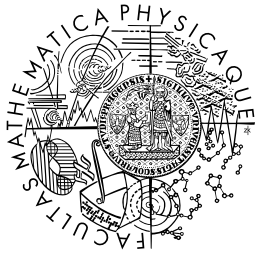

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Zuzana Rezková

On a matrix approach for constructing quadratic almost perfect nonlinear functions

Department of Algebra

Supervisor of the bachelor thesis: Dr. rer. nat. Faruk Göloğlu

Study programme: Mathematics

Study branch: Mathematics for Information Technologies

Prague 2020

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ....

Zuzana Rezková

I would like to thank my supervisor Dr. rer. nat. Faruk Göloğlu for introducing the topic to me and for his helpful comments and consultations. I would also like to thank my partner and my family for supporting me in my studies.

Title: On a matrix approach for constructing quadratic almost perfect nonlinear functions

Author: Zuzana Rezková

Department: Department of Algebra

Supervisor: Dr. rer. nat. Faruk Göloğlu, Department of Algebra

Abstract: Search for new APN functions is an important topic in symmetric cryptography. The matrix approach for constructing quadratic APN functions was described by Y. Yu, M. Wang and Y. Li in 2014. The approach takes advantage of the one to one correspondence between quadratic homogenous APN functions and quadratic APN matrices. The aim of this thesis is to explain the matrices used in the original paper and show that similar matrices can be constructed directly from the algebraic normal form of the APN function. In Chapter 2 we introduce the original method adding extra theorems and expanding the proofs for better understanding. In Chapter 3 we define the matrices obtained simply from the algebraic normal form. In Chapter 4 we give examples of the matrices for chosen APN functions and show how they are related.

Keywords: Boolean functions, APN functions, matrix approach, algebraic normal form

Contents

Introduction **2**

1 Preliminaries **3**
1.1 Used notation . . . 3
1.2 Boolean functions . . . 3
1.3 ANF representation . . . 4
1.4 Finite field representation . . . 5
1.5 APN functions and their properties . . . 6
1.6 Equivalence respecting APNness . . . 7

2 Finite field approach **8**
2.1 Matrix representation of F . . . 8
2.2 Correspondence between QAMs and APN functions . . . 12
2.3 EA equivalence in terms of QAMs . . . 14
2.4 Properties of QAMs . . . 16

3 ANF approach **21**
3.1 Matrix representation of ANF . . . 21
3.2 Correspondence between QAMs and ANFs . . . 23

4 Examples **26**
4.1 Finite field approach . . . 26
4.1.1 Trace and Bases . . . 26
4.1.2 Basis choice . . . 27
4.1.3 Function F_1 . . . 27
4.1.4 Function F_2 . . . 28
4.2 ANF approach . . . 29
4.2.1 ANF computation . . . 29
4.2.2 Corresponding matrices for $\widetilde{G_1}, \widetilde{G_2}$ . . . 32

Conclusion **33**

Bibliography **34**

Introduction

Boolean functions $\mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ used in cryptography are needed to be resistant to the differential attack. When $m = n$, the most resistant functions are so called almost perfect nonlinear (APN) functions (see [1]). Therefore, finding new APN functions is an important topic in cryptography.

In [2] a matrix approach for finding new APN functions was introduced by Y. Yu, M. Wang and Y. Li. The method focuses on finding new quadratic APN functions on $\mathbb{F}_{2^n}$. It led to finding more than 471 new APN functions on $\mathbb{F}_{2^7}$ and more than 2252 new APN functions on $\mathbb{F}_{2^8}$ (see [2, p. 588]). The aim of Chapters 3 and 4 of this thesis is to show that similar results (as in [2]) could be obtained from the ANF representation of a Boolean function.

In Chapter 1 we explain the basics of Boolean functions. We also give the definition of APN functions and show some of their properties. Chapter 2 deals with the matrix approach from [2]. We expand the original work and add our own proofs when needed. The results lead to an algorithm the explanation of which we have omitted, because it was out of scope of the thesis. The algorithm can be found in [2, p. 597-599]. In Chapter 3 we prove that a similar matrix (as in [2]) can be constructed from the ANF of a Boolean function. For Chapter 4 we choose APN functions

$$x \mapsto x^3 \text{ and } x \mapsto x^3 + \mathrm{Tr}(x^9)$$

on $\mathbb{F}_{2^5}$ and compute the coresponding matrices from their finite field and ANF representation.

1. Preliminaries

1.1 Used notation

The following notation will be used throughout the thesis.

- Let $n, m, k \in \mathbb{N}$.
- The finite field with two elements will be denoted by $\mathbb{F}_2$.
- We denote the finite field with 2^n elements by $\mathbb{F}_{2^n}$.
  The multiplicative group of $\mathbb{F}_{2^n}$ will be denoted by $\mathbb{F}_{2^n}^*$.
- $\vec{v}$ denotes a column vector from $\mathbb{F}_{2^n}^m$ (or $v \in \mathbb{F}_2^m$ depending on the context).
  v_i denotes the i-th coordinate of $\vec{v}$.
- A zero vector will be denoted by $\vec{0}$.
- $\vec{e_i}$ denotes the i-th vector of the standard basis for $\mathbb{R}^n$ (see [3, p. 365]).
- Let A be a matrix. The i-th row of A will be denoted by $A_{i,*}$. The j-th column of A will be denoted by $A_{*,j}$. The element in the i-th row, j-th column of this matrix will be denoted by $A_{i,j}$.
- I_n denotes an $n \times n$ identity matrix.
- $\mathcal{P}(N)$ stands for the power set of $N = \{1, \ldots, n\}$.
- Let S be a set. $|S|$ denotes the cardinality of S.
- The polynomial ring in variable x over $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}[x]$.
- A quadratic function (see Definition (7)) without linear and constant term is said to be *quadratic homogenous*.
- Let $L : V \to W$ be a linear map between vector spaces, then

$$\begin{aligned} \mathrm{Ker}(L) &= \{\vec{v} \in V \mid L(\vec{v}) = \vec{0}\}, \\ \mathrm{Im}(L) &= \{L(\vec{v}) \in W \mid \vec{v} \in V\}. \end{aligned}$$

1.2 Boolean functions

Definition 1. [4, p. 6] A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function*.

Definition 2. [1, p. 4] A function F such that

$$\begin{aligned} F : \mathbb{F}_2^n &\to \mathbb{F}_2^m \\ F(\vec{x}) &\mapsto (f_1(\vec{x}), \ldots, f_m(\vec{x}))^\top \end{aligned}$$

is called a *vectorial Boolean function* (for brevity further denoted by (n, m)-function).
Binary Boolean functions $f_1, \ldots, f_m$ are said to be *coordinate functions* of F.

For every Boolean function there exists a finite field representation and a unique algebraic normal form (ANF) representation. Both of these representations can be used to examine Boolean functions. We will give the definitions and properties of both in the next sections.

1.3 ANF representation

Definition 3. [4, p. 9] Suppose $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a binary Boolean function. We define the *algebraic normal form (ANF)* of f (denoted as $\widetilde{f}$) as an element of

$$\mathbb{F}_2[x_1, \ldots, x_n] \Big/ (x_1 + x_1^2, \ldots, x_n + x_n^2)$$

such that $\widetilde{f}(\vec{x}) = f(\vec{x})\ \forall \vec{x} \in \mathbb{F}_2^n$.

Remark. [4, p. 9] For $a_I \in \mathbb{F}_2$ the ANF of f can be written as

$$\widetilde{f}(\vec{x}) = \sum_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \in \mathcal{P}(N)} a_I \vec{x}^I.$$

In other words, $\widetilde{f}$ is a multivariate polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ such that every variable appears in it with exponent at most 1.

Theorem 1. *[4, p. 10] For every binary Boolean function f there exists a unique ANF representation of f.*

Definition 4. [4, p. 12] The *algebraic degree* of a binary Boolean function f is defined as $d^\circ f = \max\{|I| \mid a_I \neq 0\}$.

We can extend the definition of ANF to the vectorial Boolean functions as follows.

Definition 5. [1, p. 9] Let F be an (n, m)-function. The *ANF* of F (denoted as $\widetilde{F}$) is defined as an element of

$$\mathbb{F}_2^m[x_1, \ldots, x_n] \Big/ (x_1 + x_1^2, \ldots, x_n + x_n^2)$$

such that $\widetilde{F}(\vec{x}) = F(\vec{x})\ \forall \vec{x} \in \mathbb{F}_2^n$.

Remark. [1, p. 9] For $\vec{a_I} \in \mathbb{F}_2^m$ the ANF of a vectorial Boolean function can be written as

$$\widetilde{F}(\vec{x}) = \sum_{I \in \mathcal{P}(N)} \vec{a_I} \left(\prod_{i \in I} x_i \right) = \sum_{I \in \mathcal{P}(N)} \vec{a_I} \vec{x}^I.$$

In other words, $\widetilde{F}$ is a multivariate polynomial in $\mathbb{F}_2^m[x_1, \ldots, x_n]$ such that every variable appears in it with exponent at most 1. The $\widetilde{F}$ can be obtained from the ANFs of the coordinate functions of F. Since the $\widetilde{f_i}$ exists and is unique for every $f_i,\ i \in \{0, \ldots, m\}$, F is also uniquely represented by $\widetilde{F}$ (see [1, p. 9]).

Definition 6. [1, p. 9] The *algebraic degree* of a vectorial Boolean function f is defined as $d^\circ F = \max\{|I| \mid a_I \neq \vec{0}\}$.

Definition 7. An (n, m)-function F satisfying $d^\circ F = 1$ is called *linear*.
An (n, m)-function F having $d^\circ F = 2$ is called *quadratic*.

Remark. A quadratic homogenous (n, n)-function (in terms of the ANF representation) can be represented as:

$$\widetilde{F}(\vec{x}) = \sum_{\substack{I \in \mathcal{P}(N) \\ |I|=2}} \vec{a_I} \vec{x}^I.$$

1.4 Finite field representation

Lemma 2. *[5, p. 31] The finite field $\mathbb{F}_{2^n}$ is a vector space of dimension n over its subfield $\mathbb{F}_2$.*

The lemma leads us to representing the elements of $\mathbb{F}_{2^n}$ with respect to a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Definition 8. Let $x \in \mathbb{F}_{2^n}$ and $B = (\alpha_1, \ldots, \alpha_n)$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then the vector $\vec{\lambda} = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_2^n$ such that

$$x = \sum_{i=1}^{n} \lambda_i \cdot \alpha_i$$

is said to be the *coordinate vector of x with respect to B* and denoted by $[x]_B$.

Theorem 3. *[1, p. 10] Any (n, n)-function F admits a unique univariate polynomial representation over $\mathbb{F}_{2^n}$, of degree at most $2^n - 1$:*

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

A useful property of the finite field $\mathbb{F}_{2^n}$ follows.

Lemma 4. *[5, p. 16] Assume $a, b \in \mathbb{F}_{2^n}, i \in \mathbb{N}$. Then $(a + b)^{2^i} = (a^{2^i} + b^{2^i})$.*

In this thesis we will work with quadratic homogenous (n, n)-functions, therefore we need to understand how to determine *quadratic* functions from their finite field representation.

Definition 9. The *Hamming weight* of $j \in \mathbb{N}_0$, denoted by $w_H(j)$, is defined as the number of nonzero coordinates of the binary expansion of j.

