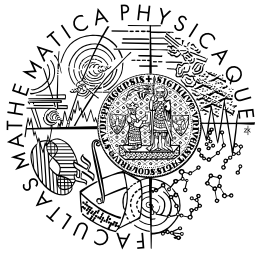

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Michal Maršálek

APN functions with non-classical Walsh spectra

Department of Algebra

Supervisor of the bachelor thesis:	Dr. rer. nat. Faruk Göloglu
Study programme:	Mathematics
Study branch:	Mathematics for Information Technologies

Prague 2019

I declare that I carried out this bachelor 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 ..... signature of the author

I would like to thank my supervisor, Dr. rer. nat. Faruk Gölogluu for introducing me to the topic and for a lot of patient explaining. I would like to thank my family for supporting me in my studies.

Title: APN functions with non-classical Walsh spectra

Author: Michal Maršálek

Department: Department of Algebra

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

Abstract: An interesting class of Boolean functions are APN functions - these functions are "as far" from linear functions as possible. Most of the quadratic APN functions have the same (=classical) Walsh spectrum - a sort of footprint of the function. The aim of this thesis is to describe a method which might lead to a generalisation of a sporadic example of a quadratic APN function with non-classical Walsh spectrum. Up until recently, it was believed that no such function exists. This was proven to be false in 2009, as an example of such function in dimension 6 was introduced. In this thesis, we describe the construction and then deduce necessary conditions for some free coefficients in order to reduce the search space to a level which enables a computer search.

Keywords: Boolean function, APN, non-classical spectrum, Walsh spectrum, Computer search

Contents

Introduction

One of the main tasks of cryptography is to enable two entities to communicate in a secret fashion, that is, if someone listens to their conversation, they are unable to find out what they are talking about. This is done by transforming the plaintext (the message) into a ciphertext and sending the ciphertext instead. Nowadays, both plaintext and ciphertext can be thought of as a sequence of bits - elements of $\mathbb{F}_2$. In order to make sure the cipher is secure, we need to study the properties of the functions we compose the cipher from. A function transforming a fixed length (dimension) string of bits to another fixed length string of bits and ones is called a Boolean function.

In the following pages, we will be describing a search for a Boolean function with particular properties. Linear transformations are very easy to understand and analyze (using linear algebra) and as such are usually not good for cryptographic purposes. On the other hand, just not being linear does not mean much for cryptographic suitability of a function. Using linear and differential cryptanalysis, one can "attack" a function if it is "close" to linear in some sense. The "further" a function is from being linear the better. Perfect nonlinearity of a function $\mathbb{F}_2^n \to \mathbb{F}_2^n$ (that is for any input difference we can get any output difference) is not possible due to the characteristic of 2 (addition is the same as subtraction).

The best we achieve is half of the output differences being possible. This is called almost perfect nonlinearity or APN for short. There are infinite families of APN functions (that is, there are known APN functions in an infinite number of dimensions). We can represent Boolean function in different ways, i. e. as a polynomial in the input bits. Most of the known APN functions are quadratic - that is the degree of this polynomial is 2.

A useful attribute of a Boolean function is what is called a Walsh transform and the corresponding Walsh spectrum of a function. Among other uses, the Walsh spectrum is invariant under some kind of equivalence on Boolean functions. Interestingly, for a long time, all known APN functions had the same (depending on the dimension) "classical" spectrum and it was conjectured that all APN functions do. However, in 2009 a sporadic example (meaning it is not an infinite family) in dimension 6 was introduced.

In this thesis, we will describe a construction of quadratic functions with non-classical spectra and we will try to understand the functions in this class and whether it's possible for a function in this class to be APN. Better understanding of such constructions might lead to finding another examples of APN functions with non-classical spectra or even an infinite family of such functions. In the following chapters, we deduce necessary conditions for the functions in order to be APN with a goal of making a computer search feasible. Furthermore, we prove that an infinite subclass of functions in this construction cannot be APN. At the end of the thesis we describe the computer searches we performed.

Preliminaries

In this chapter we will describe the basic theory of Boolean functions upon which the rest of this thesis is built. This chapter's sources are [1], [2] and [3] where the theory of Boolean functions can also be found in a greater depth.

Definition (Boolean function)**.** A Boolean function is a function $\mathbb{F}_2^n \to \mathbb{F}_2$.

Definition (Vectorial Boolean function)**.** A vectorial Boolean function is a function $\mathbb{F}_2^n \to \mathbb{F}_2^m$.

Definition (Coordinate function)**.** Let $F = (f_1, \ldots, f_m) : \mathbb{F}_2^n \to \mathbb{F}_2^m$. The functions $f_i : \mathbb{F}_n^2 \to \mathbb{F}_2$ are called coordinate functions of F.

Remark. The vectorspace $\mathbb{F}_2^n$ can be endowed with a structure of the field $\mathbb{F}_{2^n}$ as both are n-dimensional vectorspaces over $\mathbb{F}_2$. So we can represent a vectorial Boolean function $\mathbb{F}_2^n \to \mathbb{F}_2^n$ as a function $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ instead. In this form, the function can be conveniently described as a polynomial (according to the following theorem).

Theorem 1 (Lagrange's interpolation)**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then there exists an unique polynomial $p_f \in \mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$, such that $\forall x \in \mathbb{F}_{2^n} : f(x) = p_f(x)$.*

Proof. Existence: Let

$$l_a(x) := \prod_{b \in \mathbb{F}_{2^n} \setminus \{a\}} \frac{x + f(b)}{a + f(b)}$$

. Then $l_a(x) \in \{0, 1\}$ and $l_a(x) = 1 \iff a = x$. Let $p_f(x) := \sum_{a \in \mathbb{F}_{2^n}} f(a) l_a(x)$. Then $\forall x \in \mathbb{F}_{2^n} : f(x) = p_f(x)$.

Uniqueness: Let $p, q \in \mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$, such that $\forall x \in \mathbb{F}_{2^n} : f(x) = p(x) = q(x)$.
Let $r(x) = (p + q)(x)$. Then $\forall x \in \mathbb{F}_{2^n} : r(x) = p(x) + q(x) = 0$ and so r has 2^n roots. But since $\deg(r) \leq 2^n - 1$ it must be a zero polynomial. Therefore, $p = q$. □

Theorem 2 (Frobenius)**.** *The mappings $\sigma_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, 0 \leq i < n$ given by $\sigma_i(\alpha) = \alpha^{2^i}$ are distinct, and form all automorphisms of $\mathbb{F}_{2^n}$.*

Definition (Linearized polynomial)**.** We say a polynomial L is linearized if it is of the form $L(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ for some $a_i \in \mathbb{F}_{2^n}$.

Remark. The set of all linearized polynomials in $\mathbb{F}_{2^n}[x]$ correspond to the set of all linear functions $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Definition (Algebraic normal form)**.** Each function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be uniquely written down in a form $f(x_1, \ldots, x_n) = \sum_{I \subset \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$, where $a_I \in \mathbb{F}_2$, that is, as a polynomial from $\mathbb{F}_2[x_1, \ldots, x_n]$ where each x_i appears with exponents at most 1 (since $\forall b \in F_2 : b = b^2$). This representation is called the algebraic normal form of f.

Definition (Algebraic degree)**.** Algebraic degree of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the degree of its algebraic normal form.
Algebraic degree of a Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the maximum algebraic degree of its coordinate functions.

Remark. Functions with an algebraic degree of 1, are linear nonzero functions plus a constant.

Definition (Quadratic function)**.** We say a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is quadratic, if its algebraic degree is 2.

Lemma 3. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a quadratic function, $a \in \mathbb{F}_2^n$.*
Then $D_{f,a} : \mathbb{F}_2^n \to \mathbb{F}_2^m, x \mapsto f(x+a) + f(x) + f(a) + f(0)$ is a linear function.

Proof. A vectorial function is linear if and only if all its coordinate functions are linear. Let f_i be a coordinate function of f.
Using its Algebraic normal form, we can write

$$f_i(x_1, \ldots, x_n) = \sum_{0 \le i < n} A_i x_i + \sum_{0 \le i < j < n} B_{ij} x_i x_j + C.$$

Then

$$\begin{aligned} D_{f_i,a}(x) = f(x+a) + f(x) + f(a) + f(0) = \\ \sum_{0 \le i < n} A_i(x_i + a_i) + \sum_{0 \le i < j < n} B_{ij}(x_i + a_i)(x_j + a_j) + C + \\ + \sum_{0 \le i < n} A_i x_i + \sum_{0 \le i < j < n} B_{ij} x_i x_j + C + \\ + \sum_{0 \le i < n} A_i a_i + \sum_{0 \le i < j < n} B_{ij} a_i a_j + C + \\ + C = \sum_{0 \le i < j < n} B_{ij}(x_i a_j + a_i x_j) \end{aligned}$$

Therefore, $\forall x, y \in \mathbb{F}_2^n$, we have

$$\begin{aligned} D_{f_i,a}(x) + D_{f_i,a}(y) = \sum_{0 \le i < j < n} B_{ij}(x_i a_j + a_i x_j) + \sum_{0 \le i < j < n} B_{ij}(y_i a_j + a_i y_j) = \\ = \sum_{0 \le i < j < n} B_{ij}((x_i + y_i)a_j + a_i(x_j + y_j)) = D_{f_i,a}(x+y). \end{aligned}$$

□

Definition (Absolute trace)**.** A function

$$\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2, u \mapsto u + u^2 + u^{2^2} + \cdots + u^{2^{n-1}}$$

is called the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ or an absolute trace.

Remark. Trace is $\mathbb{F}_2$-linear, meaning that $\mathrm{Tr}(0) = 0$ and $\forall u, v \in \mathbb{F}_{2^n} : \mathrm{Tr}(u+v) = \sum_{i=0}^{n-1}(u+v)^{2^i} = \sum_{i=0}^{n-1} u^{2^i} + v^{2^i} = \mathrm{Tr}(u) + \mathrm{Tr}(v)$.

