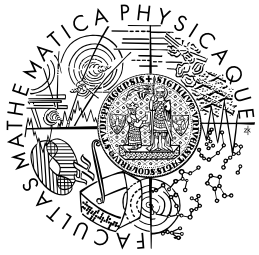

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Dáša Krasnayová

Constructions of APN permutations

Department of Algebra

Supervisor of the master thesis:	Dr. rer. nat. Faruk Göloğlu
Study programme:	Mathematics
Study branch:	Mathematical Methods of Information Security

Prague 2016

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

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 .....

Název práce: Kosntrukce APN permutací

Autor: Dáša Krasnayová

Katedra: Katedra algebry

Vedoucí diplomové práce: Dr. rer. nat. Faruk Göloğlu, Katedra algebry

Abstrakt: V této práci zkoumáme rodinu vektorových boolovských funkcí na $\mathbb{F}_{2^{2m}}$, která je inspirována Kimovou funkcí, s cílem najít nové APN permutace na $\mathbb{F}_{2^{2m}}$ pro $m > 2$. Funkce této rodiny jsou definované jako $F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2}$, kde parametry b, c a d jsou z $\mathbb{F}_{2^m}$. V této práci jsou prezentovány nutné a postačující podmínky, které zaručují, že tyto funkce jsou APN nebo ekvivalentní permutaci. K nalezení podmínek na APN byla použita metoda využívající Trace-0/Trace-1 rozklad. Metoda využívající exponenciální sumy byla použita k odvození podmínek, za kterých je funkce z této rodiny ekvivalentní permutaci určitého typu. Získané podmínky pak byly použity k hledání APN permutací v tělesech $\mathbb{F}_{2^6}$ a $\mathbb{F}_{2^{10}}$.

Klíčová slova: vektorové boolovské funkce, CCZ ekvivalence, APN permutace

Title: Constructions of APN permutations

Author: Dáša Krasnayová

Department: Department of Algebra

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

Abstract: In this thesis, we examine a family of vectorial boolean functions on $\mathbb{F}_{2^{2m}}$ inspired by Kim function, in order to find new APN permutations on $\mathbb{F}_{2^{2m}}$ for $m > 2$. The functions of this family are defined as $F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2}$, where parameters b, c and d are from $\mathbb{F}_{2^m}$. Necessary and sufficient conditions for this functions to be APN or equivalent to a permutation are presented in this thesis. To find conditions for being APN, Trace-0/Trace-1 decomposition method is used. A method using exponential sums is used to deduce which functions of this family is CCZ-equivalent to a certain type of permutation. These results were then used to search for APN permutations on $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^{10}}$.

Keywords: vectorial boolean functions, CCZ equivalence, APN permutations

I would like to thank my supervisor Dr. rer. nat. Faruk Gölogˇlu for consultations and many useful comments.

Contents

Introduction

Existence of APN permutations in even dimension has been an interesting problem for many years now. It was long believed that there are no such functions in even dimension. In odd case, on the other hand, there are many APN permutations known - for example *Gold functions* on $\mathbb{F}^{2^n}$

$$f(x) = x^{2k+1},$$

where $\gcd(n, k) = 1$ are all APN permutations if n is odd. In even dimension they are still APN, but they are not permutations.

In [1] Dillon formulated

The Big APN Problem. Does there exist an APN permutation on $\mathbb{F}_2^n$ if n is even?

This problem was resolved for $n \leq 4$ for example in [2] and there are no such functions in those dimensions. However, in 2009 the first example of an APN permutation in dimension six was presented in [3]. The function is known as *Kim function* or κ *function* and is defined as

$$\kappa(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $x^6 + x^4 + x^3 + x + 1$. $\kappa(x)$ was proven to be APN using code theory. The function also has some several interesting properties, such as

$$\kappa(\lambda z) = \lambda^3 \kappa(z),$$

for every $\lambda \in \mathbb{F}_{2^3}$, which is often referred to as the *subspace property.*

In [3], authors express hope that

> '... much of the structure, if not all, should generalize to higher dimensions,'

and update the Big APN Problem:

The Big APN Problem. Does there exist an APN permutation on $\mathbb{F}_2^n$ if n is even and greater than six?

Therefore, it seems to be a good idea to try to mimic behaviour of the Kim function in order to find a new APN permutation in even dimension. In [4], a new infinite family of APN functions of the form

$$f_k(x) = x^{2^k+1} + (\mathrm{tr}_m^n(x))^{2^k+1},$$

is introduced, where $n = 2m$, m is even and $\gcd(n, k) = 1$. Other then monomials, this is the first family of functions satisfying the subspace property. Unfortunately, these functions are not equivalent to a permutation. In this thesis we study functions on $\mathbb{F}_{q^2}$ of the form

$$F(x) = x^3 + bx^{3q} + cx^{2q+1} + bx^{q+2},$$

where $q = 2^m$ and $b, c, d \in \mathbb{F}_q$. Functions of this form satisfy the subspace property and Kim function is equivalent to a member of this family.

In Chapter 1, basic definitions and theorems about boolean and APN functions are introduced, as well as basic types of equivalence of boolean functions.

More specific lemmas and definitions necessary for our work can be found in Chapter 2.

The main contribution of this thesis is in chapters 3 and 4. In Chapter 3, we present conditions for parameters b, c, d under which the function F is APN. To find these conditions, a method using *Trace-0/Trace-1* decomposition introduced in the second chapter is used. Conditions for F to be equivalent to a permutation are in Chapter 4. In Conclusion, these results are used to find APN permutations from our family of functions in $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^{10}}$.

1. Basic theory

In this chapter, basic theory about APN functions will be presented, including an introduction to boolean functions, definition and some of the features of APN functions and two most commonly used equivalences of boolean functions that preserve property of being APN.

1.1 Boolean functions

Definition 1.1 (Boolean function)**.** *A* boolean function *is a function from* $\mathbb{F}_2^n$ *to* $\mathbb{F}_2$ *for some non-negative integer* n*. A function from* $\mathbb{F}_2^n$ *to* $\mathbb{F}_2^m$*, where* $n \geq m \geq 1$*,* n, m *non-negative integers, is called a* vectorial boolean function*.*

Every boolean function can be uniquely written as

$$f(\boldsymbol{x}) = f(x_1, x_2, \ldots, x_n) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} a_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}},$$

where $a_{\boldsymbol{u}} \in \mathbb{F}_2$ and $\boldsymbol{x}^{\boldsymbol{u}} = \prod_{i=1}^n x_i^{u_i}$. This way of writing a function is called the *algebraic normal form (ANF)* of f. We can see that every function of this form is a boolean function. Let f be a boolean function given by a table. We can write this function in ANF using atomic functions $\delta_{\boldsymbol{x}}$, where $x \in \mathbb{F}_2^n$ and

$$\delta_{\boldsymbol{x}}(\boldsymbol{y}) = \prod_{i=1}^{n} (x_i + y_i + 1).$$

As we can see, $\delta_{\boldsymbol{x}}(\boldsymbol{y}) = 1$ if and only if $\boldsymbol{x} = \boldsymbol{y}$. Function f can be then written as

$$\sum_{\boldsymbol{x} \in \mathbb{F}_2^n} = f(\boldsymbol{x}) \delta_{\boldsymbol{x}}.$$

Moreover we can notice that number of ANFs is the same as the number of all boolean functions on n variables (2^{2^n}).

Example. Let f be a function given by table:

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

In this case

$$\begin{aligned} f(x_1, x_2) &= 0(0 + x_1 + 1)(0 + x_2 + 1) + 1(0 + x_1 + 1)(1 + x_2 + 1) \\ &\quad + 1(1 + x_1 + 1)(0 + x_2 + 1) + 0(1 + x_1 + 1)(1 + x_2 + 1) \\ &= (x_1 + 1)x_2 + x_1(x_2 + 1) = x_1x_2 + x_2 + x_1x_2 + x_1 = x_1 + x_2. \end{aligned}$$

Definition 1.2 (Degree of a function)**.** *A* degree of a function $f = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} a_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}}$ *is a number*

$$deg(f) = \max\{w_H(\boldsymbol{u}) : a_{\boldsymbol{u}} \neq 0\},$$

where $w_H(\boldsymbol{u})$ *is a weight of a vector* $\boldsymbol{u}$*, i.e. number of nonzero* u_i*s.*

Algebraic normal form of a vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is

$$F(x_1, x_2, \ldots, x_n) = \sum_{\boldsymbol{u} \in \mathbb{F}_2^n} a_{\boldsymbol{u}} \boldsymbol{x}^{\boldsymbol{u}},$$

where $a_{\boldsymbol{u}} \in \mathbb{F}_2^m$.

This notation of (vectorial) boolean functions is called a *multivariate notation*. Another way of thinking this functions is considering $\mathbb{F}_{2^n}$ instead of $\mathbb{F}_2^n$. $\mathbb{F}_{2^n}$ is a field and also a vector space over $\mathbb{F}_2$. If we choose a basis β of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $\beta = \{\beta_1, \ldots, \beta_n\}$, then $\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_2^n$ such that $\varphi(\beta_i) = \boldsymbol{e}_i$, where $\boldsymbol{e}_i$ is a vector with one in its i-th component and zeroes elsewhere; is an isomorphism of vector spaces. As we can see, this isomorphism in not unique and depends on the choice of the basis β.

This notation is called a *univariate notation* and will be used from now on. In this notation, vectorial boolean functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ correspond to polynomials in $\mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$ ($\alpha^{2^n} = \alpha$ for every $\alpha \in \mathbb{F}_{2^n}$). We can see that every polynomial is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and number of the functions is the same as the number of the polynomials.

We will use atomic functions for writing a vectorial boolean function as a polynomial as well. This time it will be functions δ_α of the form

$$\delta_\alpha(x) = (1 - (x - \alpha)^{2^n - 1}),$$

which is 1 if $x = \alpha$ and 0 otherwise. Function F then can be written as

$$F(x) = \sum_{\alpha \in \mathbb{F}_{2^n}} F(\alpha)\delta_\alpha(x),$$

for every $x \in \mathbb{F}_{2^n}$.

In this notation the *degree of a function* $F(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i$, $\alpha_i \in \mathbb{F}_{2^n}$ is defined as $\max\{w_H(i) : \alpha_i \neq 0\}$, where $w_H(i)$ is a Hamming weight of i, which is the number of ones in the binary representation of i.

Lemma 1.1. *The degree of a function is well defined. (Definition in univariate notation corresponds to the Definition 1.2.)*

Proof. Let $\beta = \{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $F = \sum_{i=0}^{2^n-1} \alpha_i x^i$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. We can express $x = \sum_{j=1}^{n} \beta_j x_j$, where $x_j \in \mathbb{F}_2$ and $i = \sum_{s=0}^{n-1} i_s 2^s$, where $i_s \in \mathbb{F}_2$. Then

$$\begin{aligned} F &= \sum_{i=0}^{2^n-1} \alpha_i \left(\sum_{j=1}^{n} \beta_j x_j \right)^i = \sum_{i=0}^{2^n-1} \alpha_i \left(\sum_{j=1}^{n} \beta_j x_j \right)^{\sum_{s=0}^{n-1} i_s 2^s} \\ &= \sum_{i=0}^{2^n-1} \alpha_i \prod_{s=0}^{n-1} \left(\sum_{j=1}^{n} \beta_j^{2^s} x_j \right)^{i_s}. \end{aligned}$$

If we expand the product and use the isomorphism φ, we get the ANF of corresponding function F in multivariate notation. Since

$$\deg\left(\prod_{s=0}^{n-1}\left(\sum_{j=1}^{n}\beta_j^{2^s}x_j\right)^{i_s}\right)=\sum_{s=0}^{n-1}i_s=w_H(i),$$

the degree of F is $\max\{w_H(i):\alpha_i\neq 0\}$ in both notations.

□

Definition 1.3 (Trace)**.** *The* trace tr_m^n *for some* $n\geq m, m|n$ *is a boolean function from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^m}$ *such that*

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

Remark (Basic properties of trace). Trace is a linear function, i.e.

$$\mathrm{tr}_m^n(ax+by)=a\,\mathrm{tr}_m^n(x)+b\,\mathrm{tr}_m^n(y)$$

for every $a,b\in\mathbb{F}_{2^m}$ and $x,y\in\mathbb{F}_{2^n}$. For every integers m,n,ℓ such that $m,\ell|n$ and $m|\ell$,

$$\mathrm{tr}_m^n(x)=\mathrm{tr}_m^\ell(\mathrm{tr}_\ell^n(x))$$

for every $x\in\mathbb{F}_{2^n}$.

Moreover,

$$\begin{aligned}tr_1^n(x^2)&=\sum_{i=0}^{n-1}(x^2)^{2^i}=\sum_{i=0}^{n-1}(x)^{2^{i+1}}=\sum_{i=1}^{n-1}(x)^{2^i}+x^{2^n}=\sum_{i=1}^{n-1}(x)^{2^i}+x^{2^0}\\&=\sum_{i=0}^{n-1}(x)^{2^i}=\mathrm{tr}_1^n(x),\end{aligned}$$

for every $x\in\mathbb{F}_{2^n}$.

Definition 1.4 (Linearized polynomial)**.** *A polynomial* $f\in\mathbb{F}_{2^n}$ *is called a* linearized polynomial *if*

$$f(x)=\sum_{i=0}^{n-1}a_ix^{2^i},$$

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

Remark. We can see that every linear vectorial boolean function is represented by a linearized polynomial. Only in this case there is $f(x+y)=f(x)+f(y)$ for every $x,y\in\mathbb{F}_{2^n}$, since $(x+y)^{2^i}=x^{2^i}+y^{2^i}$.

Lemma 1.2. *Let* F *be a linear function. Then* F *is a* k *to* 1 *function if and only if the dimension of* $\ker(F)$ *is* k.

Proof. We can see this immediately from the structure of the solutions of a linear equation. □

We will be interested in the vectorial boolean functions where $m=n$ in particular. From now on, we will write $\mathbb{F}$ instead of $\mathbb{F}_{2^n}$ and assume that F is a function from $\mathbb{F}$ to $\mathbb{F}$.