Theorem 5. *[1, p. 11] Assume F is an (n, n)-function defined by*

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

Then $\max_{0 \le j \le 2^n-1}\{w_H(j) \mid c_j \neq 0\} = d^\circ F$.

Corollary 6. *If* $\max_{0 \le j \le 2^n-1}\{w_H(j) \mid c_j \neq 0\}$ *equals*

- *1, then F is linear,*

- *2, then F is quadratic.*

Remark. Note that F being quadratic homogenous in terms of the ANF representation does not imply F being quadratic homogenous in terms of the finite field representation. We will later show that APNness is affinely invariant, therefore in both representation we can focus on quadratic homogenous functions only.

Remark. Every quadratic homogenous (n, n)-function F (in terms of the finite field representation) can be represented as

$$\sum_{1 \leq t < i \leq n}^{n} c_{i,t} x^{2^{i-1}+2^{t-1}}.$$

1.5 APN functions and their properties

All of the following definitions can be similarly formulated for the finite field representation just by changing $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$.

Definition 10. Let F be an (n, n)-function. We define

$$A_{b,a}^F = \{x \in \mathbb{F}_2^n \mid F(x) + F(x+a) = b\}.$$

Definition 11. [1, p. 26] $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is said to be almost perfect nonlinear (APN) if

$$\forall a \in \mathbb{F}_2^n \setminus \{\vec{0}\},\ \forall b \in \mathbb{F}_{2^n} :\ |A_{b,a}^F| \leq 2.$$

Remark. Note that due to the characteristics of 2 if $F(x) + F(x+a) + b = 0$ for $x = \tilde{x} \in \mathbb{F}_{2^n}$ then it also holds for $x = \tilde{x} + a$. Therefore,

$$|\{x \in \mathbb{F}_{2^n} \mid F(x) + F(x+a) + b = 0\}|$$

is always even.

Lemma 7. *Let L be an affine (n, n)-function. Suppose F, G are (n, n)-functions such that F is quadratic homogenous, G is quadratic such that*

$$\forall x \in \mathbb{F}_2^n :\ G(x) = F(x) + L(x).$$

Then F is APN if and only if G is APN.

Proof.
It is easily seen that $A_{b,a}^G = A_{L(a)+b,a}^F$:

$$\begin{aligned} G(x) + G(x+a) + b &= F(x) + L(x) + F(x+a) + L(x+a) + b \\ &= F(x) + L(x) + F(x+a) + L(x) + L(a) + b \\ &= F(x) + F(x+a) + L(a) + b. \end{aligned}$$

Therefore,

$$\left(\forall a, b \in \mathbb{F}_2^n, a \neq \vec{0} : |A_{b,a}^G| \leq 2\right) \iff \left(\forall a, c \in \mathbb{F}_2^n, a \neq \vec{0} : |A_{c,a}^F| \leq 2\right).$$

□

Remark. Lemma (7) shows that when studying quadratic APN functions we can focus on quadratic homogenous (n, n)-functions only.

1.6 Equivalence respecting APNness

There are two notions of equivalence respecting the APNness of a function. The CCZ-equivalence is stronger then the EA-equivalence, but in terms of quadratic functions they are the same.

Definition 12. [2, p. 588] Two (n, n)-functions F_1, F_2 are called

- Extended affine equivalent (EA-equivalent) if there exist A_1, A_2 affine permutations on $\mathbb{F}_{2^n}$ and A_3 an affine function on $\mathbb{F}_{2^n}$ such that

$$F_2(x) = A_1(F_1(A_2(x))) + A_3(x),$$

- Carlet-Charpin-Zinoniev equivalent (CCZ-equivalent) if there exists an affine permutation which maps the graph G_{F_1} onto the graph G_{F_2}, where

$$G_{F_i} = \{(x, F_i(x)) \mid x \in \mathbb{F}_{2^n}\}, \text{ for } i \in \{1, 2\}.$$

Remark. CCZ-equivalence is a generalization of EA-equivalence.

Theorem 8. *[1, p. 42] If two (n, n)-functions F, G are CCZ-equivalent, then F is APN if and only if G is APN.*

Theorem 9. *[2, p. 588] Let F, G be quadratic (n, n)-functions. Then F, G are CCZ-equivalent if and only if they are EA-equivalent.*

Remark. Finding a new (not CCZ-equivalent to a known one) quadratic APN function is simplified to finding an APN function that is EA-inequivalent to any known quadratic APN function.

2. Finite field approach

In this chapter we will explain the basics of the method introduced in [2]. We will follow the structure of the original paper and add theorems and lemmas for easier understanding. We will also slightly change the notation. From now on let

$$F(x) = \sum_{1 \le t < i \le n}^{n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

be a finite field representation of a quadratic homogenous (n, n)-function.

2.1 Matrix representation of F

In this section we will explain how to construct the corresponding matrix for given function F. Most of this section can be found in [2, p. 589-591]. In comparison with the original paper, we will divide the content into separate statements and add proofs when needed. We will also add Lemma (13) that will be later useful in Chapter (4).

Definition 13. [2, p. 589] Let us denote by $E_F = (e_{i,t})_{n \times n} \in \mathbb{F}_{2^n}^{n \times n}$ the *coefficient matrix of* F obtained as follows:

$$e_{i,t} = \begin{cases} c_{i,t} & \text{if } 1 \le t < i \le n, \\ 0 & \text{otherwise.} \end{cases}$$

Remark. Note that because of F being quadratic homogenous, E_F becomes lower triangular with zeros in the main diagonal. If it were not quadratic homogenous, the coefficients of the linear terms would be in the main diagonal.

Definition 14. For $x \in \mathbb{F}_{2^n}$ we define $\underline{x} = (x^{2^0}, x^{2^1}, \ldots, x^{2^{n-1}})^\top$.

Lemma 10. *[2, p. 590] Let $x \in \mathbb{F}_{2^n}$. Then $F(x) = \underline{x}^\top E_F \ \underline{x}$.*

Proof.
We have

$$\begin{aligned} \underline{x}^\top E_F \ \underline{x} &= (x^{2^0}, x^{2^1}, \ldots, x^{2^{n-1}}) \begin{pmatrix} 0 & 0 & \ldots & 0 \\ e_{2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ e_{n,1} & e_{n,2} & \ldots & 0 \end{pmatrix} \begin{pmatrix} x^{2^0} \\ x^{2^1} \\ \vdots \\ x^{2^{n-1}} \end{pmatrix} \\ &= \sum_{1 \le i < t \le n} e_{i,t} x^{2^{i-1}+2^{t-1}} \\ &= \sum_{1 \le i < t \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} \\ &= F(x). \end{aligned}$$

□

Definition 15. [2, p. 589] Let $B = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{2^n}^n$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. We define

$$M_B = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2^{n-1}} & \alpha_2^{2^{n-1}} & \ldots & \alpha_n^{2^{n-1}} \end{pmatrix}.$$

Lemma 11. *Let $B = (\alpha_1, \ldots, \alpha_n)$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then $\underline{x} = M_B \cdot [x]_B$.*

Proof.
Let us denote $[x]_B = (\lambda_1, \ldots, \lambda_n) \in \mathbb{F}_2^n$. Because of the finite characteristic of $\mathbb{F}_{2^n}$, we obtain:

$$x^{2^k} = (\sum_{i=1}^{n} \lambda_i \alpha_i)^{2^k} = \sum_{i=1}^{n} (\lambda_i \alpha_i)^{2^k} = \sum_{i=1}^{n} \lambda_i^{2^k} \alpha_i^{2^k} = \sum_{i=1}^{n} \lambda_i \alpha_i^{2^k}.$$

And therefore

$$\underline{x} = \begin{pmatrix} x^{2^0} \\ x^{2^1} \\ \vdots \\ x^{2^{n-1}} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} \lambda_i \alpha_i \\ \sum_{i=1}^{n} \lambda_i \alpha_i^2 \\ \vdots \\ \sum_{i=1}^{n} \lambda_i \alpha_i^{2^{n-1}} \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2^{n-1}} & \alpha_2^{2^{n-1}} & \ldots & \alpha_n^{2^{n-1}} \end{pmatrix} [x]_B.$$

□

Corollary 12. *[2, p. 590] By combining the results we obtain $\forall x \in \mathbb{F}_{2^n}$:*

$$F(x) = [x]_B^\top M_B^\top E_F M_B [x]_B.$$

Definition 16. [1, p. 17] The derivative of F at $a \in \mathbb{F}_{2^n}$ is defined as

$$D_a F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},$$
$$D_a F(x) = F(x) + F(x + a).$$

Definition 17. [2, p. 590] Let B be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. We will denote the matrix $E_F + E_F^\top$ by C_F. The matrix

$$H_{F,B} = M_B^\top (E_F + E_F^\top) M_B$$

will be called *the corresponding matrix of F (with respect to the basis B).*

Lemma 13. *Let B be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Let $F_1, F_2, F_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be quadratic homogenous functions with corresponding matrices $H_{F_1,B}, H_{F_2,B}, H_{F_3,B}$ respectively. If $F_3(x) = F_1(x) + F_2(x)$ for all $x \in \mathbb{F}_{2^n}$, then $H_{F_3,B} = H_{F_1,B} + H_{F_2,B}$.*

Proof. By definition $E_{F_3} = E_{F_1} + E_{F_2}$. Therefore

$$\begin{aligned} H_{F_3,B} &= M_B^\top (E_{F_3}^\top) M_B \\ &= M_B^\top (E_{F_1} + E_{F_2} + E_{F_1}^\top + E_{F_2}^\top) M_B \\ &= M_B^\top (E_{F_1} + E_{F_1}^\top) M_B + M_B^\top (E_{F_2} + E_{F_2}^\top) M_B \\ &= H_{F_1,B} + H_{F_2,B}. \end{aligned}$$

□

To continue we first need to prove an auxiliary lemma.

Lemma 14. *Let $A \in \mathbb{F}_{2^n}^{n\times n}$. Then $\forall \vec{u}, \vec{v} \in \mathbb{F}_{2^n}^n :\ \vec{v}^\top A\vec{u} = \vec{u}^\top A^\top \vec{v}$.*

Proof.
We have

$$\begin{aligned}
\vec{v}^\top A\vec{u} &= \sum_{i=1}^{n} v_i \cdot \sum_{t=1}^{n} u_t \cdot A_{i,t},\\
\vec{u}^\top A^\top \vec{v} &= \sum_{i=1}^{n} u_i \cdot \sum_{t=1}^{n} v_t \cdot A_{t,i} = \sum_{i=1}^{n} v_i \cdot \sum_{t=1}^{n} u_t \cdot A_{i,t},\\
\vec{v}^\top A\vec{u} &= \vec{u}^\top A^\top \vec{v}.
\end{aligned}$$

□

The following definition and lemma explain the definition of matrix $H_{F,B}$.

