On Designs and Multiplier Groups Constructed from Almost Perfect Nonlinear Functions

Yves Edel[1]* and Alexander Pott[2]

[1] Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, B-9000 Ghent, Belgium
[2] Department of Mathematics, Otto-von-Guericke-University Magdeburg, D-39016 Magdeburg, Germany

Abstract. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an almost perfect nonlinear function (APN). The set $D_f := \{(a, b) : f(x + a) - f(x) = b \text{ has two solutions}\}$ can be used to distinguish APN functions up to equivalence. We investigate the multiplier groups of theses sets D_f. This extends earlier work done by the authors [1].

1 Introduction

The investigation of highly nonlinear functions is of interest in cryptography. We do not want to go into details about applications of highly nonlinear functions, but we refer to the literature, in particular [2, 3].

There are several concepts of nonlinearity. Here we focus on differential nonlinearity. If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is linear, then

$$f(x + a) - f(x) = b \tag{1}$$

has 0 or 2^n solutions (we have 2^n solutions if $b = f(a)$). In order to be "as nonlinear as possible", the maximum number of solutions to (1) should be small for $a \neq 0$. We have $f(x + a) - f(x) = f((x + a) + x) - f(x + a)$ (note that the computations are done in a vector space over $\mathbb{F}_2$), hence if x is a solution of (1), then $x + a$ is a solution, too, so the number of solutions is always even. This motivates the following definition:

Definition 1. *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called* **almost perfect nonlinear** *or* **APN** *if the equations*

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

have 0 or 2 solutions for all $a, b \in \mathbb{F}_2^n$, $a \neq 0$.

The main goal in the investigation of APN functions are *constructions*. There are by now many constructions known (they are summarized in [3]), hence it is necessary to find powerful methods how to *distinguish* APN functions. There are several papers

* 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.

which survey some possible ways to distinguish functions up to equivalence ([4–6, 1, 7]). Here we will investigate the sets

$$D_f := \{(a, b) \ : \ f(x + a) - f(x) = b \text{ has two solutions}\}. \tag{2}$$

If f and g are equivalent (we will explain different concepts of equivalence in Section 2), then the sets D_f and D_g are, in a certain sense, equivalent. Hence inequivalence of the sets D_f and D_g implies inequivalence of the functions f and g. We will investigate, in particular, the *multiplier group*. Together with the so called *triple intersection numbers*, the sets D_f seem to be appropriate to distinguish equivalence classes of f. In Section 4, we summarize our computational results and pose some (what we think) interesting questions.

If f is an almost bent function (Definition 5), then the set D_f is a Hadamard difference set, equivalently its indicator function $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{C}$ is a bent function. Therefore, the ideas which we are going to develop in this note may be applied not just to the sets D_f constructed from APN functions but to arbitrary bent functions or Hadamard difference sets. We expect that it is possible to characterize certain highly symmetric bent functions by the automorphism or multiplier groups of the corresponding designs or difference sets. In this context, we refer to the interesting paper [8] which explains the orders of the multiplier groups $\mathcal{M}(D_f)$ for the Gold power mappings if n is odd. Moreover, it shows that the designs $\mathcal{D}_f$, hence also the functions f, are not equivalent for different Gold power mappings (if n is odd), see also [7]

In this paper, we investigate different concepts of equivalence for different types of structures. Table 1 summarizes our notation.

Table 1. Different types of *equivalence*

type of equivalence	reference	remark
graph equivalence of f and g	Definition 2	$f, g : \mathbb{F}_2^n \to \mathbb{F}_2^n$
multiplier equivalence of A and B	Definition 3	$A, B \in \mathbb{C}[G]$
design equivalence of A and B	Definition 4	$A, B \in \mathbb{C}^{(n,n)}$ or $A, B \in \mathbb{C}[G]$

If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, then graph equivalence is the same as multiplier equivalence for the sets G_f and G_g (Remark 3). Multiplier equivalence always implies design equivalence (5), but not vice versa (Example 1). We note that there is no concept of "multiplier equivalence" for arbitrary matrices $A \in \mathbb{C}^{(n,n)}$.

We will discuss these types of equivalence for the sets G_f and D_f related to APN functions f. Table 2 shows the *known* implications between these equivalences.

This paper is partly motivated by the question whether the converse of any of these implications hold. To the best of our knowledge, there is no example of a pair of APN functions f and g which violates any of the possible converse implications in the diagram Table 1.

Table 2. Dependencies between equivalences of G_f and D_f

G_f multiplier equivalent to $G_g \Rightarrow$	G_f design equivalent to G_g
$\Downarrow$	$\Downarrow$
D_f multiplier equivalent to $D_g \Rightarrow$	D_f design equivalent to D_g

2 APN functions

The most important definition for this paper is Definition 1. In order to investigate APN functions, group rings are an adequate algebraic tool.

Let $\mathbb{K}$ be a field, and let G be a (multiplicatively written) abelian group. In this paper, $\mathbb{K}$ will be almost exclusively the field $\mathbb{C}$ of complex numbers, and the group will be in most cases an elementary abelian group whose order is a power of 2.

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

A subset A of G can be identified with the group algebra element $\sum_{g\in A} g$, which we denote (by abuse of notation) by A, again. If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a mapping, then its associated **graph** G_f is the set $\{(x, f(x)) : x \in \mathbb{F}_2^n\}$ which is a subset of $G = \mathbb{F}_2^n \times \mathbb{F}_2^n$. We denote the corresponding group algebra element in $\mathbb{C}[G]$ by G_f, too. In G, we denote the subgroup $\{(x, 0) : x \in \mathbb{F}_2^n\}$ by H, and the subgroup $\{(0, x) : x \in \mathbb{F}_2^n\}$ by N. The following proposition is obvious:

Proposition 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then f is APN if and only if there is a subset D_f in $G = \mathbb{F}_2^n \times \mathbb{F}_2^n$ such that*

$$G_f^2 = 2^n + 2 \cdot D_f. \tag{3}$$

Remark 1. The set D_f contains no element of the form $(0, x)$, $x \in \mathbb{F}_2^n$, hence $D_f \cap N = \{\}$. Therefore, N is sometimes called a **forbidden subgroup**.