Definition (Relative trace)**.** Let $k \mid n$. A function

$$\mathrm{Tr}_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}, u \mapsto u + u^{2^k} + u^{2^{2k}} + \cdots + u^{2^{n/k-1}}$$

is called the relative trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$.

Remark. The relative trace is $\mathbb{F}_{2^k}$-linear, meaning that $\forall u, v \in \mathbb{F}_{2^n} : \mathrm{Tr}_k^n(u+v) = \sum_{i=0}^{n/k-1}(u+v)^{2^{ki}} = \sum_{i=0}^{n/k-1} u^{2^{ki}} + v^{2^{ki}} = \mathrm{Tr}_k^n(u) + \mathrm{Tr}_k^n(v)$ and
$\forall u \in \mathbb{F}_{2^n}, q \in \mathbb{F}_{2^k} \subset \mathbb{F}_{2^n} : \mathrm{Tr}_k^n(qu) = \sum_{i=0}^{n/k-1} q^{2^{ki}} u^{2^{ki}} = \sum_{i=0}^{n/k-1} qu^{2^{ki}} = q \cdot \mathrm{Tr}_k^n(u)$.
In another words, solutions to $\mathrm{Tr}_k^n(x) = 0$ are a vector subspace of $\mathbb{F}_{2^n}$.

Definition (Walsh transform)**.** A Walsh or Walsh-Hadamard transform of a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a function $\widehat{F} : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ defined by

$$\widehat{F}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + x \cdot u}$$

Remark. The products in the exponent in the previous definition are any scalar products and so for $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, we might use the trace:

$$\widehat{F}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathrm{Tr}_1^m(vF(x)) + \mathrm{Tr}_1^n(xu)}$$

Notation. By $\{*a^{\wedge\wedge k}, b*\}$ we denote a multiset where a has a multiplicity of k and b has a multiplicity of 1.

Definition (Walsh spectrum)**.** The multiset of all the values of a (vectorial) Boolean function F is called the Walsh spectrum of F, denoted $\mathcal{W}_F$.
$\mathcal{W}_F = \{*\widehat{F}(u, v); u \in \mathbb{F}_{2^m}, v \in \mathbb{F}_{2^n}*\}$

Proposition 4. *Let $n = 2m, f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m, F = (f, g) : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then $\mathcal{W}_f \subset \mathcal{W}_F$.*

Proof.

$$\widehat{f}(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot f(x) + x \cdot u} = \sum_{x \in \mathbb{F}_2^n} (-1)^{(v,0) \cdot (f(x), g(x)) + x \cdot u} = \widehat{F}(u, (v, 0))$$

□

Definition (Almost perfect nonlinearity)**.** A Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if, for every $a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n$ the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions.

Lemma 5. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Boolean function.*
Then f is APN $\iff \forall a \in \mathbb{F}_{2^n} : |\{f(x) + f(x + a) | x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$.

Proof. Let f be APN. Then $|\{f(x) + f(x + a) | x \in \mathbb{F}_{2^n}\}| =$
$|\{b \in \mathbb{F}_{2^n} : f(x) + f(x + a) = b \text{ has 2 solutions}\}| = 2^n/2 = 2^{n-1}$.
Let $|\{f(x) + f(x + a) | x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$.
Then for each $b \in |\{f(x) + f(x + a); x \in \mathbb{F}_{2^n}\}|$, the number of solutions of $f(x) + f(x + a) = b$ is $\leq 2^n/2^{n-1} = 2$. Since the number of solutions to
$f(x) + f(x + a) = b$ is even (if x is a solution, than $x + a$ is also a solution), it means, that f is APN. □

Proposition 6. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic Boolean function.*
Then f is APN $\iff$ $f(x)+f(x+a)+f(a) = 0$ has exactly 2 solutions $\forall a \in \mathbb{F}_{2^n}^*$.

Proof. According to Lemma 3, solutions to $f(x)+f(x+a)+f(a)+f(0) = 0$ form a vector subspace of $\mathbb{F}_{2^n}$. Therefore, for each $b \in \mathbb{F}_{2^n}$, the number of solutions of $f(x) + f(x + a) = b$ is either zero, or the same as the number of solutions of $f(x) + f(x + a) = f(a) + f(0)$. □

Theorem 7 ([3], page 161)**.**
Power mappings on $\mathbb{F}_{2^n}$, $x \mapsto x^d$ for the following exponents are APN.

Name	Exponents d	Conditions	Reference
Gold functions	$2^i + 1$	$\gcd(i, n) = 1$	[4]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[5]
Welch function	$2^k + 3$	$n = 2k + 1$	[6]
Niho function	$2^k + 2^{k/2} - 1$, k even $2^k + 2^{(3k+1)/2} - 1$, k odd	$n = 2k + 1$	[7]
inverse function	$2^{2k} - 1$	$n = 2k + 1$	[4]
Dobbertin function	$2^{4k} + 2^{3k} + 2^{2k} + 2^k - 1$	$n = 5k$	[8]

Remark. Mappings $x \mapsto x^3$ are always APN (for each n) as directly follows from the last theorem.

Remark. Most of the known APN functions are quadratic and most of them share the same "classical" Walsh spectrum.

Definition (Classical spectra)**.** We say that the Walsh spectrum of an APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is classical if it only contains values $\{0, \pm 2^m, \pm 2^{m+1}, 2^{2m}\}$ for even $n = 2m$ or $\{0, \pm 2^{m+1}, 2^{2m+1}\}$ for odd $n = 2m + 1$.

The only known quadratic function with non-classical spectrum was given in [9] for $m = 3$. In the following pages we will be investigating an approach that might lead to another example, in $m = 4$.

Remark. For $u \in \mathbb{F}_{2^n}$, by $1/u^i$ or u^{-i} we usually mean u^{2^n-1-i}.

Definition (Extended-affine equivalence)**.** We say that two Boolean functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are extended-affine (EA) equivalent, if there exist affine permutations $L_1, L_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an affine function $L_3 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $L_1 \circ F \circ L_2 + L_3 = G$.

Theorem 8. *Let $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be two EA equivalent Boolean functions. Then F is APN if and only if G is APN.*

Proof. G is APN $\iff$
$\forall a \in \mathbb{F}_{2^n}^* : |\{G(x) + G(x + a) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
$\forall a \in \mathbb{F}_{2^n}^* : |\{L_1 \circ F \circ L_2(x) + L_1 \circ F \circ L_2(x + a) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
$\forall a \in \mathbb{F}_{2^n}^* : |\{L_1(F(L_2(x) + F(L_2(x + a))) + L_1(0) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
$\forall a \in \mathbb{F}_{2^n}^* : |\{F(L_2(x)) + F(L_2(x) + L_2(a) + L_2(0)) : x \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
$\forall a \in \mathbb{F}_{2^n}^* : |\{F(y) + F(y + L_2(a) + L_2(0)) : y \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
$\forall b \in \mathbb{F}_{2^n}^* : |\{F(y) + F(y + b) : y \in \mathbb{F}_{2^n}\}| = 2^{n-1} \iff$
F is APN.
We substituted $y = L_2(x)$ and $b = L_2(a) + L_2(0)$ since L_2 is a permutation. □

Theorem 9. *Let $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be two EA equivalent Boolean functions. Then F and G have the same Walsh spectrum.*

Definition (Cyclotomic coset)**.** Let $s, n \in \mathbb{N}, n \geq 2$. The cyclotomic coset of s is given by $C_s = \{2^i s \pmod n | i \in \mathbb{N}\}$.

Notation. We will denote $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ and $\mathbb{F}^{**} = \mathbb{F} \setminus \{0, 1\}$.

1. The general construction

1.1 A known example of APN function with non-classical spectrum

An example of an APN function with non-classical spectrum $\mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ was given in [9] (page 18). Its univariate representation has the form

$$X \mapsto X^3 + U^{11}X^5 + U^{13}X^9 + X^{17} + U^{11}X^{33} + X^{48} \tag{1.1}$$

where U is a generator of $\mathbb{F}_{2^6}^*$. The Walsh spectrum of this function is:

$$\{*0^{\wedge\wedge 891}, 8^{\wedge\wedge 2944}, 16^{\wedge\wedge 256}, 32^{\wedge\wedge 4}, 64*\}.$$

.

1.2 Description of the construction

To find an APN function with non-classical Walsh spectrum $F : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ we consider functions
$f, g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, where

$$f, g \text{ are quadratic, } f \text{ has non-classical spectrum}$$

$$g(x, y) = L(x, y) + g_x(x) + g_y(y)$$

$$L(x, y) = \sum_{0 \le i,j < m} a_{ij} x^{2^i} y^{2^j}$$

$$g_x(x) = \sum_{0 \le i,j < m} b_{ij} x^{2^i + 2^j}$$

$$g_y(y) = \sum_{0 \le i,j < m} c_{ij} y^{2^i + 2^j}$$

$$a_{ij}, b_{ij}, c_{ij} \in \mathbb{F}_{2^m}, 0 \le i, j < m$$

where f, g give a bivariete representation of F.
Since f has a non-classical spectrum, F also does (Proposition 4), so we need to find g, such that F is APN. We will fix the function f and will search for the function g. Trying all coefficients a_{ij}, b_{ij}, c_{ij} and checking the resulting function for APNness is computationally infeasible, so we want to restrict the search space by making some assumptions and finding necessary conditions for g.
It is reasonable to expect we can check $\approx 2^{24}$ functions in a second, $\approx 2^{45}$ functions in a month.
For a search with $m = 4$, even if we fix the functions g_x, g_y, there is an unfeasible number ($16^{16} = 2^{64}$) of coefficients a_{ij} to try. We would like to decrease the number of coefficients a_{ij} we try to something around 2^{45}.