Definition 18. Let $a \in \mathbb{F}_{2^n}$, we define a mapping

$$\begin{aligned}
L_a : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n},\\
x &\mapsto D_a(x) + F(a).
\end{aligned}$$

Lemma 15. *[2, p. 590] If $a \in \mathbb{F}_{2^n}$, then $\forall x \in \mathbb{F}_{2^n}$:*

$$L_a(x) = [x]_B^\top H_{F,B}[a]_B.$$

Proof.
Using the definition of $D_aF(x)$ we obtain:

$$\begin{aligned}
L_a(x) &= F(x) + F(x+a) + F(a)\\
&= \underline{x}^\top E_F \underline{x} + (\underline{x} + \underline{a})^\top E_F(\underline{x} + \underline{a}) + \underline{a}^\top E_F \underline{a}\\
&= \underline{x}^\top E_F \underline{x} + \underline{x}^\top E_F \underline{x} + \underline{x}^\top E_F \underline{a} + \underline{a}^\top E_F \underline{x} + \underline{a}^\top E_F \underline{a} + \underline{a}^\top E_F \underline{a}\\
&= \underline{x}^\top E_F \underline{a} + \underline{a}^\top E_F \underline{x}.
\end{aligned}$$

Now we can use Lemma (14):

$$\underline{a}^\top E_F \underline{x} = \underline{x}^\top E_F^\top \underline{a}.$$

And therefore, we obtain:

$$\begin{aligned}
L_a(x) &= \underline{x}^\top E_F \underline{a} + \underline{x}^\top E_F^\top \underline{a}\\
&= \underline{x}^\top (E_F + E_F^\top)\underline{a}\\
&= \underline{x}^\top C_F \underline{a}\\
&= (M_B[x]_B)^\top C_F M_B[a]_B\\
&= [x]_B^\top H_{F,B}[a]_B.
\end{aligned}$$

□

Corollary 16. *[2, p. 590] For given $a \in \mathbb{F}_{2^n}$ the function $L_a : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a linear mapping between vector spaces.*

Proof.
To prove the linearity of scalar multiplication we need to consider two cases for $b \in \mathbb{F}_2$:

- If $b = 0$, then

$$L_a(b \cdot x) = L_a(\vec{0}) = 0 = b \cdot (L_a(x)),$$

- if $b = 1$, then

$$L_a(b \cdot x) = [x]_B^\top H_{F,B}[a]_B = b \cdot (L_a(x)).$$

Let $x, y \in \mathbb{F}_{2^n}$. We prove the linearity of addition as follows:

$$\begin{aligned} L_a(x+y) &= [x+y]_B^\top H_{F,B}[a]_B \\ &= ([x]_B + [y]_B)^\top H_{F,B}[a]_B \\ &= [x]_B^\top H_{F,B}[a]_B + [y]_B^\top H_{F,B}[a]_B \\ &= L_a(x) + L_a(y). \end{aligned}$$

□

Lemma 17. *M_B is invertible over $\mathbb{F}_{2^n}$.*

Proof.
M_B is a square $n \times n$ matrix. Therefore, we only need to prove that the mapping $\vec{v} \mapsto M_B \cdot \vec{v}$ is injective for $\vec{v} \in \mathbb{F}_{2^n}^n$. Let $M_B \cdot \vec{v} = \vec{0}$,

$$v_1 \cdot \begin{pmatrix} \alpha_1 \\ \alpha_1^2 \\ \dots \\ \alpha_1^{2^{n-1}} \end{pmatrix} + v_2 \cdot \begin{pmatrix} \alpha_2 \\ \alpha_2^2 \\ \dots \\ \alpha_2^{2^{n-1}} \end{pmatrix} + \dots + v_n \cdot \begin{pmatrix} \alpha_n \\ \alpha_n^2 \\ \dots \\ \alpha_n^{2^{n-1}} \end{pmatrix} = \vec{0}.$$

Because of $\alpha_1, \dots, \alpha_n$ being a basis and therefore linearly independent, we obtain $\vec{v} = \vec{0}$. We have proved that the mapping is injective.

□

Theorem 18. *[2, p. 591] From the matrix $H_{F,B}$ and the basis B we can uniquely construct the quadratic homogenous function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Vice versa the quadratic homogenous function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and the basis B give us the unique matrix $H_{F,B}$.*

Proof.
Construction of $H_{F,B}$ with respect to B and F has already been shown. Suppose $H_{F,B} \in \mathbb{F}_{2^n}^{n \times n}$ is a symmetric matrix with only zeros in the main diagonal. Let B be a basis of $\mathbb{F}_{2^n}$ such that:

$$H_{F,B} = M_B^\top (E_F + E_F^\top) M_B.$$

According to Lemma (17) there exists M_B^{-1} and it is evident that there exists $(M_B^\top)^{-1} = (M_B^{-1})^\top$. We obtain:

$$(M_B^\top)^{-1} H_{F,B} \cdot M_B^{-1} = E_F + E_F^\top.$$

By definition E_F is a lower triangular matrix. Therefore, the above equality immediately gives us E_F.

□

2.2 Correspondence between QAMs and APN functions

The one to one correspondence between quadratic homogenous functions and so called quadratic APN matrices will be proved in this section. It will cover the rest of [2, p. 589-591]. The proof of Theorem (21) is based on the proof of [2, Theorem 1], but extra steps for better understanding will be added. From now on we will abbreviate $M_B, E_F, C_F, H_{F,B}$ and $[x]_B$ to M, E, C, H and $[x]$, respectively.

Definition 19. [2, p. 589] Let $\vec{v} = (v_1, \ldots, v_m)^\top \in \mathbb{F}_{2^n}^m$. We define:

- $\mathrm{Span}_{\mathbb{F}_2}(\vec{v}) = \mathrm{Span}_{\mathbb{F}_2}(\vec{v}^\top) = \mathrm{Span}_{\mathbb{F}_2}(v_1, \ldots, v_m) = \{\sum_{i=1}^m \lambda_i \cdot v_i \mid \lambda_i \in \mathbb{F}_2\}$,
- $\mathrm{Rank}_{\mathbb{F}_2}(\vec{v}) = \mathrm{Rank}_{\mathbb{F}_2}(\vec{v}^\top)$ as the dimension of $\mathrm{Span}_{\mathbb{F}_2}(\vec{v})$ over $\mathbb{F}_2$.

Remark. [2, p. 589] Let $B = (\alpha_1, \ldots, \alpha_n)$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Suppose

$$\forall i \in \{1, \ldots, m\} : \ [v_i]_B = (\gamma_{i,1}, \ldots, \gamma_{i,n})$$

and define a matrix $\Gamma = (\gamma_{i,j})_{m \times n}$. Then $\mathrm{Rank}_{\mathbb{F}_2}(\vec{v}) = \mathrm{Rank}(\Gamma)$.

Lemma 19. *Let $P \in \mathbb{F}_2^{n \times n}$ be invertible. Then $\forall \vec{v} \in \mathbb{F}_{2^n}^n$:*

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{v}) = \mathrm{Rank}_{\mathbb{F}_2}(P\vec{v}).$$

Proof.
Let Γ be a matrix as in the remark above. We can see that $\mathrm{Rank}_{\mathbb{F}_2}(P\vec{v}) = \mathrm{Rank}(P \cdot \Gamma)$. We know that multiplying by an invertible matrix does not change the rank of a matrix (see [3, p. 467, 502]). Therefore,

$$\mathrm{Rank}_{\mathbb{F}_2}(P\vec{v}) = \mathrm{Rank}(P \cdot \Gamma) = \mathrm{Rank}(\Gamma) = \mathrm{Rank}_{\mathbb{F}_2}(\vec{v}).$$

□

Definition 20. [2, p. 589] A matrix $J \in \mathbb{F}_{2^n}^{n \times n}$ is said to be a *quadratic APN matrix (QAM)* if all of the following hold:

- J is symmetric,
- the elements in the main diagonal are zero,

- for any nonzero $\vec{\lambda} \in \mathbb{F}_2^n$: $\mathrm{Rank}_{\mathbb{F}_2}(J \cdot \vec{\lambda}) = n - 1$.

Remark. The third condition is equal to every nonzero linear combination of the n rows (or columns due to the symmetry) having rank $n - 1$ over $\mathbb{F}_2$.

Theorem 20 (Rank-nullity theorem)**.** *[6, p. 52] Assume that V, W are vector spaces such that V has a finite dimension. Let $L : V \to W$ be a linear mapping, then*

$$\dim(\mathrm{Ker}(L)) + \dim(\mathrm{Im}(L)) = \dim(V).$$

Theorem 21. *[2, p. 590] H is a QAM if and only if (quadratic homogenous) F is APN.*

Proof.
Let $a \in \mathbb{F}_{2^n}^*$, we define a linear mapping L_a as in Definition (18). It is easily seen that $\{0, a\} \subseteq \mathrm{Ker}(L_a)$:

$$\begin{aligned} L_a(0) &= F(0+a) + F(0) + F(a) = 0, \\ L_a(a) &= F(a+a) + F(a) + F(a) = 0. \end{aligned}$$

First, suppose F is APN. Note that H is by definition symmetric with only zeros in the main diagonal:

$$\begin{aligned} &H^\top = (M^\top C M)^\top = M^\top (E + E^\top)^\top M = M^\top (E + E^\top) M = M^\top (C) M = H, \\ &H_{i,i} = (M^\top E M)_{i,i} + (M^\top E^\top M)_{i,i} = (M^\top E M)_{i,i} + (M^\top E M)_{i,i}^\top = 0. \end{aligned}$$

Therefore, we only need to check the third property of a QAM. Because of the APNness of F the following holds:

$$\begin{aligned} |\{x \in \mathbb{F}_{2^n} \mid x \in \mathrm{Ker}(L_a)\}| &= |\{x \in \mathbb{F}_{2^n} \mid L_a(x) = 0\}| \\ &= |\{x \in \mathbb{F}_{2^n} \mid F(x) + F(x+a) + F(a) = 0\}| \leq 2. \end{aligned}$$

The inequality and $\{0, a\} \subseteq \mathrm{Ker}(L_a)$ implies:

$$\mathrm{Ker}(L_a) = \{0, a\} \Rightarrow \dim_{\mathbb{F}_2}(\mathrm{Ker}(L_a)) = 1.$$

Finally, from Lemma (15) and Theorem (20):

$$\mathrm{Rank}_{\mathbb{F}_2}(H \cdot [a]) = \mathrm{Rank}_{\mathbb{F}_2}(L_a) = n - \dim_{\mathbb{F}_2}(\mathrm{Ker}(L_a)) = n - 1.$$

In the same manner if H is a QAM, Theorem (20) gives us $\dim \mathrm{Ker}(L_a) = 1$. We only need to show that $F(x) + F(x+a) = b$ has 0 or 2 solutions for any $a \in \mathbb{F}_{2^n}^*,\ b \in \mathbb{F}_{2^n}$. Because

$$\{F(a) + b \mid b \in \mathbb{F}_{2^n}\} = \{b \in \mathbb{F}_{2^n}\},$$

it is sufficient to compute the number of solutions of

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

First, let us consider $b \notin \mathrm{Im}(L_a)$. Then

$$|\{x \in \mathbb{F}_{2^n} :\ F(x) + F(x+a) = F(a) + b\}| = |\{x \in \mathbb{F}_{2^n} :\ L_a(x) = b\}| = 0.$$

Second, let $b \in \mathrm{Im}(L_a)$. Then there exists $\tilde{x}$ such that $F(\tilde{x})+F(\tilde{x}+a) = F(a)+b$ which also yields $\tilde{x}+a$ as a solution. If $y \in \mathbb{F}_{2^n}, y \notin \{\tilde{x}, \tilde{x}+a\}$, then the linearity of L_a implies that:

$$L_a(y+\tilde{x}) = b+b = 0 \Rightarrow y+\tilde{x} \in \mathrm{Ker}(L_a) \Rightarrow y+\tilde{x} \in \{0, a\} \Rightarrow y \in \{\tilde{x}, \tilde{x}+a\},$$

which contradicts our assumption. Thus, $F(x)+F(x+a)+b = 0$ has always 0 or 2 solutions.