Proposition 1 shows that we may construct many more APN functions from a given one by applying affine transformations to G_f. Functions which can be constructed from f in this way are called *equivalent* to f. More precisely, we have

Definition 2. *Two functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called* **graph equivalent** *if there is an automorphism φ of $G = \mathbb{F}_2^n \times \mathbb{F}_2^n$ and an element $g \in G$ such that $\varphi(G_f) = G_g + g$. Here "addition plus g" means that we add g to all elements of G_f, hence it is not "addition" in the group algebra.*

Remark 2. If $g = (a, b)$, $a, b \in \mathbb{F}_2^n$, then $G_f + g$ is the graph of the mapping $x \mapsto f(x + a) + b$.

Definition 3. *Let G be a multiplicatively written abelian group. We say that two group algebra elements A and B in $\mathbb{C}[G]$ are* **multiplier** *equivalent if there is a group automorphism φ of G such that $\varphi(A) = Bg$ for some $g \in G$. Note that we have to write $B \cdot g$ instead of "$B + g$" since we write G multiplicatively. In Definition 2, the group was written additively.*

Remark 3. The terminology "multiplier equivalence" is motivated by the investigation of difference sets, see [4] or [9], for instance. Note that graph equivalence for two functions f and g is the same as multiplier equivalence of G_f and G_g.

Remark 4. An automorphism φ of G does not fix, in general, the subgroups H and N setwise. If $\varphi(N) \neq N$, then $\varphi(G_f)$ is, in general, not the graph of a mapping $H \to N$. That makes the definition of graph equivalence seemingly less attractive since not all the elements in the orbit of G_f under group automorphisms are graphs of functions $H \to N$. We refer to [10] for a thorough discussion of graph equivalence (in that papers, the term *CCZ equivalence* was used, since CCZ equivalence was first introduced in a paper by Carlet, Charpin and Zinoviev [11].

There is another nice way to interpret graph equivalence via code equivalence. We will introduce this concept in Section 3.

The group algebra over $\mathbb{C}$ (or any algebra over an algebraically closed field) can be also described as a subalgebra of a matrix algebra: We label the rows and columns of a matrix with the elements of G. If $A = \sum_{g \in G} a_g \, g \in \mathbb{C}[G]$, then we define an embedding ι of $\mathbb{C}[G]$ into $\mathbb{C}^{(|G|,|G|)}$ by $\iota(A) = (a_{g,h})_{g,h \in G}$ with $a_{g,h} = a_{g^{-1}h}$. It is easy to see and well known that ι is an injective homomorphism (actually independent from G being abelian or not). Equation (3) becomes

$$(\iota(G_F))^2 = 2^n + 2 \cdot \iota(D_F). \tag{4}$$

Since the group is elementary abelian, G_f is symmetric, and (4) shows that any two different rows of $\iota(G_f)$ have inner product 0 or 2. We may think of this property as the "defining" property of an APN mapping, and this property is preserved by row and column permutations. This gives rise to another concept of "equivalence", which we call *design equivalence*:

Definition 4. *Two matrices A and B in $\mathbb{C}^{(n,n)}$ are called* **design equivalent** *if there are permutation matrices P and Q such that $B = P \cdot A \cdot Q$. If G is a group of oder n, then we call two group algebra elements A and B design equivalent if $\iota(A)$ and $\iota(B)$ have this property.*

Remark 5. If $A, B \in \mathbb{C}[G]$ are multiplier equivalent, then $\iota(A)$ and $\iota(B)$ are design equivalent, but not vice versa, as the following example shows:

Example 1. We define the two sets

$$A := \{x \in \mathbb{F}_2^6 \ : \ x_1x_2 + x_3x_4 + x_5x_6 = 1\}$$
$$B := \{x \in \mathbb{F}_2^6 \ : \ x_1x_2 + x_3x_4 + x_5x_6 + x_1x_5x_3 = 1\}$$

Using Magma [12] it is not very difficult to see that $\iota(A)$ and $\iota(B)$ are design equivalent. For this purpose, we define two *designs* using the matrices $\iota(A)$ and $\iota(B)$ as their incidence matrices: You may think of a design simply as a matrix with entries 0 and 1, where the columns correspond to points of the design, and the rows are the incidence vectors of blocks, see [9] for background from design theory. Magma checks quickly that the two designs corresponding to A and B are isomorphic which shows that there are permutation matrices P and Q such that $\iota(B) = P \cdot \iota(A) \cdot Q$. But the two sets are not multiplier equivalent since the function $f(x_1, \ldots, x_6) = x_1x_2 + x_3x_4 + x_5x_6$ which defines A is quadratic, and the function $g(x_1, \ldots, x_6) = x_1x_2 + x_3x_4 + x_5x_6 + x_1x_5x_3$ is of degree 3.

We note that the two functions f and g are *bent functions*, and the sets A and B are (Hadamard) difference sets, see Definition 6.

Two subsets associated with an APN function f are the graph G_f (which is basically the function) and D_f (which is a kind of derivative). In Section 3, we will investigate D_f in more detail. We note that design equivalence of the sets G_f and G_g (or graph equivalence of f and g) implies design equivalence of D_f and D_g. We state a more general result:

Proposition 2. *If $A, B \in \mathbb{C}^{(n,n)}$ are design equivalent, then $A^* \cdot A$ is design equivalent to $B^* \cdot B$, where " * " denotes "complex conjugate transpose".*

Proof. Write $B = PAQ$ for suitable permutation matrices P and Q. Then $Q^T A^* A Q = B^* B$. □

Since we may also add a multiple of the identity matrix to design equivalent matrices and do not destroy equivalence in this way, we obtain the following corollary:

Corollary 1. *If G_f and G_g are design equivalent for APN functions f and g, then D_f and D_g are also design equivalent, since $\iota(D_f) = \iota(G_f)^* \iota(G_f) - 2^n \, I$.*

There is another concept, closely related to APN functions, called "almost bentness". It is connected with the Walsh transform, which can be easily described in terms of group rings.

As before, let G be an abelian group 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). In our cases, this condition is trivially satisfied since $\mathbb{K}$ will be the field of complex numbers.

