On the equivalence of nonlinear functions

Yves EDEL [a,1] Alexander POTT [b]

[a] *Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, B-9000 Ghent, Belgium*

[b] *Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, D-39016 Magdeburg, Germany*

Abstract. Recently, many new almost perfect nonlinear (APN) and almost bent (AB) functions have been constructed. These functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$ play an important role in cryptography. In this article, we will summarize different concepts of equivalence between these functions, and discuss some invariants.

Two codes can be associated with APN and AB functions. This is useful to distinguish functions up to equivalence. We give a short proof about the dimension of one of these codes.

We slightly extend the known concepts of equivalence to the more general case of functions $\mathbb{F}_2^n \to \mathbb{F}_2^m$. Moreover, we show that CCZ equivalence is the same as extended affine equivalence if F is a vectorial bent function.

Keywords. nonlinear functions, almost bent functions, difference sets

1. Introduction

Many symmetric cryptographic algorithms use S-boxes as a main ingredient. Such S-boxes are functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. In order to be resistant against *linear* [28] and *differential* [2] attacks, they should satisfy certain *nonlinearity* properties. To define the two relevant concepts of nonlinearity (corresponding to linear and differential attacks), we define the following characteristics of F:

$$\delta_F(a,b) := |\{x \in \mathbb{F}_2^n \ : \ F(x+a) - F(x) = b\}|\,, \tag{1}$$

$$\mathcal{W}_F(a,b) := \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle a,x\rangle + \langle b,F(x)\rangle}, \tag{2}$$

where $\langle\ ,\ \rangle$ denotes the standard inner product on a finite dimensional vector space. In order to be resistant against *differential* attacks, the value

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

should be as small as possible. Resistance against *linear attacks* requires that

[1] The research of the first author takes place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-Bcrypt.

$$\Lambda_F := \max_{a\in\mathbb{F}_2^n,\, b\in\mathbb{F}_2^m,\, b\neq 0} |\mathcal{W}_F(a,b)|$$

is as small as possible.

The multiset

$$\{* \quad \delta_F(a,b) \ : \ a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m \quad *\}$$

is called the **differential spectrum** of F, and the multiset

$$\mathcal{W}_F := \{* \quad \mathcal{W}_F(a,b) \ : \ a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m \quad *\}$$

is called the **Walsh spectrum** of F. The set

$$\{\pm\mathcal{W}_F\}$$

is called the **extended Walsh spectrum**. For background on Boolean and vectorial functions defined on $\mathbb{F}_2^n$, we refer to the excellent articles [15] and [16].

2. Group algebras

There is a close connection between the differential and the Walsh spectrum. This is best explained using group algebra notation. For the following very elementary facts in representation theory, we refer the reader to any textbook in advanced algebra.

Let $\mathbb{K}$ be a field, and let G be a (multiplicatively written) abelian group. The set of formal sums

$$\sum_{g\in G} a_g \cdot g, \quad a_g \in \mathbb{K}$$

is called the **group algebra** $\mathbb{K}[G]$ where addition and multiplication on $\mathbb{K}[G]$ is defined as follows:

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

and

$$\big(\sum_{g\in G} a_g \cdot g\big) \cdot \big(\sum_{g\in G} b_g \cdot g\big) := \sum_{g\in G} \big(\sum_{h\in G} a_h b_{gh^{-1}}\big) \cdot g.$$

Moreover,

$$\lambda \cdot \big(\sum_{g\in G} a_g \cdot g\big) := \sum_{g\in G} (\lambda a_g) \cdot g$$

for $\lambda \in \mathbb{K}$.

Given a finite abelian group G of order v, there are v different homomorphisms $\chi : G \to \mathbb{K}^*$, provided that $\mathbb{K}$ contains a v^*-th root of unity (v^* is the exponent of G, i.e. it is the least common multiple of the orders of the elements in G). These homomorphisms are called **characters**. The set of characters form a group $\widehat{G}$: If χ_1 and χ_2 are two characters, then $\chi_1 \cdot \chi_2 : G \to \mathbb{K}^*$ is the character with $(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$. The identity element in this **character group** is the so called trivial character or **principal character** $\chi_0 : G \to \mathbb{K}^*$ with $\chi_0(g) = 1$ for all $g \in G$. The group $\widehat{G}$ is isomorphic to G.

If ψ is an automorphism of G, then the mapping χ^ψ defined by $\chi^\psi(g) := \chi(\psi(g))$ is a character, again.

We can extend characters (by linearity) to homomorphisms $\mathbb{K}[G] \to \mathbb{K}$: We define $\chi(\sum_{g\in G} a_g \cdot g) := \sum_{g\in G} a_g \cdot \chi(g)$. Note that these mappings are indeed homomorphisms, which means that they satisfy $\chi(A \cdot B) = \chi(A) \cdot \chi(B)$ and $\chi(A + B) = \chi(A) + \chi(B)$. The element

$$\sum_{\chi\in\widehat{G}} \chi(A) \cdot \chi \in \mathbb{K}[\widehat{G}]$$

is called the **Fourier transform** of $A \in \mathbb{K}[G]$.

The following **orthogonality relations** are well known and easy to prove:

$$\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ |G| & \text{if } \chi = \chi_0, \end{cases}$$

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0 & \text{if } g \neq 1, \\ |G| & \text{if } g = 1. \end{cases}$$

Moreover,

$$a_g = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(A) \cdot \chi(g^{-1}),$$

where $A = \sum_{g\in G} a_g\, g$. This last statement is called the **Fourier inversion formula**. In other words: If we know all the character values $\chi(A)$ of some group algebra element $A \in \mathbb{K}[G]$, then we know A.

If $A = \sum_{g\in G} a_g \cdot g \in \mathbb{K}[G]$, the coefficient of the identity element in $A \cdot A^{(-1)}$ is $\sum_{g\in G} a_g^2$. Here we have used the notation $A^{(-1)}$ for the element $\sum_{g\in G} a_g \cdot g^{-1}$. If we apply Fourier inversion, we obtain

$$\sum_{g\in G} a_g^2 = \frac{1}{|G|} \sum_{\chi\in\widehat{G}} \chi(A) \cdot \chi(A^{(-1)}).$$

This is usually called the **Parseval** equation.

