{'}(x) = x^3 + x^6 + x^{144} + Tr_1^8(x)(Tr_2^8(x))$$

is an APN function.

Remark 5.31. We have checked the CCZ-equivalence of

$$F^{'}(x) = x^3 + x^6 + x^{144} + Tr_1^8(x)(Tr_2^8(x))$$

with known examples of APN functions listed in Appendix 2 of [3]. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^9.$$

In this example, we have $T = \{0, 1\}$.

Example 5.32. The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as
$F^{'}(x) = \beta^{126}x^{192} + \beta^{119}x^{144} + \beta^{221}x^{132} + \beta^{222}x^{129} + \beta^{79}x^{96} + \beta^{221}x^{72} + \beta^{187}x^{66} + \beta^{148}x^{48}$
$+ \beta^{187}x^{36} + \beta^{237}x^{24} + \beta^{231}x^{12} + \beta^{119}x^{9} + \beta^{244}x^{6} + \beta^{236}x^{3} + Tr_1^8(x)(Tr_2^8(x))$
is an APN function, here β is the root of $x^8 + x^4 + x^3 + x^2 + 1$.

Remark 5.33. We have checked the CCZ-equivalence of
$F^{'}(x) = \beta^{126}x^{192} + \beta^{119}x^{144} + \beta^{221}x^{132} + \beta^{222}x^{129} + \beta^{79}x^{96} + \beta^{221}x^{72} + \beta^{187}x^{66} +$
$\beta^{148}x^{48} + \beta^{187}x^{36} + \beta^{237}x^{24} + \beta^{231}x^{12} + \beta^{119}x^{9} + \beta^{244}x^{6} + \beta^{236}x^{3} + Tr_1^8(x)(Tr_2^8(x))$
with known examples of APN functions listed in Appendix 2 of [3]. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^3 + x^6 + x^{72}.$$

In this example, we have $T = \{0, 1\}$.

Example 5.34. The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as
$F^{'}(x) = \beta^{86}x^{192} + \beta^{224}x^{129} + \beta^{163}x^{96} + \beta^{102}x^{66} + \beta^{129}x^{48} + \beta^{102}x^{36} + \beta^{170}x^{33} +$
$\beta^{14}x^{24} + \beta^{170}x^{18} + \beta^{101}x^{12} + \beta^{58}x^{6} + \beta^{254}x^{3} + Tr_1^8(x)(Tr_2^8(x))$
is an APN function, here β is the root of $x^8 + x^4 + x^3 + x^2 + 1$.

Remark 5.35. We have checked the CCZ-equivalence of
$F^{'}(x) = \beta^{86}x^{192} + \beta^{224}x^{129} + \beta^{163}x^{96} + \beta^{102}x^{66} + \beta^{129}x^{48} + \beta^{102}x^{36} + \beta^{170}x^{33} +$
$\beta^{14}x^{24} + \beta^{170}x^{18} + \beta^{101}x^{12} + \beta^{58}x^{6} + \beta^{254}x^{3} + Tr_1^8(x)(Tr_2^8(x))$
with known examples of APN functions listed in Appendix 2 of [3]. We found that $F^{'}(x)$ is CCZ-equivalent to APN function
$F(x) = \beta^{126}x^{192} + \beta^{119}x^{144} + \beta^{221}x^{132} + \beta^{222}x^{129} + \beta^{79}x^{96} + \beta^{221}x^{72} + \beta^{187}x^{66} +$
$\beta^{148}x^{48} + \beta^{187}x^{36} + \beta^{237}x^{24} + \beta^{231}x^{12} + \beta^{119}x^{9} + \beta^{244}x^{6} + \beta^{236}x^{3} + Tr_1^8(x)(Tr_2^8(x)).$
In this example, we have $T = \{0, 1\}$.

Example 5.36. The function $F^{'}$ from $\mathbb{F}_{2^8}$ to $\mathbb{F}_{2^8}$ is defined as
$F^{'}(x) = \beta^{113}x^{192} + \beta^{56}x^{144} + \beta^{68}x^{132} + \beta^{155}x^{129} + \beta^{91}x^{96} + \beta^{78}x^{72} + \beta^{159}x^{66} + \beta^{30}x^{48}$
$+ \beta^{194}x^{36} + \beta^{14}x^{33} + \beta^{238}x^{24} + \beta^{91}x^{18} + \beta^{100}x^{12} + \beta^{96}x^{9} + \beta^{222}x^{6} + \beta^{178}x^{3} +$
$Tr_1^8(x)(Tr_2^8(x))$
is an APN function, here β is the root of $x^8 + x^4 + x^3 + x^2 + 1$.

Remark 5.37. We have checked the CCZ-equivalence of
$F^{'}(x) = \beta^{113}x^{192} + \beta^{56}x^{144} + \beta^{68}x^{132} + \beta^{155}x^{129} + \beta^{91}x^{96} + \beta^{78}x^{72} + \beta^{159}x^{66} + \beta^{30}x^{48} +$
$\beta^{194}x^{36} + \beta^{14}x^{33} + \beta^{238}x^{24} + \beta^{91}x^{18} + \beta^{100}x^{12} + \beta^{96}x^{9} + \beta^{222}x^{6} + \beta^{178}x^{3} + Tr_1^8(x)(Tr_2^8(x))$
with known examples of APN functions listed in Appendix 2 of [3]. We found that $F^{'}(x)$ is CCZ-equivalent to APN function

$$F(x) = x^3 + \beta^{245}x^{33} + \beta^{183}x^{66} + \beta^{21}x^{144}.$$

In this example, we have $T = \{0, 1\}$.

Case $n = 10$

In this case, we applied Theorem 5.13 on the following functions
$F_1(x) = x^3$ (Gold APN function in Table 1.2)
$F_2(x) = x^9$ (Gold APN function in Table 1.2)
$F_3(x) = x^{57}$ (Kasami APN function in Table 1.2)
$F_4(x) = x^{339}$ (Dobbertin APN function in Table 1.2)
$F_5(x) = x^6 + x^{33} + \beta^{31}x^{192}$ (M.7 in Table 1.6)
$F_6(x) = x^{33} + x^{72} + \beta^{31}x^{258}$ (M.7 in Table 1.6)
$F_7(x) = x^3 + Tr_1^{10}(x^9)$ (M.9 in Table 1.6)
$F_8(x) = x^3 + \beta^{1012}x^{33}$ Table 1.4

Remark 5.38. Unfortunately, we are unable to find the set w for the above listed APN functions on $\mathbb{F}_{2^{10}}$.

Chapter 6

Equivalence of Göloğlu infinite family of APN functions

In Section 6.1, we discuss the Göloğlu infinite family of APN functions. In Section 6.2, we prove that the Göloğlu family of APN functions is extended affine equivalent to the Gold family of APN functions. In Section 6.3, we discuss an error in MAGMA, which occurs during the testing of code equivalence between the Göloğlu and the Gold family of APN functions.

6.1 Göloğlu family of APN functions

We have discussed in Theorem 4.11 that Budaghyan, Carlet and Leander found an infinite family of APN functions by using the switching approach. It is an interesting problem to find other families of APN functions similar to Budaghyan, Carlet and Leander family of APN functions.
In 2015, Göloğlu found a family of APN functions which is similar to Budaghyan, Carlet and Leander family of APN function. The Göloğlu family of APN functions is described as follows.