The 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.

The inversion formula implies what is called **Parseval's equation**:

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

Characters in elementary abelian 2-groups $\mathbb{F}_2^m$ can be easily described. We take any nondegenerate symmetric bilinear form $(\cdot|\cdot)$. Then the mapping $\chi_u : \mathbb{F}_2^m \to \mathbb{F}_2^m$ with $\chi_u(v) := (-1)^{(u|v)}$ is a character.

Quite often, $\mathbb{F}_2^m$ is realized as the additive group of $\mathbb{F}_{2^m}$. In this case, we may take the trace-bilinear form $(u|v) := \mathsf{tr}(u \cdot v)$, where $u, v \in \mathbb{F}_{2^m}$ and tr is the usual trace function $\mathsf{tr}(x) = x + x^2 + x^4 + \ldots + x^{2^{m-1}}$.

The multiset of character values of a group algebra element is called the **Walsh spectrum**. It is not invariant under equivalence since adding an element g to G_f gives multiplication of $\chi(G_f)$ by $\chi(g)$. The multiset of *absolute values* of the character values, which is called the **extended Walsh spectrum**, is invariant under graph equivalence. If f is APN, then Equation (3) gives the following connection between the Walsh

coefficients of D_f and G_f:

$$\frac{\chi(G_f)^2 - 2^n}{2} = \chi(D_f).$$

Therefore, the extended Walsh spectrum of f uniquely determines the Walsh spectrum of D_f and vice versa.

If f is linear then $G_f^2 = 2^n G_f$, hence the *nonzero* character values have absolute value 2^n. There must be a nonzero character value $\chi(G_f)$ for some nontrivial character χ: Otherwise G_f would be a group algebra element with $\chi_0(G_f) = 2^n$ and $\chi(G_f) = 0$ for all other characters. Fourier inversion shows that this is possible only if $G_f = \frac{1}{2^n}G$, which is absurd since G_f has coefficients 0 and 1. Hence, another nonlinearity criteria is to minimize the maximum nontrivial Walsh coefficient (in absolute value) of G_f. One can show that there is at least one character χ with $\chi(G_f)^2 \geq 2^{n+1}$ (apply Parseval's equation to G_f^2 and note that all coefficients in G_f^2 are even).

Definition 5. *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is* **almost bent (AB)** *if $|\chi(G_f)| \leq 2^{(n+1)/2}$ for all nontrivial characters χ.*

Remark 6. If f is an AB function, then the nontrivial character values are 0 and $\pm 2^{(n+1)/2}$. Moreover, AB functions can exist only for n odd, see [3], for instance.

From the proof that the maximum Walsh coefficient is $2^{(n+1)/2}$, the following Proposition follows almost immediately:

Proposition 3. *[13] Any AB function is APN.*

Remark 7. The converse of this proposition is not true. First of all, APN functions do exist also if n is even, where no AB functions can exist. Moreover, there are also APN functions with n odd which are not AB, for instance the mapping x^{-1}.

We are mainly interested in APN functions rather than AB functions. The following Theorem is important and justifies that the concept of "design equivalence" is also useful if one investigates the Walsh coefficients of functions:

Theorem 1. *Let A and B be elements in $\mathbb{C}[G]$, where G is an arbitrary abelian group. If A and B are design equivalent, then the extended Walsh spectrum of A and B are the same.*

Proof (Compare with the proof of Proposition 2). It is well known that the vectors $(\chi(h))_{h \in G}$ are eigenvectors of $\iota(A)$ with eigenvalue $\chi(A)$: Note that

$$\sum_{h \in G} a_{g^{-1}h} \chi(h) = \sum_{h \in G} a_h \chi(gh) = \chi(A) \cdot \chi(g),$$

hence all the elements in the matrix algebra $\iota(\mathbb{C}[G])$ can be diagonalized simultaneously, since it is an algebra of commuting matrices.

Let $\iota(B) = P \cdot \iota(A) \cdot Q$ for some permutation matrices P and Q. The extended Walsh spectrum of A is the multiset of eigenvalues of $A^* \cdot A$, where $A^* = \sum_{g \in G} \overline{a_g} g^{-1}$

since $\chi(A^*) = \overline{\chi(A)}$, the complex conjugate of $\chi(A)$. It is not difficult to see that $\iota(A^*) = \iota(A)^*$, where $\iota(A)^*$ is the complex conjugate transpose matrix of $\iota(A)$. We have $\iota(B)^* \cdot \iota(B) = Q^T \cdot \iota(A)^* \cdot \iota(A) \cdot Q$, hence the multisets of eigenvalues of $\iota(B)^* \cdot \iota(B)$ and $\iota(A)^* \cdot \iota(A)$ coincide. □

If f is AB, then $\chi(D_f) = 2^{n-1}$ if $\chi(G_f) = 2^{(n+1)/2}$ and $\chi(D_f) = -2^{n-1}$ if $\chi(G_f) = 0$. Therefore, D_f is a subset of $\mathbb{F}_2^{2n}$ with $|\chi(D_f)|^2 = 2^{2n-2}$ for all nontrivial characters χ and $\chi_0(D_f) = 2^{2n-1} - 2^{n-1}$. Subsets with this property are called *Hadamard difference sets*. The indicator function of a Hadamard difference set D, i.e. the function $\mathrm{ind}(x) = 1$ if $x \in D$ and $\mathrm{ind}(x) = 0$ otherwise, is called a *bent* function. More precisely:

Definition 6. *Let G be an abelian group of order $4u^2$. A subset D of G, $|D| = 2u^2 - u$, such that the list of differences $d - d'$ with $d, d' \in D$, $d \neq d'$, covers every nonidentity element of G exactly $u^2 - u$ times is called a* **Hadamard difference set** *of type $-$. The complement D' of D has the property that every element is covered exactly $u^2 + u$ times, and the order of D' is $2u^2 + u$ (Hadamard difference sets of type $+$).*

Remark 8. For the general definition of difference sets and many references and examples and theoretical approaches, we refer to [9].