□

Corollary 22. *[2, p. 591] There is a one to one correspondence between QAMs and quadratic homogenous APN functions.*

2.3 EA equivalence in terms of QAMs

From Remark (1.6) we know that finding new quadratic APN functions can be restricted to finding EA-inequivalent ones. Therefore, in this section we will focus on how to determine the EA-equivalence from the corresponding matrices of the functions. Most of this section is rewritten (with little changes in the formulations) from [2, p. 591-595]. The proofs of Theorem (24) and Theorem (23) are based on the original ones with extra steps added.

Lemma 23. *[2, p. 591] Assume $H, W_1, W_2 \in \mathbb{F}_{2^n}^{n\times n}$ such that $H = W_1 + W_1^\top = W_2 + W_2^\top$. Then $\exists A \in \mathbb{F}_{2^n}^{n\times n}$ symmetric such that $W_2 = W_1 + A$.*

Proof.
Let us set $S = \{W \in \mathbb{F}_{2^n}^{n\times n} \ : \ W + W^\top = H\}$. Note that $W_1, W_2 \in S$.
Suppose A is $n \times n$ symmetric matrix over $\mathbb{F}_{2^n}$. Then

$$\begin{aligned}(W_1+A)+(W_1+A)^\top &= W_1 + A + W_1^\top + A^\top \\ &= W_1 + A + W_1^\top + A \\ &= W_1 + W_1^\top \\ &= H.\end{aligned}$$

Therefore, $W_1 + A \in S$. Let $\widetilde{S}$ denote the set

$$\{W_1 + A \ : \ A \in \mathbb{F}_{2^n}^{n\times n} \text{ is symmetric}\}.$$

We have proved that $W_1 + A \in \widetilde{S} \Rightarrow W_1 + A \in S$, thus $S \subseteq \widetilde{S}$. It is easily seen that

$$|S| = 2^{n^2\cdot(n-1)/2} = |\widetilde{S}|.$$

We obtain $S = \widetilde{S}$. Finally by the above $W_2 \in S \Rightarrow W_2 \in \widetilde{S} \Rightarrow W_2 = W_1 + A$ for A symmetric.

□

Theorem 24. *[2, p. 592] Let $H_{F_1} \in \mathbb{F}_{2^n}^{n\times n}$ be a symmetric matrix with zeros in the main diagonal, let $H_{F_2} \in \mathbb{F}_{2^n}^{n\times n}$. Suppose $P \in \mathbb{F}_2^{n\times n}$ is an invertible matrix such that $H_{F_2} = P^\top H_{F_1} P$. Then the quadratic functions F_1, F_2 defined by these matrices relative to the basis B are EA-equivalent.*

Proof.
Let F_1, F_2 be quadratic homogenous (n,n)-functions with coefficient matrices E_{F_1}, E_{F_2} respectively. For brevity of notation let us set $W_1 = M^\top E_{F_1} M$ and $W_2 = M^\top E_{F_2} M$. Under the assumptions of the theorem we get:

$$W_2 + W_2^\top = H_{F_2} = P^\top H_{F_1} P = P^\top W_1 P + P^\top W_1^\top P.$$

Lemma (23) states there exists $A = (a_{i,j})_{n\times n} \in \mathbb{F}_{2^n}^{n\times n}$ symmetric such that $W_2 = A + P^\top W_1 P$. Using the expression from Corollary (12) we obtain:

$$\begin{aligned} F_1(x) &= [x]^\top M^\top E_{F_1} M[x] = [x]^\top W_1[x], \\ F_2(x) &= [x]^\top M^\top E_{F_2} M[x] \\ &= [x]^\top W_2[x] \\ &= [x]^\top (A + P^\top W_1 P)[x] \\ &= [x]^\top A[x] + [x]^\top P^\top W_1 P[x]. \end{aligned}$$

Let $T_A(x) = [x]^\top A[x]$ and $T_P(x) = P[x]$ for brevity. That means:

$$F_2(x) = F_1(T_P(x)) + T_A(x).$$

To complete the proof it is sufficient to show that T_A is an affine mapping and T_P is an affine permutation. Let $x, y \in \mathbb{F}_{2^n}$.

- Due to symmetry of A we obtain

  $$T_A(x) = [x]^\top A[x] = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}[x]_i[x]_j = \sum_{i=1}^{n} a_{i,i}[x]_i^2 = \sum_{i=1}^{n} a_{i,i}[x]_i.$$

  We use the above expression to prove the linearity of addition.

  $$\begin{aligned} T_A(x+y) &= \sum_{i=1}^{n} a_{i,i}[x+y]_i = \sum_{i=1}^{n} a_{i,i}([x]+[y])_i \\ &= \sum_{i=1}^{n} a_{i,i}[x]_i + \sum_{i=1}^{n} a_{i,i}[y]_i = T_A(x) + T_A(y). \end{aligned}$$

  For the linearity of the scalar multiplication we just need to consider:

  $$\begin{aligned} T_A(0\cdot x) &= T_A(0) = 0 = 0 \cdot T_A(x), \\ T_A(1\cdot x) &= T_A(x) = 1 \cdot T_A(x). \end{aligned}$$

- It is clear that

  $$\begin{aligned} T_P(x+y) &= P([x]+[y]) = P[x] + P[y] = T_P(x) + T_P(y), \\ T_P(0\cdot x) &= T_P(0) = 0 = 0 \cdot T_P(x), \\ T_P(1\cdot x) &= T_P(x) = 1 \cdot T_P(x). \end{aligned}$$

  It is assumed that P is invertible. Therefore, we can prove surjectivity of the mapping. Suppose $T_P(x) = T_P(y)$, then

  $$\begin{aligned} P[x] &= P[y], \\ P^{-1}P[x] &= P^{-1}P[y], \\ [x] &= y, \\ x &= y. \end{aligned}$$

  That implies that T_P is bijective, because it is a surjective mapping between finite spaces.

□

Lemma 25. *[2, p. 593] Let* $\mathrm{Lin}(x) \in \mathbb{F}_{2^n}[x]$ *be a linear function. Every quadratic function* $Q[x] \in \mathbb{F}_{2^n}[x]$ *with* $Q(0) = 0$ *can be denoted as*

$$Q(x) = \sum_{1 \le t < i \le n} c_{i,t} x^{2^{i-1}+2^{t-1}} + \mathrm{Lin}(x).$$

Theorem 26. *[2, p. 594] Let* $H = (h_{i,j})_{n\times n} \in \mathbb{F}_{2^n}^{n\times n}$ *be symmetric with only zeros in the main diagonal. Suppose* $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *is a linear permutation. Let* $H' = (L(h_{i,j}))_{n\times n}$*. Then the quadratic homogenous functions defined by* H *and* H' *relative to the basis* B *are EA-equivalent.*

Corollary 27. *[2, p. 594] Let* H, H' *be matrices as in the theorem above. Then* H *is a QAM if and only if* H' *is a QAM.*

Corollary 28. *[2, p. 595] Let* F_1, F_2 *be two quadratic homogenous functions with corresponding matrices* H_{F_1}, H_{F_2}*, respectively. If there exist an invertible matrix* $P \in \mathbb{F}_2^{n\times n}$ *and a linear permutation* $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such that*

$$\forall i, j \in \{1, \dots, n\} : \ (H_{F_2})_{i,j} = L((P^\top H_{F_1} P)_{i,j}),$$

then F_1 *is EA-equivalent to* F_2*.*

2.4 Properties of QAMs

This section will show how to determine whether a given matrix is a QAM. This section corresponds to [2, 595-597]. Furthermore, Theorems (29) and (30) will be proved to make the statement of Corollary (34) clear. The results stated in this section were used to design an efficient algorithm for constructing new QAMs from already known ones. The algorithm will be omitted in this thesis, for details see [2, p. 597-599]. Throughout this section let $r, c \in \mathbb{N}$ such that $r, c \le n$.

Definition 21. [2, p. 596] The matrix $A \in \mathbb{F}_{2^n}^{r\times c}$ satisfying

$$\forall \vec{\lambda} \in \mathbb{F}_2^c \setminus \{\vec{0}\} : \ \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda} \cdot A) \ge r - 1$$

is called *proper*. Otherwise we say the matrix is *improper*.

Remark. The definition of improper matrix was not originally used in [2].

Remark. Any QAM is by definition proper.

Definition 22. [6, p. 29] A *submatrix* of a matrix A is a matrix B obtained by deleting from A some (or none) rows and columns.

Theorem 29. *Assume that* $H \in \mathbb{F}_{2^n}^{n\times n}$ *is a QAM. Then every* $A \in \mathbb{F}_{2^n}^{r\times n}$ *submatrix of* H *is proper.*

Proof.
The definition of a QAM states that

$$\forall \vec{\lambda} \in \mathbb{F}_2^n,\ \vec{\lambda} \neq \vec{0} :\ \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda} \cdot H) = n - 1.$$

For $r = n$ the submatrix A equals H and therefore the assertion is true (because being a QAM implies being proper). Assume $r < n$, $\vec{v} \in \mathbb{F}_2^r \backslash \{\vec{0}\}$. $I_R \subseteq \{1, \ldots, n\}$ denotes the set of indices of the undeleted rows. Let $\vec{\lambda} \in \mathbb{F}_2^n$ such that

$$\lambda_i = \begin{cases} v_i & i \in I_R, \\ 0 & \text{otherwise.} \end{cases}$$

It can be easily seen that $\vec{\lambda} \neq \vec{0}$. The choice of the vector $\vec{\lambda}$ yields:

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{v}^\top \cdot A) = \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot H) = n - 1.$$

This gives that A is proper.

□

Remark. Equivalently if there exists A a submatrix of H such that A is not proper, then H is not a QAM. However, we will give few theorems that will show we can avoid going through all the submatrices and check just some of them.

Theorem 30. *If $A \in \mathbb{F}_{2^n}^{r \times c},\ r < c$ is proper, then any square $r \times r$ submatrix of A is also proper.*

Proof.
Let B denote the square submatrix and $\vec{v} \in \mathbb{F}_2^r,\ \vec{v} \neq \vec{0}$. I_C stands for the set of indices of undeleted columns. We assume A to be proper, which means $\mathrm{Rank}_{\mathbb{F}_2}(\vec{v} \cdot A) \geq c - 1$. We can see that for $i \in I_C$:

$$(\vec{v}^\top \cdot B)_i = (\vec{v}^\top \cdot A)_i.$$

We obtain the following inequality:

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{v}^\top \cdot B) \geq \mathrm{Rank}_{\mathbb{F}_2}(\vec{v}^\top \cdot A) - (c - r) \geq r - 1.$$

□

Corollary 31. *Let $A \in \mathbb{F}_{2^n}^{r \times r}$ be a submatrix of $H \in \mathbb{F}_{2^n}^{n \times n}$. If A is not proper, then there exists a $r \times n$ submatrix of H that is not proper.*

To prove the next theorem we first need to show a useful property of proper matrices.