We will identify subsets $T \subseteq G$ with the group algebra element $\sum_{g\in T} g$, which we will also denote by T. The subset $T \subseteq G$ is uniquely determined by the v character sums $\sum_{g\in T} \chi(g)$, i.e. by the values $\chi(T)$ (using Fourier inversion).

In this section, we have written the group multiplicatively. However, in many practical examples the groups under consideration are written additively (usually our groups are elementary abelian 2-groups). We hope that this is not the source for confusion!

3. Relative difference sets and designs

Let G be an abelian multiplicatively written group which contains a subgoup N of order n. Let m be the index of N in G. A **relative difference set** $R \subseteq G$ with parameters (m, n, k, λ) is a k-subset of G such that the list of *differences* (which are quotients since we write the group multiplicatively)

$$\{* \quad r \cdot r'^{-1} \; : \; r, r' \in R \quad *\}$$

covers every element in $G \setminus N$ exactly λ times. No nonidentity element in N has such a representation. If we identify R with its group algebra element $R \in \mathbb{C}[G]$, then

$$R \cdot R^{(-1)} = k + \lambda \cdot (G - N).$$

We say that R is an (m, n, k, λ) relative difference set (RDS). A simple example is the set $\{0, 1, 3\}$ in $\mathbb{Z}_8$ relative to $N = \{0, 4\}$, which is a $(4, 2, 3, 1)$-RDS.

Simple counting shows $k(k-1) = \lambda(v - n)$, which is an elementary necessary condition. There are many constructions and many more necessary conditions on RDS's known. We refer to [30] for a slightly outdated survey article: However, that article contains some of the still most important constructions of RDS's. Much more has been done, since, however it is more difficult to describe these new constructions; instead, we refer to [33], for instance.

If $G \cong H \times N$, then the RDS is called **splitting**. The above mentioned example in $\mathbb{Z}_8$ is non splitting. If R is splitting and $k = m$, then the relative difference set R describes a function $F : H \to N$: Since no element in N has a difference representation, each coset of N (labelled by elements in H) contains exactly one element from R. Therefore, for each $h \in H$ there is a unique element $g_h \in N$ such that $(h, g_h) \in R$. This defines a function $F : H \to N$ by $F(h) := g_h$. A function $F : H \to N$ defines a relative difference set $\{(h, F(h) \; h \in H\}$ in $G \times H$ if and only if

$$F(x \cdot a) \cdot F(x)^{-1} = b$$

has precisely λ solutions in x for each choice of $a \in H$ and $b \in N$ with $a \neq 0$. Functions F corresponding to relative difference sets with parameters $(m, n, m, m/n)$ are called **bent**. Bent functions are the same objects as splitting $(m, n, m, m/n)$ relative difference sets. We refer the reader to [31] and [18] for a thorough discussion about the connection between relative difference sets and the corresponding functions.

With each RDS, we may associate a design. In this paper, a **design** is an incidence structure with a finite number v of points and a finite number b of blocks. Blocks are simply sets of points. In design theory, one is interested in incidence structure with some "nice" properties, for instance that any two distinct points are contained in a unique block. We refer the reader to the comprehensive treatment [1] for background from design theory.

Any subset R in G gives rise to an incidence structure with $|G|$ points and $|G|$ blocks: The points are simply the elements in G, and the blocks are the *translates* $Rg := \{rg \ : \ r \in R\}$.We call this design the **development** of R (abbreviated dev(R)).

If an element $a \in G$ has λ representations $r \cdot r'^{-1}$, then

$$|R \cdot g \cap R \cdot (ga)| = \lambda.$$

Moreover, there are precisely λ blocks containing the elements g and ga: We have $g, ga \in Rh$ if and only if $r\, r'^{-1} = a$.

Every design gives rise to a $v \times b$ incidence matrix M with entries from a field $\mathbb{K}$. Let

$$M = (m_{p,B})_{p \text{ point}, B \text{ block}} \in \mathbb{K}^{(v,b)},$$

where the rows a labelled by points and the columns by blocks. The (p, B)-entry of M is 1 if p is incident with B, otherwise the entry is 0.

If the design is the development of a subset $R \subseteq G$, we may obtain an incidence matrix as follows: Label rows and columns by elements from G. Then all entries in the incidence matrix are 0, except the entries in positions (g, h) with $g^{-1}h \in R$. In other words, the row corresponding to the identity is the characteristic function of R.

More generally, one can define an injective homomorphism $\Psi : \mathbb{K}[G] \to \mathbb{K}^{(v,v)}$ as follows: We label the rows and columns of the matrices in $\mathbb{K}^{(v,v)}$ by the elements from G. Then we define

$$\Psi(\sum_{g \in G} a_g \cdot g) := (m_{x,y})_{x,y \in G}$$

where $m_{x,y} := a_{x^{-1}y}$. It is not difficult to check that this mapping is an injective homomorphism. Therefore, the group algebra $\mathbb{K}[G]$ is simply the subalgebra of *group invariant matrices* in the matrix algebra $\mathbb{K}^{(v,v)}$. This may have some interesting implications regarding the equivalence of cryptographic relevant functions, as we will discuss in Section 6.

4. Almost perfect nonlinear and almost bent functions

Now let us apply these elementary facts from representation theory to functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Our ambient group algebra will be $\mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^m]$. Characters $\chi_{a,b}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ are the mappings defined by $\chi_{a,b}(x, y) := (-1)^{\langle a,x \rangle + \langle b,y \rangle}$, where $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$.

We define the **graph** $G_F := \{(x, F(x)) \ : \ x \in \mathbb{F}_2^n\}$ of F: The graph is a subset of $\mathbb{F}_2^n \times \mathbb{F}_2^m$, and it is uniquely determined by the character values $\chi_{a,b}(G_F)$. The multiset of character values is the Walsh spectrum of F. We have to be a little bit careful here: The Walsh spectrum does not determine F; we also need to know which value in the Walsh spectrum occurs for which character, so we need to know the Fourier transform of G_F.

The problem to find functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with small Λ_F can be reformulated in terms of characters as follows: Find F such that

$$\max_{a \in \mathbb{F}_2^n,\, b \in \mathbb{F}_2^m,\, b \neq 0} |\chi_{a,b}(G_F)|$$

is as small as possible.