We summarize the discussion above in the following Proposition:

Proposition 4. *[11] If $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is AB, then the set D_f is a Hadamard difference set of type $-$.*

Many examples of Hadamard difference sets are known if G is an elementary abelian 2-group. Again, we refer to [2]. The most classical construction is the following:

Example 2. If $m = 2n$ is even, then the set

$$D := \{x \in \mathbb{F}_2^{2n} \ : \ x_1x_2 + x_3x_4 + \cdots + x_{2n-1}x_{2n} = 1\}$$

is a Hadamard difference set of type $-$.

It seems that only very few of the known Hadamard difference sets can be constructed as a set D_f for some AB function f. For instance, there are, up to affine equivalence, precisely 4 different Hadamard difference sets in $\mathbb{F}_2^6$ (see [14, 15]), but only one of them occurs as D_f, since there is, up to affine equivalence, just one AB function $f : \mathbb{F}_2^3 \to \mathbb{F}_2^3$. The Hadamard difference set in this case is the classical quadratic example in 2. However, for larger n, the D_f's are other bent functions. For quadratic functions, they all belong to the Maiorana-McFarland class, as we will see later. Here we just mention this important class of Hadamard difference sets:

*Example 3 (***Maiorana-McFarland construction***, see [16]).* Let $H_1, \ldots, H_{2^n-1}$ be the $2^n - 1$ different hyperplanes in $\mathbb{F}_2^n$. Let $g_1, \ldots, g_{2^n}$ be arbitrary elements in $\mathbb{F}_2^n$. Let $v_1, \ldots v_{2^n-1}$ be different elements of $\mathbb{F}_2^n$. Then the set

$$\bigcup_{i=1}^{2^n-1} (v_i, H_i + g_i) \subset \mathbb{F}_2^n \times \mathbb{F}_2^n$$

is a Hadamard difference set of type $-$.

Remark 9. The Hadamard difference set in Example 2 is of Maiorana-McFarland type.

3 APN functions and their groups

If $f, g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are APN functions (or any functions), then we have called the two functions *graph equivalent* if G_f and G_g are *multiplier equivalent*. The group of affine transformations $v \mapsto \varphi(v) + g$ preserves the APN property, but, as explained in the last Section, may map G_f to some group algebra element which is not the graph of a function.

Let us describe several groups corresponding to a group algebra element $A \in \mathbb{C}[G]$ in general. Then we may apply the definitions both to G_f and D_f.

Definition 7. *Let G be a multiplicatively written group G, and let $A \in \mathbb{C}[G]$. The* **multiplier group** *$\mathcal{M}(A)$ of A consists of all automorphisms φ of G such that $\varphi(A) = A \cdot g$ for some $g \in G$. The* **automorphism group** *of A consists of all affine transformations $\tau_{\varphi,g} : x \mapsto \varphi(x) \cdot g$ such that $\tau_{\varphi,g}(A) = A \cdot h$ for some $h \in G$. The* **design automorphism group** *$Aut(A)$ consists of all pairs of permutation matrices (P, Q) such that $P \cdot \iota(A) \cdot Q = \iota(A)$.*

Remark 10. The automorphism group of A is contained in the design automorphism group of A, hence the **translations** $x \mapsto x \cdot g$ are design automorphisms.

Remark 11. The group generated by $\mathcal{M}(A)$ and the translations is the normalizer of the group of all translations $x \mapsto x \cdot g$, $g \in G$, in the design automorphism group.

From now on, G is always an elementary abelian group $\mathbb{F}_2^m$. We are going to describe how we can determine the multiplier group of A and how we can explain multiplier equivalence of two subsets $A, B \in G$ via code equivalence. We define an $(m+1) \times |A|$-matrix A^{ext} over $\mathbb{F}_2$ as follows: The columns of the matrix are the vectors $(1, v)^T$ with $v \in A$. The row space of this matrix is called the *code* $\mathcal{A}$ of A^{ext}. We define the analogous matrix for a subset B. If A and B are equivalent, then obviously $|A| = |B|$, and denote this number by a. The two codes $\mathcal{A}$ and $\mathcal{B}$ are called **code equivalent** if there is a permutation matrix P of size $a \times a$ and an invertible matrix U of size $m + 1 \times m + 1$ such that

$$U \cdot A^{\text{ext}} = A^{\text{ext}} \cdot P,$$

see [17], for instance. Since both the row space of A^{ext} and of B^{ext} contain the all-one-vector $(1, \ldots, 1)$, we may assume without loss of generality that the first row of U is $(1, 0, \ldots, 0)$. Thus, U is of type

$$\begin{pmatrix} 1 & 0 \cdots & 0 \\ v_1 & * \cdots & * \\ \vdots & \vdots \ddots & \vdots \\ v_m & * \cdots & * \end{pmatrix},$$

i.e. there is an invertible matrix $W \in \mathbb{F}_2^{(m,m)}$ and $v \in \mathbb{F}_2^m$ such that

$$U = \begin{pmatrix} 1 & 0 \\ v & W \end{pmatrix}.$$

This shows that there is an automorphism φ (defined by the matrix W) of $\mathbb{F}_2^m$ and an element $v \in \mathbb{F}_2^m$ such that $\varphi(A) + v = B$. We summarize this discussion in the following Theorem:

Theorem 2. *Two subsets A, B of $\mathbb{F}_2^m$ are multiplier equivalent (see Definition 3) if and only if the codes defined by the rows of the extended matrices A^{ext} and B^{ext} are isomorphic.*

Given a permutation matrix P, the corresponding matrix U is, in general, not unique. However, if the rank of A^{ext} is $m+1$, then U and hence W is uniquely determined by P. This shows the following:

Corollary 2. *Let A be a subset of $\mathbb{F}_2^m$, such that $m+1$ is the $\mathbb{F}_2$-rank of A^{ext}. Then the automorphism group of the code $\mathcal{A}$ is isomorphic to the automorphism group of A.*

The condition in Corollary 2 is satisfied for the sets G_f and D_f corresponding to APN functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $n > 2$:

Proposition 5. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function, $n > 2$. Then the $\mathbb{F}_2$-rank of the matrices D_f^{ext} and G_f^{ext} is $2n+1$.*