Definition 1.5 (Walsh transform)**.** *The* Walsh transform *of a function F is a function $\hat{F} : \mathbb{F} \times \mathbb{F} \to \{1, -1\}$ such that*

$$\hat{F}(a, b) = \sum_{x \in \mathbb{F}} \chi(aF(x) + bx),$$

where $\chi(y) = (-1)^{\mathrm{tr}_1^n(y)}$ for every $y \in \mathbb{F}$.

Remark. We can see that χ is a character and therefore for every subspace V of $\mathbb{F}$, we have

$$\sum_{x \in V} \chi(ax) = \begin{cases} |V|, & \text{if } a \in V^+, \\ 0, & \text{otherwise,} \end{cases}$$

where $V^+ = \{a \in F | \, \mathrm{tr}_1^n(ax) = 0 \text{ for every } x \in V\}$ and $a \in \mathbb{F}$.

1.2 Almost perfect nonlinear functions

Definition 1.6 (Almost Perfect Nonlinear function)**.** *A function F is called* Almost Perfect Nonlinear (APN) *if*

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

has two or zero solutions $x \in \mathbb{F}$ for every $a, b \in \mathbb{F}$, $a \neq 0$.

Remark. For a perfect nonlinear function,

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

would have exactly one solution for every pair a, b, $a \neq 0$. However, this is not possible in fields with characteristic two because if x is a solution, then $x + a$ is a solution as well:

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

This concept can be defined more generally. We say that function F is *differentially δ-uniform* if and only if for every non-zero $a \in \mathbb{F}$ and $b \in \mathbb{F}$ there are at most δ solutions of equation $F(x + a) + F(x) = b$. The smaller δ is, the more resistant F is to differential cryptanalysis. As we have shown above, the best δ in our case is 2 and therefore APN functions have optimal resistance to differential cryptanalysis.

Definition 1.7 (Derivatives)**.** Derivatives *of a function F are functions $D_a F(x) : \mathbb{F} \to \mathbb{F}$, $a \in \mathbb{F}^*$,*

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

Remark. We can notice that degree of a derivative of a function is always smaller then degree of the function. For example the derivative at c of a quadratic function $F(x) = ax^3 + bx^5$ is

$$\begin{aligned} D_c F(x) &= ax^3 + bx^5 + a(x + c)^3 + b(x + c)^5 + ac^3 + bc^5 \\ &= ax^3 + bx^5 + ax^3 + ax^2 c + axc^2 + ac^3 + bx^5 + bx^4 c + bxc^4 \\ &\quad + bc^5 + ac^3 + bc^5 \\ &= bcx^4 + acx^2 + (ac^2 + bc^4)x, \end{aligned}$$

which is a linear function.

Lemma 1.3. *F is an APN function if and only if $|D_aF| = |\{D_aF(x) : x \in \mathbb{F}\}| = \frac{|\mathbb{F}|}{2}$ for every $a \in \mathbb{F}^*$.*

Proof. We can observe that

$$\begin{aligned} |D_aF| &= |\{F(x) + F(x+a) + F(a) + F(0) : x \in \mathbb{F}\}| \\ &= |\{F(x) + F(x+a) : x \in \mathbb{F}\}| \\ &= |\{b \in \mathbb{F} : F(x) + F(x+a) = b \text{ has a solution }\}|. \end{aligned}$$

If F is an APN function, we know that

$$2|\{b \in \mathbb{F} : F(x) + F(x+a) = b \text{ has a solution }\}| = |\mathbb{F}|$$

since $F(x)+F(x+a) = b$ has 0 or 2 solutions and for every x, $F(x)+F(x+a) = b$ for some $b \in \mathbb{F}$. Our observation then yields $|D_aF| = \frac{|\mathbb{F}|}{2}$.

Now suppose that $|D_aF| = \frac{|\mathbb{F}|}{2}$. Since $F(x)+F(x+a) = F(x+a)+F(x+a+a)$, if $F(x) + F(x+a) = b$ has a solution y, than $y + a$ is also a solution and the equation has at least 2 solutions. The observation from the beginning of this proof implies that there is a solution of the equation for exactly one half of b-s. This means that every equation has 0 or 2 solutions.

□

Theorem 1.4 (Mentioned in [5] (special case of Gold functions))**.** *$F(x) = x^3$ is an APN function.*

Proof. We will use Lemma1.3. Let $a \in \mathbb{F}^*$.

$$\begin{aligned} |D_aF| &= |\{x^3 + (x+a)^3 + a^3 : x \in \mathbb{F}\}| = |\{x^3 + x^3 + ax^2 + a^2x : x \in \mathbb{F}\}| \\ &= |\{ax^2 + a^2x : x \in \mathbb{F}\}| = |\{a^3y^2 + a^3y : y \in \mathbb{F}\}| \\ &= |\{a^3(y^2 + y) : y \in \mathbb{F}\}|. \end{aligned}$$

Since y^2+y is a linearized polynomial and $y^2+y = y(y+1) = 0$ has two solutions, $|D_aF| = |\mathbb{F}|/2$ for every $a \in \mathbb{F}^*$ and x^3 is APN. □

Another known examples of APN functions, which are mentioned in [5] are power functions:

- multiplicative inverse permutation: $F(X) = X^{2^n-2}$ for n odd,
- Gold functions: $F(X) = X^{2^i+1}$, where $\gcd(n, i) = 1$,
- Kasami functions: $F(X) = X^{2^{2i}-2^i+1}$ with $\gcd(n, i) = 1$,
- Dobbertin functions: $F(X) = X^d$, $d = 2^{4n/5} + 2^{3n/5} + 2^{2n/5} + 2^{n/5} - 1$ for n divisible by 5,

and also some non-power functions, for example:

- $F(X) = X^3 + uX^{36}$, where $u \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and $n = 10$ or 12,
- $F(X) = X^3 + \alpha^{15}X^{528}$, where α is a primitive element of $\mathbb{F}_{2^{12}}$ and $n = 12$.

However, none of these APN functions are permutations for n even. As written in [5], it was proven that no power function is a permutation in $\mathbb{F}_{2^n}$ for n even. Moreover, in [2] the author shows that no function with coefficients in subfield $\mathbb{F}_{2^{n/2}}$ can be a permutation - but it can still be equivalent to one.

The first and only known APN permutation was presented in [3] it is a function on $\mathbb{F}_{2^6}$ defined as

$$\kappa = \kappa(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $x^6 + x^4 + x^3 + x + 1$.

1.3 Equivalence of Boolean functions

Definition 1.8 (Extended Affine Equivalence)**.** *Vectorial boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called* Extended Affine equivalent*, i.e. $f \approx_{EA} g$, if there exist linear functions L_1, L_2 and L_3 such that*

$$L_1 \circ f \circ L_2(x) + L_3(x) = g(x),$$

for every $x \in \mathbb{F}_{2^n}$ and L_1 and L_2 are permutations.

Lemma 1.5. *If $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are EA-equivalent, then $\deg f = \deg g$ and $|D_a g| = |D_b f|$, where $b = L(a)$ for every $a, b \in \mathbb{F}_{2^n} \setminus \{0\}$ and some permutation L.*

Proof. Since L_1, L_2 and L_3 are all linear, the degree of f is the same as degree of g.
Since $f \approx_{EA} g$, there exist L_1, L_2, L_3 from the Definition 1.8. The size of $D_a g$ does not depend on linear transformations so we can write:

$$\begin{aligned}
|D_a g| &= |\{L_1 \circ f \circ L_2(x) + L_3(x) + L_1 \circ f \circ L_2(x+a) + L_3(x+a) \\
&\quad + L_1 \circ f \circ L_2(a) + L_3(a) + L_1 \circ f \circ L_2(0) + L_3(0) : x \in \mathbb{F}_{2^n}\}| \\
&= |\{L_1 \circ f \circ L_2(x) + L_3(x) + L_1 \circ f \circ L_2(x+a) + L_3(x) + L_3(a) : x \in \mathbb{F}_{2^n}\}| \\
&= |\{L_1(f \circ L_2(x) + f(L_2(x) + L_2(a))) : x \in \mathbb{F}_{2^n}\}| \\
&= |\{f(L_2(x)) + f(L_2(x) + L_2(a)) : x \in \mathbb{F}_{2^n}\}| \\
&= |\{f(y) + f(y+b)) : y \in \mathbb{F}_{2^n}\}| = |D_b f|,
\end{aligned}$$

where $y = L_2(x)$ and $b = L_2(a)$. □

From Lemma 1.5 we see, that if $f \approx_{EA} g$ and f is APN, then g is APN as well. However, from the definition of APN function, we can see that if f is a permutation, f is APN if and only if f^{-1} is APN but f and f^{-1} are not always EA equivalent, since their degrees are usually not the same. Therefore we would like to have a more general equivalence.

Definition 1.9 (Graph of a function)**.** *For boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we define a* graph of f *as a set*

$$G_f = \{(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} : f(x) = y\}.$$

Definition 1.10 (CCZ equivalence)**.** *Boolean functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called* CCZ-equivalent *if their graphs G_f, G_g are affine equivalent, that is, if there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $y = f(x)$ if and only if $L_2(x, y) = g(L_2(x, y))$ (or $L(G_f) = G_g$).*

Lemma 1.6. *For a boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $L = (L_1, L_2)$ an affine automorphism of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, $L(G_f)$ is a graph of a function if and only if $f_1(x) = L_1(x, f(x))$ is a permutation of $\mathbb{F}_{2^n}$. Moreover, if we denote $f_2 = L_2(x, f(x))$, $L(G_f)$ is graph of a function $f_2 \circ f_1^{-1}$.*

Proof. We can see that

$$L(G_f) = \{(L_1(x, f(x)), L_2(x, f(x))) : x \in \mathbb{F}_{2^n}\} = \{(f_1(x), f_2(x)) : x \in \mathbb{F}_{2^n}\}. \tag{1.1}$$

Since domain of f_1 is finite, f_1 is a permutation if and only if it is injective. Therefore f_1 is not a permutation if and only if there are $x_1, x_2 \in \mathbb{F}_{2^n}$ such that $x_1 \neq x_2$ and $f_1(x_1) = f_1(x_2)$. Since L is a permutation, if $f_1(x_1) = f_1(x_2) = a$ for some $x_1 \neq x_2$, then $f_2(x_1) \neq f_2(x_2)$, which means that $(a, f_2(x_1))$ and $(a, f_2(x_2))$ are both in $L(G_f)$ and therefore this is not a graph of a function.

On the other hand, if f_1 is a permutation, we can write (1.1) as

$$L(G_f) = \{(f_1(f_1^{-1}(x)), f_2(f_1^{-1}(x))) : x \in \mathbb{F}_{2^n}\} = \{(x, f_2 \circ f_1^{-1}(x)) : x \in \mathbb{F}_{2^n}\},$$

which is a graph of a function $f_2 \circ f_1^{-1}$. □

Lemma 1.7. *If two functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are EA-equivalent, they are also CCZ-equivalent.*

Proof. If $f \approx_{EA} g$, there exist affine functions L_1, L_2, L_3 such that

$$L_1 \circ f \circ L_2(x) + L_3(x) = g(x).$$

We want to show that there is an affine automorphism $\mathcal{L} = (\mathcal{L}_1, \mathcal{L}_2)$ such that

$$\mathcal{L}(G_f) = G_g.$$

We will define

$$\mathcal{L}_1(x, y) = L_2^{-1}(x)$$

and

$$\mathcal{L}_2(x, y) = L_3 \circ L_2^{-1}(x) + L_1(y).$$

Then according to Lemma 1.6, since L_2 is a permutation, $\mathcal{L}(G_f)$ is a graph of a function $f_2 \circ f_1^{-1}$.

$$f_2 \circ f_1^{-1}(x) = f_2(\mathcal{L}_1^{-1}(x, f(x)) = f_2(L_2(x)) = L_3 \circ L_2^{-1}(L_2(x)) + L_1(y)$$

□

Notice that if $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation, than $f \approx_{CCZ} f^{-1}$. Automorphism L is in this case defined as $L(x, y) = (y, x)$ for every $x, y \in \mathbb{F}_{2^n}$. Function

$f_1(x) = L_1(x, f(x)) = f(x)$ is a permutation, since f is a permutation and since $f_2(x) = x$,

$$L(G_f) = \{(f(x), x) : x \in \mathbb{F}_{2^n}\} = \{(x, f^{-1}(x)) : x \in \mathbb{F}_{2^n}\}$$

is indeed a graph of function f^{-1}. Following Lemma and Theorem will show that this equivalence is not too general, which means that if $f \approx_{CCZ} g$, then f is APN if and only if g is APN.

Lemma 1.8 (Proposition 10 in [5]). *For every $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and every $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, we define a function*

$$\gamma_f(a, b) = \begin{cases} 1, & \text{if } f(x) + f(x + a) = b \text{ has a solution,} \\ 0, & \text{otherwise.} \end{cases}$$

Function f is APN if and only if weight of a function γ_f is $2^{2n-1} - 2^{n-1}$. (Weight of function γ_f is number of pairs (a, b) such that $\gamma_f(a, b) \neq 0$.)