Before we will present a well known bound on Λ_F, we explain how the $\delta_F(a, b)$ arise in the context of group algebras. We emphasize that in our case (where the group algebra is $\mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^m]$), we have $A^{(-1)} = A$ for all $A \in \mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^m]$.

Lemma 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Then*

$$G_F \cdot G_F = \sum_{x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m} \delta_F(x, y) \cdot (x, y) \tag{3}$$

in $\mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^m]$.

Since $\chi(G_F) \cdot \chi(G_F) = \chi(G_F \cdot G_F)$, the character values on the right hand side of (3) are determined by the character values $\chi(G_F)$, but not vice versa.

Some of the values in the differential spectrum are independent from F. We have:

$$\delta_F(0, 0) = 2^n,$$
$$\delta_F(0, b) = 0 \quad \text{if } b \neq 0.$$

If we apply Fourier inversion to compute $\delta_F(0, 0)$, we get

$$2^n = \frac{1}{2^{n+m}} \sum_{\chi \in \widehat{G}} \chi(G_F^2) = \frac{1}{2^{n+m}} \sum_{a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m} \chi_{a,b}(G_F^2).$$

Similarly to the differential values $\delta_F(0, b)$, some of the Walsh coefficients $\chi_{a,b}(G_F)$ are known:

$$\chi_{0,0}(G_F) = 2^n,$$
$$\chi_{a,0}(G_F) = 0 \quad \text{if } a \neq 0,$$

hence we obtain

$$2^{2n+m} - 2^{2n} = \sum_{a \in \mathbb{F}_2^n,\, b \in \mathbb{F}_2^m,\, b \neq 0} \chi_{a,b}(G_F^2).$$

Since there are $2^{n+m} - 2^n$ characters $\chi_{a,b}$ with $b \neq 0$, we have the following theorem, see [19]:

Theorem 1. *If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, then there is at least one character $\chi_{a,b}$, $b \neq 0$ with $|\chi_{(a,b)}(G_F)| \geq 2^{n/2}$. If $2^{n/2}$ is the largest possible character value, i.e. $\Lambda_F = 2^{n/2}$, then $|\chi_{(a,b)}(G_F)| = 2^{n/2}$ for all $b \neq 0$. In this case, G_F is a relative difference set with parameters $(2^n, 2^m, 2^n, 2^{n-m})$ in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ relative to $\{(0, x) : x \in \mathbb{F}_2^m\}$, i.e. $\delta_F(a, b) = 2^{n-m}$ for all $a \neq 0$.*

Note that the function F is **bent** if we have equality in Theorem 1. For such bent functions, we have $\Delta_F = 2^{n-m}$, and that is the smallest possible value. The part of Theorem 1 which states that G_F is an RDS if F is bent is a consequence of the Fourier inversion formula. The character bound follows from Parseval's equation.

It has been shown in [29] and [32] that bent functions cannot exist if $m > n/2$:

Theorem 2. *There are no bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if $m > n/2$. Bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ exist for all even m with $m \leq n/2$.*

The "classical" bent functions are those $\mathbb{F}_2^{2n} \to \mathbb{F}_2$. There are several easy constructions (via quadratic functions), but also more elaborate ones, see [15], for instance. Not much seems to be known about Λ_F and Δ_F if $n/2 < m < n$. If n is odd, not much is known for $1 \leq m < n$. For instance if $m = 1$, the problem to determine the minimum value of Λ_F is equivalent to finding the covering radius of the first order Reed-Muller code. This is known for the case n even (and the solutions, i.e. the vectors far away from the Reed-Muller code, are given by the classical bent functions), but it is open for the case n odd. If n is odd and $n = m$, we have the following bound (see [19]):

Theorem 3. *If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, then there is at least one character $\chi_{a,b}$, $b \neq 0$, with $|\chi_{(a,b)}(G_F)| \geq 2^{(n+1)/2}$. If this is the maximum (non trivial) character value, i.e. if $\Lambda_F = 2^{(n+1)/2}$, then $\chi_{(a,b)}(G_F) \in \{0, \pm 2^{(n+1)/2}\}$ for all $b \neq 0$.*

Functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $\Lambda_F = 2^{(n+1)/2}$ are called **almost bent**. They are "as bent as possible" in the sense that the Walsh spectrum is as flat as possible: Bent functions give rise to flat spectra, i.e. all character values $\chi_{a,b}(G_F)$, $b \neq 0$, have the same absolute value.

What can we say about the differential spectrum of functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$? There are no bent functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$: We may quote Theorem 2 or use a more elementary argument: According to Theorem 1, such a bent function would correspond to a relative $(n, n, n, 1)$ difference set, hence $F(x+a)+F(x) = b$ has exactly one solution (in x) for all $a \neq 0$. But this is impossible since the solutions come in pairs: If $F(x+a)+F(x) = b$, then $F((x + a) + a) + F(x + a) = b$, hence $x + a$ is another solution (different from x if $a \neq 0$)). This shows $\Delta_F \geq 2$ if $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. We call a function F with $\Delta_F = 2$ **almost perfect nonlinear** (APN). Using Fourier inversion, it is not difficult to show that any AB function is APN, see [19], again:

Theorem 4. *Any AB function is APN.*

There are several examples of APN and AB functions. Two of them are described below.

The converse of Theorem 4 is not true, since there are, for instance, APN functions with n even, but there are no AB functions with n even. There are also APN functions if n is odd which are not AB, for instance the function $x \mapsto x^{-1}$ is APN if n is odd, but it is not AB.

The fundamental group algebra identity corresponding to an APN function F is as follows:

$$G_F \cdot G_F = 2^n + 2D_F \quad \in \mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^n], \tag{4}$$

where D_F corresponds to a subset of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ which is disjoint from $\{(0,x) : x \in \mathbb{F}_2^n\}$.

The following Theorem is contained in the interesting article [17]. Its proof is not difficult:

Theorem 5. *If F is AB, then the set D_F corresponds to a bent function, i.e. the mapping $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ with $f(u,v) = 1$ if $(u,v) \in D_F$, and 0 otherwise, is bent.*

The set D_F (the support of the function f) is a so called *Hadamarad difference set*. One may think of G_F as a "root" of $2^n + 2D_F$. In our opinion, it is interesting to ask:

Problem. *Which Hadamard difference sets $D \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$ admit a decomposition*

$$T^2 = 2^n + 2D$$

for a suitable subset $T \subseteq \mathbb{F}_2^{2n}$.