Proof. It is shown in [18], for instance, that the rank of G_f^{ext} is $2n+1$. In other words, there is no vector $v \in \mathbb{F}_2^{2n}$ such that $(v|w) = 1$ for all $w \in G_f$ or $(v|w) = 0$ for all $w \in G_f$. The matrix D_f has the vectors $w + w'$, $w, w' \in G_f$, $w \neq w'$, as columns. If the rank of D_f^{ext} were smaller than $2n+1$, there would be a vector v with $(v|w) + (v|w') = 1$ or $= 0$ for all $w, w' \in G_f$, $w \neq w'$. Obviously, it is impossible that $(v|w) + (v|w') = 1$ for all w, w': We choose three different elements w_1, w_2 and w_3 in G_f. Then $(v|w_1) + (v|w_2) = 1$ and $(v|w_2) + (v|w_3) = 1$, hence $(v|w_1) + (v|w_3) = 0$. If $(v|w) + (v|w') = 0$ for all w, w', we had $(v|w) = (v|w')$ for all $w, w' \in G_f$, which contradicts $\text{rank}(G_f^{\text{ext}}) = 2n+1$, as indicated at the beginning of this proof. □

Since it is rather easy (using Magma) to determine the automorphism groups of "small" codes (we can handle the codes associated with D_f up to $n = 8$), Magma provides us with a powerful tool to determine the automorphism and the multiplier groups of both sets G_f and D_f associated with APN functions. It seems to be harder to determine the design automorphism groups, see also [8].

4 Computational results

It seems to be quite difficult to determine invariants like the automorphism groups of the sets D_f and G_f theoretically. Therefore, we do not include a table of all known infinite families of APN functions here, since we cannot prove any theoretical results about these series. We refer to [3] for the known families. Here we just mention that by now many infinite families of so called quadratic APN functions are known: We call f **quadratic** if the functions $x \mapsto f(x+a) + f(x) + f(a) + f(0)$ are linear.

Many APN's for small values of n ($n \leq 12$) are constructed by computer, which are not yet members of infinite families of APN functions. With the exception of one

example in [1], all recently constructed functions are graph equivalent to a quadratic function.

Besides the many quadratic examples, we think that the classical *Kasami* family is one of the most interesting series:

Proposition 6 ([19, 20], see also [21]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the power mapping x^d, where $d = 2^i + 1$ or $d = 2^{2i} - 2^i + 1$. If $\gcd(i, n) = 1$ (if n is odd) or $n/\gcd(i, n)$ is odd (if n is even), then f is APN. The cases $d = 2^i + 1$ are called the* **Gold** *cases, the cases $d = 2^{2i} - 2^i + 1$ the* **Kasami** *cases.*

Remark 12. The Gold power mappings are quadratic.

In the next tables, we determine the orders of the multiplier groups of the sets D_f, where f is one of the APN functions in [1] with $n \leq 8$.

Another question is whether the sets D_f or G_f are equivalent. It turns out that in all known examples with $n \leq 9$ so far, the sets D_f are not design equivalent if the functions are not graph equivalent. This implies, in view of Corollary 1, that also the G_f are not design equivalent for functions which are not graph equivalent. So we think that one should try to find criteria to distinguish the "designs" corresponding to G_f and D_f theoretically. The situation with the sets D_f is similar: The sets D_f are "weaker", i.e. when you compute D_f from G_f, you "loose" information about f. There seems to be no reason that a set A can occur as the set D_f for just one APN function f, but for the small examples in our tables, that is the situation.

Let us summarize this observation in the following proposition:

Proposition 7. *The sets D_f and therefore also the sets G_f are pairwise design inequivalent for the different APN functions listed in [1].*

Proof. The proof relies on computations done with Magma. We have checked some invariants which are easy to compute (Walsh spectrum, $\mathbb{F}_2$-ranks, full (design) automorphism groups). However, this is not sufficient to distinguish all the sets D_f. In this case, we computed the so called *triple intersection numbers*: We may think of D_f as a $0-1$ matrix $\iota(D_f)$. Given three different rows of $\iota(D_f)$, we call the number of columns where all rows have entry 1 a *triple intersection number*.

The spectrum, i.e. the multiset of all these triple intersection numbers, is an invariant under design isomorphism. We used these numbers in order to distinguish the isomorphism type of the sets which could not be distinguished otherwise. □

We think that it should be possible to determine some of the invariants which we discussed here (triple intersection numbers, automorphism groups) as well as some of the invariants discussed elsewhere (in particular the $\mathbb{F}_2$-ranks of the incidence matrices $\iota(D_f)$ and $\iota(G_f)$) theoretically, in particular, if the functions f are quadratic. If f is quadratic, then the functions $x \mapsto f(x + a) - f(x)$ are (affinely) linear for all $a \in \mathbb{F}_2^n$. Hence the sets

$$H_a := \{f(x + a) - f(x) \ : \ x \in \mathbb{F}_2^n\}$$

are (affine) hyperplanes of codimension 1. The sets D_f are (for quadratic f)

$$D_f = \bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (a, H_a).$$

If f is AB, these are precisely Maiorana-McFarland Hadamard difference sets.

APN functions f for which the sets H_a are always affine hyperplanes are called *crooked*, see [22]. There is an interesting conjecture about crooked functions, see [23, 24] for partial results towards this conjecture.

Conjecture 1. A crooked functions must be quadratic.

As mentioned above, we know no example of a set D_f such that there exists a function g which is graph or design inequivalent to f and which satisfies $D_g = D_f$.

Question 1. Do the sets D_f determine f up to graph or design equivalence?

We note that the first author of this paper describes an interesting way how to reconstruct f from D_f if f is quadratic (under some additional assumption) [25].

Finally, we know of no example of an APN function f such that the "classical" example of a Hadamard difference set (Example 2) occurs as the set D_f (if $n > 3$).

Conjecture 2. Show that none of the bent functions D_f which occur from APN functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are quadratic (Example 2).