Theorem 6.1. *[70] Let $F_k : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a function defined by*

$$F_k(x) = x^{2^k+1} + (Tr^n_m(x))^{2^k+1}$$

and $n = 2m$, $Tr^n_m(x) = x + x^{2^m}$. The function F_k is APN on $\mathbb{F}_{2^n}$ if and only if m is even and $gcd(k, n) = 1$.

There are three interesting properties of the Göloğlu family of APN functions. The first property of the Göloğlu family is that it is obtained by the addition of a vectorial Boolean function to the Gold family of APN functions. The second property of the Göloğlu family is that the polynomial coefficients are from the simplest possible field $\mathbb{F}_2$. The third property of the Göloğlu family is that his family of APN functions satisfies the subspace property. The subspace property of vectorial Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is defined in the following way. Let $n = 2m$ be a positive integer. A function F from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ satisfies the subspace property if there is an integer k such that

$$F(\lambda x) = \lambda^{2^k+1}F(x)$$

for every $\lambda \in \mathbb{F}_{2^m}$.
The subspace property is studied in the context of APN permutations with n even. The first APN permutation was found in 2009 by Dillon [58] which is CCZ-equivalent to the Kim function k from $\mathbb{F}_{2^6}$ to $\mathbb{F}_{2^6}$. The Kim function is

$$k(x) = x^3 + x^{10} + \alpha x^{24},$$

where α is the primitive element of $\mathbb{F}_{2^6}^*$. The Kim function is the only known APN function that satisfies the subspace property.

6.2 Equivalence of Göloğlu APN functions

In this section, we prove that the Göloğlu family of APN functions is EA equivalent to the Gold family of APN functions.

Theorem 6.2. *Let $n = 2m = 4t$, where m is an even positive integer and $t > 0$. Let Tr_m^n is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$: $Tr_m^n(x) = x + x^q$, where $q = 2^m$. The APN function*

$$F(x) = x^{2^k+1} + (Tr_m^n(x))^{2^k+1}$$

is EA equivalent to Gold APN function

$$G(x) = x^{q^2/2^k+q}$$

with $gcd(k,n) = 1$.

Proof. Let α be primitive element of $\mathbb{F}_4$. Let L_1, L_2 be the linear mappings defined by

$$L_1(x) = \alpha x^{2^k q} + \alpha^2 x^{2^k}$$

and

$$L_2(y) = \alpha^2 y^q + \alpha y.$$

Note that $\alpha^q = \alpha$, $\alpha^{2^k} = \alpha^2$, $\alpha^{2^{1-k}} = \alpha$, $\alpha + \alpha^2 = 1$. The linear mappings $L_1(x)$ and $L_2(x)$ are permutations. Indeed, it is easy to see that $L_1(x) = 0$ and $L_2(y) = 0$ have only 0 as a solution.
If $L_2(y) = 0$, this implies that $L_2^q(y) = 0$, which gives

$$\alpha^2 y^q + \alpha y = 0 \Rightarrow \alpha^2 y^q = \alpha y$$

and

$$(\alpha^2 y^q + \alpha y)^q = 0 \Rightarrow \alpha^{2q} y^{q^2} = \alpha^q y^q$$

Assume that $y \neq 0$, multiply both sides of the above equations, we get

$$\alpha^{2q+2} = \alpha^{q+1}$$

$$\alpha = \alpha^2$$

which contradicts the fact that α is the primitive element of $\mathbb{F}_4$.
Similarly, $L_1(x) = 0$ implies that $L_1^q(x) = 0$, which gives

$$\alpha x^{2^k q} + \alpha^2 x^{2^k} = 0 \Rightarrow \alpha x^{2^k q} = \alpha^2 x^{2^k}$$

and

$$(\alpha x^{2^k q} + \alpha^2 x^{2^k})^q = 0 \Rightarrow \alpha^q x^{2^k q^2} = \alpha^{2q} x^{2^k q}$$

Assume that $x \neq 0$, multiply both sides of the above equations, we get

$$\alpha^{q+1} = \alpha^{2q+2}$$

$$\alpha^2 = \alpha$$

which contradicts the fact that α is the primitive element of $\mathbb{F}_4$. Now, we have

$$\begin{aligned} G \circ L_1(x) &= \left(\alpha x^{2^k q} + \alpha^2 x^{2^k}\right)^{q^2/2^k + q} \\ &= \left(\alpha x^{2^k q} + \alpha^2 x^{2^k}\right)^{q^2/2^k} \left(\alpha x^{2^k q} + \alpha^2 x^{2^k}\right)^q \\ &= \left(\alpha^{q^2/2^k} x^{q^3} + \alpha^{2^{1-k} q^2} x^{q^2}\right) \left(\alpha^q x^{2^k q^2} + \alpha^{2q} x^{2^k q}\right) \\ &= \left(\alpha^2 x^q + \alpha x\right) \left(\alpha x^{2^k} + \alpha^2 x^{2^k q}\right) \\ &= \alpha^3 x^{2^k + q} + \alpha^4 x^{2^k q + q} + \alpha^2 x^{2^k + 1} + \alpha^3 x^{2^k q + 1} \end{aligned}$$

Since $\alpha^3 = 1$ and $\alpha^2 + \alpha = 1$,then the above equation becomes

$$\begin{aligned} G \circ L_1(x) &= x^{2^k + q} + \alpha x^{2^k q + q} + \alpha^2 x^{2^k + 1} + x^{2^k q + 1} \\ &= \left(\alpha^2 + \alpha\right) x^{2^k + q} + \alpha x^{2^k q + q} + \alpha^2 x^{2^k + 1} + \left(\alpha^2 + \alpha\right) x^{2^k q + 1} \\ &= \alpha^2 x^{2^k + q} + \alpha x^{2^k + q} + \alpha x^{2^k q + q} + \alpha^2 x^{2^k + 1} + \alpha^2 x^{2^k q + 1} + \alpha x^{2^k q + 1} \end{aligned}$$

After combining terms with same coefficients, we get

$$G \circ L_1(x) = \alpha^2 \left(x^{2^k + q} + x^{2^k + 1} + x^{2^k q + 1}\right) + \alpha \left(x^{2^k + q} + x^{2^k q + q} + x^{2^k q + 1}\right)$$

Re-arranging the terms, we get

$$\begin{aligned} G \circ L_1(x) &= \alpha^2 \left(x^{2^k+1} + x^{2^k+q} + x^{2^kq+1}\right) + \alpha \left(x^{(2^k+1)q} + x^{2^kq+1} + x^{2^k+q}\right) \\ &= \alpha^2 \left(x^{(2^k+1)q} + x^{2^kq+1} + x^{2^k+q}\right)^q + \alpha \left(x^{(2^k+1)q} + x^{2^kq+1} + x^{2^k+q}\right) \\ &= \alpha^2 \left(x^{2^k+1} + (tr_m^n(x))^{2^k+1}\right)^q + \alpha \left(x^{2^k+1} + (tr_m^n(x))^{2^k+1}\right) \\ &= \alpha^2 \left(F(x)\right)^q + \alpha \left(F(x)\right) \\ &= L_2 \circ F(x). \end{aligned}$$

□

Remark 6.3. Note that $G^{'}(x) = (G(x))^q = (x^{q^2/2^k+q})^q = (x^{2^{m-k}+1})$ is the equivalent representation of $G(x)$.