There are several constructions of APN and AB functions. It is not the purpose of this paper to summarize these, but we just refer to the literature ([4,7,10,11,13,14,23,24]) for the most recent new constructions.

Basically all constructions of APN and AB functions make use of the identification of $\mathbb{F}_2^n$ with the additive group of $\mathbb{F}_{2^n}$. Any mapping $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be described by a polynomial. This polynomial description makes it possible (sometimes) to obtain information about the functions $F(x+a) - F(x)$, which have to be 2-to-1 mappings if F is APN. Also the Walsh spectrum is somewhat easier to determine if the function F is given as a polynomial: The characters of $\mathbb{F}_{2^n}$ are given by the trace mapping $x \mapsto (-1)^{\mathsf{tr}(\alpha \cdot x)}$, where $\alpha \in \mathbb{F}_{2^n}$ and tr denotes the usual trace function $\mathbb{F}_{2^n} \to \mathbb{F}_2$. However, we emphasize that the APN property (and also the Walsh spectrum) are related to the additive structure of $\mathbb{F}_{2^n}$, only. This phenomenon occurs frequently in connection with problems about difference sets: You use one algebraic structure of the field to *construct* a set, but then you *interpret* this set *relative to* the other algebraic structure of the field. Popular examples are the squares in $\mathbb{F}_p$ (Paley difference sets in the additive group of $\mathbb{F}_p$) or the Singer cycle (hyperplane of $\mathbb{F}_{2^n}$, interpreted in the multiplicative group of $\mathbb{F}_{2^n}$).

Until recently, only AB and APN *power* mappings were known: More precisely, all examples have been *equivalent* to a power mapping. However, in this context it is not so clear what is meant by "equivalent", hence we postpone the discussion of equivalence issues until we have described different concepts of equivalence.

At this point, we would like to describe two very important constructions of APN/AB functions on $\mathbb{F}_{2^n}$:

Construction GOLD**:** The mappings $x \mapsto x^{2^i+1}$ are APN if $\gcd(i,n) = 1$. If n is odd, these functions are AB. The GOLD power mappings are examples of quadratic functions: We say that a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is **quadratic** if the functions $x \mapsto F(x+a) - F(x)$ are affine for all $a \in \mathbb{F}_2^n$, but F is not affine. Equivalently, in the polynomial description of F, all the exponents are of type $2^i + 2^j$, and at least one exponent is different from 0 and 2^i. Except an example in [24], see also [5], all recently constructed APN functions are quadratic.

Construction KASAMI**:** The mappings $x \mapsto x^{2^{2i}-2^i+1}$ are APN if $\gcd(i,n) = 1$. If n is odd, these functions are AB.

5. Equivalence of functions

The question arises whether these functions are *equivalent*. We are now going to discuss several different concepts of equivalence. This is best done using the graphs G_F of the functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Affine equivalence: Functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are **affine equivalent** if there are linear bijective mappings $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and elements $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m$ such that $\mathcal{L}(G_{F_1}) + (a, b) = G_{F_2}$, where $\mathcal{L} : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ is the linear mapping

$$\mathcal{L}(x, y) := (\psi(x), \phi(y)).$$

We define

$$\begin{aligned} & H := \{(x, 0) \ : \ x \in \mathbb{F}_2^n\} \\ \text{and} \quad & N := \{(0, y) \ : \ y \in \mathbb{F}_2^m\}. \end{aligned}$$

Then $\mathcal{L} : H \times N \to H \times N$ is a linear mapping which fixes H and N setwise. With respect to a basis $\{b_1, \dots b_n, c_1, \dots c_m\}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ such that the set $\{b_1, \dots, b_n\}$ generates H and $\{c_1, \dots, c_m\}$ generates N, the linear mapping $\mathcal{L}$ is represented by

$$\begin{pmatrix} L_1 & 0_{n,m} \\ 0_{m,n} & L_4 \end{pmatrix} \tag{5}$$

where $0_{n,m}$ and $0_{m,n}$ denote the 0-matrices of sizes (n, m) and (m, n). An invariant for affine equivalence is the extended Walsh spectrum and the differential spectrum. We have to work with the extended Walsh spectrum since $\chi(G_F + (a, b)) = \chi(G_F) \cdot \chi(a, b)$, so that adding (a, b) to the elements in G_F may change the sign of the character values.

Extended affine equivalence: Functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called **extended affine equivalent** if there are linear bijective mappings $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$, elements $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m$ and a linear mapping $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $\mathcal{L}(G_{F_1}) + (a, b) = G_{F_2}$: Here $\mathcal{L}$ is defined via

$$\mathcal{L}(x, y) := (\psi(x), \phi(y) + \alpha(x)),$$

and it can be represented by

$$\begin{pmatrix} L_1 & 0_{n,m} \\ L_3 & L_4 \end{pmatrix}. \tag{6}$$

In this case, the subgroup N is fixed by $\mathcal{L}$. Again, the extended Walsh spectrum and the differential spectrum is invariant under extended affine equivalence. The **algebraic degree** is another invariant for extended affine equivalence. It is defined as follows: The function F can be described by m coordinate functions $\mathbb{F}_2^n \to \mathbb{F}_2$. These functions can be described by multivariate polynomials, and the maximum degree of these functions is the algebraic degree.

CCZ equivalence: More generally, we may look at regular matrices of the form

$$\begin{pmatrix} L_1 & L_2 \\ L_3 & L_4 \end{pmatrix}. \tag{7}$$

In this case, we speak about *CCZ* equivalence: The term “CCZ” refers to *Carlet, Charpin* and *Zinoviev*, who introduced this concept for APN and AB functions in [17]. We say that F_1 and F_2 are **CCZ-equivalent** if there are linear mappings $\psi : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$, $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $\beta : \mathbb{F}_2^m \to \mathbb{F}_2^n$ such that $\mathcal{L}(G_{F_1}) + (a,b) = G_{F_2}$, where

$$\mathcal{L}(x,y) = (\psi(x) + \beta(y), \phi(y) + \alpha(x)) \tag{8}$$

is bijective. There is a subtle difference between the concept of (extended) affine and CCZ equivalence: In the case of (extended) affine equivalence, we may apply any linear mapping of type (5) or (6) to the graph of a function F in order to get the graph of another function which has the same extended Walsh spectrum and the same differential spectrum. If we do the same for linear mapping of type (7), the resulting group algebra element is not necessarily described by a function: We can say that the Fourier transform of $\mathcal{L}(G_F)$ is the same as those of G_F, and similarly both group algebra elements have the same differential properties, but $\mathcal{L}(G_F)$ is not necessarily a function. Another difference to the case of extended affine equivalence is that the algebraic degree is not an invariant. For instance, if F is a permutation, then F^{-1} is CCZ equivalent to F, but the degree of F^{-1} is, in general, different from the degree of F. This argument shows that CCZ equivalence is more general than EA equivalence. Other examples in [12] show that there are a lot more possibilities to construct CCZ but not EA equivalent functions, starting from the GOLD case.