4.1 Tables of APN functions, $n \leq 8$

In Tables 5–7, we recall the list of APN functions constructed via "switching" in [1]. For the convenience of the reader, we use the same numbering as in [1], which is related to the switching process that has been used to construct the examples. We emphasize that this list of APN functions is complete only if $n = 5$ (see [26]): For $n \geq 6$, many more APN functions may exist. For $n \leq 4$, only one APN function exists (up to graph equivalence), which is x^3. The examples listed here are graph inequivalent, and the sets G_f are pairwise design inequivalent. This follows from [1].

In the tables, u always denotes a primitive element in the respective field.

Table 3. Used primitive polynomials $p(x)$

n	$p(x)$
5	$x^5 + x^2 + 1$
6	$x^6 + x^4 + x^3 + x + 1$
7	$x^7 + x + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$

4.2 Tables of orders of multiplier groups

In Tables 9–11, we determine the multiplier groups and automorphism groups of G_f and D_f. This extends the tables in [1], where we did not determine the multiplier groups of D_f.

Moreover, we point out that in [1] there is a misprint in Table 10. The order of the group $\mathcal{M}(G_f)$ for $n = 8$, for the function f No. 1.2 is incorrect. The correct value is contained in Table 11.

Table 4. All graph equivalence classes of APN's in $\mathbb{F}_2^5$

$n = 5$	
No.	$F(x)$
1.1	x^3
1.2	x^5
2.1	x^{-1}

Table 5. Known graph equivalence classes of APN's in $\mathbb{F}_2^6$

$n = 6$	
No.	$F(x)$
1.1	x^3
1.2	$x^3 + u^{11}x^6 + ux^9$
2.1	$x^3 + ux^{24} + x^{10}$
2.2	(No. 2.1) $+u^3(\mathsf{tr}(u^{10}x^3 + u^{53}x^5) + \mathsf{tr}_{8/2}(u^{36}x^9))$
2.3	(No. 2.1) $+\mathsf{tr}(u^{34}x^3 + u^{48}x^5) + \mathsf{tr}_{8/2}(u^9x^9)$
2.4	(No. 2.1) $+u^2(\mathsf{tr}(u^{24}x^3 + u^{28}x^5) + \mathsf{tr}_{8/2}(x^9))$
2.5	(No. 2.3) $+u^{42}(\mathsf{tr}(u^{10}x^3 + u^{51}x^5) + \mathsf{tr}_{8/2}(u^9x^9))$
2.6	(No. 2.3) $+u^{23}(\mathsf{tr}(u^{31}x^3 + u^{49}x^5) + tr_{8/2}(u^9x^9))$
2.7	(No. 2.3) $+u^{12}(\mathsf{tr}(u^{42}x^3 + u^{13}x^5) + \mathsf{tr}_{8/2}(u^{54}x^9))$
2.8	(No. 2.3) $+u(\mathsf{tr}(u^{51}x^3 + u^{60}x^5) + \mathsf{tr}_{8/2}(u^{18}x^9))$
2.9	(No. 2.3) $+u^{14}(\mathsf{tr}(u^{18}x^3 + u^{61}x^5) + \mathsf{tr}_{8/2}(u^{18}x^9))$
2.10	(No. 2.3) $+u^{17}(\mathsf{tr}(u^{50}x^3 + u^{56}x^5))$
2.11	(No. 2.3) $+u^{19}(\mathsf{tr}(u^{11}x^3 + u^7x^5 + u^{38}x^7 + u^{61}x^{11} + u^{23}x^{13}) + \mathsf{tr}_{8/2}(u^{54}x^9) + \mathsf{tr}_{4/2}(u^{42}x^{21}))$
2.12	(No. 2.4) $+u(\mathsf{tr}(u^{54}x^3 + u^{47}x^5) + tr_{8/2}(u^9x^9))$

Table 6. Known graph equivalence classes of APN's in $\mathbb{F}_2^7$

$n = 7$	
No.	$F(x)$
1.1	x^3
1.2	$x^3 + \mathsf{tr}(x^9)$
2.1	$x^{34} + x^{18} + x^5$
2.2	$x^3 + x^{17} + x^{33} + x^{34}$
3.1	x^5
4.1	x^9
5.1	x^{13}
6.1	x^{57}
7.1	x^{-1}
8.1	$x^{65} + x^{10} + x^3$
9.1	$x^3 + x^9 + x^{18} + x^{66}$
10.1	$x^3 + x^{12} + x^{17} + x^{33}$
10.2	$x^3 + x^{17} + x^{20} + x^{34} + x^{66}$
11.1	$x^3 + x^{20} + x^{34} + x^{66}$
12.1	$x^3 + x^{12} + x^{40} + x^{72}$
13.1	$x^3 + x^5 + x^{10} + x^{33} + x^{34}$
14.1	$x^3 + x^6 + x^{34} + x^{40} + x^{72}$
14.2	$1\ x^3 + x^5 + x^6 + x^{12} + x^{33} + x^{34}$
14.3	(No. 14.1) $+u^{27}(\mathsf{tr}(u^{20}x^3 + u^{94}x^5 + u^{66}x^9))$

5 Some recent new results on APN functions

In this paper we have discussed the problem how to determine the isomorphism class of an APN function using the set D_f. We think that finding good invariants for the equivalence classes of designs is a challenging problem.

In this section, we would like to mention three very interesting recent results on APN functions which are not quite related to the topic of this paper, but which deserves to be mentioned.

5.1 Nonquadratic APN functions

We have noted that the many new examples of APN functions which have been constructed in the last few years are all graph equivalent to quadratic functions. There is only one exception: A single example of a new nonquadratic APN function $\mathbb{F}_2^6 \to \mathbb{F}_2^6$ has been constructed in [1]. This function (Case 2.11 in our table 5) is also inequivalent to a power mapping. It is the only nonquadratic example on $\mathbb{F}_2^6$ which is known. It is not yet a member of an infinite family. The construction uses a "switching" of known quadratic APN functions (switching means "changing one coordinate function", see [1].