Remark 6.4. The above proof follows the same line of proof given in corollary 2 of [50].

Remark 6.5. Budaghyan, Helleseth, Li and Sun has independently uploaded the same results on IACR archive [71].

6.3 MAGMA Computation Error

In this section, we discuss the reason why Göloğlu believes that his family of APN functions is new up to CCZ-equivalence. As we know that there does not exist any theoretical method for checking of CCZ-equivalence between two APN functions. Göloğlu checked the CCZ-equivalence of his family of APN functions with other infinite families of APN function by using the MAGMA [4] built in test for code equivalence.

On $\mathbb{F}_{2^8}$, he found that his family of APN functions is CCZ-equivalent to the Gold family of APN function. On $\mathbb{F}_{2^{12}}$, due to computational error in MAGMA built in test for code equivalence, he found that his family of APN function is CCZ-inequivalent to the Gold family of APN functions. After this observation on $\mathbb{F}_{2^{12}}$, he claimed that his family of APN functions is new up to CCZ-equivalence.

One may think that it might be the case that MAGMA does not work for this particular class of APN functions. We have tested other APN functions which we know that they are EA equivalent with each other, see Proposition 5.3. We found that MAGMA also gave error in these particular cases.

In Section 1.4, we have discussed several interesting CCZ-invariants. Among these CCZ-invariant, one invariant is the order of automorphism groups of $M(G_F)$. Recall that, if we describe the function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in the form of matrix of dimension $(2n+1) \times 2^n$ as

$$H_F := \begin{bmatrix} 1 \\ x \\ F(x) \end{bmatrix}_{x \in \mathbb{F}_2^n},$$

where the row space generated the code C_F, then $M(G_F)$ is just the automorphism group of the code C_F. In [30], authors have discussed certain conditions on the order of automorphism groups of $M(G_F)$ which are as follows:

Theorem 6.6. *If F is an APN mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $F(x+a)+F(x)$ is affine for all $a \in \mathbb{F}_2^n$, then $M(G_F)$ contains an elementary abelian group of order 2^n.*

It follows that the order of automorphism group of linear code associated with the Gold and the Göloğlu infinite family of APN function contain a factor of 2^n. We have used MAGMA function to compute the order of the automorphism groups of linear codes associated with the Gold and the Göloğlu infinite family of APN functions on $\mathbb{F}_{2^{12}}$. MAGMA computational results gave the output 1 as the order of automorphism group of linear code associated with the Gold and the Göloğlu infinite family of APN function respectively which is incorrect. This shows that the MAGMA function for the computation of order of automorphism group also gives incorrect results.

Remark 6.7. We have used MAGMA version $v2.23-9$ in our computations. We have also informed the MAGMA team about the malfunctioning cases that we have observed.

Appendix A

Computational Results

Here, we discuss the computational results of Section 4.5. First, we start with the case $n = 6$.

Case $n = 6$

For $n = 6$, Yu, Wang and Li used Gold APN function $F(x) = x^3$ to construct QAC C_{ij}^k, $1 \leq i, j, k \leq 6$. They changed one row and column in C_{ij}^k, $1 \leq i, j, k \leq 6$ to generate 13 CCZ-inequivalent quadratic APN functions.
We choose two quadratic APN functions other than Gold APN function which are

$$F_1(x) = x^3 + \alpha^{11}x^6 + \alpha * x^9$$

and

$$F_2(x) = x^3 + \alpha x^{24} + x^9$$

from Table 1.5, where α is the root of $x^6 + x^4 + x^3 + x + 1$.
We describe $F_1(x)$ and $F_2(x)$ in terms of QAC's C_{ij}^k, $1 \leq i, j, k \leq 6$ and D_{ij}^k, $1 \leq i, j, k \leq 6$ respectively. We apply the Yu, Wang and Li approach to the QAC C_{ij}^k, $1 \leq i, j, k \leq 6$ and D_{ij}^k, $1 \leq i, j, k \leq 6$ respectively. We found that the Yu, Wang and Li approach generates 13 CCZ-inequivalent quadratic APN functions using C_{ij}^k,
$1 \leq i, j, k \leq 6$ and D_{ij}^k, $1 \leq i, j, k \leq 6$ respectively.

Remark A.1. Note that the classification of quadratic APN function for $n = 6$ is complete [56]. There are only 13 CCZ-inequivalent quadratic APN functions listed in Table 1.5.
Our computational results show that we can also generate these 13 CCZ-inequivalent quadratic APN functions from QAC's corresponding to the functions $F_1(x)$ and $F_2(x)$.

Case $n = 7$

For $n = 7$, we choose six quadratic APN functions including Gold APN function from Table 7 [30] which are

$$\begin{aligned} F_1(x) &= x^3, \\ F_2(x) &= x^3 + x^9 + x^{18} + x^{66}, \\ F_3(x) &= x^3 + x^{12} + x^{17} + x^{33}, \\ F_4(x) &= x^3 + x^{12} + x^{40} + x^{72}, \\ F_5(x) &= x^3 + x^5 + x^{10} + x^{33} + x^{34} \\ F_6(x) &= x^3 + x^6 + x^{34} + x^{40} + x^{72} \end{aligned}$$

here α is the root of $x^7 + x + 1$. These quadratic APN functions have nice univariate representation in $\mathbb{F}_{2^7}$.
First, we describe F_1 in terms of QAC C_{ij}^k, $1 \leq i,j,k \leq 7$. We apply the YWL approach to C_{ij}^k, $1 \leq i,j,k \leq 7$. We found that the YWL approach generates 1 CCZ-inequivalent quadratic APN functions which is
$G_1(x) = \alpha^{23} * x^{80} + \alpha^{59} * x^{68} + \alpha^{62} * x^{66} + \alpha^{61} * x^{65} + \alpha^{119} * x^{48} + \alpha^{28} * x^{36} + \alpha^{31} * x^{34} + \alpha^{30} * x^{33} + \alpha^{64} * x^{24} + \alpha^{15} * x^{18} + \alpha^{79} * x^{17} + \alpha^{100} * x^{12} + \alpha^{103} * x^{10} + \alpha^{102} * x^9 + \alpha^{51} * x^6 + \alpha^{115} * x^5 + \alpha^{57} * x^3$.

Remark A.2. Note that YWL approach on QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_1(x)$ generates several quadratic APN functions but all of them are CCZ-equivalent with $G_1(x)$. The same observation holds for $F_2(x), \ldots, F_6(x)$.