In the case of bent functions, CCZ equivalence is the same as extended affine equivalence. More generally, we prove:

Theorem 6. *If R_1 and R_2 are both relative (m,n,k,λ)-difference sets in the (multiplicatively written) group G relative to a subgroup N, then any automorphism $\psi : G \to G$ with $\psi(R_1) = R_2 \cdot g$ has to fix N setwise.*

Proof. Note that $R_1 \cdot R_1^{(-1)} = (R_2 g) \cdot (R_2 g)^{(-1)} = k + \lambda(G - N)$, hence Ψ has to fix the subgroup N setwise since $\lambda \neq 0$. □

This theorem slightly generalizes [26]. In particular, we have

Corollary 1. *If F_1, F_2 are bent functions $\mathbb{F}_2^n \to \mathbb{F}_2^m$ which are CCZ equivalent via a linear mapping $\mathcal{L}$ as defined in (8), then $\beta : \mathbb{F}_2^m \to \mathbb{F}_2^n$ has to be the zero map.*

Proof. If there is one element $y \in \mathbb{F}_2^m$ with $y \neq 0$, then $\mathcal{L}(0,y) \notin N$, hence N is not fixed setwise. □

This corollary has been proven independently by Budaghyan and Carlet [8]. A slightly more general result is the following:

Theorem 7. *Let $F, F' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions. If there is an isomorphism $\mathcal{L}$ on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ with $\mathcal{L}(G_F) + (a,b) = G_{F'}$ such that F' is CCZ equivalent but not EA equivalent to F, then there is a subgroup N' of order 2^m in $\mathbb{F}_2^n \times \mathbb{F}_2^m$ with $N' \neq \{0\} \times \mathbb{F}_2^m$ such that no nonzero element in N' has a representation as a difference with elements from G_F. In other words, the coefficients of the nonzero elements in N' are 0 in $G_F \cdot G_F$.*

Proof. If F is CCZ but not EA equivalent to some other function F', there must be a linear mapping $\mathcal{L}$ such that $\mathcal{L}(N) \neq N$, and $\mathcal{L}(G_F)+(a,b)$ is the graph of some function F', but $\mathcal{L}(G_F)$ is the graph of a function, too, hence we may assume $(a,b) = (0,0)$. The element $G_{F'}$ contains exactly one element from each coset of N. This shows that $\mathcal{L}^{-1}(G_{F'})$ contains exactly one element from each coset of $\mathcal{L}^{-1}(N) =: N'$. Therefore, the group algebra element $G_F \cdot G_F$ has coefficients 0 for all nonzero elements in N'. □

It is possible that $\mathcal{L}$ does not fix N, but the function described by $\mathcal{L}(G_F)$ is EA equivalent to F. An example is given in [12]. In general, this situation is characterized through the following Theorem:

Theorem 8. *Let $F, F' : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be functions which are CCZ equivalent via the linear mappping $\mathcal{L}$, i.e. $\mathcal{L}(G_F) + (a,b) = G_{F'}$. Using the notation from Theorem 7, the function F is EA equivalent to F' if and only if there is a linear isomorphism $\mathcal{L}'$ with $\mathcal{L}'(N) = N'$, $\mathcal{L}'(G_F) + (a', b') = G_F$.*

Proof. If F and F' are EA equivalent, there is a linear bijection $\mathcal{L}''$ with $\mathcal{L}''(G_F) + (a'', b'') = G_{F'}$, $\mathcal{L}''(N) = N$. Then $\mathcal{L}^{-1} \circ \mathcal{L}''$ gives the desired isomorphism $\mathcal{L}'$.

Conversely, $\mathcal{L}'' = \mathcal{L} \circ \mathcal{L}'$ gives the affine equivalence. □

The first non power examples of APN and AB functions have been found in [12]: These are EA inequivalent to power mappings, however they are CCZ equivalent to power mappings. In [23], the first examples not CCZ equivalent to power mappings have been described. That paper started quite an extensive search for APN functions. References have been given above.

The knowledge about the inequivalence of the known series of APN and AB functions is still unsatisfactory. A systematic investigation of the (in)equivalence of the GOLD power mappings is contained in [9]. As a result, the GOLD power mappings x^{2^i+1}, $i < n/2$, $\gcd(i,n) = 1$, are pairwise CCZ inequivalent. Moreover, they are CCZ inequivalent to the KASAMI power mappings (except in small (trivial) cases. Proofs are by "brute force": You take two functions and try to construct a linear mapping (defined as a linearized polynomial) that maps the graph of one function to those of the other function. Finally, after heavy computations, you see that this is impossible. It would be nice, but apparently difficult, to compute some CCZ invariants associated with the functions. We say more about invariants in the next section.

6. Equivalence of functions and designs

Now we return to designs and discuss isomorphism issues in this context. We have seen already that, for RDS's, CCZ equivalence is the same as extended affine equivalence. However, there is another possibility to generalize EA equivalence for RDS's to another more general (and, from a design theoretic point of view, more relevant) concept. We refer to [25] for more on this design theoretic approach.

If M_1 and M_2 are incidence matrices of designs, then we say that the designs are **isomorphic** if and only if there are permutation matrices P and Q such that $P \cdot M_1 \cdot Q = M_2$. In this way, we may identify the automorphism groups with the set of all pairs (P, Q) of permutation matrices such that $P \cdot M_1 \cdot Q = M_1$. Let us assume that the designs are given as the developments of subsets of a group G. Not all of the isomorphism (or automorphisms) have a nice interpretation in terms of group automorphisms: Let M_1 and M_2 be two matrices in $\Psi(\mathbb{K}[G])$, i.e. they are group developed from sets R_1 and R_2. We say that the designs are **equivalent** if there is a group automorphism ϕ and a group element $g \in G$ such that $\phi(R_1) = R_2 g$. In this case, the designs dev(R_1) and dev(R_2) are isomorphic.