Proof. Weight of γ_f is $|\{(a, b) : F(x) + F(x + a) = b \text{ has a solution}, a \neq 0\}|$. We can write

$$\begin{aligned} &|\{(a, b) : F(x) + F(x + a) = b \text{ has a solution}, a \neq 0\}| \\ &\quad = \sum_{a \in \mathbb{F}_{2^n} \setminus \{0\}} |\{F(x) + F(x + a) : x \in F[2]^n\}| = \sum_{a \in \mathbb{F}_{2^n} \setminus \{0\}} |D_a f|. \end{aligned}$$

We know that in the field $\mathbb{F}_{2^n}$, which has even characteristic, $|D_a f| \leq |\mathbb{F}_{2^n}|/2 = 2^{n-1}$. Therefore

$$|\{(a, b) : F(x) + F(x + a) = b \text{ has a solution}, a \neq 0\}| \leq (2^n - 1)2^{n-1},$$

which is equal to $2^{2n-1} + 2^{n-1}$. Now we can see that the weight of γ_f is equal $2^{2n-1} + 2^{n-1}$ if and only if $|D_a f| = 2^{n-1}$ for every $a \in \mathbb{F}_{2^n} \setminus \{0\}$, which is true if and only if f is APN. □

Theorem 1.9 (Proposition 18 in [5]). *If two functions $f, g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are CCZ-equivalent, then f is APN if and only if g is APN.*

Proof. Since $f \approx_{CCZ} g$, there is an affine automorphism $L = (L_1, L_2)$ such that $L(G_f) = G_g$. L can be written as $\mathcal{L} + \alpha$, where $\mathcal{L}$ is a linear automorphism of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ and $\alpha \in \mathbb{F}_{2^n}$. $\gamma_g(a, b) = 1$ if and only if there are $x, y \in \mathbb{F}_{2^n}$ such that $f_1(x) + f_1(y) = L_1(x, f(x)) + L_1(y, f(y)) = a$ and $f_2(x) + f_2(y) = L_2(x, f(x)) + L_2(y, f(y)) = b$. This is equivalent to saying there are $x, y \in \mathbb{F}_{2^n}$ such that

$$\begin{aligned} L(x, f(x)) + L(y, f(y)) &= \mathcal{L}(x, f(x)) + \alpha + \mathcal{L}(y, f(y)) + \alpha \\ &= \mathcal{L}(x + y, f(x) + f(y)) = (a, b). \end{aligned}$$

This happens if and only if $\gamma_f(\mathcal{L}^{-1}(a, b)) = 1$. Therefore $\gamma_g = \gamma_f \circ \mathcal{L}^{-1}$, weight of both functions is the same and f is APN if and only if g is APN. □

2. Preliminary lemmas

In this chapter, we present some known Lemmas, which will be used in Chapter 3 and 4.

Definition 2.1. *For $\mathbb{F}_{q^2}$, where $q = 2^n$, we define*

$$\mathcal{T}_1 = \{g \in \mathbb{F}_{q^2} : g^q + g = 1\} \cup \{1\}.$$

Lemma 2.1 (Trace-0/Trace-1 decomposition)**.** *Every $X \in \mathbb{F}_{q^2}^*$ can be uniquely written as $X = xg$, where $x \in \mathbb{F}_{q^2}^*$, $x^q + x = 0$ and $g \in \mathcal{T}_1$.*

Remark. Note that $\{x \in \mathbb{F}_{q^2}^* : x^q + x = 0\} = \{x \in \mathbb{F}_{q^2}^* : \mathrm{tr}_n^{2n}(x) = 0\} = \mathbb{F}_q^*$ and $x^q = x$ for every $x \in \mathbb{F}_q$.

Proof. We will show that $|\mathbb{F}_{q^2}^*| = |\mathcal{T}_1| \cdot |\mathbb{F}_q^*| = q^2 - 1$. Then it is sufficient to prove that $xg = yh$ for some $x, y \in \mathbb{F}_q$ and $g, h \in \mathcal{T}_1$ only if $x = y$ and $g = h$, since we know that $\mathbb{F}_q$ and $\mathcal{T}_1$ are subsets of $\mathbb{F}_{q^2}$.

We can notice that $a^q + a = \mathrm{tr}_n^{2n}(a)$, which is a linear function, and $g^q + g = 1$ has a solution in $\mathbb{F}_{q^2}$. Since $|\ker(a^q + a)| = |\mathbb{F}_q| = q$, it actually has q solutions and $|\mathcal{T}_1| = q + 1$. Therefore $|\mathcal{T}_1||\mathbb{F}_q^*| = (q+1)(q-1) = q^2 - 1$.

Let $xg = yh$ for some $x, y \in \mathbb{F}_q$ and $g, h \in \mathcal{T}_1$. Then

$$\begin{aligned}(xg)^q + xg &= (yh)^q + yh\\ x(g^q + g) &= y(h^q + h).\end{aligned}$$

If $g = 1$, we have $0 = y(h^q + h)$ and since y is invertible, $h^q + h = 0$. This is possible only if $h = 1 = g$. This gives us $x \cdot 1 = y \cdot 1$ and $x = y$.

If $g \neq 1$, then also $h \neq 1$. Hence $h^q + h = g^q + g = 1$ and $x = y$. Therefore $xg = xh$ and $g = h$. □

Lemma 2.2. *For every $g \in \mathcal{T}_1 \setminus \{1\}$, any $X \in \mathbb{F}_{q^2}$ can be uniquely written as $X = xg + y$, where $x, y \in \mathbb{F}_q$.*

Proof. We know that the number of pairs (x, y) is the same as the number of elements $X \in \mathbb{F}_{q^2}$. Obviously, for every pair (x, y), $xg + y$ is an element of $\mathbb{F}_{q^2}$. Therefore it is enough to prove that if for some $x, y, a, b \in \mathbb{F}_q$

$$xg + y = ag + b,$$

then $x = a$ and $y = b$.

Let $x, y, a, b \in \mathbb{F}_q$ then we have

$$\begin{aligned}xg + y &= ag + b\\ (x + a)g + (y + b) &= 0.\end{aligned}$$

Applying tr_n^{2n}, we get

$$\begin{aligned}(x + a)^q g^q + (x + a)g + (y + b)^q + (y + b) &= 0\\ (x + a)(g + 1) + (x + a)g + (y + b) + (y + b) &= 0\\ x + a &= 0.\end{aligned}$$

Hence $x = a$ and since $xg + y = xg + b$, $y = b$ as well. □

Lemma 2.3. *For every non-negative integer m,*

$$2^m \bmod 3 = \begin{cases} 1, & \text{for } m \text{ even,} \\ 2, & \text{for } m \text{ odd.} \end{cases}$$

Proof. Every non-negative m can be written as $m = 2k + \ell$, where $k \in \mathbb{Z}_0^+$ and $\ell \in \{0, 1\}$. Then we can write

$$2^m \bmod 3 = 2^{2k} \cdot 2^\ell \bmod 3 = 4^k \cdot 2^\ell \bmod 3 = 2^\ell = \begin{cases} 1, & \text{if } \ell = 0 \ (m \text{ is even}), \\ 2, & \text{if } \ell = 1 \ (m \text{ is odd}). \end{cases}$$

□

Definition 2.2 (Hyperplane)**.** *A* hyperplane *in $\mathbb{F}_{2^n}$ is an $(n-1)$-dimensional subspace of $\mathbb{F}_{2^n}$, which is an n-dimensional vector space over $\mathbb{F}_2$.*

Lemma 2.4 (Can be found in [6])**.** *The number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_p$, where p is a prime number, is*

$$\binom{n}{k}_p = \frac{(p^n - 1)(p^n - p) \dots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \dots (p^k - p^{k-1})}.$$

Proof. Every k-dimensional subspace is given by k linearly independent vectors. First vector can be chosen as an arbitrary non-zero element of $\mathbb{F}_{p^n}$, which means we have $p^n - 1$ possible choices. The second vector can not be generated by the first. The first vector generates a subspace of dimension 1, which has p elements and therefore we have $p^n - p$ different choices for the second vector. First two vectors generate a subspace of dimension two, which has p^2 elements. Hence we have $p^n - p^2$ vectors, which can be chosen as the third vector. If we proceed this way we can compute that we have $(p^n - 1)(p^n - p) \dots (p^n - p^{k-1})$ possible k-tuples of linearly independent vectors.

Many different k-tuples of independent vectors, however, generate the same subspace. Therefore to find the number of subspaces, the number of k-tuples must be divided by the number of linearly independent k-tuples that generate the same subspace. In other words, we have to find the number of all k-tuples of linearly independent vectors in a k-dimensional vector space, which is the same task as in the first part of this proof, with $n = k$. Every k-dimensional subspace can be therefore generated in $(p^k - 1)(p^k - p) \dots (p^k - p^{k-1})$ ways.

Hence the number of k-dimensional subspaces of an n-dimensional vector space is

$$\frac{(p^n - 1)(p^n - p) \dots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \dots (p^k - p^{k-1})}.$$

□

Lemma 2.5. *Every hyperplane in $\mathbb{F}_{2^n}$ can be uniquely written as*

$$H_\alpha = \{x : x \in \mathbb{F}_{2^n}, \mathrm{tr}_1^n(\alpha x) = 0\},$$

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

Proof. Since trace $\mathrm{tr}_1^n(\alpha x)$ is a linear function and $\mathrm{Im}(\mathrm{tr}_1^n(\alpha x)) = \{0,1\}$, which is a subspace of dimension 1, the $\ker(\mathrm{tr}_1^n(\alpha x)) = H_\alpha$ is a $(n-1)$-dimensional subspace, i.e. a hyperplane.

We want to prove that $H_\alpha = H_\beta$ if and only if $\alpha = \beta$. Then the Lemma will be proven, since according to Lemma 2.4 the number of hyperplanes in $\mathbb{F}_{2^n}$ is

$$\frac{(2^n-1)(2^n-2)\dots(2^n-2^{n-2})}{(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}$$
$$= \frac{(2^n-1)2(2^{n-1}-1)2(2^{n-1}-2)\dots 2(2^{n-1}-2^{n-3})}{(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-3})2^{n-1}} = \frac{(2^n-1)2^{n-2}}{2^{n-2}} = 2^n-1,$$

which is exactly the number of non-zero elements of $\mathbb{F}_{2^n}$.

Assume that $H_\alpha = H_\beta$. This means that for every $x \in \mathbb{F}_{2^n}$,

$$\mathrm{tr}_1^n(\alpha x) = \mathrm{tr}_1^n(\beta x).$$

This can be rewritten as

$$\mathrm{tr}_1^n(\alpha x) + \mathrm{tr}_1^n(\beta x) = 0$$
$$\mathrm{tr}_1^n((\alpha+\beta)x) = 0,$$

for every $x \in \mathbb{F}_{2^n}$. This means that $H_{\alpha+\beta} = \mathbb{F}_{2^n}$, which is not a hyperplane. Therefore $\alpha + \beta = 0$ and equivalently $\alpha = \beta$. □

Definition 2.3 (Affine hyperplane)**.** *An* affine hyperplane *of* $\mathbb{F}_{2^n}$ *is either a hyperplane and therefore* H_α *for some non-zero* α*, or its complement* $\overline{H_\alpha} = \{x : x \in \mathbb{F}_{2^n}, \mathrm{tr}_1^n(\alpha x) = 1\}$.

Lemma 2.6. *An intersection of two affine hyperplanes* H_1, H_2 *is an empty set if and only if they are complements, i.e.* $\{H_1, H_2\} = \{H_\alpha, \overline{H_\alpha}\}$ *for some non-zero* $\alpha \in \mathbb{F}_{2^n}$.

Proof. If $H_1 \cap H_2 = \emptyset$, then $|H_1 \cup H_2| = 2^{n-1} + 2^{n-1} = 2^n$, which means that $H_1 \cup H_2 = \mathbb{F}_{2^n}$. This yields that $\overline{H_1} = \mathbb{F}_{2^n} \setminus H_1 = H_2$ and therefore H_1 and H_2 are complements. □

Lemma 2.7. *For every* $\gamma \in \mathbb{F}_{2^n}^*$

$$\mathrm{Im}\left(\gamma(x^2+x)\right) = H_{\gamma^{-1}}.$$

Proof. We know that $\mathrm{Im}(x^2+x) = H_1$. If $y \in \mathrm{Im}\left(\gamma(x^2+x)\right)$, there is $x \in \mathbb{F}_{2^n}$ such that $y = \gamma(x^2+x)$ and therefore

$$\mathrm{tr}_1^n(\gamma^{-1}y) = \mathrm{tr}_1^n\left(\gamma^{-1}\gamma(x^2+x)\right) = \mathrm{tr}_1^n(x^2+x) = 0.$$

Hence $y \in H_{\gamma^{-1}}$ and $\mathrm{Im}\left(\gamma(x^2+x)\right) \subseteq H_{\gamma^{-1}}$. Since $\gamma(x^2+x)$ is a linearised polynomial and equation

$$\gamma x^2 + \gamma x = 0$$

has two solutions, number of elements of $\mathrm{Im}\left(\gamma(x^2+x)\right)$ has 2^{n-1} elements. This is the same number of elements as in $H_{\gamma^{-1}}$ and therefore the two sets are equal. □

3. Conditions for APN functions

Let $q = 2^m$, $m > 1$ and F be a function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^2}$ such that

$$F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2},$$

where $b, c, d \in \mathbb{F}_q$. In this chapter, we will find out if this function can be APN and if it can, what are the conditions for b, c and d. This function was inspired by the only APN permutation in even dimension found so far in [3]:

$$\kappa(x) = x^3 + x^{10} + ux^{24}, \tag{3.1}$$

which is an APN function CCZ-equivalent to a permutation on $\mathbb{F}_{2^6}$ and u is a primitive element of $\mathbb{F}_{2^6}$. This function is not of our form since u is not in the subfield $\mathbb{F}_{2^3}$, but it is linearly equivalent to a function of this form.

Moreover, both κ and functions of our form satisfy the subspace property with $k = 1$.

Definition 3.1 (Subspace property)**.** *We say that a function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ satisfies the* subspace property*, if there is an integer k such that*

$$f(\lambda X) = \lambda^{2^k+1} f(X)$$

for every $\lambda \in \mathbb{F}_q$ and $X \in \mathbb{F}_{q^2}$.

Since F is a quadratic function, its derivatives are linear and F is APN if and only if all its derivatives are 2:1 maps. Hence, for F to be APN, we have to prove that

$$D_A F(X) = 0$$

has exactly two solutions $X_1, X_2 \in \mathbb{F}_{q^2}$ for every $A \in \mathbb{F}_{q^2}^*$. However, we can compute

$$D_A F(0) = F(0) + F(0 + A) + F(0) + F(A) = 0,$$

which implies that 0 is always a solution. We will find conditions for b, c, d, such that $D_A F(X) = 0$ has exactly one solution $X \in \mathbb{F}_{q^2}^*$ for every $A \in \mathbb{F}_{q^2}^*$.