Similarly, we describe $F_2(x), \ldots, F_6(x)$ in terms of QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ respectively. We apply the YWL approach to C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_2(x), \ldots, F_6(x)$ respectively. We found the following results:
1. The QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_2(x)$ generates 2 CCZ-inequivalent quadratic APN functions which are
$G_2(x) = \alpha^2 * x^{96} + \alpha^{76} * x^{80} + \alpha^{120} * x^{72} + \alpha^{86} * x^{68} + \alpha^{74} * x^{66} + \alpha^{44} * x^{65} + \alpha^2 * x^{48} + \alpha^{80} * x^{40} + \alpha^{53} * x^{33} + \alpha^{79} * x^{24} + \alpha^{86} * x^{20} + \alpha^{74} * x^{18} + \alpha^{94} * x^{17} + \alpha^{37} * x^{12} + \alpha^{43} * x^{10} + \alpha^{98} * x^9 + \alpha^{10} * x^5 + \alpha^{112} * x^3$
and
$G_3(x) = \alpha^{81} * x^{96} + \alpha^{101} * x^{80} + \alpha^{33} * x^{72} + \alpha^{126} * x^{68} + \alpha^{114} * x^{66} + \alpha^{44} * x^{65} + \alpha^{74} * x^{48} + \alpha^{123} * x^{40} + \alpha^{68} * x^{36} + \alpha^{25} * x^{34} + \alpha^{76} * x^{33} + \alpha^{124} * x^{24} + \alpha^{103} * x^{20} + \alpha^{112} * x^{18} + \alpha^{14} * x^{17} + \alpha^{77} * x^{12} + \alpha^{46} * x^{10} + \alpha^{27} * x^9 + \alpha^{104} * x^6 + \alpha^{40} * x^5 + \alpha^{26} * x^3$.
2. The QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_3(x)$ generates 2 CCZ-inequivalent quadratic APN functions which are
$G_4(x) = \alpha^{120} * x^{96} + \alpha^{15} * x^{80} + \alpha^{117} * x^{72} + \alpha^5 * x^{68} + \alpha^2 * x^{66} + x^{65} + \alpha^{94} * x^{48} + x^{40} + \alpha^{59} * x^{36} + \alpha^{89} * x^{34} + \alpha^{63} * x^{33} + \alpha^2 * x^{24} + \alpha^{59} * x^{20} + \alpha^{32} * x^{18} + \alpha^2 * x^{17} + \alpha^{36} * x^{12} + \alpha^{42} * x^{10} + \alpha * x^9 + \alpha^{18} * x^6 + \alpha^{55} * x^5 + \alpha^{115} * x^3$
and

$G_5(x) = \alpha^4 * x^{96} + \alpha^4 * x^{80} + \alpha^{84} * x^{72} + \alpha^{106} * x^{68} + \alpha^4 * x^{66} + \alpha^{33} * x^{65} + \alpha^{92} * x^{48} + \alpha^{101} * x^{40} + \alpha^{110} * x^{36} + \alpha^{109} * x^{34} + \alpha^{107} * x^{33} + \alpha^{53} * x^{24} + \alpha^{84} * x^{20} + \alpha^8 * x^{18} + \alpha^{109} * x^{17} + \alpha^{81} * x^{12} + \alpha^{35} * x^{10} + \alpha^{32} * x^9 + \alpha^{67} * x^6 + \alpha^{109} * x^5 + \alpha^{122} * x^3$.

3. The QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_4(x)$ generates 3 CCZ-inequivalent quadratic APN functions which are

$G_6(x) = \alpha^{110} * x^{96} + \alpha^9 * x^{80} + \alpha^{39} * x^{72} + \alpha^{43} * x^{68} + \alpha^{48} * x^{66} + \alpha^{49} * x^{65} + \alpha^{25} * x^{48} + \alpha^{74} * x^{40} + \alpha^8 * x^{36} + \alpha^{122} * x^{34} + \alpha^{84} * x^{33} + \alpha^{114} * x^{24} + \alpha^{74} * x^{20} + \alpha * x^{18} + \alpha^{120} * x^{17} + \alpha^{67} * x^{12} + \alpha^{53} * x^{10} + \alpha^{48} * x^9 + \alpha^{108} * x^6 + \alpha^{38} * x^5 + \alpha^{49} * x^3$,

$G_7(x) = \alpha^{102} * x^{96} + \alpha^{102} * x^{80} + \alpha^{30} * x^{72} + \alpha^{37} * x^{68} + \alpha^{106} * x^{66} + \alpha^{93} * x^{65} + \alpha^{63} * x^{48} + \alpha^{22} * x^{40} + \alpha^{53} * x^{36} + \alpha^{109} * x^{34} + \alpha^{15} * x^{33} + \alpha^{19} * x^{24} + \alpha^{11} * x^{20} + \alpha^{54} * x^{18} + \alpha^{115} * x^{17} + \alpha^{60} * x^{12} + \alpha^{104} * x^{10} + \alpha^{105} * x^9 + \alpha^{99} * x^6 + \alpha^{121} * x^5 + \alpha^{108} * x^3$

and

$G_8(x) = \alpha^{80} * x^{96} + \alpha^{113} * x^{80} + \alpha^{101} * x^{72} + \alpha^{114} * x^{68} + \alpha^{119} * x^{66} + \alpha^3 * x^{65} + \alpha^{113} * x^{48} + \alpha^{117} * x^{40} + \alpha^{39} * x^{36} + \alpha * x^{34} + \alpha^{116} * x^{33} + \alpha^{119} * x^{24} + \alpha^{113} * x^{20} + \alpha^{115} * x^{18} + \alpha^{24} * x^{17} + \alpha^3 * x^{12} + \alpha^{59} * x^{10} + \alpha^{124} * x^9 + \alpha^{52} * x^6 + \alpha^{50} * x^5 + \alpha^{26} * x^3$.

4. The QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_5(x)$ generates 6 CCZ-inequivalent quadratic APN functions which are

$G_9(x) = \alpha^{110} * x^{96} + \alpha^{100} * x^{72} + \alpha^{81} * x^{68} + \alpha^{103} * x^{66} + \alpha^{59} * x^{65} + x^{48} + \alpha^{92} * x^{40} + \alpha^{38} * x^{36} + \alpha^{59} * x^{34} + \alpha^{79} * x^{33} + \alpha^{117} * x^{24} + \alpha^{98} * x^{20} + \alpha^{120} * x^{18} + \alpha^{76} * x^{17} + \alpha^{10} * x^{12} + \alpha^{119} * x^{10} + \alpha^3 * x^9 + \alpha^{125} * x^6 + \alpha^{55} * x^3$,

$G_{10}(x) = \alpha^{122} * x^{96} + \alpha^{50} * x^{80} + \alpha^{118} * x^{72} + \alpha^{117} * x^{68} + \alpha^{84} * x^{66} + \alpha^{99} * x^{65} + \alpha^{13} * x^{48} + \alpha^{76} * x^{40} + \alpha^{106} * x^{36} + \alpha^{124} * x^{34} + \alpha^{43} * x^{33} + \alpha^{58} * x^{24} + \alpha^{118} * x^{20} + \alpha^{30} * x^{18} + \alpha^{13} * x^{17} + \alpha^{86} * x^{12} + \alpha^{70} * x^{10} + \alpha^{64} * x^9 + \alpha^{110} * x^6 + \alpha^{70} * x^5 + \alpha^{43} * x^3$,

$G_{11}(x) = \alpha^{75} * x^{96} + \alpha^{118} * x^{80} + \alpha^{53} * x^{72} + \alpha^{22} * x^{68} + \alpha^{22} * x^{66} + \alpha^{50} * x^{65} + \alpha^{14} * x^{48} + \alpha^{66} * x^{40} + \alpha^{99} * x^{36} + \alpha^{99} * x^{34} + \alpha^{39} * x^{33} + \alpha^{90} * x^{24} + \alpha^{93} * x^{20} + \alpha^{126} * x^{18} + \alpha^{55} * x^{17} + \alpha^{80} * x^{12} + \alpha^{38} * x^{10} + \alpha^{87} * x^9 + \alpha^{74} * x^6 + \alpha^{115} * x^5 + \alpha^{30} * x^3$,