5.2 APN permutations

Until recently, no APN permutation on $\mathbb{F}_2^n$ with n even was known, and it was conjectured that none can exist. This conjecture was shattered recently by John F. Dillon

Table 7. Known graph equivalence classes of APN's in $\mathbb{F}_2^8$

$n = 8$	
No.	$F(x)$
1.1	x^3
1.2	$x^3 + \mathsf{tr}(x^9)$
1.3	(No. 1.1) $+u(\mathsf{tr}(u^{63}x^3 + u^{252}x^9))$
1.4	(No. 1.2) $+u^{38}(\mathsf{tr}(u^{84}x^3 + u^{213}x^9))$
1.5	(No. 1.2) $+u^{51}(\mathsf{tr}(u^{253}x^3 + u^{102}x^9))$
1.6	(No. 1.3) $+u^{154}(\mathsf{tr}(u^{68}x^3 + u^{235}x^9))$
1.7	(No. 1.4) $+u^{69}(\mathsf{tr}(u^{147}x^3 + u^{20}x^9))$
1.8	(No. 1.5) $+u^{68}(\mathsf{tr}(u^{153}x^3 + u^{51}x^9))$
1.9	(No. 1.6) $+u^{35}(\mathsf{tr}(u^{216}x^3 + u^{116}x^9))$
1.10	(No. 1.7) $+u^{22}(\mathsf{tr}(u^{232}x^3 + u^{195}x^9))$
1.11	(No. 1.8) $+u^{85}(\mathsf{tr}(u^{243}x^3 + u^{170}x^9))$ $\quad (\sim x^9 + \mathsf{tr}(x^3))$
1.12	(No. 1.9) $+u^{103}(\mathsf{tr}(u^{172}x^3 + u^{31}x^9))$
1.13	(No. 1.10) $+u^{90}(\mathsf{tr}(u^{87}x^3 + u^{141}x^5 + u^{20}x^9) + \mathsf{tr}_{16/2}(u^{51}x^{17} + u^{102}x^{34}))$
1.14	(No. 1.11) $+u^5(\mathsf{tr}(u^{160}x^3 + u^{250}x^9))$
1.15	x^9
1.16	(No. 1.14) $+u^{64}(\mathsf{tr}(u^{133}x^3 + u^{30}x^9))$
1.17	(No. 1.16) $+u^{78}(\mathsf{tr}(u^{235}x^3 + u^{146}x^9))$
2.1	$x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48}$
3.1	$x^3 + u^{24}x^6 + u^{182}x^{132} + u^{67}x^{192}$
4.1	$x^3 + x^6 + x^{68} + x^{80} + x^{132} + x^{160}$
5.1	$x^3 + x^5 + x^{18} + x^{40} + x^{66}$
6.1	$x^3 + x^{12} + x^{40} + x^{66} + x^{130}$
7.1	x^{57}

Table 8. Orders of the groups of the sets G_f and D_f for $n = 5$

No.	$\lvert\mathcal{M}(G_F)\rvert$	$\frac{\lvert\mathrm{Aut}(G_f)\rvert}{2^{2n}\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathcal{M}(D_f)\rvert}{\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathrm{Aut}(D_f)\rvert}{2^{2n}\lvert\mathcal{M}(D_f)\rvert}$
1.1	$2^5 \cdot 5 \cdot 31$	1	1	1
1.2	$2^5 \cdot 5 \cdot 31$	1	32	1
2.1	$2 \cdot 5 \cdot 31$	1	1	1

Table 9. Orders of the groups of the sets G_f and D_f for $n = 6$

No.	$\lvert\mathcal{M}(G_F)\rvert$	$\frac{\lvert\mathrm{Aut}(G_f)\rvert}{2^{2n}\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathcal{M}(D_f)\rvert}{\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathrm{Aut}(D_f)\rvert}{2^{2n}\lvert\mathcal{M}(D_f)\rvert}$
1.1	$2^6 \cdot 6 \cdot 63$	1	1	2
1.2	$2^6 \cdot 63$	1	1	2
2.1	$2^7 \cdot 7$	1	1	1
2.2	2^6	1	1	1
2.3	2^6	1	1	1
2.4	2^6	1	1	1
2.5	$2^6 \cdot 5$	1	1	1
2.6	$2^6 \cdot 5$	1	1	1
2.7	2^6	1	1	1
2.8	2^6	1	1	1
2.9	2^6	1	1	1
2.10	2^6	1	1	1
2.11	2^3	1	1	1
2.12	$2^6 \cdot 7$	1	2	1

Table 10. Orders of the groups of the sets G_f and D_f for $n = 7$

No.	$\lvert\mathcal{M}(G_F)\rvert$	$\frac{\lvert\mathrm{Aut}(G_f)\rvert}{2^{2n}\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathcal{M}(D_f)\rvert}{\lvert\mathcal{M}(G_f)\rvert}$	$\frac{\lvert\mathrm{Aut}(D_f)\rvert}{2^{2n}\lvert\mathcal{M}(D_f)\rvert}$
1.1	$2^7 \cdot 7 \cdot 127$	1	1	1
1.2	$2^7 \cdot 7$	1	1	1
2.1	$2^7 \cdot 7$	1	1	1
2.2	$2^7 \cdot 7$	1	1	1
3.1	$2^7 \cdot 7 \cdot 127$	1	1	1
4.1	$2^7 \cdot 7 \cdot 127$	1	2^7	1
5.1	$7 \cdot 127$	1	1	1
6.1	$7 \cdot 127$	1	1	1
7.1	$2 \cdot 7 \cdot 127$	1	1	1
8.1	$2^7 \cdot 7$	1	1	1
9.1	$2^7 \cdot 7$	1	1	1
10.1	$2^7 \cdot 7$	1	1	1
10.2	$2^7 \cdot 7$	1	1	1
11.1	$2^7 \cdot 7$	1	1	1
12.1	$2^7 \cdot 7$	1	1	1
13.1	$2^7 \cdot 7$	1	1	1
14.1	$2^7 \cdot 7$	1	1	1
14.2	$2^7 \cdot 7$	1	1	1
14.3	2^7	1	1	1