We can notice that

$$\begin{aligned} F(kX) &= k^3X^3 + bk^{3q}X^{3q} + ck^{2q}kX^{2q+1} + dk^q k^2 X^{q+2} \\ &= k^3(X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2}) = k^3 F(X) \end{aligned} \tag{3.2}$$

for every $k \in \mathbb{F}_q$. Lemma 2.1 yields that A can be written as $A = ah$, where $a \in \mathbb{F}_q^*$ and $h \in \mathcal{T}_1$. Since $D_A F(X)$ is 2:1 if and only if $D_A F(aX)$ and

$$\begin{aligned} D_A F(aX) &= F(aX) + F(aX + ah) + F(ah) = a^3 \left[F(X) + F(X + h) + F(h)\right] \\ &= a^3 D_h F(X), \end{aligned}$$

whether $D_A F(X)$ is 2:1 only depends on h.

3.1 Case $h = 1$

Let us first consider $h = 1$.

$$\begin{aligned} D_1F(X) &= F(X) + F(X+1) + F(0) + F(1) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} \\ &\quad + (X+1)^3 + b(X+1)^{3q} + c(X+1)^{2q+1} + dX^{q+2} + F(1) \\ &= X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} + X^3 + X^2 + X + 1 \\ &\quad + b(X^{3q} + X^{2q} + X^q + 1) + c(X^{2q+1} + X^{2q} + X + 1) \\ &\quad + d(X^{q+2} + X^q + X^2 + 1) + F(1) \\ &= X(1+c) + X^2(1+d) + X^q(b+d) + X^{2q}(b+c). \end{aligned} \tag{3.3}$$

Since we are looking for solutions $X \in \mathbb{F}_{q^2}^*$, Lemma 2.1 yields that X can be uniquely written as $X = xg$, where $x \in \mathbb{F}_q$ and $g \in \mathcal{T}_1$.

$$\begin{aligned} D_1F(xg) &= xg(1+c) + x^2g^2(1+d) + x^qg^q(b+d) + x^{2q}g^{2q}(b+c) \\ &= xg(1+c) + x^2g^2(1+d) + x(g+1)(b+d) + x^2(g+1)^2(b+c) \\ &= x^2g^2(1+b+c+d) + xg(1+b+c+d) + x^2(b+c) + x(b+d) \end{aligned} \tag{3.4}$$

if $g \neq 1$ and

$$D_1F(xg) = x(1+c) + x^2(1+d) + x(b+d) + x^2(b+c) = (x^2+x)(1+b+c+d)$$

if $g = 1$. We can see that function $D_1F(X)$ is 2:1 if and only if $1+b+c+d \neq 0$. Therefore if F is APN, $1+b+c+d \neq 0$ and we will assume this holds in the rest of this chapter. We also know two solutions of $D_1F(X)$, which are 0 and 1. This means that (3.4) should have no solutions.

As we proved in Lemma 2.2, every element of $\mathbb{F}_{q^2}$ can be uniquely written as $kg + \ell$ where $k, \ell \in \mathbb{F}_q$. If we could write (3.4) this way and $g \neq 1$, it is zero if and only if $k = \ell = 0$, which will help us find solutions. Since

$$\mathrm{tr}_m^{2m}(g^3) = g^3 + g^{3q} = g^3 + g^3 + g^2 + g + 1 = g^2 + g + 1,$$

we can write $g^2 = g + \mathrm{tr}_m^{2m}(g^3) + 1$. We will denote $S_g = \mathrm{tr}_m^{2m}(g^3) = g^2 + g + 1$. Now we can write (3.4) as

$$\begin{aligned} &gx(1+b+c+d) + (g+S_g+1)x^2(1+b+c+d) \\ &\quad = g(x^2+x)(1+b+c+d) + x^2(1+d) + x(b+d) + x^2S_g(1+b+c+d) \end{aligned} \tag{3.5}$$

We will denote $A = (x^2+x)(1+b+c+d)$ and $B = x^2(1+d) + x(b+d) + x^2S_g(1+b+c+d)$. If $X = xg$, $g \neq 1$ is a solution, then both A and B are equal 0. If $x \neq 1$, A is not 0 and the equation has no solution. If $x = 1$, we get equation

$$\begin{aligned} (1+d) + (1+b) + S_g(1+b+c+d) &= 0 \\ (1+b) + S_g(1+b+c+d) &= 0 \\ S_g &= \frac{1+b}{1+b+c+d} \end{aligned}$$

We will now need the following Lemma.

Lemma 3.1 (Part of Lemma 1 in [4]). *Let $g \in \mathcal{T}_1 \setminus \{1\}$. Then*

$$\mathrm{tr}_1^{2m}\left(g^{2^k+1}\right) = \begin{cases} 1, & \text{if } m+k \text{ is odd,} \\ 0, & \text{if } m+k \text{ is even.} \end{cases}$$

This Lemma implies that

$$\mathrm{tr}_1^m(S_g) = \mathrm{tr}_1^m \mathrm{tr}_m^{2m}(g^3) = \mathrm{tr}_1^{2m}(g^3) = \begin{cases} 1, & \text{if } m \text{ is even,} \\ 0, & \text{if } m \text{ is odd.} \end{cases}$$

If $\mathrm{tr}_1^m((1+b)/(1+b+c+d)) = 1$ and m is odd or $\mathrm{tr}_1^m((1+b)/(1+b+c+d)) = 0$ and m is even, the equation has no solution and F can be APN. Otherwise, there could be a solution. S_g is a 2:1 function and therefore it can have $q/2$ different values for $g \in \mathcal{T}_1 \setminus \{1\}$. There is exactly $q/2$ elements of $\mathbb{F}_q$ trace of which is equal 0 and $q/2$ elements with trace 1. This means that if $\mathrm{tr}_1^m((1+b)/(1+b+c+d)) = \mathrm{tr}_1^m(S_g)$ then there is always some solution g. The following table sums up the conditions for b, c, d that we found considering $h = 1$.

m odd	m even
$1+b+c+d \neq 0$	
$\mathrm{tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 1$	$\mathrm{tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 0$

Table 3.1: First conditions

3.2 Case $h \neq 1$

Now we will compute $D_hF(X)$:

$$\begin{aligned} D_hF(X) &= F(X) + F(X+h) + F(h) + F(0) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} \\ &\quad + (X+h)^3 + b(X+h)^{3q} + c(X+h)^{2q+1} + d(X+h)^{q+2} \\ &\quad + h^3 + bh^{3q} + ch^{2q+1} + dh^{q+2} \\ &= X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2} + X^3 + X^2h + Xh^2 + h^3 \\ &\quad + b\left(X^{3q} + X^{2q}h^q + X^qh^{2q} + h^{3q}\right) + c\left(X^{2q+1} + X^{2q}h + Xh^{2q} + h^{2q+1}\right) \\ &\quad + d\left(X^{q+2} + X^qh^2 + X^2h^q + h^{q+2}\right) + h^3 + bh^{3q} + ch^{2q+1} + dh^{q+2} \\ &= X^2h + Xh^2 + b\left(X^{2q}(h+1) + X^q(h^2+1)\right) + c\left(X^{2q}h + X(h^2+1)\right) \\ &\quad + d\left(X^qh^2 + X^2(h+1)\right) \\ &= X\left(h^2 + ch^2 + c\right) + X^2\left(h + dh + d\right) + X^q\left(bh^2 + b + dh^2\right) \\ &\quad + X^{2q}\left(ch + bh + b\right). \end{aligned} \tag{3.6}$$

According to Lemma 2.2, we can write X as $xh + y$, where $x, y \in \mathbb{F}_q$. We get

$$
\begin{aligned}
D_hF(xh+y) &= (xh+y)(h^2+ch^2+c)+(x^2h^2+y^2)(h+dh+d)\\
&\quad+(xh+x+y)(bh^2+b+dh^2)+(x^2h^2+x^2+y^2)(bh+b+ch)\\
&= (xh^3+cxh^3+cxh+yh^2+cyh^2+cy)\\
&\quad+(x^2h^3+x^2dh^3+dx^2h^2+y^2h+dy^2h+dy^2)\\
&\quad+(x^2bh^3+x^2bh^2+x^2ch^3+x^2bh+x^2b+x^2ch+y^2bh+y^2b+y^2ch)\\
&\quad+(xbh^3+xbh+xdh^3+xbh^2+xb+xdh^2+ybh^2+yb+ydh^2)\\
&= h^3\left(x+cx+x^2+cx^2+bx^2+bx+dx+dx^2\right)\\
&\quad+h^2\left(y+cy+dx^2+bx^2+bx+dx+dy+by\right)\\
&\quad+h\left(cx+y^2+dy^2+bx^2+cx^2+by^2+cy^2+bx\right)\\
&\quad+\left(dy^2+bx^2+by^2+bx+by+cy\right)\\
&= h^3(x^2+x)(1+b+c+d)+h^2(y(1+b+c+d)+(x^2+x)(b+d))\\
&\quad+h(y^2(1+b+c+d)+(x^2+x)(b+c))\\
&\quad+b(x^2+x)+b(y^2+y)+dy^2+cy. \qquad (3.7)
\end{aligned}
$$

We can see that there are always two solutions of equation $D_hF(xh+y)=0$, $(x,y)=(0,0)$ and $(x,y)=(1,0)$, which correspond to $X=0$ and $X=h$. For F to be APN there has to be no other solution of this equation. We will proceed as in the first case - we will try to write (3.7) in the form $Ah+B$, where $A,B\in\mathbb{F}_q$. Then (x,y) is a solution if and only if A and B are both zero. From the previous case we know that we can write h^2 as $h+S_h+1$. We can write

$$h^3 = h(h^2+h+1)+(h^2+h) = hS_h+(h^2+h).$$

We will denote $h^2+h=T_h$. It is obvious that $T_h\in\mathbb{F}_q$, since $S_h\in\mathbb{F}_q$ and $T_h=S_h+1$. Now we will fix h and write S and T instead of S_h and T_h. We will denote $\Delta=1+b+c+d$, $\Lambda=b+d$ and $\Gamma=b+c$. We can now rewrite (3.7):

$$
\begin{aligned}
D_hF(xh+y) &= (Sh+T)(x^2+x)\Delta+(h+T)(y\Delta+(x^2+x)\Lambda)\\
&\quad+h(y^2\Delta+(x^2+x)\Gamma)+b(x^2+x)+b(y^2+y)+cy+dy^2\\
&= (x^2+x)\left(T(\Delta+\Lambda)+b\right)+Ty\Delta+b(y^2+y)+cy+dy^2\\
&\quad+h\left((x^2+x)(S\Delta+\Lambda+\Gamma)+\Delta(y^2+y)\right).
\end{aligned}
$$

Notice that $\Lambda+\Gamma=b+d+b+c=c+d$. We will denote

$$A(x,y)=(x^2+x)(S\Delta+c+d)+\Delta(y^2+y)$$

and

$$B(x,y)=(x^2+x)\left(T(\Delta+\Lambda)+b\right)+Ty\Delta+b(y^2+y)+cy+dy^2.$$

According to Lemma 2.2, (x,y) is a solution of $D_hF(xh+y)=0$ if and only if $A(x,y)=B(x,y)=0$. $A(x,y)=0$ means

$$(x^2+x)(S\Delta+c+d)=\Delta(y^2+y). \qquad (3.8)$$

Let us first consider the case when $S\Delta + c + d = 0$ which is equivalent to

$$S = \frac{c+d}{\Delta}.$$

We already know from the conditions in Table 3.1 that

$$\mathrm{tr}_1^m(S) \neq \mathrm{tr}_1^m\left(\frac{1+b}{\Delta}\right) = \mathrm{tr}_1^m\left(\frac{c+d}{\Delta}\right) + \mathrm{tr}_1^m(1),$$

which means that $S\Delta + c + d = 0$ happens if and only if $\mathrm{tr}_1^m(1) = \sum_{i=0}^{m-1} 1 = 1$. This is true for m odd.

3.2.1 m is odd and $S\Delta + c + d = 0$

Equation (3.8) is then

$$0 = (y^2 + y)\Delta.$$

This means that $A(x, y) = 0$ for every $(x, 1)$ and $(x, 0)$, where $x \in \mathbb{F}_q$ but for F to be APN $B(x, y)$ should be zero only for $(0, 0)$ and $(1, 0)$. If $y = 0$, the only solutions for x of equation $B(x, 0) = 0$ should be 0 and 1.

$$\begin{aligned} B(x,0) &= 0 \\ (x^2 + x)\left(T(\Delta + \Lambda) + b\right) &= 0, \end{aligned}$$

which has exactly two solutions $x = 0$ and $x = 1$ if and only if $T(\Delta + \Lambda) + b \neq 0$. However, since

$$T + 1 = S = \frac{c+d}{1+b+c+d} = 1 + \frac{1+b}{1+b+c+d},$$

we know that $T = \frac{1+b}{1+b+c+d}$. Now we get

$$\begin{aligned} \frac{1+b}{1+b+c+d}(1+c) &= b \\ 1 + bc + b + c &= b + b^2 + bc + bd \\ 1 + b^2 + bd + c &= 0 \end{aligned}$$

For m odd we therefore get another condition:

$$1 + c + b^2 + bd \neq 0. \tag{3.9}$$

For $y = 1$ there should be no solution of $B(x, 1) = 0$:

$$\begin{aligned} B(x,1) &= 0 \\ (x^2 + x)\left(T(1+c) + b\right) + T\Delta + c + d &= 0 \\ (x^2 + x)\left(\frac{(1+b)(1+c)}{\Delta} + b\right) + 1 + b + c + d &= 0 \\ (x^2 + x)\frac{1 + b + c + bc + b + b^2 + bc + bd}{\Delta} &= \Delta \\ (x^2 + x)\frac{1 + b^2 + c + bd}{\Delta} &= \Delta. \end{aligned}$$

From the case $y = 0$ we already know that $1 + c + b^2 + bd \neq 0$ and we can write

$$x^2 + x = \frac{\Delta^2}{1 + b^2 + c + bd}.$$

A function $x^2 + x$ on the left hand side of the equation is a 2:1 map and its image is H_1, which is a set of all elements $\alpha \in \mathbb{F}_q$ such that $\mathrm{tr}_1^m(\alpha) = 0$. Therefore this equation has a solution if and only if

$$\mathrm{tr}_1^m\left(\frac{\Delta^2}{1 + b^2 + c + bd}\right) = 0.$$

Therefore if m is odd, for F to be APN there has to be

$$\mathrm{tr}_1^m\left(\frac{\Delta^2}{1 + b^2 + c + bd}\right) = 1.$$

3.2.2 $S\Delta + c + d \neq 0$

Now we assume that $S\Delta + c + d \neq 0$ and we can rewrite (3.8):

$$x^2 + x = (y^2 + y)\frac{\Delta}{S\Delta + c + d}. \tag{3.10}$$

Then replacing (x^2+x) in $B(x, y) = 0$ gives us an equation with only one variable y, which can be written as $Ey^2 + Fy = 0$, where $E, F \in \mathbb{F}_q$. This equation should have only solution $y = 0$ since in that case equation (3.10) has exactly those two solutions for x which it should have - $(1, 0)$ and $(0, 0)$.