$G_{12}(x) = \alpha^{114} * x^{96} + \alpha^{87} * x^{80} + \alpha^{52} * x^{72} + \alpha^{46} * x^{68} + \alpha^{118} * x^{66} + \alpha^{34} * x^{65} + \alpha^{97} * x^{48} + \alpha^{22} * x^{40} + \alpha^{120} * x^{36} + \alpha^{120} * x^{34} + \alpha^{51} * x^{33} + \alpha^{46} * x^{24} + \alpha^{96} * x^{20} + \alpha^{95} * x^{18} + \alpha^{41} * x^{17} + \alpha^{13} * x^{12} + \alpha^{99} * x^{10} + \alpha^{48} * x^9 + \alpha^5 * x^6 + \alpha^{43} * x^5 + \alpha^{59} * x^3$,

$G_{13}(x) = \alpha^{68} * x^{96} + \alpha^4 * x^{80} + \alpha^{85} * x^{72} + \alpha^{108} * x^{68} + \alpha^3 * x^{66} + \alpha^{10} * x^{65} + \alpha^{116} * x^{48} + \alpha^{67} * x^{40} + \alpha^{44} * x^{36} + \alpha^{99} * x^{34} + \alpha^{80} * x^{33} + \alpha^{66} * x^{24} + \alpha^{102} * x^{20} + \alpha^{37} * x^{18} + x^{17} + \alpha^{98} * x^{12} + \alpha^{50} * x^{10} + \alpha^{35} * x^9 + \alpha^{25} * x^6 + \alpha^{54} * x^5 + \alpha^{52} * x^3$

and

$G_{14}(x) = \alpha^{100} * x^{96} + \alpha^{12} * x^{80} + \alpha^{76} * x^{72} + x^{68} + \alpha^{106} * x^{66} + \alpha^{74} * x^{65} + \alpha^{71} * x^{48} + \alpha^{29} * x^{40} + \alpha^{117} * x^{36} + \alpha^{122} * x^{34} + \alpha^{70} * x^{33} + \alpha^{104} * x^{24} + \alpha^9 * x^{20} + \alpha^{37} * x^{18} + \alpha^{117} * x^{17} + \alpha^{102} * x^{12} + \alpha^{126} * x^{10} + \alpha^{70} * x^9 + \alpha^{98} * x^6 + \alpha^{62} * x^5 + \alpha^{113} * x^3$.

5. The QAC C_{ij}^k, $1 \leq i,j,k \leq 7$ that corresponds to $F_6(x)$ generates 3 CCZ-inequivalent quadratic APN functions which are

$G_{15}(x) = \alpha^{22} * x^{96} + \alpha^{92} * x^{80} + \alpha^{111} * x^{72} + \alpha^{101} * x^{68} + \alpha^{61} * x^{66} + \alpha^{86} * x^{65} + \alpha^{86} * x^{48} + \alpha^{33} * x^{40} + \alpha^{124} * x^{36} + \alpha^{91} * x^{34} + \alpha^{74} * x^{33} + \alpha^{75} * x^{24} + \alpha^{57} * x^{20} + \alpha^{29} * x^{18} + \alpha^{16} * x^{17} + \alpha^{16} * x^{12} + \alpha^{120} * x^{10} + \alpha^{15} * x^9 + \alpha^{123} * x^6 + \alpha^8 * x^5 + \alpha^{17} * x^3$,

$G_{16}(x) = \alpha^{56} * x^{96} + \alpha^{81} * x^{80} + \alpha^{13} * x^{72} + \alpha^{79} * x^{68} + \alpha^{38} * x^{66} + \alpha^{75} * x^{65} + \alpha^5 * x^{48} +$

$\alpha^{80} * x^{40} + \alpha^{9} * x^{36} + \alpha^{43} * x^{34} + \alpha^{9} * x^{33} + \alpha^{28} * x^{24} + \alpha^{27} * x^{20} + x^{18} + \alpha^{5} * x^{17} + \alpha^{106} * x^{12} + \alpha^{61} * x^{10} + \alpha^{123} * x^{9} + \alpha^{115} * x^{6} + \alpha^{56} * x^{5} + \alpha^{104} * x^{3}$
and
$G_{17}(x) = \alpha^{90} * x^{96} + \alpha^{104} * x^{80} + \alpha^{71} * x^{72} + \alpha^{24} * x^{68} + \alpha^{121} * x^{66} + \alpha^{95} * x^{65} + \alpha^{32} * x^{48} + \alpha^{117} * x^{40} + \alpha^{75} * x^{36} + \alpha^{64} * x^{34} + \alpha^{125} * x^{33} + \alpha^{91} * x^{24} + \alpha^{117} * x^{20} + \alpha^{116} * x^{18} + \alpha^{117} * x^{17} + \alpha^{2} * x^{12} + \alpha^{7} * x^{10} + \alpha^{63} * x^{9} + \alpha^{110} * x^{6} + \alpha^{116} * x^{5} + \alpha^{37} * x^{3}$.
We have checked the CCZ-equivalence of $G_1(x), \dots, G_{17}(x)$ with known examples of quadratic APN function given in Appendix 1 of YWL paper [3]. We found that $G_1(x), \dots, G_{17}(x)$ are contained in Appendix 1 of YWL paper.
Now, we are interested in applying the YWL approach on the EA-equivalent examples of quadratic APN function.
First, we choose a random invertible matrix P of dimension 7×7 over $\mathbb{F}_2$. We compute

$$P^T C_{ij}^k P,$$

for $k = 1, \dots, 7$ to obtain EA equivalent QAC that corresponds to the function $F_1(x)$. We apply the YWL approach to the $P^T C_{ij}^k P,\ 1 \le i, j, k \le 6$.
We found that the YWL approach generate 1 CCZ-inequivalent quadratic APN functions which is
$G_{14}(x) = \alpha^{121} * x^{96} + \alpha^{26} * x^{80} + \alpha^{121} * x^{72} + \alpha^{22} * x^{68} + \alpha^{9} * x^{66} + \alpha^{42} * x^{65} + \alpha^{40} * x^{48} + \alpha^{85} * x^{40} + \alpha^{2} * x^{36} + \alpha^{80} * x^{34} + \alpha^{78} * x^{33} + \alpha^{74} * x^{24} + \alpha^{74} * x^{20} + \alpha^{68} * x^{18} + \alpha^{64} * x^{17} + \alpha^{62} * x^{12} + \alpha^{50} * x^{10} + \alpha^{104} * x^{9} + \alpha^{34} * x^{6} + \alpha^{118} * x^{5} + \alpha^{100} * x^{3}$.
We checked the CCZ-equivalence of $G_{14}(x)$ with the known examples of quadratic APN functions. We found that $G_{14}(x)$ is CCZ-equivalent with $G_1(x)$. We repeat the above procedure with 100 random invertible matrix. We always get 1 CCZ-inequivalent quadratic APN function. This function is always CCZ-equivalent with $G_1(x)$.

Remark A.3. We are unable to find new quadratic APN function for $n = 7$ by apply YWL approach to $F_2(x), \dots, F_6(x)$.

Now, we consider the case $n = 8$.