If F is APN, then

$$F(x,y) + F(x+u, y+v) + F(u,v) = 0$$

or equivalently

$$\begin{aligned} f(x,y) + f(x+u, y+v) + f(u,v) &= 0 \\ g(x,y) + g(x+u, y+v) + g(u,v) &= 0 \end{aligned} \tag{1.2}$$

has two solutions $\forall u, v \in \mathbb{F}_{2^m}, (u,v) \neq (0,0)$.

The motivation behind trying this construction for $m = 4$ is, that for $m = 3$ and $f(x,y) = x^2y + xy^2 + xy$ it lead to finding APN functions $\mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ with the same spectrum as eq. (1.1) (which are equivalent to it).

In the next sections, we will be describing two choices of f,
i. e. $f(x,y) = x^2y + xy + xy^2$ and $f(x,y) = x^2y + xy^2$, focusing on the case $m = 4$.

We choose these functions because of their simplicity (and because the first one lead to the known example). Computer experiment shows that both of these functions have non-classical spectrum in $\mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$.

Lemma 10. *For each $u, v \in \mathbb{F}_{2^m}, (u,v) \neq (0,0)$, $f(x,y)+f(x+u,y+v)+f(u,v) = 0$ must have at most $2 \cdot 2^m$ solutions in order for Equation (1.2) to have two solutions.*

Proof. According to Proposition 6, solutions to $f(x,y)+f(x+u,y+v)+f(u,v) = 0$ as well as solutions to $g(x,y)+g(x+u,y+v)+g(u,v) = 0$ form a vector subspace of $\mathbb{F}_{2^n}$.
Let $A_{u,v,b} = \{(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} | f(x,y) + f(x+u,y+v) + f(u,v) = b\}$,
$B_{u,v,b} = \{(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} | g(x,y) + g(x+u,y+v) + g(u,v) = b\}$.
Assume that $g(x,y) + g(x+u,y+v) + g(u,v) = 0$ has two solutions, that is $\forall b \in \mathbb{F}_{2^m} : |B_{u,v,b}| \leq 2$. Each pair $(x,y) \in A_{u,v,0}$ makes $g(x,y) + g(x+u,y+v) + g(u,v) = b$ for some $b \in \mathbb{F}_{2^m}$. Since $|\mathbb{F}_{2^m}| = 2^m$ and $|B_{u,v,b}| \leq 2$, this means that $|A_{u,v,0}| \leq 2 \cdot 2^m$. □

Proposition 11.
1. *The function $f(x,y) = x^2y + xy^2$ has the following spectra:*
   $m = 3$: $\{0^{\wedge\wedge 399}, -16^{\wedge\wedge 42}, 16^{\wedge\wedge 70}, 64\}$
   $m = 4$: $\{0^{\wedge\wedge 1455}, -16^{\wedge\wedge 1200}, 16^{\wedge\wedge 1360}, -64^{\wedge\wedge 30}, 64^{\wedge\wedge 50}, 256\}$
2. *The function $f = x^2y + xy^2 + xy$ has the following spectra:*
   $m = 3$: $\{0^{\wedge\wedge 267}, -8^{\wedge\wedge 84}, 8^{\wedge\wedge 108}, -16^{\wedge\wedge 18}, 16^{\wedge\wedge 30}, -32, 32^{\wedge\wedge 3}, 64\}$
   $m = 4$: $\{0^{\wedge\wedge 2271}, -16^{\wedge\wedge 600}, 16^{\wedge\wedge 680}, -32^{\wedge\wedge 224}, 32^{\wedge\wedge 288}, -64^{\wedge\wedge 12}, 64^{\wedge\wedge 20}, 256\}$

Proof. Computer calculation. □

We leave calculating the spectra of these functions for general m for future work.

Proposition 12. *For $m = 3, 4, 5$, both $f = x^2y + xy^2$ and $f = x^2y + xy^2 + xy$ satisfy Lemma 10.*

Proof. Computer calculation. □

2. Fixing $f = x^2y + xy + xy^2$

Throughout this chapter, we will assume $f(x,y) = x^2y + xy^2 + xy$. When we substitute $f(x,y) = x^2 + xy + xy^2$ into Equation (1.2), we get that

$$\begin{aligned}
0 &= f(x,y) + f(x+u, y+v) + f(u,v) \\
&= xy + x^2y + xy^2 + uv + u^2v + uv^2 \\
&\quad + (x+u)(y+v) + (x+u)^2(y+v) + (x+u)(y+v)^2 \\
&= xv + yu + x^2v + yu^2 + xv^2 + y^2u \\
&= x(v+v^2) + y(u+u^2) + x^2v + y^2u \\
&\qquad \text{and} \\
0 &= g(x,y) + g(x+u, y+v) + g(u,v)
\end{aligned}$$

have two common solutions.

2.1 Conditions from differences $u = 0$ or $v = 0$

For $u = 0$, we get that

$$\begin{aligned}
0 &= x(v+v^2) + x^2v, \\
0 &= g(x,y) + g(x, y+v) + g(0,v).
\end{aligned} \tag{2.1}$$

have two common solutions.

Similarly, from $v = 0$, we get that

$$\begin{aligned}
0 &= y(u+u^2) + y^2u, \\
0 &= g(x,y) + g(x+u, y) + g(u,0)
\end{aligned} \tag{2.2}$$

have two common solutions.

Proposition 13. *If $F = (f,g)$ is APN, then g_x and g_y are APN.*

Proof. Since $\forall (x,y) \in \{0\} \times \mathbb{F}_{2^m}$ solves the first equation of (2.1),
$g(0,y) + g(0,y+v) + g(0,v) = 0$ cannot have any other solutions, other than $y \in \{0, v\}$. But since $g(0,y) = g_y(y)$ it means, that g_y is APN.
By similar argument, from $v = 0$ and Equation (2.2), we get that g_x is APN. □

Lemma 14. *If $F = (f,g)$ is APN, then*

(a) $\forall v \in \mathbb{F}_{2^m}^{**}, y \in \mathbb{F}_{2^m} : g(v+1,y) + g(v+1, y+v) + g(0,v) \neq 0$,

(b) $\forall u \in \mathbb{F}_{2^m}^{**}, x \in \mathbb{F}_{2^m} : g(x,u+1) + g(x+u, u+1) + g(u,0) \neq 0$.

Proof.

(a) $(x,y) \in \{(0,0),(0,v)\}$ are two common solutions of Equation (2.1).
This means, that since $(x,y) \in \{v+1\} \times \mathbb{F}_{2^m}$ solves the first equation of (2.1), it cannot solve the second one.
This gives us $\forall v \in \mathbb{F}_{2^m}^{**}, y \in \mathbb{F}_{2^m} : g(v+1,y) + g(v+1, y+v) + g(0,v) \neq 0$.

(b) By similar argument, from $v = 0$ and Equation (2.2), we get that $\forall u \in \mathbb{F}_{2^m}^{**}, x \in \mathbb{F}_{2^m} : g(x, u+1) + g(x+u, u+1) + g(u, 0) \neq 0$.

□

To proceed further, we should fix the functions g_x, g_y. Proposition 13 tells us, that they need to choose them to be APN.
For the sake of simplicity, let us fix $g_x(x) = x^3, g_y(y) = \alpha y^3, \alpha \neq 0$.
The function g_x is APN according to Theorem 7 and the function g_y is EA-equivalent to it and thus (according to Theorem 8) also APN.
Different more complicated choices of g_x, g_y might lead to more or less equivalent results as simpler choices. For example let $m = 4$ and $g_x(x) = x^9, g_y(y) = \alpha y^9$. Then $g(x, y) = (x^3 + \alpha' y^3 + L'(x, y))^2$, where $\alpha' = \alpha^8$, and $L'(x, y) = L(x, y)^8 = \sum_{0 \leq i,j < m} a_{i-3,j-3} x^{2^i} y^{2^j}$

Proposition 15. *In order for the construction to work, we need*

(a) $0 = x^2u + u^2x + L(u, u+1)$ *has solutions* $\iff u \in \mathbb{F}_2$,

(b) $0 = \alpha y^2 u + \alpha v^2 x + L(v+1, v)$ *has solutions* $\iff v \in \mathbb{F}_2$.

Proof.

(a) If $u \in \mathbb{F}_2$, then $x = 0$ solves the equation.
Let $u \notin \mathbb{F}_2$, then Lemma 14 (b) yields

$$\begin{aligned} 0 &\neq g(x, u+1) + g(x+u, u+1) + g(u, 0) \\ &= x^3 + \alpha(u+1)^3 + L(x, u+1) + (x+u)^3 + \alpha(u+1)^3 + \\ &\quad + L(x+u, u+1) + u^3 + \alpha 0^3 + L(u, 0) \\ &= x^3 + L(x, u+1) + (x+u)^3 + L(x+u, u+1) + u^3 \\ &= x^3 + L(u, u+1) + x^3 + x^2u + xu^2 + u^3 + u^3 \\ &= x^2u + u^2x + L(u, u+1) \end{aligned}$$

(b) If $v \in \mathbb{F}_2$, then $y = 0$ solves the equation.
Let $v \notin \mathbb{F}_2$, then Lemma 14 (a) yields

$$0 \neq \alpha y^2 u + \alpha v^2 x + L(v+1, v)$$

□

Notation. Recall, that $L(x, y) = \sum_{0 \leq i,j < m} a_{ij} x^{2^i} y^{2^j}$.
Through the rest of this chapter, we let

$$A_{ij} = a_{ij} + a_{ji}, B_i = a_{i-1,i-1} + \sum_{0 \leq j < m} a_{ij} \tag{2.3}$$

(where the indices are modulo m).
This allows us to write

$$L(x, x+1) = \sum_{0 \leq i,j < m} a_{ij} x^{2^i + 2^j} + \sum_{0 \leq i,j < m} a_{ij} x^{2^i} = \sum_{0 \leq i < j < m} A_{ij} x^{2^i + 2^j} + \sum_{0 \leq i < m} B_i x^{2^i} \tag{2.4}$$

Lemma 16. *This notation implies*

$$\sum_{0\le i<j<m} A_{ij} = \sum_{0\le i<m} B_i.$$

Proof.

$$\sum_{i=0}^{m} B_i = \sum_{i=0}^{m}\left(a_{i-1,i-1} + \sum_{j=0}^{m} a_{ij}\right) = \sum_{i=0}^{m} a_{i-1,i-1} + \sum_{i=0}^{m}\sum_{j=0}^{m} a_{ij} =$$

$$\sum_{i=0}^{m} a_{i-1,i-1} + \sum_{0\le i<j<m} (a_{ij} + a_{ji}) + \sum_{0\le i=j<m} a_{i-1,j-1} = \sum_{0\le i<j<m} A_{ij}$$

□

2.2 Generalisation to large fields

In this section we will show that the construction does not result in an APN function for large values of m.