$$\begin{aligned}
0 &= (y^2 + y)\left(\frac{\Delta}{S\Delta + \Lambda + \Gamma}\right)(T(\Delta + \Lambda) + b) + Ty\Delta + b(y^2 + y) + cy + dy^2 \\
0 &= y^2\left(\frac{\Delta}{S\Delta + c + d}(T(1 + c) + b) + b + d\right) \\
&\quad + y\left(\frac{\Delta}{S\Delta + c + d}(T(1 + c) + b) + T\Delta + b + c\right)
\end{aligned} \tag{3.11}$$

$$\begin{aligned}
E(S\Delta + c + d) &= \Delta T(1 + c) + \Delta b + S\Delta b + bc + bd + S\Delta d + cd + d^2 \\
&= \Delta T(1 + c) + \Delta b + \Delta b + \Delta Tb + bc + bd + \Delta d + \Delta Td + cd + d^2 \\
&= \Delta T(1 + b + c + d) + bc + d(b + c + d + \Delta) = \Delta^2 T + bc + d
\end{aligned}$$

$$\begin{aligned}
F(S\Delta + c + d) &= \Delta T(1 + c) + \Delta b + ((T + 1)\Delta + c + d)(\Delta T + b + c) \\
&= \Delta T + \Delta Tc + \Delta b + (\Delta T)^2 + \Delta Tb + \Delta Tc + \Delta^2 T + \Delta b + \Delta c + c\Delta T + bc \\
&\quad + c^2 + d\Delta T + bd + cd \\
&= \Delta T(1 + \Delta T + b + \Delta + c + d) + c(\Delta + b + c + d) + bd \\
&= \Delta^2 T^2 + bd + c
\end{aligned}$$

We get

$$E = \frac{\Delta^2 T + bc + d}{S\Delta + c + d} = \frac{\Delta^2 T + bc + d}{\Delta T + \Delta + c + d} = \frac{\Delta^2 T + bc + d}{\Delta T + 1 + b}$$

and

$$F = \frac{\Delta^2 T^2 + bd + c}{S\Delta + c + d} = \frac{\Delta^2 T^2 + bd + c}{\Delta T + 1 + b}.$$

If $E = 0$, which is under our conditions equivalent to $\Delta^2 T + bc + d = 0$, equation (3.11) has a non-zero solution if and only if $F = 0$ as well. In this case every y is a solution and for example $(1, 1)$ is also a solution of (3.10) and F is not APN. This happens only if $\Delta^2 T + bc + d = 0$ and $\Delta^2 T^2 + bd + c$ which means that

$$T = \frac{bc + d}{\Delta^2}$$

and

$$T^2 = \frac{bd + c}{\Delta^2},$$

which can happen only if $tr_1^m\left((bd + c)/\Delta^2\right) = 1$. This yields that

$$\left(\frac{bc + d}{\Delta^2}\right)^2 = \frac{bd + c}{\Delta^2}$$
$$b^2c^2 + d^2 = \Delta^2(bd + c).$$

This gives us another condition - if

$$tr_1^m\left(\frac{bd + c}{\Delta^2}\right) = 1$$

and $(bc+d)/\Delta^2 \neq (1+b)^2/\Delta^2$ in the case when m is odd then $b^2c^2+d^2 \neq \Delta^2(bd+c)$. Notice that the condition $(bc+d)/\Delta^2 \neq (1+b)^2/\Delta^2$ is equivalent to $bc+d \neq 1+b^2$, which is equivalent to the condition (3.9).

If $E \neq 0$, we have another solution

$$\frac{F}{E} = \frac{\Delta^2 T^2 + bd + c}{\Delta^2 T + bc + d}.$$

Now we can substitute y in equation (3.10) with $\frac{F}{E}$ and we will also substitute S with $T + 1$. We get

$$x^2 + x = \left(\frac{F}{E} + \frac{F^2}{E^2}\right)\frac{\Delta}{\Delta T + \Delta + c + d}$$
$$x^2 + x = \frac{\Delta F}{E^2}\left(\frac{E + F}{\Delta T + 1 + b}\right)$$

We can simplify the fraction in the parentheses.

$$\begin{aligned}\frac{E + F}{\Delta T + 1 + b} &= \frac{\Delta^2 T + bc + d + \Delta^2 T^2 + bd + c}{(\Delta T + 1 + b)^2} \\ &= \frac{\Delta^2 T^2 + (1 + b + c + d)\Delta T + (1 + b)(c + d)}{(\Delta T + 1 + b)^2} \\ &= \frac{(\Delta T + 1 + b)(\Delta T + c + d)}{(\Delta T + 1 + b)^2} = \frac{\Delta T + c + d}{\Delta T + 1 + b}\end{aligned}$$

Simplified equation is then:

$$x^2 + x = \Delta \frac{F}{E^2} \frac{(\Delta T + c + d)}{\Delta T + 1 + b}$$
$$x^2 + x = \frac{\Delta(T\Delta + c + d)(T^2\Delta^2 + bd + c)(T\Delta + 1 + b)^2}{(T\Delta^2 + bc + d)^2(T\Delta + 1 + b)^2}$$
$$x^2 + x = \frac{\Delta(T\Delta + c + d)(T^2\Delta^2 + bd + c)}{(T\Delta^2 + bc + d)^2}.$$

Since trace of $x^2 + x$ is 0 for every $x \in \mathbb{F}_q$, the solution only makes sense if trace of the right hand side is 0 as well. There should be no solution for $y \neq 0$, which is equivalent to $F \neq 0$ and $\Delta^2 T^2 + bd + c \neq 0$. Therefore for such T there has to be

$$\mathrm{tr}_1^m \left(\frac{\Delta(T\Delta + c + d)(T^2\Delta^2 + bd + c)}{(T\Delta^2 + bc + d)^2} \right) = 1.$$

Now we can update Table 3.1.

m odd	m even
$\Delta = 1 + b + c + d \neq 0$	
$\mathrm{tr}_1^m \left(\frac{1+b}{1+b+c+d}\right) = 1$	$\mathrm{tr}_1^m \left(\frac{1+b}{1+b+c+d}\right) = 0$
$1 + c + b^2 + bd \neq 0$	–
$\mathrm{tr}_1^m \left(\frac{\Delta^2}{1+b^2+c+bd}\right) = 1$	–
if $\mathrm{tr}_1^m \left(\frac{bd+c}{\Delta^2}\right) = 1$, then $b^2c^2 + d^2 \neq \Delta^2(bd + c)$	
$\mathrm{tr}_1^m \left(\frac{\Delta(T\Delta+c+d)(T^2\Delta^2+bd+c)}{(T\Delta^2+bc+d)^2}\right) = 1,$ for every T such that $\mathrm{tr}_1^m(T) = 1$, $\Delta T + 1 + b \neq 0$, $T\Delta^2 + bc + d \neq 0$ and $\Delta^2 T^2 + bd + c \neq 0$	

Table 3.2: APN conditions

Theorem 3.2. *Function $F : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that*

$$F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2},$$

$b, c, d \in \mathbb{F}_q$ is APN if and only if b, c and d satisfy all conditions in Table 3.2.

4. Conditions for permutations

In this chapter we will determine which functions from the previous chapter, i.e. functions on $\mathbb{F}_{q^2}$ represented by a polynomial

$$F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2},$$

where $b, c, d \in \mathbb{F}_q$ and $q = 2^m$; are CCZ-equivalent to a permutation of a certain type. We will denote $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_{q^2}$. We will use the following theorems.

Theorem 4.1 (Proved in [3]). *For $F : \mathbb{F} \to \mathbb{F}$ we define $\mathcal{F}$ a set of zeroes of the Walsh transform of F, i.e.*

$$\mathcal{F} = \{(a, b) : \hat{F}(a, b) = 0\}.$$

Function F is CCZ-equivalent to a permutation if and only if there exist subspaces U, V of dimension $2m$ such that $U, V \subseteq \mathcal{F} \cup \{0\}$ and

$$U \cap V = \{0\}.$$

In general, it is very difficult to find such subspaces and therefore in this thesis we will be only interested in permutations of κ type. For the κ function (3.1), the subspaces U and V from Theorem 4.1 are of the type

$$U = \{(xg_1, yh_1) : x, y \in \mathbb{K}\}$$
$$V = \{(xg_2, yh_2) : x, y \in \mathbb{K}\},$$

where $g_1, g_2, h_1, h_2 \in \mathcal{T}_1$, such that $g_1 \neq g_2$, $h_1 \neq h_2$, $g_1 \neq h_1$ and $g_2 \neq h_2$. As we can see from Lemma 2.1, their intersection is $\{(0, 0)\}$ and dimension $2m$. These specific subspaces are easier to find using the following theorem.

Theorem 4.2 (Proved in [3]). *A function $F : \mathbb{F} \to \mathbb{F}$ is equivalent to a permutation of κ type, if and only if there are $g_1, g_2, h_1, h_2 \in \mathcal{T}_1$ such that*

$$\sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \left(\sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \right)^2 = q^4,$$
$$\sum_{A \in g_2\mathbb{K}} \sum_{B \in h_2\mathbb{K}} \left(\sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \right)^2 = q^4,$$

where $g\mathbb{K} = \{gx, x \in \mathbb{K}\}$ and $g_1 \neq h_1$, $g_2 \neq h_2$, $g_1 \neq g_2$ and $h_1 \neq h_2$.

Proof. We can see that $U \subseteq \mathcal{F} \cup \{(0, 0)\}$ is equivalent to saying

$$\hat{F}(A, B) = \sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) = \begin{cases} 0, & \text{for every } (A, B) \in U \setminus \{(0, 0)\}, \\ q^2, & \text{for } (A, B) = (0, 0). \end{cases}$$

Therefore

$$\sum_{(A,B) \in U} \sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) = q^2.$$

Since $\hat{F}(A,B)$ can be negative, this is not equivalent. However, if we take sum of squares of the Walsh transform, it will be equivalent to $U \subseteq \mathcal{F} \cup \{(0,0)\}$ again, since the sum would grow if there were any non-zero terms for some non-zero (A,B). Finally, we can see that $U = g_1\mathbb{K} \times h_1\mathbb{K}$ and $U \subseteq \mathcal{F} \cup \{(0,0)\}$ is therefore equivalent to

$$\sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \left(\sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \right)^2 = q^4.$$

□

Let us apply this theorem to our case. We want to find b, c and d such that equation

$$\sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \left(\sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \right)^2 = q^4 \tag{4.1}$$

has a solution. If there are two solutions $(g_1, h_1), (g_2, h_2)$ satisfying conditions in Theorem 4.2, then f is equivalent to a permutation.

Left side can be written in the following way:

$$\begin{aligned}
&\sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \left(\sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \right)^2 = \\
&\quad = \sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \sum_{Y \in \mathbb{F}} \chi\left(AF(Y) + BY\right) \\
&\quad = \sum_{A \in g_1\mathbb{K}} \sum_{B \in h_1\mathbb{K}} \sum_{X \in \mathbb{F}} \chi\left(AF(X) + BX\right) \sum_{Z \in \mathbb{F}} \chi\left(AF(X+Z) + B(X+Z)\right) \\
&\quad = \sum_{A \in g_1\mathbb{K}} \sum_{X,Z \in \mathbb{F}} \chi\left(A(F(X) + F(X+Z))\right) \sum_{B \in h_1\mathbb{K}} \chi\left(BZ\right) \\
&\quad = \sum_{A \in g_1\mathbb{K}} \sum_{X,Z \in \mathbb{F}} \chi\left(A(F(X) + F(X+Z))\right) \sum_{b \in \mathbb{K}} \chi\left(bh_1Z\right)
\end{aligned} \tag{4.2}$$

If we focus on the last part, we can see that

$$\sum_{b \in \mathbb{K}} (-1)^{\mathrm{tr}_1^n(bh_1Z)} = \sum_{b \in \mathbb{K}} (-1)^{\mathrm{tr}_1^m(b\,\mathrm{tr}_n^m(h_1Z))} = \begin{cases} q, & \text{if } \mathrm{tr}_m^n(h_1Z) = 0, \\ 0, & \text{otherwise.} \end{cases}$$

This means that (4.2) is 0 for Z such that $\mathrm{tr}_m^n(h_1Z) \neq 0$. From the remark after Lemma 2.1, $\mathrm{tr}_m^n(h_1Z) = 0$ if and only if $h_1Z \in \mathbb{K}$, equivalently if $Z \in h_1^{-1}\mathbb{K}$. If $h_1^{-1} \notin \mathcal{T}_1$, it can be uniquely written as ah^* such that $a \in \mathbb{K}$ and $h^* \in \mathcal{T}_1$. In this case $h_1^{-1}\mathbb{K} = h^*\mathbb{K}$. This relationship defines an equivalence.