Lemma 32. *[2, p. 596] Let $A \in \mathbb{F}_{2^n}^{r \times c}$ be a proper matrix. Let $P \in \mathbb{F}_2^{c \times c}$ and $P' \in \mathbb{F}_2^{r \times r}$ be invertible. Then matrices AP and $P'A$ are both proper.*

Proof.
Lemma (19) states that

$$\forall \vec{\lambda} \in \mathbb{F}_2^r :\ \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot A) = \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot (AP)).$$

Therefore, A being proper implies that AP is proper. In the same manner we can see that $P'A$ is also proper.

□

Theorem 33. *[2, p. 596] Suppose that $A \in \mathbb{F}_{2^n}^{r\times c}$, $r < c$ is a proper matrix satisfying*

$$\forall i \in \{1, \dots r\} : \ a_{i,i} = 0$$
$$\forall i, j \in \{1, \dots r\} : \ a_{i,j} = a_{j,i}.$$

Then also $A^\top$ is proper.

Proof.
Let $\vec{\lambda} \in \mathbb{F}_2^c$. For brevity let us denote $\vec{b} = A \cdot \vec{\lambda}$. We only need to show that for any nonzero $\vec{\lambda}$:

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot A^\top) \geq r - 1.$$

An equivalent formulation is:

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{b}) \geq r - 1.$$

We can divide this proof into two separate parts.

1. Suppose $(\lambda_{r+1}, \dots, \lambda_c) = \vec{0}$. Let us denote by A_r the matrix obtained from A by choosing only the first r columns and rows. It can be easily seen that

   $$\vec{b} = A_r \cdot (\lambda_1, \dots, \lambda_r) = (\lambda_1, \dots, \lambda_r)^\top \cdot A_r.$$

   Where the last equality holds due to the symmetry of A_r. Because we assumed A to be proper we obtain:

   $$\begin{aligned} \mathrm{Rank}_{\mathbb{F}_2}((\lambda_1, \dots, \lambda_r)^\top \cdot A_r) &\geq \mathrm{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot A) - (c - r) \\ &\geq c - 1 - (c - r) \\ &= r - 1. \end{aligned}$$

2. Now consider the other case when $(\lambda_{r+1}, \dots, \lambda_c) \neq \vec{0}$. We will show that in this case $\mathrm{Rank}_{\mathbb{F}_2}(\vec{b}) = r$. We will prove it by contradiction. Suppose that

   $$\mathrm{Rank}_{\mathbb{F}_2}(\vec{b}) < r.$$

   Therefore, $\exists \vec{v} \in \mathbb{F}_2^r \setminus \{\vec{0}\}$ such that $\sum_{i=1}^r v_i \cdot b_i = 0$. Consider the following matrices A', A'', A'''. First,

   $$A' = A \cdot P_1 = A \cdot \begin{pmatrix} 1 & \cdots & 0 & \lambda_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & \vdots \\ 0 & \cdots & 0 & \lambda_c \end{pmatrix} = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,c-1} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{r,1} & \cdots & a_{r,c-1} & b_r \end{array}\right).$$

   Without loss of generality let $\lambda_c = 1$, otherwise we would permute the columns of P_1. This assumption implies P_1 being invertible and Lemma

(32) states that A' is proper. Second,

$$A'' = P_2 \cdot A' = \begin{pmatrix} v_1 & \cdots & \cdots & v_r \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \vdots & 1 \end{pmatrix} \cdot A'$$

$$= \left(\begin{array}{ccc|c} \sum_{i=1}^{r} v_i a_{i,1} & \cdots & \sum_{i=1}^{r} v_i a_{i,c-1} & \sum_{i=1}^{r} v_i b_i \\ a_{2,1} & \cdots & a_{2,c-1} & b_2 \\ \vdots & \ddots & \vdots & \vdots \\ a_{r,1} & \cdots & a_{r,c-1} & b_r \end{array}\right).$$

We can again without loss of generality assume that $v_1 = 1$ and thus P_2 is invertible. Again according to Lemma (32) A'' is proper. Third, let us compute A''' as follows:

$$A''' = A'' \cdot P_3 = A'' \cdot \begin{pmatrix} v_1 & 0 & \cdots & \cdots & 0 \\ v_2 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ v_r & \vdots & \ddots & & \vdots \\ 0 & \vdots & & \ddots & \vdots \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & \cdots & \cdots & 1 \end{pmatrix}$$

$$= \left(\begin{array}{ccc|c} \sum_{j=1}^{r} v_j (\sum_{i=1}^{r} v_i a_{i,j}) & \cdots & \sum_{i=1}^{r} v_i a_{i,c-1} & \sum_{i=1}^{r} v_i b_i \\ \sum_{j=1}^{r} v_j a_{2,j} & \cdots & a_{2,c-1} & b_2 \\ \vdots & \ddots & \vdots & \vdots \\ \sum_{j=1}^{r} v_j a_{r,j} & \cdots & a_{r,c-1} & b_r \end{array}\right).$$

Using similar arguments as for A', A'' we obtain that A''' is proper. However, $\vec{v}$ is a vector such that $\sum_{i=1}^{r} v_i b_i = 0$. Therefore, $A'''_{1,c} = 0$. Similarly, from zero diagonal and symmetry of A we can see that $A'''_{1,1} = 0$. This contradicts A''' being proper, because

$$\mathrm{Rank}_{\mathbb{F}_2}(\vec{e_1}^{\top} \cdot A''') \leq c - 2.$$

We have proved that $A^{\top}$ is proper.

□

Corollary 34. *[2, p. 596] Let $H \in \mathbb{F}_{2^n}^{n \times n}$ be a QAM. Then every submatrix of H must be proper.*

Proof.
Let $r < c$. Theorems (29) and (30) state that every $r \times n$ and $r \times r$ submatrix of H must be proper. Suppose $A \in \mathbb{F}_{2^n}^{r \times c}$ is a submatrix of H. Then there is a

proper matrix $K \in \mathbb{F}_{2^n}^{r \times n}$ such that A is a submatrix of K. And clearly for any nonzero $\vec{\lambda} \in \mathbb{F}_2^r$:

$$\text{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot A) \geq \text{Rank}_{\mathbb{F}_2}(\vec{\lambda}^\top \cdot K) - (n - c) \geq n - 1 - n + c = c - 1.$$

Which implies that A is proper. Finally, from Theorem (33) we obtain that any $c \times r$ submatrix of H is proper.

□

Corollary 35. *Let $A \in \mathbb{F}_{2^n}^{c \times r}, r < c$ be a submatrix of $H \in \mathbb{F}_{2^n}^{n \times n}$. If A is not proper, then there exists a $r \times c$ submatrix of H that is not proper.*

Remark. Given a matrix over $H \in \mathbb{F}_{2^n}^{n \times n}$ we only need to check all $r \times c$ submatrices of H with $r < c$ to decide whether there exists a improper submatrix of H. In other words, going through all submatrices would not give us new information.

3. ANF approach

In this chapter we will show that the matrices from Chapter (2) can be obtained directly from the ANF representation of a Boolean function. We will show that the one to one correspondence with APN functions also holds in this case. From now on let $\widetilde{F}$ be the ANF of a quadratic homogenous (in terms of the ANF) (n, n)-function such that

$$\widetilde{F}(\vec{x}) = \sum_{\substack{I \in \mathcal{P}(N) \\ |I|=2}} \vec{a_I} \left(\prod_{i \in I} x_i \right) = \sum_{\substack{I \in \mathcal{P}(N) \\ |I|=2}} \vec{a_I} \vec{x}^I.$$

3.1 Matrix representation of ANF

Definition 23. Let us denote by $E_{\widetilde{F}} = (e_{i,j})_{n \times n} \in (\mathbb{F}_2^n)^{n \times n}$ the *coefficient matrix of* $\widetilde{F}$ obtained as follows:

$$e_{i,j} = \begin{cases} \vec{a}_{\{i,j\}} & \text{if } 1 \leq j < i \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly $C_{\widetilde{F}}$ will stand for $E_{\widetilde{F}} + E_{\widetilde{F}}^\top$.

Remark. In this representation the elements of $E_{\widetilde{F}}, C_{\widetilde{F}}$ are vector from $\mathbb{F}_2^n$.

Example. Let $n = 3$. We define

$$\begin{aligned} \widetilde{F} : \mathbb{F}_2^3 &\to \mathbb{F}_2^3, \\ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &\mapsto \begin{pmatrix} x_1 x_2 \\ x_1 x_2 + x_1 x_3 \\ x_2 x_3 \end{pmatrix}. \end{aligned}$$

Using the ANF notation we can rewrite $\widetilde{F}(\vec{x})$ as:

$$\widetilde{F}((x_1, x_2, x_3)^\top) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \cdot x_1 x_2 + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \cdot x_1 x_3 + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \cdot x_2 x_3.$$

We can see that

$$\begin{aligned} \vec{a}_{\{1,2\}} &= (1, 1, 0)^\top, \\ \vec{a}_{\{1,3\}} &= (0, 1, 0)^\top, \\ \vec{a}_{\{2,3\}} &= (0, 0, 1)^\top. \end{aligned}$$

And therefore

$$C_{\widetilde{F}} = \begin{pmatrix} \vec{0} & (1,1,0)^\top & (0,1,0)^\top \\ (1,1,0)^\top & \vec{0} & (0,0,1)^\top \\ (0,1,0)^\top & (0,0,1)^\top & \vec{0} \end{pmatrix}.$$

Definition 24. Let $A \in (\mathbb{F}_2^n)^n$, $\vec{v} \in \mathbb{F}_2^n$. We define

$$A \cdot \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \sum_{i=1}^{n} v_i \cdot A_{*,i}.$$

Remark. Here $\sum_{i=1}^{n} v_i \cdot A_{*,i}$ denotes a scalar multiplication.

Lemma 36. *Given* $\vec{x} = (x_1, \ldots, x_n)^\top \in \mathbb{F}_2^n$:

$$\widetilde{F}(\vec{x}) = \vec{x}^\top \cdot E_{\widetilde{F}} \cdot \vec{x}.$$

Proof.
We have

$$\begin{aligned}
\vec{x}^\top \cdot E_{\widetilde{F}} \cdot \vec{x} &= (x_1, \ldots, x_n) \begin{pmatrix} 0 & 0 & \ldots & 0 \\ e_{2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ e_{n,1} & e_{n,2} & \ldots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\
&= \sum_{1 \le i < j \le n} e_{i,j} \cdot x_i \cdot x_j \\
&= \sum_{1 \le i < j \le n} \vec{a}_{\{i,j\}} \cdot x_i \cdot x_j \\
&= \sum_{\substack{I \in \mathcal{P}(N) \\ |I|=2}} \vec{a_I} \vec{x}^I \\
&= \widetilde{F}(x).
\end{aligned}$$

□

Definition 25. [1, p. 17] We define the derivative of $\widetilde{F}$ at $\vec{a} \in \mathbb{F}_2^n$ as

$$D_a \widetilde{F}(\vec{x}) = \widetilde{F}(\vec{x} + \vec{a}) + \widetilde{F}(\vec{x}).$$

Lemma 37. *If* $\vec{a} \in \mathbb{F}_2^n$, *then* $\forall \vec{x} \in \mathbb{F}_2^n$:

$$D_a \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{a}) = \vec{a}^\top \cdot C_{\widetilde{F}} \cdot \vec{x}.$$

Remark. It can be easily seen that Lemma (14) holds for the matrix $E_{\widetilde{F}}$ and vectors $\vec{u}, \vec{v} \in \mathbb{F}_2^n$ as well.