Case $n = 8$

For $n = 8$, we choose seven quadratic APN functions including Gold APN function which are

$$F_1(x) = x^3,$$
$$F_2(x) = x^3 + u^{125}x^{33} + u^{183}x^{66} + u^{21}x^{144},$$
$$F_3(x) = x^3 + u^{65}x^{18} + u^{120}x^{66} + u^{135}x^{144},$$
$$F_4(x) = x^9,$$
$$F_5(x) = x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48},$$
$$F_6(x) = x^3 + u^{24}x^6 + u^{182}x^{132} + u^{67}x^{192}$$

$$F_7(x) = x^3 + x^5 + x^{18} + x^{40} + x^{66}$$

from Table 9 [30], where α is the root of $x^8 + x^4 + x^3 + x^2 + 1$. These APN functions have nice univariate representation in $\mathbb{F}_{2^8}$.
First, we describe $F_1(x)$ in terms of QAC C_{ij}^k, $1 \le i, j, k \le 8$. We apply the YWL approach to C_{ij}^k, $1 \le i, j, k \le 8$. We found that the YWL approach generate 2 CCZ-inequivalent quadratic APN functions which are
$G_1(x) = \alpha^{145} * x^{192} + \alpha^{235} * x^{144} + \alpha^{130} * x^{132} + \alpha^{67} * x^{130} + \alpha^{214} * x^{129} + \alpha^{70} * x^{96} + \alpha^{115} * x^{72} + \alpha^{155} * x^{66} + \alpha^{239} * x^{65} + \alpha^{160} * x^{48} + \alpha^{55} * x^{36} + \alpha^{247} * x^{34} + \alpha^{139} * x^{33} + \alpha^{205} * x^{24} + \alpha^{245} * x^{18} + \alpha^{74} * x^{17} + \alpha^{100} * x^{12} + \alpha^{37} * x^{10} + \alpha^{184} * x^9 + \alpha^{140} * x^6 + \alpha^{224} * x^5 + \alpha^{67} * x^3$,
$G_2(x) = \alpha^{60} * x^{192} + \alpha^{150} * x^{144} + \alpha^{45} * x^{132} + \alpha^{138} * x^{130} + \alpha^{193} * x^{129} + \alpha^{240} * x^{96} + \alpha^{30} * x^{72} + \alpha^{224} * x^{66} + \alpha^{126} * x^{65} + \alpha^{75} * x^{48} + \alpha^{225} * x^{36} + \alpha^{63} * x^{34} + \alpha^{118} * x^{33} + \alpha^{120} * x^{24} + \alpha^{59} * x^{18} + \alpha^{216} * x^{17} + \alpha^{15} * x^{12} + \alpha^{108} * x^{10} + \alpha^{163} * x^9 + \alpha^{209} * x^6 + \alpha^{111} * x^5 + \alpha^{17} * x^3$.

Remark A.4. Note that YWL approach on QAC C_{ij}^k, $1 \le i, j, k \le 8$ that corresponds to $F_1(x)$ generates several quadratic APN functions but all of them are CCZ-equivalent with $G_1(x)$ and $G_2(x)$. The same observation holds for $F_2(x), \ldots, F_7(x)$.

Similarly, we describe $F_2(x), \ldots, F_7(x)$ in terms of QAC's C_{ij}^k, $1 \le i, j, k \le 8$ respectively. We apply the YWL approach to C_{ij}^k, $1 \le i, j, k \le 8$ corresponding to $F_2(x), \ldots, F_7(x)$ respectively. We found that the following results:
1. The QAC C_{ij}^k, $1 \le i, j, k \le 8$ that corresponds to $F_2(x)$ generates 1 CCZ-inequivalent quadratic APN functions which is
$G_3(x) = \alpha^{186} * x^{192} + \alpha^{157} * x^{160} + \alpha^{28} * x^{144} + \alpha^{188} * x^{136} + \alpha^{68} * x^{132} + \alpha^5 * x^{130} + \alpha^{158} * x^{129} + \alpha^{225} * x^{96} + \alpha^{148} * x^{80} + \alpha^{127} * x^{72} + \alpha^7 * x^{68} + \alpha * x^{66} + \alpha^{174} * x^{65} + \alpha^{11} * x^{48} + \alpha^{82} * x^{40} + \alpha^{217} * x^{36} + \alpha^{253} * x^{34} + \alpha^{147} * x^{33} + \alpha^{187} * x^{24} + \alpha^{67} * x^{20} + \alpha^{102} * x^{18} + \alpha^{145} * x^{17} + \alpha^{198} * x^{10} + \alpha^{72} * x^9 + \alpha^{78} * x^6 + \alpha^{207} * x^5 + \alpha^{150} * x^3$.
2. The QAC C_{ij}^k, $1 \le i, j, k \le 8$ that corresponds to $F_3(x)$ generates 1 CCZ-inequivalent quadratic APN functions which is
$G_4(x) = \alpha^{252} * x^{192} + \alpha^{173} * x^{160} + \alpha^{226} * x^{144} + \alpha^{218} * x^{136} + \alpha^{98} * x^{132} + \alpha^{24} * x^{130} + \alpha^{65} * x^{129} + \alpha^{136} * x^{96} + \alpha^2 * x^{80} + \alpha^{181} * x^{72} + \alpha^{61} * x^{68} + \alpha^{15} * x^{66} + \alpha^{244} * x^{65} + \alpha^{180} * x^{48} + \alpha^{173} * x^{34} + \alpha^{16} * x^{33} + \alpha^{225} * x^{24} + \alpha^{105} * x^{20} + \alpha^{46} * x^{18} + \alpha^{60} * x^{17} + \alpha^{218} * x^{10} + \alpha^{61} * x^9 + \alpha^{98} * x^6 + \alpha^{196} * x^5 + \alpha^{206} * x^3$.
3. The QAC C_{ij}^k, $1 \le i, j, k \le 8$ that corresponds to $F_4(x)$ generates 2 CCZ-inequivalent quadratic APN functions which are
$G_5(x) = \alpha^{135} * x^{192} + \alpha^{225} * x^{144} + \alpha^{30} * x^{136} + \alpha^{120} * x^{132} + \alpha^{23} * x^{129} + \alpha^{60} * x^{96} + \alpha^{136} * x^{72} + \alpha^{180} * x^{66} + x^{65} + \alpha^{150} * x^{48} + \alpha^{210} * x^{40} + \alpha^{45} * x^{36} + \alpha^{203} * x^{33} + \alpha^{226} * x^{24} + \alpha^{15} * x^{18} + \alpha^{90} * x^{17} + \alpha^{121} * x^{12} + \alpha^{75} * x^{10} + \alpha^{177} * x^9 + \alpha^{165} * x^6 + \alpha^{240} * x^5 + \alpha^{68} * x^3$
and
$G_6(x) = \alpha^{77} * x^{136} + \alpha * x^{129} + \alpha^{197} * x^{72} + \alpha^{121} * x^{65} + \alpha^2 * x^{40} + \alpha^{181} * x^{33} + \alpha^{32} * x^{24} + \alpha^{211} * x^{17} + \alpha^{182} * x^{12} + \alpha^{122} * x^{10} + \alpha^{224} * x^9 + \alpha^{106} * x^5 + \alpha^{46} * x^3$.
4. The QAC C_{ij}^k, $1 \le i, j, k \le 8$ that corresponds to $F_5(x)$ generates 1 CCZ-

inequivalent quadratic APN functions which is
$G_7(x) = \alpha^8 * x^{160} + \alpha^{101} * x^{144} + \alpha^{173} * x^{130} + \alpha^{122} * x^{129} + \alpha^{128} * x^{96} + \alpha^{221} * x^{80} + \alpha^{38} * x^{66} + \alpha^{242} * x^{65} + \alpha^{238} * x^{48} + \alpha^{233} * x^{40} + \alpha^{113} * x^{36} + \alpha^{84} * x^{34} + \alpha^{207} * x^{33} + \alpha^{71} * x^{24} + \alpha^{206} * x^{20} + \alpha^{206} * x^{18} + \alpha^{123} * x^{17} + \alpha^{143} * x^{10} + \alpha^{92} * x^9 + \alpha^{23} * x^6 + \alpha^{227} * x^5 + \alpha^{134} * x^3$.