Definition 4.1. *We say that $g_1 \sim g_2$ for some $g_1, g_2 \in \mathbb{F}$, if $g_1\mathbb{K} = g_2\mathbb{K}$.*

Therefore in (4.2) we can write h^* instead of h_1^{-1} and assume that $h^* \in \mathcal{T}_1$.

$$q \sum_{A \in g_1\mathbb{K}} \sum_{X \in \mathbb{F}} \sum_{Z \in h^*\mathbb{K}} \chi\left(A(F(X) + F(X+Z))\right))$$

which gives us a new equation:

$$\sum_{A\in g_1\mathbb{K}}\sum_{X\in\mathbb{F}}\sum_{Z\in h^*\mathbb{K}}\chi\left(A(F(X)+F(X+Z))\right))=q^3$$
$$\sum_{a,z\in\mathbb{K}}\sum_{X\in\mathbb{F}}\chi\left(ag_1(F(X)+F(X+zh^*))\right))=q^3$$

Now we will substitute zY for X. We can do this because for $z\neq 0$ it is a permutation and for $z=0$ we are replacing $F(X)+F(X+0\cdot h^*)$ with $F(0\cdot Y)+F(0\cdot Y+0\cdot h^*)$, which both equal 0 and therefore the sum does not change. This substitution gives us following:

$$\sum_{a,z\in\mathbb{K}}\sum_{Y\in\mathbb{F}}\chi\left(g_1az^3(F(Y)+F(Y+h^{-1}))\right)=q^3$$
$$\sum_{a,z\in\mathbb{K}}\sum_{Y\in\mathbb{F}}(-1)^{\mathrm{tr}_1^m\left(az^3\,\mathrm{tr}_m^n(g_1(F(Y)+F(Y+h^*)))\right)}=q^3$$

Suppose that

$$\mathrm{tr}_m^n\left(g_1(F(Y)+F(Y+h^*))\right)=\begin{cases}0, & \text{for } k \text{ elements } Y\in\mathbb{F},\\ \text{non-zero value}, & \text{for } q^2-k \text{ elements } Y\in\mathbb{F}.\end{cases}$$

Denote $\tau_Y=\mathrm{tr}_m^n\left(g_1(F(Y)+F(Y+h^*))\right)$ and $\mathcal{J}=\{Y\in\mathbb{F}:\tau_Y\neq 0\}$. Notice that $|\mathcal{J}|=q^2-k$ and $|\mathbb{F}\setminus\mathcal{J}|=k$. We can now rewrite the left hand side:

$$\sum_{Y\notin\mathcal{J}}\sum_{a,z\in\mathbb{K}}(-1)^{\mathrm{tr}_1^m(0)}+\sum_{Y\in\mathcal{J}}\sum_{a,z\in\mathbb{K}}(-1)^{tr_1^m(az^3\tau_Y)}=kq^2+\sum_{Y\in\mathcal{J}}\sum_{z\in\mathbb{K}}\sum_{a\in\mathbb{K}}(-1)^{tr_1^m(a(z^3\tau_Y))}.$$

We know that

$$\sum_{a\in\mathbb{K}}(-1)^{tr_1^m(a(z^3\tau_Y))}=\begin{cases}q, & \text{if } z^3\tau_Y=0,\\ 0, & \text{otherwise.}\end{cases}$$

Since in this case $\tau_Y\neq 0$, the sum is non-zero only if $z^3=0$, which is equivalent to $z=0$ since $\mathbb{K}$ is a field. We get equation

$$\begin{aligned}kq^2+(q^2-k)q&=q^3\\ kq^2+q^3-kq&=q^3\\ kq(q-1)&=0.\end{aligned}$$

From the definition, $q>1$ and therefore the only solution is $k=0$. This means that we have to find g_1,h_1 such that $g_1(F(Y)+F(Y+h^*))$ is not in $\mathbb{K}$ for any $Y\in\mathbb{F}$.

Values of g_1 and h^* cannot be both equal 1 since $g_1(F(Y)+F(Y+h^*))$ would be in $\mathbb{K}$ whenever Y is in $\mathbb{K}$. If g_1 and h^* are in $\mathcal{T}_1\setminus\{1\}$, they can be written in the form $g_1=g+\beta$ and $h^*=g+\alpha$, where $g\in\mathcal{T}_1\setminus\{1\}$ and $\alpha,\beta\in\mathbb{K}$. Y from our equation then can be written as $Y=xg+y$, where $x,y\in\mathbb{K}$. Since $g_1\neq h_1$, we have three cases. If $g_1,h_1\neq 1$, we have equation

$$(g+\beta)\left(F(xg+y)+F(xg+y+g+\alpha)\right),\tag{4.3}$$

if $h_1 = h_1^{-1} = h^* = 1$, we have

$$(g+\beta)\left(F(xg+y)+F(xg+y+1)\right), \tag{4.4}$$

and if $g_1 = 1$, we get

$$(F(xg+y)+F(xg+y+g+\alpha)) \tag{4.5}$$

Now we will solve each of these cases separately.

4.1 Expression (4.4)

Let us start with (4.4). We will expand it using (3.3):

$$\begin{aligned}
(g+\beta)\left(F(xg+y)+F(xg+y+1)\right) &= (g+\beta)\left(D_1F(xg+y)+F(1)\right)\\
&= (g+\beta)((xg+y)(1+c)+(x^2g^2+y^2)(1+d)+(xg+x+y)(b+d)\\
&+ (x^2g^2+x^2+y^2)(b+c)+1+b+c+d)\\
&= (g+\beta)(g^2x^2\Delta+gx\Delta+x^2(b+c)+x(b+d)+y^2\Delta+y\Delta+\Delta)\\
&= g^3x^2\Delta+g^2(x\Delta+\beta x^2\Delta)+g(x^2\Gamma+x\Lambda+\Delta(y^2+y+1)+\beta x\Delta)\\
&+ \beta x^2(b+c)+\beta x(b+d)+\beta\Delta(y^2+y+1)
\end{aligned}$$

We can notice that last three terms are all in $\mathbb{K}$ and therefore if the whole expression is in $\mathbb{K}$ or not is not affected by their value and we will not write terms that are in $\mathbb{K}$ explicitly from now on. Using S and T defined in previous chapter, we can write $g^3 = Sg+T$ and $g^2 = g+T$ and we get:

$$\begin{aligned}
&g(S\Delta x^2+\Delta x+\beta x^2\Delta+x^2\Gamma+x\Lambda+\Delta(y^2+y+1)+\beta x\Delta)+\text{terms in }\mathbb{K}\\
&= g\left(x^2(\Delta S+\Delta\beta+b+c)+x(1+c+\beta\Delta)+\Delta(y^2+y+1)\right)+\text{terms in }\mathbb{K}.
\end{aligned}$$

This expression is never in $\mathbb{K}$ if and only if the expression in parentheses is never 0, equivalently, if equation

$$x^2(\Delta S+\Delta\beta+b+c)+x(1+c+\beta\Delta)=\Delta(y^2+y+1) \tag{4.6}$$

has no solution for $x, y \in \mathbb{K}$. We will denote $A = \Delta S+\Delta\beta+b+c$ and $B = 1+c+\beta\Delta$. If one of them is equal 0 and the other one is non-zero, the function on the left hand side is a permutation and therefore the equation has always a solution. If both are zero and m is even, we get equation

$$0=\Delta(y^2+y+1),$$

which always has a solution since y^2+y+1 has a root ω in $\mathbb{F}_q$, where ω is a generator of $\mathbb{F}_4 \leq \mathbb{F}_q$.

If m is odd, $\omega \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and according to Lemma 2.3, $\omega^q = \omega^{q \bmod 3} = \omega^2 = \omega+1$, which means that $\omega \in \mathcal{T}_1 \setminus \{1\}$. Since g was chosen as an arbitrary element of $\mathcal{T}_1 \setminus \{1\}$, we can assume that $g = \omega$. In this case $S_\omega = \omega^2+\omega+1 = 0$. If both A and B are zero, we get the same equation

$$0=\Delta(y^2+y+1),$$

but this time $y^2+y+1=0$ has no solution in $\mathbb{F}_q$. Therefore if $A=\Delta\beta+b+c=0$, $B=1+c+\Delta\beta=0$ and $\Delta\neq 0$, our equation (4.6) has no solution for $x,y\in\mathbb{F}_q$. This can happen only if $\Delta\neq 0$ and

$$\beta=\frac{b+c}{\Delta}=\frac{1+c}{\Delta},$$

which means that $b=1$ and $\Delta=c+d$. This gives us a very specific condition - if m is odd, $c+d\neq 0$ and $b=1$, we have solution

$$\left(\omega+\frac{1+c}{c+d},1\right). \tag{4.7}$$

If A and B are both non-zero, we can rewrite left hand side of equation (4.6). Since $x\to\frac{B}{A}x$ is a linear permutation,

$$\mathrm{Im}(Ax^2+Bx)=\mathrm{Im}\left(A\frac{B^2}{A^2}x^2+B\frac{B}{A}x\right)=\mathrm{Im}\left(\frac{B^2}{A}(x^2+x)\right).$$

Equation (4.6) has a solution if and only if equation

$$\frac{B^2}{A}(x^2+x)=\Delta(y^2+y+1)$$

has a solution. If Δ is 0, the equation always has solution $(0,y)$ and if m is even, we have solution $(0,\omega)$. Therefore we will now consider only m odd, $\Delta\neq 0$ and $g=\omega$. We can see that images of functions on both sides of the equation are affine hyperplanes in $\mathbb{K}$. If we denote $H=\mathrm{Im}\left(\frac{B^2}{A}(x^2+x)\right)$, Lemma 2.6 yields that the equation has no solution if and only if $\mathrm{Im}\left(\Delta(y^2+y+1)\right)=\bar{H}$, which is equivalent to

$$\begin{aligned}
\frac{B^2}{A}&=\Delta\\
\frac{1+c^2+\Delta^2\beta^2}{b+c+\Delta\beta}&=\Delta\\
1+c^2+\Delta^2\beta^2&=\Delta(b+c)+\Delta^2\beta\\
\Delta^2(\beta^2+\beta)&=1+c^2+\Delta(b+c)\\
\beta^2+\beta&=\frac{1+c^2+\Delta(b+c)}{\Delta^2}.
\end{aligned} \tag{4.8}$$

This means that if m is odd, $\Delta\neq 0$ and

$$\mathrm{tr}_1^m\left(\frac{1+c^2+\Delta(b+c)}{\Delta^2}\right)=0,$$

there are exactly 2 values β such that $(\omega+\beta,1)$ is a solution of equation (4.1). Now we have to check that for these solutions $A\neq 0$ and $B\neq 0$. $A=0$ means that $\beta=(b+c)/\Delta$ and since we assume that it is a solution of (4.8),

$$\begin{aligned}
\left(\frac{b+c}{\Delta}\right)^2+\frac{b+c}{\Delta}&=\frac{1+c^2+\Delta(b+c)}{\Delta^2}\\
\frac{(b+c)^2+\Delta(b+c)}{\Delta^2}&=\frac{1+c^2+\Delta(b+c)}{\Delta^2}\\
b^2+c^2&=1+c^2\\
b&=1.
\end{aligned}$$

If $b = 1$, then $\beta = (1+c)/(c+d)$ and $B = 1 + c + (c+d)\frac{1+c}{c+d} = 0$, which coincides with the solution (4.7). Now we see that the first solution is a special case of the second, since for $b = 1$ the trace looks like

$$\mathrm{tr}_1^m\left(\frac{1+c^2+\Delta(1+c)}{\Delta^2}\right) = \mathrm{tr}_1^m\left(\left(\frac{1+c}{\Delta}\right)^2 + \frac{1+c}{\Delta}\right) = 0.$$

In conclusion, there is no β such that expression (4.4) is always in $\mathbb{F} \setminus \mathbb{K}$ for m even. For m odd, if $\Delta = 1 + b + c + d \neq 0$ and

$$\mathrm{tr}_1^m\left(\frac{1+c^2+\Delta(b+c)}{\Delta^2}\right) = 0,$$

there are two solutions $(\omega + \beta, 1)$ such that β is a solution of equation

$$\beta^2 + \beta = \frac{1+c^2+\Delta(b+c)}{\Delta^2};$$

for which expression (4.4) is in $\mathbb{F} \setminus \mathbb{K}$ for every $x, y \in \mathbb{K}$. If $b = 1$, one of this solutions is $(\omega + (1+c)/(c+d), 1)$.

Theorem 4.3 (Solutions of (4.1) of type $(g_1, 1)$)**.** *If m is even, equation (4.1) has no solution $(g_1, 1)$, $g_1 \in \mathcal{T}_1$.*
If m is odd, $\Delta \neq 0$ and

$$\mathrm{tr}_1^m\left(\frac{1+c^2+\Delta(b+c)}{\Delta^2}\right) = 0,$$

equation (4.1) has exactly two solutions $(\omega+\beta_1, 1)$ and $(\omega+\beta_2, 1)$ such that β_1, β_2 are solutions of

$$\beta^2 + \beta = \frac{1+c^2+\Delta(b+c)}{\Delta^2}.$$

Equation (4.1) has no solution of the form $(g_1, 1)$ otherwise.