Proof.
From the definition of $D_a \widetilde{F}$:

$$\begin{aligned}
D_a \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{a}) &= \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{x} + \vec{a}) + \widetilde{F}(\vec{a}) \\
&= \vec{x}^\top E_{\widetilde{F}} \vec{x} + (\vec{x} + \vec{a})^\top E_{\widetilde{F}} (\vec{x} + \vec{a}) + \vec{a}^\top E_{\widetilde{F}} \vec{a} \\
&= \vec{a}^\top E_{\widetilde{F}} \vec{x} + \vec{x}^\top E_{\widetilde{F}} \vec{a}.
\end{aligned}$$

Using Lemma (14) we obtain:

$$\begin{aligned} D_a\widetilde{F}(\vec{x}) + \widetilde{F}(\vec{a}) &= \vec{a}^\top E_{\widetilde{F}}\vec{x} + \vec{a}^\top E_{\widetilde{F}}^\top \vec{x} \\ &= \vec{a}^\top C_{\widetilde{F}}\vec{x}. \end{aligned}$$

□

Definition 26. The mapping obtained in the lemma above will be denoted by:

$$\begin{aligned} L_{\vec{a}} : \mathbb{F}_2^n &\to \mathbb{F}_2^n, \\ \vec{x} &\mapsto \vec{a}^\top \cdot C_{\widetilde{F}} \cdot \vec{x}. \end{aligned}$$

Lemma 38. *$L_{\vec{a}}$ is a linear mapping between vector spaces.*

Proof.
Given a scalar $b \in \mathbb{F}_2$ we consider two cases:

- if $b = 0$, then $L_{\vec{a}}(b \cdot \vec{x}) = L_{\vec{a}}(\vec{0}) = \vec{0} = b \cdot L_{\vec{a}}(\vec{x})$,
- if $b = 1$, then clearly $L_{\vec{a}}(b \cdot \vec{x}) = L_{\vec{a}}(\vec{x}) = b \cdot L_{\vec{a}}(\vec{x})$.

We now turn to the linearity of addition. Let $\vec{x}, \vec{y} \in \mathbb{F}_2^n$, then:

$$L_{\vec{a}}(\vec{x} + \vec{y}) = \vec{a}^\top C_{\widetilde{F}}(\vec{x} + \vec{y}) = \vec{a}^\top C_{\widetilde{F}}\vec{x} + \vec{a}^\top C_{\widetilde{F}}\vec{y} = L_{\vec{a}}(\vec{x}) + L_{\vec{a}}(\vec{y}).$$

□

Definition 27. Given vectors $\vec{v}_1, \ldots, \vec{v}_m$ from $\mathbb{F}_2^n$ and matrix $A = (\vec{v}_1 | \cdots | \vec{v}_m) \in \mathbb{F}_2^{n \times m}$ we define

$$\mathrm{Rank}((\vec{v}_1, \ldots, \vec{v}_m)) = \mathrm{Rank}(A).$$

3.2 Correspondence between QAMs and ANFs

Definition 28. $J \in (\mathbb{F}_2^n)^{n \times n}$ is said to be a *QAM (quadratic homogenous APN matrix)* if all of the following holds:

- J is symmetric
- J has all diagonal elemenents equal to zero
- $\forall \vec{\lambda} \in \mathbb{F}_2^n \setminus \{\vec{0}\} : \ \mathrm{Rank}_{\mathbb{F}_2}(J \cdot \vec{\lambda}) = n - 1.$

Remark. The only difference from Definition (20) is that now the elements of the matrix are from $\mathbb{F}_2^n$.

Theorem 39. *A quadratic homogenous (n, n)-function (homogenous in terms of the ANF representation) $\widetilde{F}$ is APN if and only if $C_{\widetilde{F}}$ is QAM.*

Proof.
We prove this in the same way as Theorem (21). First, let $\widetilde{F}$ be APN. Since $\widetilde{F}$ is quadratic homogenous, $C_{\widetilde{F}} = E_{\widetilde{F}} + E_{\widetilde{F}}^{\top}$ has zero diagonal. Also, it is evident that $C_{\widetilde{F}}$ is symmetric. Therefore, we only need to prove that

$$\forall \vec{\lambda} \in \mathbb{F}_2^n \setminus \{\vec{0}\} : \ \mathrm{Rank}_{\mathbb{F}_2}(C_{\widetilde{F}} \cdot \vec{\lambda}) = n - 1.$$

Choose $\vec{a} \in \mathbb{F}_2^n \setminus \{\vec{0}\}$. A trivial verification shows that $\mathrm{Ker}(L_{\vec{a}}) = \{\vec{0}, \vec{a}\}$ and therefore $\dim_{\mathbb{F}_2}(\mathrm{Ker}(L_{\vec{a}})) = 1$.

- Since $\widetilde{F}(\vec{0}) = \vec{0}$, we get:

$$\begin{aligned} L_{\vec{a}}(\vec{a}) &= \widetilde{F}(\vec{a}) + \widetilde{F}(\vec{a}) + \widetilde{F}(\vec{0}) = \vec{0}, \\ L_{\vec{a}}(\vec{0}) &= \widetilde{F}(\vec{0}) + \widetilde{F}(\vec{a}) + \widetilde{F}(\vec{a}) = \vec{0}. \end{aligned}$$

- Since $\widetilde{F}$ is APN:

$$\begin{aligned} |\mathrm{Ker}(L_{\vec{a}})| &= |\{\vec{x} \in \mathbb{F}_2^n \mid \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{a}) + \widetilde{F}(\vec{x} + \vec{a}) = \vec{0}\}| \\ &= |\{\vec{x} \in \mathbb{F}_2^n \mid \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{x} + \vec{a}) = \widetilde{F}(\vec{a})\}| \\ &\leq 2. \end{aligned}$$

We have proved that $L_{\vec{a}}$ is linear, so we can use Theorem (20):

$$\mathrm{Rank}_{\mathbb{F}_2}(L_{\vec{a}}) = n - \dim_{\mathbb{F}_2}(\mathrm{Ker}(L_{\vec{a}})) = n - 1.$$

From the definition of $L_{\vec{a}}$ it is obvious that $\mathrm{Rank}_{\mathbb{F}_2}(C_{\widetilde{F}} \cdot \vec{a}) = \mathrm{Rank}_{\mathbb{F}_2}(L_{\vec{a}})$. Conversely, let $C_{\widetilde{F}}$ be QAM. In the same way as above obtain:

$$\mathrm{Ker}(L_{\vec{a}}) = n - \mathrm{Rank}_{\mathbb{F}_2}(L_{\vec{a}}) = n - \mathrm{Rank}_{\mathbb{F}_2}(C_{\widetilde{F}} \cdot \vec{a}) = n - (n-1) = 1.$$

Again it can be easily shown that $\{\vec{0}, \vec{a}\} \subseteq \mathrm{Ker}(L_{\vec{a}})$, thus $\mathrm{Ker}(L_{\vec{a}}) = \{\vec{0}, \vec{a}\}$. Now using the notation from Definition (10) we show that $\widetilde{F}$ is APN:

$$\begin{aligned} \max_{\substack{\vec{a},\vec{b} \in \mathbb{F}_2^n \\ \vec{a} \neq \vec{0}}} |A_{\vec{b},\vec{a}}^{\widetilde{F}}| &= \max_{\substack{\vec{a},\vec{b} \in \mathbb{F}_2^n \\ \vec{a} \neq \vec{0}}} |\{\vec{x} \in \mathbb{F}_2^n \mid \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{x} + \vec{a}) = \vec{b}\}| \\ &= \max_{\substack{\vec{a},\vec{b} \in \mathbb{F}_2^n \\ \vec{a} \neq \vec{0}}} |\{\vec{x} \in \mathbb{F}_2^n \mid \widetilde{F}(\vec{x}) + \widetilde{F}(\vec{x} + \vec{a}) + \widetilde{F}(\vec{a}) = \vec{b}\}| \\ &= \max_{\substack{\vec{a},\vec{b} \in \mathbb{F}_2^n \\ \vec{a} \neq \vec{0}}} |\{\vec{x} \in \mathbb{F}_2^n \mid L_{\vec{a}}(\vec{x}) = \vec{b}\}|. \end{aligned}$$

Choose $\vec{a} \in \mathbb{F}_2^n \setminus \{\vec{0}\}$. We only need to consider two cases.

- Suppose $\vec{b} \notin \mathrm{Im}(L_{\vec{a}})$. Then $|\{\vec{x} \in \mathbb{F}_2^n \mid L_{\vec{a}}(\vec{x}) = \vec{b}\}| = 0$.
- Suppose $\vec{b} \in \mathrm{Im}(L_{\vec{a}})$. Let $\vec{z} \in \mathbb{F}_2^n$ such that $\vec{b} = L_{\vec{a}}(\vec{z})$. It is obvious that

$$\{\vec{z}, \vec{z} + \vec{a}\} \subseteq \{\vec{x} \in \mathbb{F}_2^n \mid L_{\vec{a}}(\vec{x}) = \vec{b}\}.$$

Let $\vec{y} \in \mathbb{F}_2^n \setminus \{\vec{z}, \vec{z} + \vec{a}\}$ such that $L_{\vec{a}} = \vec{b}$. Clearly,

$$L_{\vec{a}}(\vec{z} + \vec{y}) = L_{\vec{a}}(\vec{z}) + L_{\vec{a}}(\vec{y}) = \vec{b} + \vec{b} = \vec{0}.$$

Which contradicts the choice of $\vec{y}$:

$$(\vec{y} + \vec{z}) \in \mathrm{Ker}(L_{\vec{a}}) = \{\vec{0}, \vec{a}\} \Rightarrow \vec{y} \in \{\vec{0} + \vec{z}, \vec{a} + \vec{z}\}.$$

Therefore, $|A^{\widetilde{F}}_{\vec{b},\vec{a}}| = 2$ for all $\vec{b} \in \mathrm{Im}(L_{\vec{a}})$.

□

4. Examples

In this chapter we will compute the corresponding matrices for chosen APN functions $F_1, F_2 : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ which are EA-inequivalent. We will show how the finite field approach corresponds to the ANF approach. The functions F_1, F_2 will be APN and EA-inequivalent.

4.1 Finite field approach

4.1.1 Trace and Bases

Before we give the examples we need to formulate some useful definitions and lemmas. Most of these statements can be found in [5, p. 54-63].

Definition 29. [5, p. 54] For $x \in \mathbb{F}_{2^n}$ the *trace* of x over $\mathbb{F}_2$ is defined by

$$\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}.$$

Lemma 40. *[5, p. 55] For all $x, y \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_2$:*

- $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$,
- $\mathrm{Tr}(c \cdot x) = c \cdot \mathrm{Tr}(x)$.