Lemma 17. *Let $a \in \mathbb{F}_{2^n}$. Then $x^2 + x = a$ has solutions (two) in $x \in \mathbb{F}_{2^n}$ $\iff$ $\mathrm{Tr}(a) = 0$.*

Proof. Let $x^2 + x = a$ be a solution. Then $\mathrm{Tr}(a) = \mathrm{Tr}(x^2 + x) = \mathrm{Tr}(x^2) + \mathrm{Tr}(x) = \mathrm{Tr}(x) + \mathrm{Tr}(x) = 0$.
Let $L(x) = x^2 + x$. L is a linearized polynomial and $\operatorname{Ker} L = \{0, 1\}$ $\implies$ $\dim \operatorname{Ker}(L) = 1$. For every linear mapping $\dim \operatorname{Im}(L) + \dim \operatorname{Ker}(L) = n$ and so we get $\dim \operatorname{Im}(L) = n - 1$ $\implies$ $|\operatorname{Im}(L)| = 2^{n-1}$.
Since $|\{x \in \mathbb{F}_{2^n}; \mathrm{Tr}(x) = 0\}| = 2^{n-1}$, $\operatorname{Im} L$ must be equal to this set. □

Lemma 18. *Let $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$ be a polynomial with $\le k$ nonzero coefficients. Then the number of nonzero coefficients of $\mathrm{Tr}\, f$ is $\le nk$.*

Proof. Let $I := \{i \le 2^n; a_i \neq 0\}$. Then

$$\mathrm{Tr}\, f = \mathrm{Tr} \sum_{i\in I} a_i x^i = \sum_{i\in I} \mathrm{Tr}(a_i x^i) = \sum_{i\in I}\sum_{j=0}^{n-1} a_i^j (x^i)^j$$

and so $\mathrm{Tr}\, f$ has $\le n \cdot |I| = nk$ nonzero coefficients. □

Lemma 19. *Let $a, b \in \mathbb{F}_{2^n}, k \in \mathbb{N}$. Then $(a + b)^k = \sum_{i \preceq k} a^i b^{k-i}$ where $u \preceq v$ $\iff$ $S_u \subseteq S_v$ and S_u is support of the binary representation of u.*

Lemma 20. *If F is APN, then*

(a)

$$\mathrm{Tr}\left(\frac{L(u, u+1)}{u^3}\right) = \sum_{i=1}^{q-2} u^i$$

(b)

$$\mathrm{Tr}\left(\frac{L(v+1, v)}{\alpha v^3}\right) = \sum_{i=1}^{q-2} v^i$$

Proof.

(a) If $u = 0$, then $\operatorname{Tr}\left(L(u, u+1)/u^3\right) = \operatorname{Tr}\left(L(u, u+1) \cdot u^{2^m-1-3}\right) = \operatorname{Tr} 0 = 0$.
Let $u \in \mathbb{F}_{2^m}^*$. According to Proposition 15 (a) $x^2u + u^2x + L(u, u+1) = 0$ has solutions $\iff u = 1$.
Using the substitution $x \mapsto xu$, we get an equivalent condition of

$$x^2 + x = \frac{L(u, u+1)}{u^3}$$

having solutions in $x \iff u = 1$. Lemma 17 implies that

$$\operatorname{Tr}\left(\frac{L(u, u+1)}{u^3}\right) = \begin{cases} 0, & u = 1 \\ 1, & u \neq 1 \end{cases}$$

Thus, for $u \in \mathbb{F}_{2^m}$ we have

$$\operatorname{Tr}\left(\frac{L(u, u+1)}{u^3}\right) = \begin{cases} 0, & u = 0, 1 \\ 1, & u \neq 0, 1 \end{cases}$$

Using Lagrange interpolation we can get an unique polynomial representation of the right side.
Using the fact that $u^2 + u = 0 \iff u = 0, 1$ and the fact that $u^{q-1} = 0 \iff u = 0$, we can also craft it like so:

$$(u^2 + u)^{q-1} = \sum_{i \leq q-1} u^{2i} u^{q-1-i} = \sum_{i \leq q-1} u^{q-1+i} = \sum_{i=1}^{q-2} u^i.$$

(b) Same idea, except that we will start with Proposition 15 (b).

□

Theorem 21. *For $m \in \mathbb{N}, m \geq 9$, "the construction" does not yield an APN function F.*

Proof. Assume it does. According to Lemma 20, we have

$$\operatorname{Tr}\left(\frac{L(u, u+1)}{u^3}\right) = \sum_{i=1}^{q-2} u^i.$$

Let k denote the number of nonzero coefficients of $\frac{L(u,u+1)}{u^3}$ which is also the number of nonzero coefficients of $L(u, u+1)$.
From Equation (2.4), we can see, that $k \leq \binom{m}{2} + \binom{m}{1}$.
Applying Lemma 18 to $\operatorname{Tr}\left(\frac{L(u,u+1)}{u^3}\right) = \sum_{i=1}^{q-2} u^i$ we get the following inequality:

$$2^m - 2 = q - 2 \leq m\left(\binom{m}{2} + m\right),$$

which is not satisfied for $m \geq 9$. Therefore, for such m we get a contradiction with the assumption of F being APN. □

2.3 The case $\alpha = 1$

Let us fix $m = 4$ for now and let us see what exponents we can get in

$$\frac{L(x,x+1)}{x^3} = \frac{L(x,x)}{x^3} + \frac{L(x,1)}{x^3} = \sum_{0\le i<j<4} A_{ij}x^{2^i+2^j-3} + \sum_{0\le i<4} B_i x^{2^i-3}.$$

We can look for the exponents in the table below.

i	j	2^i+2^j+15-3
0	1	15
0	2	2
0	3	6
1	2	3
1	3	7
2	3	9

i	2^i+15-3
0	-2=13
1	-1=14
2	1
3	5

The cyclotomic cosets in $\mathbb{F}_{2^4}$ are:
$C_1 = \{1,2,4,8\}$
$C_3 = \{3,6,12,9\}$
$C_5 = \{5,10\}$
$C_7 = \{7,14,13,11\}$
$C_0 = \{0\}$

Remark. Cyclotomic cosets tell us, which monomials of a polynomial will get "mixed together", when we take the trace.
For example let $h(x) = q_7x^7 + q_{11}x^{11} + q_{12}x^{12}$. Then

$$\begin{aligned}
\mathrm{Tr}(h(x)) &= q_7x^7 + (q_7x^7)^2 + (q_7x^7)^4 + (q_7x^7)^8 + \\
&\quad + q_{11}x^{11} + (q_{11}x^{11})^2 + (q_{11}x^{11})^4 + (q_{11}x^{11})^8 + \\
&\quad + q_{12}x^{12} + (q_{12}x^{12})^2 + (q_{12}x^{12})^4 + (q_{12}x^{12})^8 \\
&= q_7x^7 + q_7^2x^{14} + q_7^4x^{13} + q_7^8x^{11} + \\
&\quad + q_{11}x^{11} + q_{11}^2x^7 + q_{11}^4x^{14} + q_{11}^8x^{13} + \\
&\quad + q_{12}x^{12} + q_{12}^2x^9 + q_{12}^4x^3 + q_{12}^8x^6 \\
&= (q_7 + q_{11}^2)x^7 + (q_7^2 + q_{11}^4)x^{14} + (q_7^4 + q_{11}^8)x^{13} + (q_7^8 + q_{11})x^{11} + \\
&\quad + q_{12}x^{12} + q_{12}^2x^9 + q_{12}^4x^3 + q_{12}^8x^6
\end{aligned}$$

As we can see, coefficients q_7 are q_{11} are getting mixed in the trace (since 7 and 11 lie in the same cyclotomic coset), but they do not affect (for example) the monomial $\_x^3$ (since 3 lies in a different coset).

Proposition 22. *For $m = 4$, $\alpha \neq 1$ the construction does not work.*

Proof. Lemma 20 gives us:

$$\mathrm{Tr}\left(\frac{L(x,x)}{x^3}\right) + \mathrm{Tr}\left(\frac{L(x,1)}{x^3}\right) = \sum_{i=1}^{q-2} x^i = \mathrm{Tr}\left(\frac{L(x,x)}{\alpha x^3}\right) + \mathrm{Tr}\left(\frac{L(1,x)}{\alpha x^3}\right)$$

If we look at which terms do contribute to the monomial x^3, from the first equality we get:

$\mathrm{Tr}(x^3) = \mathrm{Tr}(A_{12}x^3 + A_{03}x^6 + A_{23}x^9) = \mathrm{Tr}(A_{12}x^3 + (A_{03}x^6)^8 + (A_{23}x^9)^2) =$
$\mathrm{Tr}(x^3A_{12}) + \mathrm{Tr}(x^3A_{03}^8) + \mathrm{Tr}(x^3A_{23}^2)$ and so $A_{12} + A_{03}^8 + A_{23}^2 = 1$.
However, at the same time, from the second equality, we get:
$A_{12} + A_{03}^8 + A_{23}^2 = \alpha$
This gives $\alpha = 1$. □

In the previous proof, we deduced the condition $A_{12} + A_{03}^8 + A_{23}^2 = 1$ from C_3. We can use cyclotomic cosets to deduce further conditions for the coefficients.