5. The QAC C_{ij}^k, $1 \leq i, j, k \leq 8$ that corresponds to $F_6(x)$ generates 1 CCZ-inequivalent quadratic APN functions which is
$G_8(x) = \alpha^{116} * x^{192} + \alpha^{131} * x^{160} + \alpha^{161} * x^{144} + \alpha^{176} * x^{136} + \alpha^{190} * x^{132} + \alpha^{178} * x^{130} + \alpha^{88} * x^{129} + \alpha^{24} * x^{96} + \alpha^{54} * x^{80} + \alpha^{69} * x^{72} + \alpha^{109} * x^{68} + \alpha^{33} * x^{66} + \alpha^{62} * x^{65} + \alpha^{90} * x^{36} + \alpha^{84} * x^{34} + \alpha^8 * x^{33} + \alpha^{120} * x^{20} + \alpha^{114} * x^{18} + \alpha^{38} * x^{17} + \alpha^{135} * x^{12} + \alpha^{129} * x^{10} + \alpha^{53} * x^9 + \alpha^{122} * x^6 + \alpha^{125} * x^5 + \alpha^{21} * x^3$.

6. The QAC C_{ij}^k, $1 \leq i, j, k \leq 8$ that corresponds to $F_7(x)$ generates 1 CCZ-inequivalent quadratic APN functions which is
$G_9(x) = \alpha^{194} * x^{192} + \alpha^{221} * x^{160} + \alpha^{194} * x^{144} + \alpha^{74} * x^{136} + \alpha^{232} * x^{132} + \alpha^{89} * x^{130} + \alpha^{231} * x^{129} + \alpha^{101} * x^{96} + \alpha^{121} * x^{80} + \alpha^{230} * x^{72} + \alpha^{191} * x^{68} + \alpha^{42} * x^{66} + \alpha^{172} * x^{65} + \alpha^{202} * x^{48} + \alpha^{111} * x^{40} + \alpha^{58} * x^{36} + \alpha^{234} * x^{34} + \alpha^{69} * x^{33} + \alpha^{173} * x^{24} + \alpha^{194} * x^{20} + \alpha^{214} * x^{18} + \alpha^{127} * x^{17} + \alpha^{120} * x^{12} + \alpha^{191} * x^{10} + \alpha^{96} * x^9 + \alpha^{251} * x^6 + \alpha^{72} * x^5 + \alpha^{212} * x^3$.

We have checked the CCZ-equivalence of $G_1(x), \ldots, G_9(x)$ with known examples of quadratic APN function given in Appendix 2 of YWL paper [3]. We found that $G_1(x), \ldots, G_9(x)$ are contained in Appendix 2 of YWL paper.

Now, we are interested in applying the YWL approach on the EA-equivalent examples of quadratic APN function.

Next, we choose a random invertible matrix P of dimension 8×8 over $\mathbb{F}_2$. We compute

$$P^T C_{ij}^k P,$$

for $k = 1, \ldots, 8$ to obtain EA equivalent QAC that corresponds to the function $F_1(x)$. We apply the YWL approach to $P^T C_{ij}^k P$, $1 \leq i, j, k \leq 8$.

We found that the YWL approach generate 2 CCZ-inequivalent quadratic APN functions which are
$G_{10}(x) = \alpha^{146} * x^{192} + \alpha^{20} * x^{160} + \alpha^{124} * x^{144} + \alpha^{115} * x^{136} + \alpha^{184} * x^{132} + \alpha^{102} * x^{130} + \alpha^{104} * x^{129} + \alpha^{84} * x^{96} + \alpha^{155} * x^{80} + \alpha^{79} * x^{72} + \alpha^{95} * x^{68} + \alpha^{14} * x^{66} + \alpha^{102} * x^{65} + \alpha^{199} * x^{48} + \alpha^{229} * x^{40} + \alpha^{121} * x^{36} + \alpha^{175} * x^{34} + \alpha^{137} * x^{33} + \alpha^{175} * x^{24} + \alpha^{37} * x^{20} + \alpha^{162} * x^{18} + \alpha^{239} * x^{17} + \alpha^{26} * x^{12} + \alpha^{215} * x^{10} + \alpha^{52} * x^9 + \alpha^{227} * x^6 + \alpha^{203} * x^5 + \alpha^{214} * x^3$
and
$G_{11}(x) = \alpha^{100} * x^{192} + \alpha^{207} * x^{160} + \alpha^{26} * x^{144} + \alpha^{209} * x^{136} + \alpha^{232} * x^{132} + \alpha^{22} * x^{130} + \alpha^{180} * x^{129} + \alpha^{39} * x^{96} + \alpha^{227} * x^{80} + \alpha^{106} * x^{72} + \alpha^{65} * x^{68} + \alpha^{162} * x^{66} + \alpha^9 * x^{65} + \alpha^{146} * x^{48} + \alpha^{116} * x^{40} + \alpha^{124} * x^{36} + \alpha^{227} * x^{34} + \alpha^{209} * x^{33} + \alpha^{111} * x^{24} + \alpha^{213} * x^{20} + \alpha^{178} * x^{18} + \alpha^{234} * x^{17} + \alpha^{181} * x^{12} + \alpha^{66} * x^{10} + \alpha^{230} * x^9 + \alpha^{40} * x^6 + \alpha^{97} * x^5 + \alpha^{62} * x^3$.

We checked the CCZ-equivalence of $G_{10}(x)$ and $G_{11}(x)$ with the known examples of quadratic APN functions. We found that $G_{10}(x)$ is CCZ-equivalent with $G_1(x)$ and $G_{11}(x)$ is CCZ-equivalent with $G_2(x)$. We repeat the above procedure with 10 random invertible matrix and we always get 2 quadratic APN function which are CCZ-equivalent with $G_1(x)$ and $G_2(x)$.

Remark A.5. We are unable to find new quadratic APN function for $n = 8$ by apply YWL approach to $F_2(x), \ldots, F_7(x)$.

Bibliography

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

[2] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology*, EUROCRYPT '93, pages 386–397, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[3] Y. Yu, M. Wang, and Y. Li. A matrix approach for constructing quadratic APN functions. Cryptology ePrint Archive, Report 2013/007, 2013. https://eprint.iacr.org/2013/007.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[5] J. Daemen and V. Rijmen. AES proposal: Rijndael, 1999.

[6] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

[7] Y. Yuyin, W. Mingsheng, and L. Yongqiang. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography*, 73(2):587–600, 2014.