4.2 Expression (4.5)

Now we can move on to expression (4.5). If we use SageMath software to expand the expression, we get:

$$\begin{aligned}
&\alpha bg^2x^2 + \alpha cg^2x^2 + \alpha dg^2x^2 + bg^3x^2 + cg^3x^2 + dg^3x^2 + \alpha^2bgx + \alpha^2cgx + \alpha^2dgx \\
&+ bg^3x + cg^3x + dg^3x + \alpha g^2x^2 + bg^2x^2 + dg^2x^2 + g^3x^2 + \alpha^3b + \alpha^3c + \alpha^3d \\
&+ \alpha^2bg + \alpha^2cg + \alpha^2dg + \alpha bg^2 + \alpha cg^2 + \alpha dg^2 + bg^3 + cg^3 + dg^3 + \alpha^2bx + \alpha^2dx \\
&+ \alpha^2gx + bg^2x + dg^2x + g^3x + \alpha bx^2 + \alpha cx^2 + bgx^2 + cgx^2 + \alpha^2by + \alpha^2cy \\
&+ \alpha^2dy + bg^2y + cg^2y + dg^2y + \alpha by^2 + \alpha cy^2 + \alpha dy^2 + bgy^2 + cgy^2 + dgy^2 + \alpha^3 \\
&+ \alpha^2b + \alpha^2d + \alpha^2g + \alpha g^2 + bg^2 + dg^2 + g^3 + bgx + cgx + bx^2 + \alpha^2y + g^2y \\
&+ \alpha y^2 + by^2 + dy^2 + gy^2 + \alpha b + \alpha c + bg + cg + bx + by + cy + b \\
&= g^3\Delta(x^2+x+1) + g^2(\alpha\Delta x^2 + \alpha\Delta + \Delta y + (b+d)(x^2+x+1)) \\
&+ g(\alpha^2\Delta x + \alpha^2\Delta + \Delta y^2 + (b+c)(x^2+x+1)) + \alpha^3\Delta + \alpha^2(b+d)(x+1) \\
&+ \alpha^2y\Delta + \alpha y^2\Delta + b(x^2+x+1) + (b+c)y + (b+d)y^2 + \alpha(b+c)(x^2+1).
\end{aligned} \tag{4.9}$$

Now we can omit terms in $\mathbb{K}$ and substitute $g^3 = Sg + T$ and $g^2 = g + T$ again.

$$\begin{aligned}&(Sg+T)\Delta(x^2+x+1)+(g+T)(\alpha\Delta x^2+\alpha\Delta+\Delta y+(b+d)(x^2+x+1))\\&+g(\alpha^2\Delta x+\alpha^2\Delta+\Delta y^2+(b+c)(x^2+x+1))\\&=g(S\Delta(x^2+x+1)+\alpha\Delta x^2+\alpha\Delta+\Delta y+(b+d)(x^2+x+1)+\alpha^2\Delta x+\alpha^2\Delta\\&+\Delta y^2+(b+c)(x^2+x+1))+\text{terms in }\mathbb{K}.\end{aligned}$$

This is in $\mathbb{F} \setminus \mathbb{K}$ for every $x, y \in \mathbb{K}$ if and only if equation

$$(x^2+x+1)(\Delta S+c+d)+\alpha^2\Delta(x+1)+\alpha\Delta(x^2+1)+\Delta(y^2+y)=0$$

has no solution (x, y), $x, y \in \mathbb{K}$. This equation can be rewritten as

$$x^2(\Delta S+c+d+\alpha\Delta)+x(\Delta S+c+d+\alpha^2\Delta)+\Delta S+c+d+\Delta(\alpha^2+\alpha)=\Delta(y^2+y)$$

If $\Delta = 0$, the equation is

$$(c+d)(x^2+x+1)=0.$$

If m is even, the equation has solutions (ω, y), where $y \in \mathbb{K}$ and ω is a generator of $\mathbb{F}_4$ for every α. If m is odd and $c \neq d$, the left hand side is always non-zero and the equation does not have a solution for any α. This means that for m odd, $c \neq d$ and $\Delta = 0$, the expression (4.5) is always in $\mathbb{F} \setminus \mathbb{K}$ for every $\alpha \in \mathbb{K}$.

Now we will assume that $\Delta \neq 0$. We will denote $A(\alpha) = \Delta S + c + d + \alpha\Delta$ and $B(\alpha) = \Delta S + c + d + \alpha^2\Delta$. If either $A(\alpha) = 0$ or $B(\alpha) = 0$, which is equivalent to $\alpha = (\Delta S + c + d)/\Delta$ or $\alpha^2 = (\Delta S + c + d)/\Delta$, then function on the left hand is a permutation and there is always a solution.

If both $A(\alpha) = 0$ and $B(\alpha) = 0$, then

$$\alpha = \alpha^2 = \frac{\Delta S + c + d}{\Delta}.$$

Thus

$$\frac{\Delta S + c + d}{\Delta} = \left(\frac{\Delta S + c + d}{\Delta}\right)^2$$

which implies that $\alpha = (\Delta S + c + d)/\Delta$ is equal to 0 or 1 and this is equivalent to $\Delta S + c + d = 0$ or $\Delta S + c + d = \Delta$. Our equation looks like

$$\begin{aligned}\Delta S + c + d + \Delta(\alpha^2 + \alpha) &= \Delta(y^2 + y)\\ \Delta S + c + d &= \Delta(y^2 + y).\end{aligned}$$

If $\Delta S + c + d = 0$, we get

$$0 = \Delta(y^2 + y),$$

which always has a solution. If $\Delta S + c + d = \Delta$, the equation is

$$\begin{aligned}\Delta &= \Delta(y^2 + y)\\ 0 &= \Delta(y^2 + y + 1),\end{aligned}$$

which has a solution if and only if m is even. If m is odd, there is no solution of this equation. $\alpha = 1$ is equivalent to $\Delta S + c + d = \Delta$, which means that $S = g^2 + g + 1 = (1 + b)/\Delta$. If

$$\mathrm{tr}_1^m\left(\frac{1+b}{\Delta}\right) = 0,$$

there are two solutions g such that $S_g = (1 + b)/\Delta$, which gives us two solutions of (4.1), where $h_1 \sim (g + 1)^{-1}$ and $g_1 = 1$.

Now we will assume that $A(\alpha)$ and $B(\alpha)$ are non-zero. Using the same method as in previous case we can say that since

$$\mathrm{Im}(A(\alpha)x^2 + B(\alpha)x) = \mathrm{Im}\left(\frac{B^2(\alpha)}{A(\alpha)(x^2+x)}\right),$$

our equation has a solution if and only if equation

$$\frac{B^2(\alpha)}{A(\alpha)}(x^2 + x) + \Delta S + c + d + \Delta(\alpha^2 + \alpha) = \Delta(y^2 + y)$$

has a solution. Images of both sides are hyperplanes, therefore the equation has no solution if and only if they are complements. Since image of the right hand side is $H_{\Delta^{-1}}$, we need the image of the left hand side to be equal $\overline{H}_{\Delta^{-1}}$, which means

$$\frac{B^2(\alpha)}{A(\alpha)} = \Delta$$

and $\Delta S+c+d+\Delta(\alpha^2+\alpha) \in \overline{H}_{\Delta^{-1}}$, in other words, $\mathrm{tr}_1^m\left(S + \Delta^{-1}(c + d) + (\alpha^2 + \alpha)\right) = 1$. The first condition can be rewritten as

$$\begin{aligned}
\frac{\Delta^2 S^2 + c^2 + d^2 + \alpha^4\Delta^2}{\Delta S + c + d + \alpha\Delta} &= \Delta \\
\Delta^2 S^2 + c^2 + d^2 + \alpha^4\Delta^2 &= \Delta^2 S + \Delta(c + d) + \Delta^2\alpha \\
\Delta^2(\alpha^4 + \alpha) &= \Delta^2(S^2 + S) + (c + d)(1 + b) \\
\alpha^4 + \alpha &= S^2 + S + \frac{(c+d)(1+b)}{\Delta^2}.
\end{aligned}$$

Since $\mathrm{tr}_1^m(\alpha^4 + \alpha) = 0$ this equation has a solution if and only if

$$\mathrm{tr}_1^m\left(S^2 + S + \frac{(c+d)(1+b)}{\Delta^2}\right) = \mathrm{tr}_1^m\left(\frac{(c+d)(1+b)}{\Delta^2}\right) = 0.$$

If for such a solution α

$$\mathrm{tr}_1^m\left(S + \Delta^{-1}(c + d) + (\alpha^2 + \alpha)\right) = 1$$

and $A(\alpha)$ and $B(\alpha)$ are non-zero, then for h_1 such that $h_1 \sim (g + \alpha)^{-1}$, $(1, h_1)$ is a solution of (4.1).

Theorem 4.4 (Solutions of (4.1) of type $(1, h_1)$)**.** *If m is odd, $c \neq d$ and $\Delta = 0$, every $(1, h)$, $h \in \mathcal{T}_1 \setminus \{1\}$ is a solution of* (4.1).

If m is odd, $\Delta \neq 0$ and

$$\mathrm{tr}_1^m\left(\frac{1+b}{\Delta}\right) = 0,$$

there are two solutions g, g' of equation

$$S_g = g^2 + g + 1 = \frac{1+b}{\Delta}$$

which give us two solutions of equation (4.1) - $(1, h_1)$ *and* $(1, h_1')$ *such that* $h_1 \sim (g+1)^{-1}$ *and* $h_1' \sim (g'+1)^{-1}$.

If

$$\mathrm{tr}_1^m\left(\frac{(c+d)(1+b)}{\Delta^2}\right) = 0,$$

for some fixed $g \in \mathcal{T}_1 \setminus \{1\}$ *we have two solutions* α_1 *and* α_2 *of equation*

$$\alpha^4 + \alpha = S^2 + S + \frac{(c+d)(1+b)}{\Delta^2}.$$

If for some $i \in \{1, 2\}$

$$\mathrm{tr}_1^m\left(S + \Delta^{-1}(c+d) + (\alpha^2 + \alpha)\right) = 1,$$

and $A(\alpha_i)$ *and* $B(\alpha_i)$ *are non-zero, then for* $h \sim (g+\alpha_i)^{-1}$ $(1, h)$ *is a solution of equation* (4.1).

Equation (4.1) *has no solution of the form* $(1, h_1)$ *otherwise.*

4.3 Expression (4.3)

We can expand (4.3) by multiplying (4.9) by $(g+\beta)$. Since we are only interested if this expression is in $\mathbb{F} \setminus \mathbb{K}$, we will ignore term that are in $\mathbb{K}$.

$$\begin{aligned}
&(g+\beta)(g^3\Delta(x^2+x+1) + g^2(\alpha\Delta x^2 + \alpha\Delta + \Delta y + (b+d)(x^2+x+1)) \\
&\quad + g(\alpha^2\Delta x + \alpha^2\Delta + \Delta y^2 + (b+c)(x^2+x+1)) + \alpha^3\Delta + \alpha^2(b+d)(x+1) \\
&\quad + \alpha^2 y\Delta + \alpha y^2\Delta + b(x^2+x+1) + (b+c)y + (b+d)y^2 + \alpha(b+c)(x^2+1)) \\
&\quad = g^4\Delta(x^2+x+1) \\
&\quad + g^3(\beta\Delta(x^2+x+1) + \alpha\Delta x^2 + \alpha\Delta + \Delta y + (b+d)(x^2+x+1)) \\
&\quad + g^2(\alpha\beta\Delta x^2 + \alpha\beta\Delta + \beta\Delta y + \beta(b+d)(x^2+x+1) + \alpha^2\Delta x + \alpha^2\Delta + \Delta y^2 \\
&\qquad + (b+c)(x^2+x+1)) \\
&\quad + g(\beta\alpha^2\Delta x + \beta\alpha^2\Delta + \beta\Delta y^2 + \beta(b+c)(x^2+x+1) + \alpha^3\Delta + \alpha^2(b+d)(x+1) \\
&\qquad + \alpha^2 y\Delta + \alpha y^2\Delta + b(x^2+x+1) + (b+c)y + (b+d)y^2 + \alpha(b+c)(x^2+1)) \\
&\qquad + \text{ terms in } \mathbb{K}.
\end{aligned}$$

As in previous cases, we will substitute $g^2 = g + T$ and $g^3 = Sg + T$. Since

$$g^4 = (g^2)^2 = g^2 + T^2 = g + T + T^2,$$

we can substitute it as well. We get

$$\begin{aligned}
&g(\Delta(x^2+x+1) + S\beta\Delta(x^2+x+1) + S\alpha\Delta x^2 + S\alpha\Delta + S\Delta y \\
&\quad + S(b+d)(x^2+x+1) + \alpha\beta\Delta x^2 + \alpha\beta\Delta + \beta\Delta y + \beta(b+d)(x^2+x+1) \\
&\quad + \alpha^2\Delta x + \alpha^2\Delta + \Delta y^2 + (b+c)(x^2+x+1) + \beta\alpha^2\Delta x + \beta\alpha^2\Delta + \beta\Delta y^2 \\
&\quad + \beta(b+c)(x^2+x+1) + \alpha^3\Delta + \alpha^2(b+d)(x+1) + \alpha^2 y\Delta + \alpha y^2\Delta \\
&\quad + b(x^2+x+1) + (b+c)y + (b+d)y^2 + \alpha(b+c)(x^2+1)) + \text{ terms in } \mathbb{K}.
\end{aligned}$$

For some α and β, this is always in $\mathbb{F}\setminus\mathbb{K}$ if and only if the expression in parentheses is non-zero for every $x, y \in \mathbb{K}$. We can rewrite the expression in the following way:

$$\begin{aligned}
&x^2(\Delta + S\beta\Delta + S\Delta\alpha + S(b+d) + \alpha\beta\Delta + \beta(b+d) + b + c + \beta(b+c) \\
&\quad + b + \alpha(b+c)) \\
&+ x(\Delta + S\beta\Delta + S(b+d) + \beta(b+d) + \alpha^2\Delta + b + c + \alpha^2\beta\Delta \\
&\quad + \beta(b+c) + \alpha^2(b+d) + b) \\
&+ \Delta + S\beta\Delta + S\Delta\alpha + S(b+d) + \alpha\beta\Delta + \beta(b+d) + \alpha^2\Delta + b + c + \alpha^2\beta\Delta \\
&\quad + \beta(b+c) + \alpha^3\Delta + \alpha^2(b+d) + b + \alpha(b+c) \\
&+ y^2(\Delta + \beta\Delta + \alpha\Delta + b + d) + y(\Delta S + \Delta\beta + \alpha^2\Delta + b + c) \\
&= x^2(S(\Delta\beta + \Delta\alpha + b + d) + \alpha(b+c) + \beta(c+d) + \alpha\beta\Delta + 1 + b + d) \\
&+ x(S(\Delta\beta + b + d) + \alpha^2(1+c) + \beta(c+d) + \alpha^2\beta\Delta + 1 + b + d) \\
&+ S(\Delta\beta + \Delta\alpha + b + d) + \alpha^3\Delta + \alpha^2(\beta\Delta + b + d) + \alpha\beta\Delta + \alpha^2\Delta + \alpha(b+c) \\
&\quad + \beta(c+d) + 1 + b + d \\
&+ y^2(\Delta\alpha + \Delta\beta + 1 + c) + y(\Delta S + \Delta\beta + \alpha^2\Delta + b + c)
\end{aligned}$$

We can denote

$$\begin{aligned}
A(\alpha,\beta) &= S(\Delta\beta + \Delta\alpha + b + d) + \alpha(b+c) + \beta(c+d) + \alpha\beta\Delta + 1 + b + d \\
B(\alpha,\beta) &= S(\Delta\beta + b + d) + \alpha^2(1+c) + \beta(c+d) + \alpha^2\beta\Delta + 1 + b + d \\
C(\alpha,\beta) &= S(\Delta\beta + \Delta\alpha + b + d) + \alpha^3\Delta + \alpha^2(\beta\Delta + b + d) + \alpha(b+c) + \alpha\beta\Delta \\
&\quad + \alpha^2\Delta + \beta(c+d) + 1 + b + d \\
D(\alpha,\beta) &= \Delta\alpha + \Delta\beta + 1 + c \\
E(\alpha,\beta) &= \Delta S + \Delta\beta + \alpha^2\Delta + b + c.
\end{aligned} \tag{4.10}$$

Now we are looking for α, β such that equation

$$A(\alpha,\beta)x^2 + B(\alpha,\beta)x + C(\alpha,\beta) = D(\alpha,\beta)y^2 + E(\alpha,\beta)y$$

has no solution (x, y).