Definition 30. [5, p. 58] Let $B = (\gamma_1, \ldots, \gamma_n)$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. B is said to be a *self-dual* basis if for $1 \leq i, j \leq n$ we have

$$\mathrm{Tr}(\gamma_i \cdot \gamma_j) = \begin{cases} 0 & \text{for } i \neq j, \\ 1 & \text{for } i = j \ . \end{cases}$$

Definition 31. [5, p. 59] A basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ of the form $(\beta, \beta^2, \ldots, \beta^{2^{n-1}})$ is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Remark. Suppose $B = (\beta, \beta^2, \ldots, \beta^{2^{n-1}})$ is a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Because $\forall x \in \mathbb{F}_{2^n} : \ x^{2^n} = x$ (see [5, 48]), we can simplify the matrix M_B (see Definition (15)) as

$$M_B = \begin{pmatrix} \beta & \beta^2 & \cdots & \beta^{2^{m-1}} \\ \beta^2 & \beta^4 & \cdots & \beta \\ \vdots & \vdots & \cdots & \vdots \\ \beta^{2^{m-2}} & \beta^{2^{m-1}} & \cdots & \beta^{2^{m-3}} \\ \beta^{2^{m-1}} & \beta & \cdots & \beta^{2^{m-2}} \end{pmatrix}.$$

Theorem 41. *[5, p. 76] If n is odd, then there exists a self-dual normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.*

4.1.2 Basis choice

Definition 32. We will consider

$$\mathbb{F}_{2^5} \simeq {}^{\mathbb{F}_2[\alpha]}\!\diagup_{(\alpha^5+\alpha^2+1)}.$$

Firstly, let us choose a basis of $\mathbb{F}_{2^5}$ over $\mathbb{F}_2$ denoted by $B = (\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$. It will be useful to choose a self-dual normal basis (the existence is guaranteed by Theorem (41)). The normality will imply that $(\alpha_i)^2 = \alpha_{i+1}$ for all $i \in \{0, \ldots, 4\}$ which will be used in several proofs. On the other hand, the self-duality will be helpful in the proof of Lemma (43). Since $\mathbb{F}_{2^5}$ is rather small, we can find the basis by searching through all of the possible options. We tried the following algorithm for all $\beta \in \mathbb{F}_{2^5}$ and found a self-dual normal basis

$$\begin{aligned} B &= (\alpha_0,\ \alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4) \\ &= (\beta,\ \beta^2,\ \beta^4,\ \beta^8,\ \beta^{16}) \\ &= (\alpha+1,\ \alpha^2+1,\ \alpha^4+1,\ \alpha^3+\alpha^2,\ \alpha^4+\alpha^3+\alpha) \end{aligned}$$

generated by $\beta = \alpha + 1$.

Algorithm 1: Search for a self-dual normal basis

```
Input: β ∈ F_{2^5}
Output: self-dual/not self-dual
for i = 0, ..., 4 do
    if Tr(β^{2^i} · β^{2^i}) ≠ 1 then
        return not self-dual
    else
        for j = i + 1, ..., 4 do
            if Tr(β^{2^i} · β^{2^j}) ≠ 0 then
                return not self-dual
return self-dual
```

Remark. If we find a sequence having these properties it has to be a basis (see e.g. [5, p. 61]). This explains why we could run the algorithm for all $\beta \in \mathbb{F}_{2^5}$.

Remark. We abbreviate M_B to M.

$$M = \begin{pmatrix} \beta & \beta^2 & \beta^4 & \beta^8 & \beta^{16} \\ \beta^2 & \beta^4 & \beta^8 & \beta^{16} & \beta \\ \beta^4 & \beta^8 & \beta^{16} & \beta & \beta^2 \\ \beta^8 & \beta^{16} & \beta & \beta^2 & \beta^8 \\ \beta^{16} & \beta & \beta^2 & \beta^8 & \beta^{16} \end{pmatrix}$$

4.1.3 Function F_1

Let us define $F_1 : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ such that $F_1(x) = x^3 = x \cdot x^2$. This function is proved to be APN (it is a Gold function - see [2, p. 50]). It is clear that F_1 is also quadratic homogenous. Therefore, we can use the approach from Chapter (2) and construct the corresponding matrix $H_{F_1,B}$.

We first need to construct E_{F_1}. From the definition of F_1 it is clear that

$$E_{F_1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Remark. We will abbreviate $H_{F_1,B}$ to H_{F_1}.

To construct H_{F_1} we will compute the element

$$(H_{F_1})_{i,j} = (M^\top E_{F_1} M)_{i,j} + (M^\top (E_{F_1})^\top M)_{i,j} = (M^\top E_{F_1} M)_{i,j} + (M^\top E_{F_1} M)_{j,i} \ .$$

Because $\forall (i,j) \neq (2,1) : \ (E_{F_1})_{i,j} = 0$, we can simplify the expression as follows:

$$\begin{aligned} (M^\top E_{F_1} M)_{i,j} &= \sum_{k=1}^{5} M^\top_{i,k} \sum_{l=1}^{5} (E_{F_1})_{k,l} M_{l,j} \\ &= M^\top_{i,2} \cdot M_{1,j} \\ &= (\beta^2)^{2^{i-1}} \cdot (\beta^{2^{j-1}})^{2^0} \\ &= \beta^{2^i} \cdot \beta^{2^{j-1}} \\ &= \beta^{2^i + 2^{j-1}}, \\ (H_{F_1})_{i,j} &= \beta^{2^i + 2^{j-1}} + \beta^{2^j + 2^{i-1}}. \end{aligned}$$

Finally, we can see that

$$H_{F_1} = \begin{pmatrix} 0 & \alpha^2{+}\alpha{+}1 & \alpha^3{+}\alpha{+}1 & \alpha^4{+}\alpha & \alpha^4{+}\alpha^3 \\ \alpha^2{+}\alpha{+}1 & 0 & \alpha^4{+}\alpha^2{+}1 & \alpha^3{+}\alpha^2{+}\alpha{+}1 & \alpha^3{+}1 \\ \alpha^3{+}\alpha{+}1 & \alpha^4{+}\alpha^2{+}1 & 0 & \alpha^4{+}\alpha^3{+}\alpha^2 & \alpha^4{+}\alpha^3{+}\alpha^2{+}\alpha{+}1 \\ \alpha^4{+}\alpha & \alpha^3{+}\alpha^2{+}\alpha{+}1 & \alpha^4{+}\alpha^3{+}\alpha^2 & 0 & \alpha^4{+}\alpha^2{+}\alpha{+}1 \\ \alpha^4{+}\alpha^3 & \alpha^3{+}1 & \alpha^4{+}\alpha^3{+}\alpha^2{+}\alpha{+}1 & \alpha^4{+}\alpha^2{+}\alpha{+}1 & 0 \end{pmatrix}.$$

4.1.4 Function F_2

We define the second function as

$$\begin{aligned} F_2 : \mathbb{F}_{2^5} &\to \mathbb{F}_{2^5}, \\ x &\mapsto x^3 + \mathrm{Tr}(x^9). \end{aligned}$$

According to [7, Corollary 1] this function is APN. For $n \geq 7$ it has been proven to be EA-inequivalent to $x \mapsto x^3$ (see [7, Corollary 3]). However, we decided to set $n = 5$ and have checked that F_1, F_2 are EA-inequivalent too. Expanding the trace function yields

$$F_2(x) = x^3 + x^9 + x^{18} + x^5 + x^{10} + x^{20}.$$

All of the exponents have Hamming weight equal to 2. Therefore, F_2 is quadratic homogenous. Note that also $\mathrm{Tr}(x^9)$ itself is quadratic homogenous. Therefore, for both of these functions a unique corresponding matrix with respect to B can be constructed.

Remark. For the simplicity of notation we will denote $\mathrm{Tr}(x)$ by F_T. Hence, we obtain for all $x \in \mathbb{F}_{2^n}$: $F_2(x) = F_1(x) + F_T(x)$. We will again denote matrices $H_{F_2,B}$ and $H_{F_T,B}$ by H_{F_2} and H_{F_T}, respectively. It can be easily seen that

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

We first compute $(H_{F_T})_{i,j}$ and then use Lemma (13) to obtain H_{F_2}. We will again make use of the fact that $\forall (i,j) \notin \{(3,1),(4,1),(4,2),(5,2),(5,3)\}$: $(E_{F_T})_{i,j} = 0$. We have

$$\begin{aligned}
(H_{F_T})_{i,j} &= (M^\top E_{F_T} M)_{i,j} + (M^\top E_{F_T} M)_{j,i}, \\
(M^\top E_{F_T} M)_{i,j} &= \sum_{k=1}^{5} M^\top_{i,k} \sum_{l=1}^{5} (E_{F_T})_{k,l} M_{l,j} \\
&= M^\top_{i,3} M_{1,j} + M^\top_{i,4} M_{1,j} + M^\top_{i,4} M_{2,j} + M^\top_{i,5} M_{2,j} + M^\top_{i,5} M_{3,j} \\
&= \beta^{2^{i+1}} \beta^{2^{j-1}} + \beta^{2^{i+2}} \beta^{2^{j-1}} + \beta^{2^{i+2}} \beta^{2^j} + \beta^{2^{i+3}} \beta^{2^j} + \beta^{2^{i+3}} \beta^{2^{j+1}} \\
&= \beta^{2^{i+1}+2^{j-1}} + \beta^{2^{i+2}+2^{j-1}} + \beta^{2^{i+2}+2^j} + \beta^{2^{i+3}+2^j} + \beta^{2^{i+3}+2^{j+1}}.
\end{aligned}$$

The obtained expression yields:

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

Now we can easily compute H_{F_2} from H_{F_1} and H_{F_T}:

$$\begin{aligned}
H_{F_2} &= H_{F_1} + H_{F_T} \\
&= \begin{pmatrix} 0 & \alpha^2+\alpha+1 & \alpha^3+\alpha & \alpha^4+\alpha+1 & \alpha^4+\alpha^3 \\ \alpha^2+\alpha+1 & 0 & \alpha^4+\alpha^2+1 & \alpha^3+\alpha^2+\alpha & \alpha^3 \\ \alpha^3+\alpha & \alpha^4+\alpha^2+1 & 0 & \alpha^4+\alpha^3+\alpha^2 & \alpha^4+\alpha^3+\alpha^2+\alpha \\ \alpha^4+\alpha+1 & \alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^3+\alpha^2 & 0 & \alpha^4+\alpha^2+\alpha+1 \\ \alpha^4+\alpha^3 & \alpha^3 & \alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^4+\alpha^2+\alpha+1 & 0 \end{pmatrix}.
\end{aligned}$$

4.2 ANF approach

4.2.1 ANF computation

To find the ANF representation of F_1, F_2, F_T we could first compute the truth tables and then apply a simple divide-and-conquer algorithm to compute the ANF (see [4, p. 10]). However, we will take an advantage of the self-dual normal basis and find the ANF straight from the finite field representation. We will denote the ANF of F_1, F_2, F_T by $\widetilde{F_1}, \widetilde{F_2}, \widetilde{F_T}$, respectively.

Remark. Given a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we compute $\widetilde{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by representing the elements of $\mathbb{F}_{2^n}$ with respect to a basis over $\mathbb{F}_2$. We continue to use the self-dual normal basis B from previous section.