[8] C. Carlet. Boolean functions for cryptography and error-correcting codes. In Yves Crama and Peter L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, 2010.

[9] E. Berlekamp and L. Welch. Weight distributions of the cosets of the (32,6) Reed-Muller code. *IEEE Transactions on Information Theory*, 18(1):203–207, January 1972.

[10] N. Patterson and D. Wiedemann. The covering radius of the r.

[11] S. Kavut, S. Maitra, and M. D. Yücel. Search for Boolean functions with excellent profiles in the rotation symmetric class. *IEEE Transactions on Information Theory*, 53(5):1743–1751, 2007.

[12] S. Kavut and M. D. Yücel. 9-variable boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Information and Computation*, 208(4):341 – 350, 2010.

[13] K.-U. Schmidt. Asymptotically optimal Boolean functions. *Arxiv e-prints*, 2017.

[14] O.S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20(3):300 – 305, 1976.

[15] A. F. Webster and S. E. Tavares. On the design of s-boxes. *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 523–534, 1986.

[16] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology — EUROCRYPT '90*, pages 161–173, Springer,Berlin, 1991.

[17] X. Lai. Additive and linear structures of cryptographic functions. In Bart Preneel, editor, *Fast Software Encryption*, pages 75–85. Springer,Berlin, 1995.

[18] E. Jan-Hendrik. Linear structures in blockciphers. In *Advances in Cryptology — EUROCRYPT' 87*, pages 249–266, Springer,Berlin, 1988.

[19] C. Carlet. Vectorial boolean functions for cryptography. In Yves Crama and Peter L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 398–473. Cambridge University Press, 2010.

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

[21] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology — EUROCRYPT' 92*, pages 92–98, Springer,Berlin, 1993.

[22] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in Cryptology — EUROCRYPT'94*, pages 356–365, Springer,Berlin, 1995.

[23] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49(1):273–288, 2008.

[24] X.-D. Hou. Affinity of permutations of F_2^n. *Discrete Applied Mathematics*, 154(2):313 – 325, 2006.

[25] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[26] L Budaghyan and C Carlet. CCZ-equivalence of single and multi output Boolean functions. *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS*, 518:43–54, 2010.

[27] S. Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.

[28] C. Bracken, E. Byrne, N. Markin, and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703 – 714, 2008.

[29] D. R. Hughes and F. C. Piper. *Design theory*. Cambridge University Press, Cambridge, second edition, 1988.

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

[31] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Transactions on Information Theory*, 14(1):154–156, January 1968.

[32] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993)*, volume 765 of *Lecture Notes in Computer Science*, page 55–64. Springer, Berlin, 1994.

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

[34] H. Janwa and R. M. Wilson. Hyperplane sections of fermat varieties in P3 in char. 2 and some applications to cyclic codes. In *10th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes:AAECC-10*, pages 180–194, Springer, Berlin, 1993.

[35] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, May 1999.

[36] H. Dobbertin. Almost perfect nonlinear power functions on GF(2^n): The niho case. *Information and Computation*, 151(12):57 – 72, 1999.

[37] T. Beth and C. Ding. *On almost perfect nonlinear permutations*, chapter Advances in Cryptology — EUROCRYPT '93, pages 65–76. Springer, Berlin, 1994.

[38] H. Dobbertin. *Almost perfect nonlinear power functions on GF(2^n): A new case for n divisible by 5*, chapter Finite Fields and Applications: Proceedings of The Fifth International Conference on Finite Fields and Applications Fq5, held at the University of Augsburg, Germany, August 2–6, 1999, pages 113–121. Springer, Berlin, 2001.

[39] M. Erickson and A. Vazzana. *Introduction to number theory*. Chapman & Hall/CRC, 1st edition, 2007.

[40] L. Budaghyan and A. Pott. On differential uniformity and nonlinearity of functions. *Discrete Mathematics*, 309(2):371 – 384, 2009.

[41] D. Jedlicka. APN monomials over $GF(2^n)$ for infinitely many n. *Finite Fields and Their Applications*, 13(4):1006 – 1028, 2007.

[42] W. G. Solomon. Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences. *Information Sciences*, 1(1):87 – 109, 1968.

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

[44] A. Canteaut, P. Charpin, and H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on F_2^m, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1):105–138, 2000.

[45] G. Lahaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary goppa codes. *IEEE Transactions on Information Theory*, 36(3):686–692, May 1990.

[46] L. Budaghyan, C. Carlet, P. Felke, and G. Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. In *2006 IEEE International Symposium on Information Theory*, pages 2637–2641, July 2006.

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

[48] C. Bracken, E. Byrne, N. Markin, and G. McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[49] L. Budaghyan and C. Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

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

[51] L. Budaghyan, C. Carlet, and G. Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, 2009.

[52] C. Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography*, 59(1):89–109, 2011.

[53] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43 – 60, 2013.

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

[55] J.F. Dillon. Slides from talk given at "polynomials over finite fields and applications", held at Banff International Research Station. 2006.

[56] Y. Edel. On quadratic APN functions and dimensional dual hyperovals. *Designs, Codes and Cryptography*, 57(1):35–44, 2010.

[57] G. Leander. *Algebraic problems in symmetric cryptography: two recent results on highly nonlinear functions*. Contemporary Mathematics 418, 2006.

[58] J.F. Dillon. Slides from talk given at conference "finite fields and their applications", in dublin. 2009.

[59] A. E. Brouwer and L. M. G. M. Tolhuizen. A sharpening of the johnson bound for binary linear codes and the nonexistence of linear codes with preparata parameters. *Designs, Codes and Cryptography*, 3(2):95–98, 1993.

[60] P. B. Thierry, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, Sept 2006.

[61] Y. Zheng and X. M. Zhang. Plateaued functions. In *Second International Conference on Information and Communication Security:ICICS'99*, pages 284–300, Springer, Berlin, 1999.

[62] R. J. McEliece. *Finite field for computer scientists and engineers*. Kluwer Academic Publishers, Norwell, MA, USA, 1987.

[63] J.F. Dillon. *Elementary hadamard difference sets*. University of Maryland, 1974.

[64] S. Kavut, S. Maitra, S. Sarkar, and M. D. Yücel. *Enumeration of 9-variable rotation symmetric boolean functions having nonlinearity > 240*, chapter Progress in Cryptology - INDOCRYPT 2006, pages 266–279. Springer, Berlin, 2006.

[65] L.J. Lapierre. Vectorial bent functions in characteristic two. *Master Thesis*, 2016.

[66] G. Leander. Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2):738–743, Feb 2006.

[67] M. G. Evoyan, G.M. Kyuregyan, and M.K. Kyuregyan. On k-switching of mappings on finite fields. *Mathematical Problems of Computer Science*, 39:5–12, 2013.

[68] A. Weil. On some exponential sums. *Proceedings of the National Academy of Sciences*, 34(5):204–207, 1948.

[69] F. Göloğlu. Private communication. 2018.

[70] F. Göloğlu. Almost perfect nonlinear trinomials and hexanomials. *Finite Fields and their Applications*, 33:258–282, 2015.

[71] L. Budaghyan, T. Helleseth, N. Li, and B. Sun. Some results on the known classes of quadratic APN functions. Cryptology ePrint Archive, Report 2016/1183, 2016. https://eprint.iacr.org/2016/1183.