We say that two function $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are **isomorphic** if dev(G_{F_1}) is isomorphic to dev(G_{F_2})

"Isomorphism" of designs is more general than "equivalence" of the corresponding difference sets. In fact, a design can be written as dev(R) for different (inequivalent) R's, as shown by the tables on difference sets in [20].

It seems to be difficult to distinguish between "isomorphism" and "equivalence" since we are not aware of parameters which are invariant only under "equivalence". All the interesting invariants with respect to "equivalence" are also invariants for "isomorphisms", let us mention just a few:

- The rank of an incidence matrix.
- The Smith normal form of an incidence matrix.
- The Automorphism group of the design.

We think that it is worth to look more carefully at this new concept of "isomorphism" corresponding to APN and AB functions: We are not aware of any pair of functions F_1 and F_2 which are not CCZ inequivalent, but the designs dev(F_1) and dev(F_2) are isomorphic. So one may try to prove that isomorphism and equivalence coincides for APN and AB functions, or one can try to find new functions as follows: Take an APN or AB function F and construct its incidence matrix M. Then compute $M' = P \cdot M \cdot Q$ for some permutation matrices P and Q. Since this design is isomorphic to the design corresponding to M, it must have a representation as the development of some $G_{F'}$. Check, whether F' is CCZ equivalent to F. We have not yet pursued this approach, but it is, in our opinion, quite interesting: You may be able to construct new APN and AB functions. We believe that as soon as you find one application of this approach, there will be many! If there are no applications of our technique, so if equivalence coincides with isomorphism, we are sure that a proof of this fact will give more insight into the theory of APN and AB functions.

If F is APN, there is not just the design defined by G_F, but also the design defined by D_F (see (4)). If F_1 and F_2 are CCZ equivalent, then dev(D_{F_1}) and dev(D_{F_2}) are equivalent, hence isomorphic. Hence the isomorphism type both of dev(D_F) and of dev(G_F) may be used to distinguish functions up to CCZ equivalence.

However, design theoretic isomorphism may be a too coarse equivalence relation. The appropriate equivalence relation is graph theoretic isomorphism, as we will explain now:

The set D_F defines a graph with 2^{2n} vertices (which are the elements in $\mathbb{F}_2^n \times \mathbb{F}_2^n$). Two vertices g and h are adjacent if $g - h \in D_F$. This relation is symmetric since

$g - h = g + h$. There is a connection between this graph and the incidence structure $dev(G_F)$. If M is an incidence matrix of $dev(G_F)$, then the matrix $\frac{1}{2}(MM^\intercal - 2^n I)$ is an adjacency matrix of the graph described by D_F. Two of the vertices in this graph, say g and h with $g \neq h$, are adjacent if the two group elements, considered as points in dev(G_F), are joined by two blocks of dev(G_F): The two (distinct) points $g = (x, y)$ and $h = (x', y')$ are in $G_F + (a, b)$ if and only if $(x - x', y - y') = (r - r', F(r) - F(r'))$ for some $r, r' \in \mathbb{F}_2^n$. Therefore, there are 0 or 2 solutions. But if the pair r, r' is a solution, then $r + a = x$ and $F(r) + b = y$, or $r' + a = x$ and $F(r') + b = y$. In particular, g and h are adjacent if and only if $g + h \in D_F$. If two designs dev(G_{F_1}) and dev(G_{F_2}) are isomorphic, the *graphs* (consisting of vertices and edges) defined by D_{F_1} and D_{F_2} are isomorphic: Note that this isomorphism in graph theoretic terms is much more restrictive than design isomorphism: In the design case, the permutation matrices P and Q multiplied on the left and right can be arbitrarily. If you consider graph isomorphism, you have to multiply by P and $P^\intercal$.

In our opinion, the determination of the automorphism groups of the designs dev(G_F) is very promising to distinguish the isomorphism type of the functions, in particular quadratic from nonquadratic functions. Experiments indicate that quadratic APNs have a much larger automorphism group than nonquadratic ones. Similarly, the ranks of the incidence matrices of quadratic functions seem to be smaller than those of nonquadratic APNs. It would be interesting to decide whether the following is true:

Problem. *Let F_1 and F_2 are APN functions where F_1 is quadratic and F_2 is not CCZ equivalent to a quadratic function. Is the $\mathbb{F}_2$ rank of an incidence matrix corresponding to dev(G_{F_1}) is strictly smaller than the rank corresponding to dev(G_{F_2})? Does this bound also hold for dev(D_{F_1}) and dev(D_{F_2})*

This question resembles a little bit the famous Hamada conjecture (which is in general not true) that the ranks of incidence matrices tend to become smaller if the automorphism groups are getting larger.

Finally, we would like to point out that the row space of the incidence matrix of a design is called the $\mathbb{K}$ *code* associated with the design. Isomorphic designs have equivalent codes, hence the code is an invariant under isomorphism. It seems that these codes (which can be also viewed as the ideals generated by G_F in $\mathbb{K}[\mathbb{F}_2^n \times \mathbb{F}_2^m]$) may be worth to investigate in order to distinguish functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ up to equivalence. However, we are not aware of a systematic investigation of these codes. But there are other codes associated with functions, which we will discuss in the next section.

7. Equivalence of functions and codes

In this final section, we will discuss relations between the different equivalence concepts for functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and code equivalence. The reader may consult the classical book [27] for background from coding theory.

Let $C(F) \in \mathbb{F}_2^{(n+m,2^n)}$ be the matrix whose columns are the vectors $\begin{pmatrix} x \\ F(x) \end{pmatrix}$, $x \in \mathbb{F}_2^n$. We extend this matrix by a first row consisting just of 1's. We call this extended matrix $C_1(F)$. By $\mathcal{C}_1(F)$, we denote the $\mathbb{F}_2$-vector space of all vectors orthogonal to the rows of $C_1(F)$. Using terminology from coding theory, the vector space $\mathcal{C}_1(F)$ is a code of length 2^n. If we multiply $C_1(F)$ by an invertible matrix M of size $n+m+1$ from the left, we get a matrix $M \cdot C_1(F)$ whose rows generate the same vector space as the rows of $C_1(F)$, hence the set of vectors orthogonal to the rows of $M \cdot C_1(F)$ is $\mathcal{C}_1(F)$, again.