Theorem 23. *Let A_{ij}, B_i be as above. Let $m = 4$. If F is APN, then*

(a) $\mathrm{Tr}(A_{01}) = 0$

(b) $B_2^2 + A_{02} = 1$

(c) $A_{12} + A_{03}^8 + A_{23}^2 = 1$

(d) $B_3 + B_3^4 = 1$

(e) $A_{13}^4 + B_0 + B_1^2 = 1$

Proof.

(a) From C_0 we get $0 = \mathrm{Tr}(A_{01})$.

(b) From C_1 we get $\mathrm{Tr}(x) = \mathrm{Tr}(B_2x + A_{02}x^2) = \mathrm{Tr}((B_2^2 + A_{02})x^2)$
$\implies B_2^2 + A_{02} = 1$.

(c) We deduced this in the previous proof.

(d) From C_5 we get $\mathrm{Tr}(B_3x^5) = x^5(B_3 + B_3^4) + x^{10}((B_3 + B_3^4)^2)$, so $B_3 + B_3^4 = 1$.

(e) From C_7 we get $\mathrm{Tr}(x^7) = \mathrm{Tr}(A_{13}x^7 + B_0x^{13} + B_1x^{14}) = \mathrm{Tr}(x^{13}(A_{13}^4 + B_0 + B_1^2))$
$\implies A_{13}^4 + B_0 + B_1^2 = 1$.

□

Lemma 24. *$x + x^4 = 1$ has four solutions for $x \in \mathbb{F}_{2^4}$.*

Proof. $x + x^4 = \mathrm{Tr}_2^4(x)$. However, since the solutions to $\mathrm{Tr}_2^4(x) = 0$ are a two dimensional vector subspace $\mathbb{F}_{2^2}$ of $\mathbb{F}_{2^4}$, $x + x^4 = a$ has four solutions for each $a \in \mathbb{F}_{2^2}$. □

Lemma 25. *When $m = 4$, the conditions given in Theorem 23 reduce the size of the search space from $16^{16} = 2^{64}$ to 2^{49}.*

Proof. The number of possible combination of values of $A_{01}, A_{02}, A_{03}, A_{12}, A_{13}, A_{23}, B_0, B_1, B_2, B_3$ is $2^{2+5\cdot4-1} = 2^{21}$.
(If we choose B_3 matching condition (d) (4 values) and $B_2, A_{03}, A_{23}, B_1, A_{13}$ freely, conditions (b), (c), (e) determine coefficients A_{02}, A_{12}, B_0 uniquely. The value of A_{01} is determined by Lemma 16), in half of the cases it will match condition (a).)

Rewriting the meaning of our notation A_{ij}, B_i into a system of equations yields:

$$\begin{array}{llllllll}
a_{00}+a_{01}+a_{02}+a_{03} & & & & & & +a_{33} & = B_0 \\
a_{00}+a_{01} & & +a_{11}+a_{12}+a_{13} & & & & & = B_1 + A_{01} \\
& a_{02} & +a_{11}+a_{12} & & +a_{22}+a_{23} & & & = B_2 + A_{02} + A_{12} \\
& & a_{03} & & +a_{13}+a_{22}+a_{23}+a_{33} & & & = B_3 + A_{03} + A_{13} + A_{23}
\end{array}$$

As we can see, the corresponding matrix

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

has rank 3 and so 3 of the coefficients $a_{ij}, i \leq j$ are uniquely determined by the other 7. Since coefficients $a_{ji}, i < j$ are uniquely determined by a_{ij} and A_{ij}, this leaves us at $2^{21+7\cdot 4} = 2^{49}$ of total combinations. □

Remark. The previous proof provides a way of generating all the matching combinations of coefficients efficiently.

Remark. In Proposition 22 we proved that α must be equal to 1 for $m = 4$. However, we can actually generalize this result to $m \geq 4$.
What enabled us to prove Proposition 22, was the fact that there existed a cyclotomic coset (C_3) that did not have any elements of the form $2^i - 3$. We need to show that this is the case in general when $m > 4$.

Lemma 26. *Let $m > 4$, let C_s be a cyclotomic coset in $\mathbb{F}_{2^m}$. Then $|C_s| \leq m$ and the total number of cyclotomic cosets in $\mathbb{F}_{2^m}$ is greater than m.*

Proof. Since $2^m \equiv 1 \pmod{2^m - 1}$, we have $C_1 = \{1, 2, 4, \ldots, 2^{m-1}\}$ and so $|C_1| = m$.
Now, $\forall s : C_s = \{s \cdot a | a \in C_1\}$ and so $|C_s| \leq |C_1| = m$.
Suppose the number of cyclotomic cosets, N is at most m. Then we have

$$2^m - 1 = \sum_{C_s \text{ is a cyclotomic coset}} |C_s| \leq N \cdot m \leq m^2.$$

This is a contradiction with $m > 4$. □

Theorem 27. *For $m \geq 4, \alpha \neq 1$ the construction does not work.*

Proof. Case $m = 4$ is proved in Proposition 22. Let $m > 4$.
Since $(2^1 - 3) \cdot 2 \equiv -2 \equiv (2^0 - 3)$, $2^0 - 3$ and $2^1 - 3$ lie in the same cyclotomic coset. This means, that numbers of the form $2^i - 3$ cover at most $m - 1$ cyclotomic classes.
Now, according to Lemma 26 there are more than m cosets and therefore there is a coset which is not covered by any number of the form $2^i - 3$.
Similar to Proposition 22 we get two conditions that say that some combination of the coefficients is supposed to be 1 and α at the same time. □

2.4 Further conditions from other differences

If $F =$ is APN then

$$f(x,y) + f(x+u, y+v) + f(u,v) = 0$$
$$g(x,y) + g(x+u, y+v) + g(u,v) = 0$$

has two solutions, that is the only common solutions to

$$x(v+v^2) + y(u+u^2) + x^2v + y^2u = 0 \tag{2.5}$$

$$x^2u + xu^2 + y^2v + yv^2 + L(u,y) + L(x,v) = 0 \tag{2.6}$$

are $(x,y) \in \{(0,0),(u,v)\}$.

Lemma 28. *If F is APN, then*
$\forall (u,v) \in \mathbb{F}_{2^m}^2 \setminus \mathbb{F}_2^2 : v(v+1) + u(u+1) + L(u,u+1) + L(v+1,v) \neq 0.$

Proof. Notice $(x,y) = (v+1, u+1)$ solves Equation (2.5). Substituting into Equation (2.6), we get:

$$\begin{aligned} 0 &= (v+1)^2u + (v+1)u^2 + (u+1)^2v + (u+1)v^2 + L(u,u+1) + L(v+1,v) \\ &= u + u^2 + v + v^2 + L(u,u+1) + L(v+1,v) \end{aligned}$$

And it cannot have any solution (unless $(x,y) = (0,0) \iff (u,v) = (1,1)$ or $(x,y) = (u,v) \iff (u,v) \in \{(0,1),(1,0)\}$). □

Theorem 29. *If F is APN, then*

(a) $\forall u \in \mathbb{F}_{2^m}^{**} : u(u+1) \neq L(u,u+1)$

(b) $\forall v \in \mathbb{F}_{2^m}^{**} : v(v+1) \neq L(v+1,v)$

(c) $\forall u,x \in \mathbb{F}_{2^m}^{*} : L(u,x) = L(x,u) \iff u = x$

Proof.

(a) This is a special case of Lemma 28 with $v = 1$.

(b) This is a special case of Lemma 28 with $u = 1$.

(c) Let $u = v$
Equation (2.5) becomes

$$(u+u^2)(x+y) + u(x^2+y^2) = 0 \tag{2.7}$$

while Equation (2.6) becomes

$$u(x^2+y^2) + u^2(x+y) + L(u,y) + L(x,u) = 0 \tag{2.8}$$

The only common solutions to Equation (3.7) and Equation (3.8) are $(x,y) \in \{(0,0),(u,u)\}$.
Since $\forall x = y$ solves Equation (2.7), it cannot solve Equation (2.8) (unless $x = 0, u = 0$ or $x = u$).
In other words we get the following condition:

$$\forall u,x \in \mathbb{F}_{2^m}^{*}, x \neq u : L(x,u) \neq L(u,x)$$

□

Remark. We do not need to know all the coefficients a_{ij} of L to evaluate $L(x, x+1)$ and therefore to check whether $x^2 + x \neq L(x, x+1)$ - knowing the values of $A_{ij}\ \forall i, j : 0 \leq i < j < m; B_i\ \forall i : 0 \leq i < m$ is sufficient.

More than that - we do not even need all the coefficients to check whether $\forall u, x \in \mathbb{F}_{2^m}^* : L(u, x) + L(x, u) = 0 \iff u = x$, knowing the values of $A_{ij}\ \forall i, j : 0 \leq i < j < m; a_{ii}\ \forall i : 0 \leq i < m$ is sufficient since

$$L(u, x) + L(x, u) = L(u, x + u) + L(u, u) + L(x, x + u) + L(x, x) =$$
$$= L(u, u) + L(x, x) + L(x + u, x + u)$$

3. Fixing $f = x^2y + xy^2$

In this section we will start with $f = x^2y + xy^2$. We will fix again $g_x(x) = x^3, g_y(y) = \alpha y^3$.

When we substitute $f(x, y) = x^2 + xy^2$ into Equation (1.2), we get that

$$\begin{aligned} 0 &= f(x,y) + f(x+u, y+v) + f(u,v) \\ &= x^2y + xy^2 + u^2v + uv^2 + (x+u)^2(y+v) + (x+u)(y+v)^2 \\ &= x^2v + u^2y + xv^2 + uy^2 \end{aligned}$$

and

$$0 = g(x,y) + g(x+u, y+v) + g(u,v)$$

have two common solutions.