Lemma 42. *The ANF of F_1 is equal to*

$$\begin{aligned}\widetilde{F_1}(x_0,x_1,x_2,x_3,x_4) = {} & x_0\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix} + x_1\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix} + x_2\begin{pmatrix}1\\0\\1\\0\\0\end{pmatrix} + x_3\begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix} + x_4\begin{pmatrix}0\\0\\1\\0\\1\end{pmatrix} + x_0x_1\begin{pmatrix}0\\0\\1\\1\\1\end{pmatrix} \\ & + x_0x_2\begin{pmatrix}0\\0\\1\\0\\1\end{pmatrix} + x_0x_3\begin{pmatrix}1\\0\\1\\0\\0\end{pmatrix} + x_0x_4\begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix} + x_1x_2\begin{pmatrix}1\\0\\0\\1\\1\end{pmatrix} + x_1x_3\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix} \\ & + x_1x_4\begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix} + x_2x_3\begin{pmatrix}1\\1\\0\\0\\1\end{pmatrix} + x_2x_4\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix} + x_3x_4\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}.\end{aligned}$$

Proof.
Let $[x]_B = (x_0, x_1, x_2, x_3, x_4)$ for given $x \in \mathbb{F}_{2^5}$. From the definition of F_1 :

$$F_1(x) = x^3 = x^2 \cdot x.$$

Let us first compute

$$\begin{aligned}x^2 &= (x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 + x_4\alpha_4)^2 \\ &= x_0\alpha_1 + x_1\alpha_2 + x_2\alpha_3 + x_3\alpha_4 + x_4\alpha_0.\end{aligned}$$

The last equality holds due to the normality of the basis. Now it is obvious that

$$\begin{aligned}x^2 \cdot x &= (x_0\alpha_1 + x_1\alpha_2 + x_2\alpha_3 + x_3\alpha_4 + x_4\alpha_0) \\ &\quad \cdot (x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 + x_4\alpha_4) \\ &= \sum_{i=0}^{4}\sum_{j=0}^{4} x_{(i-1 \bmod 5)}x_j\alpha_i\alpha_j \\ &= \sum_{i=0}^{4} x_{(i-1 \bmod 5)}x_i\alpha_{(i+1 \bmod 5)} + \sum_{i=0}^{4}\sum_{\substack{j=0\\ j\neq i}}^{4} x_{(i-1 \bmod 5)}x_j\alpha_i\alpha_j.\end{aligned}$$

We now only need to find the $[\alpha_u\alpha_v]_B$ for all $u, v \in \{0, \ldots, 4\}$. We did that by brute force and found the following.

$\alpha_u\alpha_v$	$[\alpha_u\alpha_v]_B^\top$
$\alpha_0\alpha_1$	$(1,0,0,1,0)$
$\alpha_0\alpha_2$	$(0,0,0,1,0)$
$\alpha_0\alpha_3$	$(0,1,1,0,0)$
$\alpha_0\alpha_4$	$(0,0,1,0,1)$
$\alpha_1\alpha_2$	$(0,1,0,0,1)$
$\alpha_1\alpha_3$	$(1,0,0,0,1)$
$\alpha_1\alpha_4$	$(0,0,1,1,0)$
$\alpha_2\alpha_3$	$(1,0,1,0,0)$
$\alpha_2\alpha_4$	$(1,1,0,0,0)$
$\alpha_3\alpha_4$	$(0,1,0,1,0)$

Using the representations from the table we obtain the algebraic normal formal written in this Lemma.

□

Lemma 43. *Let* $[x]_B = (x_0, x_1, x_2, x_3, x_4)$. *Then*

$$\widetilde{F_T}(x_0,x_1,x_2,x_3,x_4) = x_0x_2\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix} + x_0x_3\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix} + x_1x_3\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix} + x_1x_4\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix} + x_2x_4\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix}.$$

Proof.
We will first compute the ANF of $x^9 = x^8 \cdot x$ the same way as we did for x^3:

$$\begin{aligned} x^8 &= (x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 + x_4\alpha_4)^8 \\ &= x_0\alpha_3 + x_1\alpha_4 + x_2\alpha_0 + x_3\alpha_1 + x_4\alpha_2. \end{aligned}$$

Now we see that

$$\begin{aligned} x^8 \cdot x &= (x_0\alpha_3 + x_1\alpha_4 + x_2\alpha_0 + x_3\alpha_1 + x_4\alpha_2) \\ &\quad \cdot (x_0\alpha_0 + x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 + x_4\alpha_4) \\ &= \sum_{i=0}^{4}\sum_{j=0}^{4} x_{(i-3 \bmod 5)}x_j\alpha_i\alpha_j \\ &= \sum_{i=0}^{4} x_{(i-3 \bmod 5)}x_i\alpha_i^2 + \sum_{i=0}^{4}\sum_{\substack{j=0\\ j\neq i}}^{4} x_{(i-3 \bmod 5)}x_j\alpha_i\alpha_j. \end{aligned}$$

Due to the self-duality of B and the linearity of trace (see Lemma (40)) we obtain

$$\begin{aligned} F_T(x) = \mathrm{Tr}(x^9) &= \sum_{i=0}^{4} x_{(i-3 \bmod 5)}x_i\mathrm{Tr}(\alpha_i^2) + \sum_{i=0}^{4}\sum_{\substack{j=0\\ j\neq i}}^{4} x_{(i-3 \bmod 5)}x_j\mathrm{Tr}(\alpha_i\alpha_j) \\ &= \sum_{i=0}^{4} x_{(i-3 \bmod 5)}x_i \cdot 1 \\ &= x_0x_2 + x_1x_3 + x_2x_4 + x_3x_0 + x_4x_1. \end{aligned}$$

Finally, $[1]_B = (1,1,1,1,1)^\top$ yields the expression stated in this lemma.

□

Corollary 44. *Now we can use $\widetilde{F_1}, \widetilde{F_T}$ to compute*

$$\begin{aligned}\widetilde{F_2}(x_0,x_1,x_2,x_3,x_4) = x_0\begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix} + x_1\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix} + x_2\begin{pmatrix}1\\0\\1\\0\\0\end{pmatrix} + x_3\begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix} + x_4\begin{pmatrix}0\\0\\1\\0\\1\end{pmatrix} + x_0x_1\begin{pmatrix}0\\0\\1\\1\\1\end{pmatrix}\\ + x_0x_2\begin{pmatrix}1\\1\\0\\1\\0\end{pmatrix} + x_0x_3\begin{pmatrix}0\\1\\0\\1\\1\end{pmatrix} + x_0x_4\begin{pmatrix}0\\1\\1\\1\\0\end{pmatrix} + x_1x_2\begin{pmatrix}1\\0\\0\\1\\1\end{pmatrix} + x_1x_3\begin{pmatrix}0\\1\\1\\0\\1\end{pmatrix}\\ + x_1x_4\begin{pmatrix}1\\0\\1\\0\\1\end{pmatrix} + x_2x_3\begin{pmatrix}1\\1\\0\\0\\1\end{pmatrix} + x_2x_4\begin{pmatrix}1\\0\\1\\1\\0\end{pmatrix} + x_3x_4\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}.\end{aligned}$$

Remark. Although F_1, F_2 are quadratic homogenous, $\widetilde{F_1}, \widetilde{F_2}$ are quadratic with linear terms. Let us denote by $\widetilde{G_1}, \widetilde{G_2}$ the functions obtained from $\widetilde{F_1}, \widetilde{F_2}$ by deleting the linear terms. According to Lemma (7) functions $\widetilde{G_1}, \widetilde{G_2}$ are APN too.

4.2.2 Corresponding matrices for $\widetilde{G_1}, \widetilde{G_2}$

Now we can use $\widetilde{G_1}$ to construct the matrix $C_{\widetilde{G_1}}$:

$$C_{\widetilde{G_1}} = \begin{pmatrix} \vec{0}^\top & (0,0,1,1,1)^\top & (0,0,1,0,1)^\top & (1,0,1,0,0)^\top & (0,1,1,1,0)^\top \\ (0,0,1,1,1)^\top & \vec{0}^\top & (1,0,0,1,1)^\top & (1,0,0,1,0)^\top & (0,1,0,1,0)^\top \\ (0,0,1,0,1)^\top & (1,0,0,1,1)^\top & \vec{0}^\top & (1,1,0,0,1)^\top & (0,1,0,0,1)^\top \\ (1,0,1,0,0)^\top & (1,0,0,1,0)^\top & (1,1,0,0,1)^\top & \vec{0}^\top & (1,1,1,0,0)^\top \\ (0,1,1,1,0)^\top & (0,1,0,1,0)^\top & (0,1,0,0,1)^\top & (1,1,1,0,0)^\top & \vec{0}^\top \end{pmatrix}.$$

Similarly, we construct $C_{\widetilde{G_2}}$ from $\widetilde{G_2}$:

$$C_{\widetilde{G_2}} = \begin{pmatrix} \vec{0}^\top & (0,0,1,1,1)^\top & (1,1,0,1,0)^\top & (0,1,0,1,1)^\top & (0,1,1,1,0)^\top \\ (0,0,1,1,1)^\top & \vec{0}^\top & (1,0,0,1,1)^\top & (0,1,1,0,1)^\top & (1,0,1,0,1)^\top \\ (1,1,0,1,0)^\top & (1,0,0,1,1)^\top & \vec{0}^\top & (1,1,0,0,1)^\top & (1,0,1,1,0)^\top \\ (0,1,0,1,1)^\top & (0,1,1,0,1)^\top & (1,1,0,0,1)^\top & \vec{0}^\top & (1,1,1,0,0)^\top \\ (0,1,1,1,0)^\top & (1,0,1,0,1)^\top & (1,0,1,1,0)^\top & (1,1,1,0,0)^\top & \vec{0}^\top \end{pmatrix}.$$

It can be easily verified that

$$\left[\left(H_{\widetilde{F_1}}\right)_{i,j}\right]_B = \left(C_{\widetilde{G_1}}\right)_{i,j} \quad \text{and} \quad \left[\left(H_{\widetilde{F_2}}\right)_{i,j}\right]_B = \left(C_{\widetilde{G_2}}\right)_{i,j}$$

for all $i, j \in \{1, \ldots, 5\}$. Therefore, the matrices H_{F_1}, H_{F_2} could have been obtained straightly from the ANF representation of F_1, F_2.

Conclusion

In this thesis we explained in detail the method introduced in [2]. We added extra statements and proofs when we thought it was needed.

We showed how to construct QAMs from the ANF representation. Furthermore, we proved that there is a one to one correspondence between quadratic homogenous APN functions and QAMs obtained from the ANF representation.

Computing the examples in Chapter 4, we showed that QAMs from [2] are in fact very similar to the ANF representation. In future work it would be interesting to describe how preserving APNness and EA-equivalence is connected to matrix operations.

Bibliography

[1] C. Carlet. *Vectorial Boolean Functions for Cryptography*, page 398–469. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010. The page numbers refer to the version found at `https://www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf`.

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

[3] L. E. Knop. *Linear Algebra: A First Course with Applications*. Textbooks in Mathematics. CRC Press, 2009.

[4] C. Carlet. *Boolean Functions for Cryptography and Error-Correcting Codes*, page 257–397. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010. The page numbers refer to the version found at `https://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf`.

[5] R. Lidl and H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1997.

[6] Y. Katznelson and Y. R. Katznelson. *A (Terse) Introduction to Linear Algebra*. Student mathematical library. American Mathematical Society, 2008.

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