Two codes U_1 and U_2 in $\mathbb{F}_2^n$ are called **equivalent** if there is a permutation $\pi : \{1, \dots, 2^n\} \to \{1, \dots, 2^n\}$ such that

$$(x_1, \dots x_{2^n}) \in U_1 \qquad \Longleftrightarrow \qquad (x_{\pi(1)}, \dots x_{\pi(2^n)}) \in U_2.$$

This shows that the codes generated by two functions F_1 and F_2 are equivalent if and only if a permutation of the columns of $C_1(F_2)$ gives a matrix such that the vector space orthogonal to the rows of this permuted matrix is $\mathcal{C}_1(F_1)$. But two matrices H_1 and H_2 define the same codes (orthogonal to the rows of H_1, resp. H_2) if and only if there is an invertible matrix M with $M \cdot H_1 = H_2$. Therefore, if $\mathcal{C}_1(F_1)$ is equivalent to $\mathcal{C}_1(F_2)$, there is an invertible matrix M such that $M \cdot C_1(F_1)$ is a matrix whose columns are a permutation of the columns of $C_1(F_2)$. It is easy to see that the matrix M must be of the following type:

$$M = \begin{pmatrix} c & d & e \\ a & L_1 & L_2 \\ b & L_3 & L_4 \end{pmatrix}$$

with $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^m$, $c \in \mathbb{F}_2$, $d \in \mathbb{F}_2^n$ $e \in \mathbb{F}_2^m$ (as row vectors), and $L_1 \in \mathbb{F}_2^{(n,n)}$ and $L_2 \in \mathbb{F}_2^{(n,m)}$, $L_3 \in \mathbb{F}_2^{(m,n)}$ and $L_4 \in \mathbb{F}_2^{(m,m)}$. The first row $v :== (c\, d\, e)$ of M has the property that the inner product of v with all the columns of $C_1(F_1)$ is 1. Hence we may assume $c = 1$, $d = 0$ and $e = 0$. The first row in the matrix M has the effect that (a, b) will be added to $(x, F_1(x))$. More precisely:

$$M \cdot \begin{pmatrix} 1 \\ x \\ F_1(x) \end{pmatrix}_{x \in \mathbb{F}_2^n} = \begin{pmatrix} 1 \\ L_1 x + L_2 F_1(x) + a \\ L_3 x + L_4 F_1(x) + b \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

We summarize this in the following theorem, see also [22,6]:

Theorem 9. *Let $F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function. Then F_1 is CCZ equivalent to a function $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if the codes $\mathcal{C}_1(F_1)$ and $\mathcal{C}_1(F_2)$ are equivalent.*

It is easy to see that affine can be also formulated in terms of codes. For this purpose, we define two other matrices $C_2(F)$ and $C_3(F)$:

$$C_2(F) := \begin{pmatrix} 1 & 0 \\ x & 0 \\ F(x) & y \end{pmatrix}_{x \in \mathbb{F}_2^n,\, y \in \mathbb{F}_2^m \setminus \{0\}}$$

and

$$C_3(F) := \begin{pmatrix} 1 & 0 & 0 \\ x & 0 & z \\ F(x) & y & 0 \end{pmatrix}_{x \in \mathbb{F}_2^n,\, y \in \mathbb{F}_2^m \setminus \{0\},\, z \in \mathbb{F}_2^n \setminus \{0\}}$$

These matrices are parity check matrices of two codes $\mathcal{C}_2(F)$ and $\mathcal{C}_3(F)$.

We obtain:

Theorem 10. *Let $F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function.Then F_1 is extended affine equivalent to a function $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if the codes $\mathcal{C}_2(F_1)$ and $\mathcal{C}_2(F_2)$ are equivalent.*

In the case of affine equivalence, we need to be more careful. If $n = m$, it may be possible to swap the rows $2, \dots n+1$ and the rows $n+2, \dots, 2n+1$. This is possible if F is a permutation. We obtain:

Theorem 11. *Let $F_1 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function which is not a permutation. Then F_1 is affine equivalent to a function $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if the codes $\mathcal{C}_3(F_1)$ and $\mathcal{C}_3(F_2)$ are equivalent. If F_1 is a permutation, then F_1 or F_1^{-1} is affine equivalent to $F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if the codes $\mathcal{C}_3(F_1)$ and $\mathcal{C}_3(F_2)$ are equivalent.*

These theorems which give a relation between code equivalence and equivalence of functions are quite useful. For instance, the computer algebra package MAGMA [3] provides a powerful tool to check code equivalence, hence it is for small values of n (thanks to MAGMA) easy to distinguish the different types of equivalence. Moreover, the automorphism groups of the codes can be computed and they may be used to distinguish different functions. We note that

$$\text{Aut}(\mathcal{C}_3(F)) \subseteq \text{Aut}(\mathcal{C}_2(F)) \subseteq \text{Aut}(\mathcal{C}_1(F)).$$

In order to see this, we note that the automorphism group of the respective codes are isomorphic to subgroups of the group of invertible matrices of size $n+m+1$ over $\mathbb{F}_2$, provided that the matrices $C_i(F)$ have full rank: Automorphisms of $\mathcal{C}_i(F)$ correspond to those permutation matrices Q such that $M \cdot C_i(F) = C_i(F) \cdot Q$ for some invertible matrix M. If the columns of $\cdot C_i(F)$ are all distinct, Q is uniquely determined by M. If the above mentioned rank condition holds, different M's give different Q's. Using the representation of the automorphism groups as subgroups of GL$(n+m+1, 2)$, the inclusion given above holds.

Finally, we would like to give a (short) proof of the fact that the rank of $C_1(F)$ is $2n+1$ if $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN. This result is contained in [17]. The proof in [17] uses bounds on the minimum weight of certain codes. A more elementary proof is contained in [21].

Theorem 12. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an APN function. Then the $\mathbb{F}_2$ rank of the matrix*

$$C_1(F) = \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

is $2n+1$ if $n > 2$.