3.1 Conditions from differences $u = 0$ or $v = 0$

For $u = 0$, we get that

$$\begin{aligned} 0 &= xv^2 + x^2v, \\ 0 &= g(x,y) + g(x,y+v) + g(0,v). \end{aligned} \tag{3.1}$$

have two common solutions.

Similarly, from $v = 0$, we get that

$$\begin{aligned} 0 &= yu^2 + y^2u, \\ 0 &= g(x,y) + g(x+u,y) + g(u,0) \end{aligned} \tag{3.2}$$

have two common solutions.

Proposition 30. *If F is APN, then g_x, g_y are APN.*

Proof. Since $\forall (x, y) \in \{0\} \times \mathbb{F}_{2^m}$ solves the first equation of (3.1),
$g(0, y) + g(0, y + v) + g(0, v) = 0$ cannot have any other solutions, other than $y \in \{0, v\}$. But since $g(0, y) = g_y(y)$ it means, that g_y is APN.
By similar argument, from $v = 0$ and Equation (3.2), we get that g_x is APN. □

Lemma 31. *Let $u, v \in \mathbb{F}_{2^m}^*$. Then*

(a) $\forall y \in \mathbb{F}_{2^m} : g(v,y) + g(v,y+v) + g(0,v) \neq 0$,

(b) $\forall x \in \mathbb{F}_{2^m} : g(x,u) + g(x+u,u) + g(u,0) \neq 0$.

Proof.

(a) $(x, y) \in \{(0, 0), (0, v)\}$ are two common solutions of Equation (3.1).
This means, that since $(x, y) \in \{v\} \times \mathbb{F}_{2^m}$ solves the first equation of (3.1), it cannot solve the second one.
This gives us $\forall v \in \mathbb{F}_{2^m}^*, y \in \mathbb{F}_{2^m} : g(v,y) + g(v,y+v) + g(0,v) \neq 0$.

(b) By similar argument, from $v = 0$ and Equation (3.2), we get that $\forall u \in \mathbb{F}_{2^m}^*, x \in \mathbb{F}_{2^m} : g(x,u) + g(x+u,u) + g(u,0) \neq 0$.

□

Proposition 32. *Let $u, v \in \mathbb{F}_{2^m}^*$. If F is APN, then*

(a) $x^2u + xu^2 + L(u,u) = 0$ has no solution.

(b) $\alpha y^2 v + \alpha y v^2 + L(v,v) = 0$ has no solution.

Proof.

(a) Expanding $g(x,y) = x^3 + \alpha y^3 + L(x,y)$ in Lemma 31 (b) gives:

$$\begin{aligned} 0 &\neq g(x,u) + g(x+u,u) + g(u,0) \\ &= x^3 + \alpha u^3 + L(x,u) + (x+u)^3 + \alpha u^3 + L(x+u,u) + u^3 \\ &= x^3 + L(x,u) + (x+u)^3 + u^3 \\ &= x^2u + u^2x + L(u,u) \end{aligned}$$

(b) Similarly from Lemma 31 (a).

□

Proposition 33. *If F is APN, then*

(a)

$$\mathrm{Tr}\left(\frac{L(u,u)}{u^3}\right) = u^{q-1}$$

(b)

$$\mathrm{Tr}\left(\frac{L(v,v)}{\alpha v^3}\right) = v^{q-1}$$

Proof.

(a) Similar to Lemma 20. Applying the substitution $x \mapsto xu$ to Proposition 32 (a), we get that $x^2 + x = \frac{L(u,u)}{u^3}$ has no solutions for $u \neq 0$. Applying lemma 17, we get

$$\mathrm{Tr}\left(\frac{L(u,u)}{u^3}\right) = \begin{cases} 0, & u = 0 \\ 1, & u \neq 0 \end{cases} \qquad = u^{q-1}$$

.

(b) Analogously from Proposition 32 (b).

□

Notation. Recall, that $L(x,y) = \sum_{0\le i,j<m} a_{ij}x^{2^i}y^{2^j}$.
Through the rest of this chapter, we let

$$A_{ij} = a_{ij} + a_{ji}. \tag{3.3}$$

This allows us to write

$$L(x,x) = \sum_{0\le i,j<m} a_{ij}x^{2^i+2^j} = \sum_{0\le i<j<m} A_{ij}x^{2^i+2^j} + \sum_{0\le i<m} a_{ii}x^{2^{i+1}}. \tag{3.4}$$

Similarly as in the previous section, let us fix $m = 4$ and look at the conditions we get from the cyclotomic classes.
The exponents we can get are:

i	0	0	0	0	1	1	1	2	2	3
j	0	1	2	3	1	2	3	2	3	3
2^i+2^j+15-3	14	15	2	6	1	3	7	5	9	13

Theorem 34. *Consider A_{ij} as above. Let $m = 4$. If $F = (f,g)$ is APN, then:*

(a) $1 = \mathrm{Tr}(A_{01}) = \mathrm{Tr}(A_{01}/\alpha)$

(b) $0 = a_{11}^2 + A_{02} = (a_{11}/\alpha)^2 + A_{02}/\alpha$

(c) $0 = a_{22} + a_{22}^4 = (a_{22}/\alpha) + (a_{22}/\alpha)^4$

(d) $0 = A_{12} + A_{03}^8 + A_{23}^2 = (A_{12}/\alpha) + (A_{03}/\alpha)^8 + (A_{23}/\alpha)^2$

(e) $0 = A_{13}^4 + a_{33} + a_{00}^2 = (A_{13}/\alpha)^4 + a_{33}/\alpha + (a_{00}/\alpha)^2$

Proof.

(a) From C_{15} we get $u^{15} = \mathrm{Tr}(A_{01}u^{15}) = A_{01}u^{15} + A_{01}^2u^{30} + A_{01}^4u^{60} + A_{01}^8u^{120} = u^{15}(A_{01}+A_{01}^2+A_{01}^4+A_{01}^8) \implies A_{01}+A_{01}^2+A_{01}^4+A_{01}^8 = 1 \iff \mathrm{Tr}(A_{01}) = 1$
And also $v^{15} = \mathrm{Tr}(A_{01}v^{15}/\alpha) \implies \mathrm{Tr}(A_{01}/\alpha) = 1$.

(b) From C_1 we get $0 = \mathrm{Tr}(a_{11}u + A_{02}u^2) = \mathrm{Tr}((a_{11}^2 + A_{02})u^2)$
$\implies a_{11}^2 + A_{02} = 0$
And also $0 = \mathrm{Tr}(a_{11}v/\alpha + A_{02}v^2/\alpha) \implies (a_{11}/\alpha)^2 + A_{02}/\alpha = 0$

(c) From C_5 we get $0 = \mathrm{Tr}(a_{22}u^5) = u^5(a_{22} + a_{22}^4) + u^{10}(a_{22} + a_{22}^4)^2$
$\implies a_{22} + a_{22}^4 = 0$
And $0 = \mathrm{Tr}(a_{22}v^5/\alpha) = v^5(a_{22}/\alpha + (a_{22}/\alpha)^4) + v^{10}(a_{22}/\alpha + (a_{22}/\alpha)^4)^2 \implies a_{22}/\alpha + (a_{22}/\alpha)^4 = 0$

(d) From C_3 we get $0 = \mathrm{Tr}(A_{12}u^3 + A_{03}u^6 + A_{23}u^9) = \mathrm{Tr}(u^3(A_{12} + A_{03}^8 + A_{23}^2))$
$\implies (A_{12} + A_{03}^8 + A_{23}^2) = 0$
And $0 = \mathrm{Tr}(A_{12}v^3/\alpha + A_{03}v^6/\alpha + A_{23}v^9/\alpha) \implies A_{12}/\alpha + (A_{03}/\alpha)^8 + (A_{23}/\alpha)^2 = 0$

(e) From C_7 we get $0 = \mathrm{Tr}(A_{13}u^7 + a_{33}u^{13} + a_{00}u^{14}) = \mathrm{Tr}(u^4(A_{13}^4 + a_{33} + a_{00}^2))$
$\implies A_{13}^4 + a_{33} + a_{00}^2 = 0$.
And $0 = \mathrm{Tr}(A_{13}v^7/\alpha + a_{33}v^{13}/\alpha + a_{00}v^{14}/\alpha) \implies (A_{13}/\alpha)^4 + a_{33}/\alpha + (a_{00}/\alpha)^2 = 0$

□

Corollary 35. *Furthermore, if $\alpha \neq 1$, we have the following conditions:*

(a) $\mathrm{Tr}(A_{01}) = \mathrm{Tr}(A_{01}/\alpha) = 1$

(b) $A_{02} = 0, a_{11} = 0$

(c) $a_{22} = a_{22}^4$
$\alpha \notin \mathbb{F}_4 \implies a_{22} = 0$

(d) $A_{12} = A_{03}^8(1+\alpha^6)/(\alpha^7+\alpha^6)$
$A_{23} = A_{03}^4(1+\alpha^{11})/(\alpha^3+\alpha^{11})$

(e) $a_{33} = A_{13}^4(1+\alpha)/\alpha^2$
$a_{00} = A_{13}^2/(\alpha+\alpha^8)$

Proof.

(a) Theorem 34(a)

(b) In Theorem 34(b), if we substitute $a_{11}^2 = A_{02}$ into $(a_{11}/\alpha)^2 + (A_{02}/\alpha) = 0$, we get $A_{02}(1/\alpha^2 + 1/\alpha) = 0$. Since $\alpha \neq 1$ this means, that $A_{02} = 0$ and also $a_{11} = 0$.

(c) Substituting one condition from Theorem 34(c) to another one gives $a_{22}(1/\alpha + 1/\alpha^4) = 0$. If $\alpha \neq \mathbb{F}_4$ then $1/\alpha + 1/\alpha^4 \neq 0$ and so $a_{22} = 0$.