If exactly one of $A(\alpha,\beta)$ and $B(\alpha,\beta)$ is zero or exactly one of $D(\alpha,\beta)$ and $E(\alpha,\beta)$ is zero, we have a permutation on at least one side of our equation and therefore it always has a solution.

If $A(\alpha,\beta) = B(\alpha,\beta) = D(\alpha,\beta) = E(\alpha,\beta) = 0$, then the equation has no solution if and only if $C(\alpha,\beta) \neq 0$.

If $E(\alpha,\beta) = D(\alpha,\beta) = 0$ and $A(\alpha,\beta), B(\alpha,\beta)$ are non-zero, the image of the left hand side is a hyperplane, which is the same as hyperplane

$$\mathrm{Im}\left(\frac{B^2(\alpha,\beta)}{A(\alpha,\beta)}(x^2+x)\right).$$

Therefore the equation has a solution if and only if

$$\begin{aligned}
\frac{B^2(\alpha,\beta)}{A(\alpha,\beta)}(x^2+x) &= C(\alpha,\beta) \\
(x^2+x) &= \frac{A(\alpha,\beta)C(\alpha,\beta)}{B^2(\alpha,\beta)}
\end{aligned}$$

has a solution, which is equivalent to

$$\mathrm{tr}_1^m\left(\frac{A(\alpha,\beta)C(\alpha,\beta)}{B^2(\alpha,\beta)}\right)=0.$$

Therefore if

$$\mathrm{tr}_1^m\left(\frac{A(\alpha,\beta)C(\alpha,\beta)}{B^2(\alpha,\beta)}\right)=1,$$

$E(\alpha,\beta)=D(\alpha,\beta)=0$ and $A(\alpha,\beta), B(\alpha,\beta)$ are non-zero, then there is a solution of (4.1).

If $A(\alpha,\beta)=B(\alpha,\beta)=0$ and $D(\alpha,\beta), E(\alpha,\beta)$ are non-zero, then the image of the right hand side is a hyperplane equal to a hyperplane

$$\mathrm{Im}\left(\frac{E^2(\alpha,\beta)}{D(\alpha,\beta)}(y^2+y)\right).$$

In this case the equation has a solution if and only if

$$C(\alpha,\beta)=\frac{E^2(\alpha,\beta)}{D(\alpha,\beta)}(y^2+y)$$
$$y^2+y=\frac{C(\alpha,\beta)D(\alpha,\beta)}{E^2(\alpha,\beta)}$$

has a solution. This has no solution if

$$\mathrm{tr}_1^m\left(\frac{C(\alpha,\beta)D(\alpha,\beta)}{E^2(\alpha,\beta)}\right)=1.$$

In that case, there is a solution of an equation (4.1).

Finally, if $A(\alpha,\beta), B(\alpha,\beta), D(\alpha,\beta)$ and $E(\alpha,\beta)$ are all non-zero, images of both sides are hyperplanes and the equation has a solution if and only if

$$\frac{B^2(\alpha,\beta)}{A(\alpha,\beta)}(x^2+x)+C(\alpha,\beta)=\frac{E^2(\alpha,\beta)}{D(\alpha,\beta)}(y^2+y)$$

has a solution. Using the same idea with images of both sides of equation as in previous section, we can say that this equation has no solution if and only if

$$\frac{B^2(\alpha,\beta)}{A(\alpha,\beta)}=\frac{E^2(\alpha,\beta)}{D(\alpha,\beta)}$$

and

$$\mathrm{tr}_1^m\left(\frac{A(\alpha,\beta)C(\alpha,\beta)}{B^2(\alpha,\beta)}\right)=1.$$

Theorem 4.5 (Solutions of (4.1) of type (g_1,h_1), $g_1,h_1\in\mathcal{T}_1\setminus\{1\}$)**.** *We define $A(\alpha,\beta)$, $B(\alpha,\beta)$, $C(\alpha,\beta)$, $D(\alpha,\beta)$ and $E(\alpha,\beta)$ as in* (4.10)*. For fixed g, $(\alpha+g,h_1)$ such that $(\alpha,\beta)\in\mathbb{K}^*\times\mathbb{K}^*$ and $h_1\sim(g+\beta)^{-1}$ is a solution of equation* (4.1) *if and only if at least one of the following conditions is satisfied:*

- $A(\alpha,\beta)=B(\alpha,\beta)=D(\alpha,\beta)=E(\alpha,\beta)=0$ *and* $C(\alpha,\beta)\neq 0$,

- *$D(\alpha,\beta)=E(\alpha,\beta)=0$, $A(\alpha,\beta)$ and $B(\alpha,\beta)$ are non-zero and*

$$\mathrm{tr}_1^m\left(\frac{A(\alpha,\beta)C(\alpha,\beta)}{B^2(\alpha,\beta)}\right)=1,$$

- *$A(\alpha,\beta)=B(\alpha,\beta)=0$, $D(\alpha,\beta)$ and $E(\alpha,\beta)$ are non-zero and*

$$\mathrm{tr}_1^m\left(\frac{C(\alpha,\beta)D(\alpha,\beta)}{E^2(\alpha,\beta)}\right)=1,$$

- *$A(\alpha,\beta)$, $B(\alpha,\beta)$, $D(\alpha,\beta)$ and $E(\alpha,\beta)$ are all non-zero,*

$$\frac{B^2(\alpha,\beta)}{A(\alpha,\beta)}=\frac{E^2(\alpha,\beta)}{D(\alpha,\beta)}$$

and

$$\mathrm{tr}_1^m\left(\frac{A(\alpha,\beta)C(\alpha,\beta}{B^2(\alpha,\beta)}\right)=1.$$

Conclusion

In this thesis, we determined which functions on $\mathbb{F}_{2^{2m}}$ of the form

$$F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2}$$

with $b, c, d \in \mathbb{F}_{2^m}$ are APN in Theorem 3.2. Which of them are CCZ-equivalent to a permutation of κ type can be identified by finding solutions of (4.1) using theorems 4.3, 4.4 and 4.5. All computations leading to results in Chapter 4 were checked using SageMath software and the source code is attached.

Since the expressions are quite complicated, we applied these results using computer on small fields $\mathbb{F}_{2^6}$ and $\mathbb{F}_{2^{10}}$. To perform the computations we used SageMath software again. The source code is attached to this thesis. Since m is in our case equal 3 or 5, which is an odd number, we implemented conditions in the right part of Table 3.2. We found 112 APN functions in $\mathbb{F}_{2^6}$ and 496 APN functions in $\mathbb{F}_{2^{10}}$.

In the second step, we implemented searching for permutations using Theorem 4.3, Theorem 4.4 and Theorem 4.5. Since m is odd in both cases, We can choose g to be the generator of $\mathbb{F}_4$, denoted ω. Choosing $g = \omega$ is very convenient, since

$$S_\omega = \omega^2 + \omega + 1 = 0,$$

which makes some computations easier and expressions A, B, C, D and E defined in 4.10 shorter. Since we are only interested in permutations that are also APN, we could simplify some conditions from Theorems 4.3-4.5. For example we did not need to check whether $\Delta = 1 + b + c + d$ is non-zero since according to the Table 3.2, $\Delta \neq 0$ for all APN functions. We have not implemented the first and second condition in Theorem 4.1 either because from Table 3.2 we know that $\Delta \neq 0$ and

$$\mathrm{tr}_1^m\left(\frac{1+b}{\Delta}\right) = 1$$

for every APN function on $\mathbb{F}_{2^{2m}}$, where m is odd.

In $\mathbb{F}_{2^6}$, we expected to find some APN permutations, since κ function is linearly equivalent to a function from our family. We found 84 APN permutations. List of them can be found in Appendix A. Unfortunately, according to our results, there are no APN permutations from our family in $\mathbb{F}_{2^{10}}$.

Combining conditions from chapters 3 and 4 algebraically new and possibly infinite families of APN permutations might be found. Since the expressions in the conditions are quite complicated, we were not able to combine them and it is one of the ideas for future work.

Another idea for more research might be trying to generalize these conditions to the family with $b, c, d \in \mathbb{F}_{2^{2m}}$ or choosing general Gold function instead of X^3, which would lead to a family of functions

$$F(X) = X^{2^k+1} + bX^{(2^k+1)q} + cX^{2^k q+1} + dX^{q+2^k},$$

on $\mathbb{F}_{2^{2m}}$ with $q = 2^m$, $\gcd(k, n) = 1$ and $b, c, d \in \mathbb{F}_{2^m}$. These families have some features similar to the family chosen in this thesis, for example, they satisfy the subspace property.

A. List of APN permutations in $\mathbb{F}_{2^6}$

Function $F(X) = X^3 + bX^{24} + cX^{17} + dX^{10}$ with $b, c, d \in \mathbb{F}_{2^3}$ on $\mathbb{F}_{2^6}$ is CCZ-equivalent to an APN permutation if and only if (b, c, d) is in the following set:

$\{(\alpha^2, 0, \alpha^4), (\alpha, \alpha^3, 1), (\alpha^6, \alpha, \alpha^6), (\alpha^5, \alpha^2, 0), (0, \alpha, \alpha^6), (\alpha^6, 0, \alpha), (\alpha^2, \alpha^4, \alpha^4),$
$(\alpha^4, 0, \alpha), (\alpha^3, 1, \alpha^5), (\alpha, \alpha^6, \alpha^6), (\alpha^6, \alpha^2, \alpha^6), (\alpha^6, \alpha^6, \alpha), (\alpha^4, \alpha^2, \alpha^4), (\alpha^6, \alpha^5, 0),$
$(0, \alpha^5, \alpha^5), (\alpha^2, \alpha^2, \alpha^2), (0, \alpha^5, \alpha^2), (\alpha^2, \alpha^5, \alpha^5), (\alpha^3, 1, 1), (\alpha^4, \alpha^4, \alpha^4), (\alpha, \alpha^2, 1),$
$(\alpha^3, \alpha^3, \alpha), (\alpha, \alpha^2, 0), (\alpha^2, \alpha^4, 1), (\alpha^6, \alpha^6, \alpha^2), (\alpha^6, \alpha^5, \alpha^5), (\alpha^2, \alpha^4, 0), (\alpha^3, \alpha^5, \alpha^4),$
$(\alpha^5, \alpha^3, 0), (\alpha^6, \alpha, \alpha), (0, \alpha, 1), (\alpha, \alpha^4, \alpha), (\alpha^5, \alpha^2, \alpha^5), (\alpha^2, \alpha, \alpha^2), (\alpha^5, \alpha^6, \alpha^2),$
$(\alpha, 1, \alpha^2), (0, \alpha^3, \alpha^3), (\alpha, \alpha, \alpha), (\alpha, 1, \alpha^3), (0, \alpha^3, \alpha^4), (\alpha^5, \alpha^5, \alpha^2), (0, \alpha^6, \alpha^6), (\alpha^5, 0, \alpha^2),$
$(\alpha^2, \alpha^4, \alpha), (\alpha^5, \alpha^3, \alpha^3), (\alpha^5, \alpha^5, \alpha^4), (0, \alpha^4, \alpha^3), (\alpha^4, 1, \alpha^5), (\alpha^3, \alpha, \alpha^3), (\alpha^2, \alpha^6, 1),$
$(\alpha^5, \alpha^4, \alpha^5), (\alpha^3, \alpha^4, \alpha^3), (\alpha^4, 1, \alpha), (\alpha^5, 1, 1), (0, \alpha^6, \alpha), (\alpha, \alpha^2, \alpha^4), (\alpha^3, \alpha^4, \alpha^4),$
$(\alpha^3, 0, \alpha^4), (0, \alpha^2, \alpha^5), (\alpha^6, 1, \alpha^3), (\alpha^6, \alpha, 0), (\alpha^4, \alpha, 1), (\alpha^6, 1, 1), (\alpha^2, 1, \alpha^4), (0, \alpha^4, 1),$
$(\alpha^4, \alpha, 0), (\alpha^2, 1, \alpha^6), (\alpha^6, \alpha^3, \alpha), (\alpha, 0, \alpha^2), (\alpha^4, \alpha^3, \alpha^3), (\alpha^4, \alpha^5, 1), (\alpha^3, \alpha^3, \alpha^4),$
$(\alpha^5, \alpha^2, \alpha^2), (\alpha^3, \alpha^6, 0), (\alpha, \alpha^2, \alpha^2), (\alpha^5, 1, \alpha^6), (\alpha, 0, \alpha^6), (\alpha^4, 0, \alpha^3), (\alpha^4, \alpha, \alpha),$
$(\alpha^3, \alpha^6, \alpha^6), (0, \alpha^2, 1), (\alpha^3, \alpha^4, 0), (\alpha^4, \alpha, \alpha^2), (\alpha^2, 0, \alpha^5)\},$

where α is a generator of $\mathbb{F}_{2^3}$ with minimal polynomial $x^3 + x + 1$.

Bibliography

[1] J. F. Dillon. APN Polynomials and Related Codes. *Workshop on Polynomials over Finite Fields and Their Applictions, Banff International Research Station(BIRS), Banff, Alberta, Canada*, 2006.

[2] X.-D. Hou. Affinity of Permutations on $\mathbb{F}_2^n$. *Discrete Applied Mathematics*, 154:313–325, 2006.

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN Permutation in Dimension Six. *Finite Fields. Theory and Applications.*, 2010.

[4] F. Göloğlu. Almost prefect nonlinear trinomials and hexanomials. *Finite Fields and Their Applications*, pages 258–282, 2015.

[5] C. Carlet. Vectorial Boolean Functions for Cryptography. *Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering"*, pages 398–469, 2010.

[6] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Publishing Company, 1977.