Proof. If $rank(C_1(F)) \leq 2n$, there is an invertible matrix M such that

$$M \cdot C_1(F) = \begin{pmatrix} 1 \\ x \\ F'(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

where $F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and the last row of the matrix is 0. This shows that F is CCZ equivalent to a function F' such that $G_{F'} \subseteq U$, $|U| = 2^{2n-1}$: U consists of all vectors in $\mathbb{F}_2^{2n}$ whose last coordinate is 0. We compute $G_{F'} \cdot G_{F'}$ in $\mathbb{C}[U]$: The coefficients of the nonidentity elements are 0 or 2, and the coefficient 2 occurs $\frac{1}{2}2^n \cdot (2^n - 1)$ times. But that is the number of elements in $U \setminus N'$, where $N' = \{(0,x) \ : \ x \in \mathbb{F}_2^n\} \cap U$. Therefore, G_F is a relative $(2^n, 2^{n-1}, 2^n, 2)$ difference set in U. It is splitting since the group is elementary abelian, hence it corresponds to a bent function, which cannot exist if $n > 2$ according to Theorem 2. □

References

[1] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 2 ed., 1999.

[2] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology, 4 (1991), pp. 3–72.

[3] W. Bosma, J. Cannon, and C. Playoust, *The magma algebra system. i. the user language*, J. Symbolic Comput., 24 (1997), pp. 235–265.

[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire, *Quadratic almost perfect nonlinear functions with many terms.* IACR Cryptology ePrint Archive: 2007/115, 2007.

[5] M. Brinkmann and G. Leander, *On the classification of APN functions up to dimension five*, Des., Codes, Cryptogr., 1–3 (2008), pp. 273–288.

[6] K. Browning, J. Dillon, R. Kibler, and M. McQuistan, *APN polynomials and related codes.* submitted, 2008.

[7] L. Budaghyan and C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inf. Th., 54 (2008), pp. 2354–2357.

[8] ———, *On CCZ-equivalence and its use in secondary constructions of bent functions.* IACR Cryptology ePrint Archive: 2009/042, 2009.

[9] L. Budaghyan, C. Carlet, and G. Leander, *On inequivalence between known power APN functions*, in International Conference on Boolean Functions: Cryptography and Applications, 2008. to appear.

[10] ———, *Two classes of quadratic APN binomials inequivalent to power functions*, IEEE Trans. Inf. Th., 54 (2008), pp. 4218–4229.

[11] ———, *Constructing new APN functions from known ones*, Finite Fields Appl., (2009).

[12] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials*, IEEE Trans. Inform. Theory, 52 (2006), pp. 1141–1152.

[13] E. Byrne, C. Bracken, N. Markin, and G. McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials.* preprint, available online at: `http://mathsci.ucd.ie/~gmg/`, 2007.

[14] E. Byrne and G. McGuire, *Certain new quadratic APN functions are not APN infinitely often*, in Abstract Book of the Workshop on coding and cryptography, N. S. D. Augo and J.-P. Tillich, eds., INRIA, 2007, pp. 59–68.

[15] C. Carlet, *Boolean functions for cryptography and error correcting codes*, in Boolean Methods and Models, Y. Crama and P. Hammer, eds., Cambridge University Press, to appear.

[16] ———, *Vectorial boolean functions for cryptography*, in Boolean Methods and Models, Y. Crama and P. Hammer, eds., Cambridge University Press, to appear.

[17] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr., 15 (1998), pp. 125–156.

[18] C. Carlet and C. Ding, *Highly nonlinear mappings*, J. Complexity, 20 (2004), pp. 205–244.

[19] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, in Advances in Cryptology – EUROCRYPT 94, A. D. Santis, ed., vol. 950 of Lecture Notes in Computer Science, New York, 1995, Springer-Verlag, pp. 356–365.

[20] C. J. Colbourn and J. H. Dinitz, eds., *The CRC Handbook of Combinatorial Designs*, Boca Raton, 2006, CRC Press.

[21] J. Dillon, *APN polynomials and related codes.* personal communication, 2008.

[22] J. F. DILLON. slides from talk given at "Polynomials over Finite Fields and Appliocations", held at Banff International Research Station, 2006.

[23] Y. EDEL, G. KYUREGHYAN, AND A. POTT, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory, 52 (2006), pp. 744–747.

[24] Y. EDEL AND A. POTT, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun., (2009).

[25] F. GÖLOĞLU AND A. POTT, *Almost perfect nonlinear functions: A possible geometric approach*, in Coding Theory and Cryptography II, S. Nikova, B. Preneel, L. Storme, and J. Thas, eds., Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten, 2007, pp. 75–100.

[26] G. KYUREGHYAN AND A. POTT, *Some theorems on planar functions*, in Arithmetic of Finite Fields, J. von zur Gathen, J. L. Imaña, and Çetin Kaya Koç, eds., vol. 5130 of Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 2008, pp. 117–122.

[27] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The theory of error-correcting codes. II*, North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[28] M. MATSUI, *Linear cryptanalysis method for DES cipher.*, in Advances in Cryptology – EUROCRYPT 93, T. Helleseth, ed., vol. 765 of Lecture Notes in Computer Science, Springer-Verlag, New York, 1993, pp. 386–397.

[29] K. NYBERG, *Perfect nonlinear S-boxes*, in Advances in cryptology—EUROCRYPT '91 (Brighton, 1991), Springer, Berlin, 1991, pp. 378–386.

[30] A. POTT, *A survey on relative difference sets*, in Groups, Difference Sets, and the Monster. Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993, K. T. Arasu, J. Dillon, K. Harada, S. Sehgal, and R. Solomon, eds., Berlin, 1996, Walter de Gruyter, pp. 195–232.

[31] ———, *Nonlinear functions in abelian groups and relative difference sets*, Discrete Appl. Math., 138 (2004), pp. 177–193.

[32] B. SCHMIDT, *On* (p^a, p^b, p^a, p^{a-b})*-relative difference sets*, J. Algebraic Combin., 6 (1997), pp. 279–297.

[33] B. SCHMIDT, *Characters and Cyclotomic Fields in Finite Geometry*, vol. 1797 of Lecture Notes in Mathematics, Springer-Verlag, 2002.