(d) Substituting A_{23}^2 from one equation in Theorem 34(d) to the other gives $A_{12}(1/\alpha + 1/\alpha^2) + A_{03}^8(1/\alpha^8 + 1/\alpha^2) = 0$ and so

$$A_{12} = A_{03}^8 \frac{1/\alpha^8 + 1/\alpha^2}{1/\alpha + 1/\alpha^2} = A_{03}^8 \frac{1+\alpha^6}{\alpha^7+\alpha^6}.$$

.

Substituting A_{12} instead gives $A_{03}^8(1/\alpha^8+1/\alpha)+A_{23}^2(1/\alpha^2+1/\alpha) = 0 \implies$

$$A_{23}^2 = A_{03}^8 \frac{1/\alpha^8 + 1/\alpha}{1/\alpha^2 + 1/\alpha} = A_{03}^8 \frac{1+\alpha^7}{\alpha^6+\alpha^7}$$

$$\implies A_{23} = \left(A_{03}^8 \frac{1+\alpha^7}{\alpha^6+\alpha^7}\right)^8 = A_{03}^4 \frac{1+\alpha^{11}}{\alpha^3+\alpha^{11}}.$$

(e) Substituting a_{00} from one equation in Theorem 34(e) to the other gives $A_{13}^4(1/\alpha^4 + 1/\alpha^2) + a_{33}(1/\alpha + 1/\alpha^2) = 0$ and so

$$a_{33} = A_{13}^4 \frac{1/\alpha^4 + 1/\alpha^2}{1/\alpha + 1/\alpha^2} = A_{13}^4 \frac{1+\alpha^2}{\alpha^3+\alpha^2} = A_{13}^4 \frac{(1+\alpha)^2}{(1+\alpha)\alpha^2} = A_{13}^4(1+\alpha)/\alpha^2.$$

Substituting a_{33} instead gives $A_{13}^4(1/\alpha^4 + 1/\alpha) + a_{00}^2(1/\alpha^2 + 1/\alpha) = 0 \implies$

$$a_{00}^2 = A_{13}^4 \frac{1/\alpha^4 + 1/\alpha^2}{1/\alpha^2 + 1/\alpha} = A_{13}^4 \frac{1+\alpha^2}{\alpha^2+\alpha^3} \implies$$

$$a_{00} = \left(A_{13}^4 \frac{1+\alpha^2}{\alpha^2+\alpha^3}\right)^8 = A_{13}^2 \frac{1+\alpha}{\alpha+\alpha^9} = A_{13}^2 \frac{1+\alpha}{\alpha(1+\alpha)^8} = A_{13}^2/(\alpha+\alpha^8).$$

□

Lemma 36. *For $m = 4, \alpha = 1$, conditions in Theorem 34 reduce the search space from $16^{16} = 2^{64}$ to 2^{49}.*

Proof. Theorem 34(a) is satisfied for 8 values, Theorem 34(c) is satisfied for 4 values. Other than that, there are 11 free coefficients. $\implies 2^{3+2+11\cdot 4} = 2^{49}$. □

Lemma 37. *When $m = 4$, the conditions given in Corollary 35 reduce the search space from $16^{16} = 2^{64}$ to 2^{36} for $\alpha \in \mathbb{F}_4^{**}$ and to 2^{34} for $\alpha \notin \mathbb{F}_4$.*

Proof. Corollary 35(a) is satisfied for 4 values, Corollary 35(c) is satisfied for 4 values (resp. 1 if $\alpha \notin \mathbb{F}_4$), other than that, there are 8 free coefficients. $\implies$ $2^{2+2+8\cdot 4} = 2^{36}$ resp. $2^{2+0+8\cdot 4} = 2^{34}$ if $\alpha \notin \mathbb{F}_4$. □

3.2 Further conditions from other differences

If $F =$ is APN then

$$f(x, y) + f(x + u, y + v) + f(u, v) = 0$$

$$g(x, y) + g(x + u, y + v) + g(u, v) = 0$$

has two solutions, that is the only common solutions to

$$x^2v + u^2y + xv^2 + uy^2 = 0 \tag{3.5}$$

$$x^2u + xu^2 + \alpha(y^2v + yv^2) + L(u, y) + L(x, v) = 0 \tag{3.6}$$

are $(x, y) \in \{(0, 0), (u, v)\}$.

Lemma 38. *If F is APN, then*

(a) $\forall u, v \neq 0, u \neq v : (\alpha + 1)(u^2v + uv^2) + L(u, u) + L(v, v) \neq 0$

(b) $(1 + \alpha)(x^2u + xu^2) + L(x, u) + L(u, x) = 0 \iff x \in \{0, u\}$

(c) $\forall x \in \mathbb{F}_{2^m} : (1 + \alpha)(x^2u + xu^2) + L(u, x + u) + L(x, u) \neq 0$

(d) $L(u, u) = 0 \iff u = 0$

Proof.

(a) Since $(x, y) = (v, u)$ solves Equation (3.5), it cannot solve Equation (3.6). In other words we get the following condition:

$$(\alpha + 1)(u^2v + uv^2) + L(u, u) + L(v, v) \neq 0 \quad \forall u, v \neq 0, u \neq v.$$

To prove parts (b-d), let $u = v \in \mathbb{F}_{2^m}^*$.
Equation (3.5) becomes

$$u^2(y+x) + u(y+x)^2 = 0 \tag{3.7}$$

while Equation (3.6) becomes

$$x^2u + xu^2 + \alpha(y^2u + yu^2) + L(u,y) + L(x,u) = 0 \tag{3.8}$$

The only common solutions to Equation (3.7) and Equation (3.8) are $(x,y) \in \{(0,0),(u,u)\}$.

Now, Equation (3.7) has solutions of the form $x + y = 0$ and $x + y = u$.

(b) Let $y = x$. Substituting into Equation (3.8), we get

$$(1+\alpha)(x^2u + xu^2) + L(x,u) + L(u,x) = 0$$

and it cannot have any solution $x \in \mathbb{F}_{2^m} \setminus \{0,u\}$.

(c) Let $y = u + x$. Equation (3.8) becomes

$$(1+\alpha)(x^2u + xu^2) + L(u,x+u) + L(x,u) = 0$$

and it cannot have any solution $x \in \mathbb{F}_{2^m}$.

(d) This is a special case of (c) for $x = 0$.

□

Theorem 39. *If F is APN, $\alpha = 1$, then*

(a) $x \mapsto L(x,x)$ *is a permutation*

(b) $\forall x,u \in \mathbb{F}_{2^m}^*, x \neq u : L(x,u) \neq L(u,x)$

(c) $\forall x \in \mathbb{F}_{2^m}, u \in \mathbb{F}_{2^m}^* : L(x,u) \neq L(u,x+u)$

Proof. These are just special cases of Lemma 38 for $\alpha = 1$. □

Remark. We do not need to know all the coefficients a_{ij} of L to evaluate $L(x,x)$ and therefore to check whether $x \mapsto L(x,x)$ is a permutation - knowing the values of $a_{ii}\ \forall i : 0 \leq i < m, A_{ij}\ \forall i,j : 0 \leq i < j < m$ is sufficient.

4. Computer search

4.1 Implementation

We implemented all of the searches in the C++ language. The source code is available as an attachment.
Let $g \in \mathbb{F}_2[x], \deg g = m$ be an irreducible polynomial. Then (g) is a prime (and maximal) ideal in $\mathbb{F}_2[x]$ and therefore, $\mathbb{F}_2[x]/(g)$ is a field (of size 2^m). From each coset in $\mathbb{F}_2[x]/(g)$, we will pick an unique representative - a polynomial of degree at most $m-1$. This shall be our representation of the field $\mathbb{F}_{2^m}$.

In the C++ language we will represent each polynomial of degree at most $m-1$ using binary digits of a number $0 \dots 2^m - 1$, for example $x^3 + x + 1 \simeq 1011_2$. This means that addition corresponds to binary XOR operation and multiplication (modulo g) will have to be calculated using binary shifts and XORs. To speed up the programs, rather than calculating each multiplication every time it is needed, we will precompute a multiplication table for each pair of elements of $\mathbb{F}_{2^m}$ and store it in a two-dimensional array (where the indexes are the two elements and the values are the products). In fact, we will precalculate a few more tables for the maps $(x, y) \mapsto (x^2, y)$, $(x, y) \mapsto (x^4, y)$ etc. On the other hand, general powers are not used very often in the search, so we can just calculate them iteratively. The same goes for the inverses, which I calculate as $2^m - 2$ powers.

We shall test the APNness of $F = (f, g)$ with the following algorithm.

Algorithm 0 Test for APNness, $g(x, y) = x^3 + \alpha y^3 + L(x, y)$

Input: $a_{ij}, \alpha, R_{u,v} = \{(x, y) \in \mathbb{F}_{16}^2, f(x, y) + f(x + u, y + v) + f(u, v) = 0\}$
Output: Whether the function $F = (f, g)$ is APN

```
function testAPN({a_ij}, α, {R_{u,v}})
    for all (u, v) ∈ F_16^2, u ≠ v do
        i ← 0
        for all (x, y) ∈ R_{u,v} do
            if x^2 u + u^2 x + a y^2 v + a v^2 y + L(x, v) + L(u, y) = 0 then
                i ← i + 1
                if i > 2 then
                    return false
    return true
```

For $m = 4$, one tests takes on average $0.4\mu s$.

4.2 Search for a known example in $m = 3$

For a search in this dimension, a bruteforce search trough all values of $a_{ij}, 0 \leq i, j < 3$ is feasible.

Search 1 $m = 3, f(x,y) = x^2y + xy^2 + xy, g(x,y) = x^3 + \alpha y^3 + L(x,y), \alpha \in \mathbb{F}_8^*$

Output: All $\alpha, \{a_{ij}\}$ for which $F = (f,g)$ is APN with non-classical spectra.

```
for all (u,v) ∈ F_8^2 do
    R_{u,v} ← {(x,y) ∈ F_8^2, f(x,y) + f(x+u,y+v) + f(u,v) = 0}
for all α ∈ F_8^* do
    for all (a_00, a_01, a_02, a_10, a_11, a_12, a_20, a_21, a_22) ∈ F_8^9 do
        if testAPN({a_ij}, α, {R_{u,v}}) then
            yield {a_ij}
```

4.3 Searches in $m = 4$

Using the conditions given in Corollary 35 we can simply run through all the combinations of coefficients a_{ij} that match those conditions, and for each of them, check if what we get is what we are looking for. This is what the following two algorithms are doing, the difference being that Search 2 assumes $\alpha \notin \mathbb{F}_4$ while Search 3 only needs $\alpha \notin \mathbb{F}_2$.

Search 2 $m = 4, f(x,y) = x^2y + xy^2, g(x,y) = x^3 + \alpha y^3 + L(x,y), \alpha \in \mathbb{F}_{16} \setminus \mathbb{F}_4$

Input: $\alpha \in \mathbb{F}_{16} \setminus \mathbb{F}_4$

Output: All $\{a_{ij}\}$ for which $F = (f,g)$ is APN with non-classical spectra.

```
for all (u,v) ∈ F_16^2 do
    R_{u,v} ← {(x,y) ∈ F_16^2, f(x,y) + f(x+u,y+v) + f(u,v) = 0}
a_11 ← 0
a_22 ← 0
for all A_01 ∈ F_16, Tr(A_01) = Tr(A_01/α) = 1 do
    for all (a_01, a_02, a_13, a_31, a_03, a_30, a_12, a_23) ∈ F_16^8 do
        a_10 ← A_01 + a_01
        a_20 ← a_02
        a_33 ← (a_13 + a_31)^4 (1 + α)/α^2
        a_00 ← (a_13 + a_31)^2 / (α + α^8)
        a_21 ← (a_03 + a_30)^8 (1 + α^6)/(α^7 + α^6) + a_12
        a_32 ← (a_03 + a_30)^4 (1 + α^11)/(α^3 + α^11) + a_23
        if testAPN({a_ij}, α, {R_{u,v}}) then
            yield {a_ij}
```

This program took approximately 4 hours on 4 cores and did not find anything.

Search 3 $m = 4, f(x,y) = x^2y + xy^2, g(x,y) = x^3 + \alpha y^3 + L(x,y), \alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$

Input: $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2$
Output: All $\{a_{ij}\}$ for which $F = (f,g)$ is APN with non-classical spectra.

```
for all (u,v) ∈ F_16^2 do
    R_{u,v} ← {(x,y) ∈ F_16^2, f(x,y) + f(x+u,y+v) + f(u,v) = 0}
a_11 ← 0
for all A_01 ∈ F_16, Tr(A_01) = Tr(A_01/α) = 1 do
    for all a_22 ∈ F_16, a_22 = a_22^4 do
        for all (a_01, a_02, a_13, a_31, a_03, a_30, a_12, a_23) ∈ F_16^8 do
            a_10 ← A_01 + a_01
            a_20 ← a_02
            a_33 ← (a_13 + a_31)^4 (1 + α)/α^2
            a_00 ← (a_13 + a_31)^2 / (α + α^8)
            a_21 ← (a_03 + a_30)^8 (1 + α^6)/(α^7 + α^6) + a_12
            a_32 ← (a_03 + a_30)^4 (1 + α^11)/(α^3 + α^11) + a_23
            if testAPN({a_ij}, α, {R_{u,v}}) then
                yield {a_ij}
```

This program took approximately 26 hours on 2 cores and did not find anything.

When $\alpha = 1$, conditions in Corollary 35 are not available, and those in Theorem 34 do not restrict the search space enough to enable a search in a reasonable time. What we can do is use Theorem 39(a). Since we do not need to know all the coefficients a_{ij} to evaluate $L(x,x)$, we can expand $A_{ij} = a_{ij} + a_{ji}$ only after we check that $x \mapsto L(x,x)$ is a permutation.

Search 4 $m = 4, f(x,y) = x^2y + xy^2, g(x,y) = x^3 + y^3 + L(x,y)$

Output: All $\{a_{ij}\}$ for which $F = (f,g)$ is APN with non-classical spectra.

```
for all (u,v) ∈ F_16^2 do
    R_{u,v} ← {(x,y) ∈ F_16^2, f(x,y) + f(x+u,y+v) + f(u,v) = 0}
for all a_22 ∈ F_16, a_22 + a_22^4 = 0 do
    for all A_01 ∈ F_16, Tr(A_01) = 1 do
        for all (a_00, a_11, A_03, A_13, A_23) ∈ F_16^5 do
            A_02 ← a_11^2
            a_33 ← A_13^4 + a_00^2
            A_12 ← A_03^8 + A_23^2
            if x ↦ L(x,x) is permutation then
                for all (a_01, a_02, a_03, a_12, a_13, a_23) ∈ F_16^6 do
                    a_10 ← A_01 + a_01
                    a_20 ← A_02 + a_02
                    a_30 ← A_03 + a_03
                    a_21 ← A_12 + a_12
                    a_31 ← A_13 + a_13
                    a_32 ← A_23 + a_23
                    if testAPN({a_ij}, 1, R_{u,v}) then
                        yield {a_ij}
```

This program did not even find any permutations $x \mapsto L(x,x)$ with the conditions above.

For the case $f(x,y) = x^2y + xy^2 + xy$, we have Theorem 23, but we lack a strong condition similar to Theorem 39(a).

Search 5 $m = 4, f(x,y) = x^2y + xy^2 + xy, g(x,y) = x^3 + y^3 + L(x,y)$

Output: All a_{ij} for which $F = (f,g)$ is APN with non-classical spectra.

for all $(u,v) \in \mathbb{F}_{16}^2$ **do**
  $R_{u,v} \leftarrow \{(x,y) \in \mathbb{F}_{16}^2, f(x,y) + f(x+u, y+v) + f(u,v) = 0\}$
for all $B_3 \in \mathbb{F}_{16}, B_3 + B_3^4 = 0$ **do**
  for all $(B_1, B_2, A_{03}, A_{13}, A_{23}) \in \mathbb{F}_{16}^5$ **do**
    $A_{02} \leftarrow B_2^2 + 1$
    $A_{12} \leftarrow A_{03}^8 + A_{23}^2 + 1$
    $B_0 \leftarrow A_{13}^4 + B_1^2 + 1$
    $A_{01} \leftarrow A_{02} + A_{03} + A_{12} + A_{13} + A_{23} + B_0 + B_1 + B_2 + B_3$
    if $\mathrm{Tr}(A_{01}) = 0$ **then**
      for all $(a_{00}, a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33}) \in \mathbb{F}_{16}^7$ **do**
        $a_{21} \leftarrow A_{12} + a_{12}$
        $a_{31} \leftarrow A_{13} + a_{13}$
        $a_{32} \leftarrow A_{23} + a_{23}$
        $a_{30} \leftarrow a_{31} + a_{22} + a_{32} + a_{33} + B_3$
        $a_{20} \leftarrow a_{11} + a_{21} + a_{22} + a_{23} + B_2$
        $a_{10} \leftarrow a_{00} + a_{11} + a_{12} + a_{13} + B_1$
        $a_{03} \leftarrow A_{03} + a_{30}$
        $a_{02} \leftarrow A_{02} + a_{20}$
        $a_{01} \leftarrow A_{01} + a_{10}$
        if TESTAPN$(\{a_{ij}\}, 1, R_{u,v})$ **then**
          yield $\{a_{ij}\}$

This search takes too long to finish completely. Employing condition Theorem 29(c) could help a little bit, but it would still be too much. However, if there was an APN function with non classical spectrum within the search space, there would be a lot of other function equivalent to it. The fact that an incomplete search did not find any such function suggests, that there indeed (with high probability) is not any.

Conclusion

Through some mathematical analysis as well as some computer searches, we found out that there are no APN functions $F : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ with non-classical spectra of the form

$$F = (f, g), f, g : \mathbb{F}_{16} \to \mathbb{F}_{16},$$
$$f(x, y) = x^2y + xy^2, \text{ or } f(x, y) = x^2y + xy^2 + xy,$$
$$g(x, y) = x^3 + \alpha y^3 + \sum_{0 \le i,j < 4} a_{ij} x^{2^i} y^{2^j}, \alpha \in \mathbb{F}_{16}^*, a_{ij} \in \mathbb{F}_{16}.$$

This is only a subset of all the possible functions. There is a potential to continue with the search for different choices of f, g or even to write $F = (f, g) : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f : \mathbb{F}_{2^{n-m}} \to \mathbb{F}_{2^{n-m}}, g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, where $2m \neq n$.

Bibliography

[1] Claude Carlet. Boolean functions for cryptography and error correcting codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2:257–397, 2010.

[2] Claude Carlet. Vectorial boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

[3] Alexander Pott. Almost perfect and planar functions. *Designs, Codes and Cryptography*, 78(1):141–195, 2016.

[4] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 55–64. Springer, 1993.

[5] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes. *Information and Control*, 18(4):369–394, 1971.

[6] Hans Dobbertin. Almost perfect nonlinear power functions on gf (2/sup n/): the welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[7] Hans Dobbertin. Almost perfect nonlinear power functions on gf (2n): the niho case. *Information and Computation*, 151(1-2):57–72, 1999.

[8] Hans Dobbertin. Almost perfect nonlinear power functions on gf (2 n): a new case for n divisible by 5. In *Finite Fields and Applications*, pages 113–121. Springer, 2001.

[9] K.A. Browning, J.F. Dillon, R.E. Kibler, and M.T. McQuistan. APN polynomials and related codes. *Journal of Combinatorics, Information & System Sciences*, 34, 01 2009.