Table 11. Orders of the groups of the sets G_f and D_f for $n = 8$

No.	$\lvert\mathcal{M}(G_F)\rvert$	$\frac{\lvert\mathcal{M}(D_f)\rvert}{\lvert\mathcal{M}(G_f)\rvert}$
1.1	$2^{11} \cdot 255$	1
1.2	$2^{11} \cdot 3$	1
1.3	$2^{10} \cdot 3$	1
1.4	$2^{8} \cdot 3$	1
1.5	$2^{10} \cdot 3$	1
1.6	$2^{10} \cdot 3$	1
1.7	$2^{9} \cdot 3$	1
1.8	$2^{10} \cdot 3$	1
1.9	$2^{10} \cdot 3$	1
1.10	$2^{9} \cdot 3$	1
1.11	$2^{11} \cdot 3$	1
1.12	$2^{10} \cdot 3$	1
1.13	2^{9}	1
1.14	$2^{8} \cdot 3$	1
1.15	$2^{11} \cdot 255$	16
1.16	$2^{9} \cdot 3$	1
1.17	$2^{9} \cdot 3$	1
2.1	$2^{10} \cdot 9 \cdot 5$	1
3.1	$2^{10} \cdot 3$	1
4.1	2^{11}	1
5.1	2^{11}	1
6.1	2^{11}	1
7.1	$2^{3} \cdot 255$	1

and Adam Wolfe [27]. They constructed an APN permutation on $\mathbb{F}_2^6$. The function is graph equivalent to Example 2.1 in Table 5, and it is so far the only one! There is a nice coding theoretic interpretation for the existence of bijective APN functions, see [27]. Using this interpretation, Dillon was able to show that for small n, none of the other known APN functions is equivalent to a permutation. This has been also confirmed by the first author of this paper: He checked that none of the APN functions in [1] is graph equivalent to a permutation, except the Dillon permutation.

It is now a challenging problem to find more APN permutations or to prove that no other example may exist.

5.3 Exceptional Exponents

There are several power mappings x^d which are APN functions. The *Gold* and the *Kasami* exponents (see example 6) are APN functions for infinitely many fields $\mathbb{F}_2^n$. An exponent d with the property that there are infinitely many fields where x^d is APN has been called an exceptional exponent. It has been conjectured (see [28]) that the *Gold* and *Kasami* exponents are the only exceptional exponents. This conjecture has now been proven: A major step towards a proof is contained in [29], and the missing cases are treated in [30].

6 Conclusions

We have determined the automorphism groups of the sets D_f where f is one of the APN function on $\mathbb{F}_2^n$, $n \leq 8$, described in [1]. Surprisingly, all the sets D_f are inequivalent.

If n is odd and f is almost bent, the sets D_f are Hadamard difference sets (or, equivalently, bent functions). None of these difference sets is equivalent to the classical quadratic Hadamard difference sets.

The results of this paper indicate that the sets D_f are apparently good "distinguishers" for APN functions. In the quadratic case, they are quite easy to describe and therefore they can be used (hopefully) for theoretical (computer free) proofs for the inequivalence of quadratic APN functions.

Most of the ideas in this paper can be also used to investigate arbitrary Hadamard difference sets or related objects (like partial difference sets) in elementary abelian groups.

References

1. Edel, Y., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3** (2009) 59–81
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In Crama, Y., Hammer, P., eds.: Boolean Methods and Models. Cambridge University Press (to appear) http://www-roc.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf.
3. Carlet, C.: Vectorial boolean functions for cryptography. In Crama, Y., Hammer, P., eds.: Boolean Methods and Models. Cambridge University Press (to appear) http://www-roc.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf.

4. Edel, Y., Pott, A.: On the equivalence of nonlinear functions. In Preneel, B., Dodunekov, S., Rijmen, V., Nikova, S., eds.: Enhancing Cryptographic Primitives with Techniques from Coding Theory, NATO Advanced Research Workshop, IOS Press (2009) 87–103
5. Göloğlu, F., Pott, A.: Almost perfect nonlinear functions: A possible geometric approach. In Nikova, S., Preneel, B., Storme, L., Thas, J., eds.: Coding Theory and Cryptography II, Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten (2007) 75–100
6. Edel, Y., Kyureghyan, G., Pott, A.: A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory **52**(2) (2006) 744–747
7. Budaghyan, L., Carlet, C., Leander, G.: On inequivalence between known power APN functions. In: International Conference on Boolean Functions: Cryptography and Applications. (2008) to appear.
8. Dempwolff, U.: Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups. Comm. Algebra **34**(3) (2006) 1077–1131
9. Beth, T., Jungnickel, D., Lenz, H.: Design Theory. 2 edn. Cambridge University Press, Cambridge (1999)
10. Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory **52**(3) (2006) 1141–1152
11. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2) (1998) 125–156
12. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. i. the user language. J. Symbolic Comput. **24**(3–4) (1997) 235–265
13. Chabaud, F., Vaudenay, S.: Links between differential and linear cryptanalysis. In Santis, A.D., ed.: Advances in Cryptology – EUROCRYPT 94. Volume 950 of Lecture Notes in Computer Science., New York, Springer-Verlag (1995) 356–365
14. Preneel, B.: Analysis and Design of Cryptographic Hash Functions. PhD thesis, Katholieke Universiteit Leuven (1993)
15. Rothaus, O.S.: On "bent" functions. J. Combinatorial Theory Ser. A **20**(3) (1976) 300–305
16. McFarland, R.L.: Difference sets in abelian groups of order $4p^2$. Mitt. Math. Sem. Giessen (192) (1989) i–iv, 1–70
17. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. II. North-Holland Publishing Co., Amsterdam (1977) North-Holland Mathematical Library, Vol. 16.
18. Browning, K., Dillon, J., Kibler, R., McQuistan, M.: APN polynomials and related codes. submitted (2008)
19. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation function. IEEE Trans. Inf. Th. **14** (1968) 154–156
20. Kasami, T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. Information and Control **18** (1971) 369–394
21. Dillon, J.F.: Multiplicative difference sets via additive characters. Des., Codes, Cryptogr. **17**(1/2/3) (September 1999) 225–235
22. Bending, T.D., Fon-Der-Flaass, D.: Crooked functions, bent functions, and distance regular graphs. Electron. J. Combin. **5** (1998) Research Paper 34, 14 pp. (electronic)
23. Bierbrauer, J., Kyureghyan, G.M.: Crooked binomials. Des. Codes Cryptogr. **46**(3) (2008) 269–301
24. Kyureghyan, G.M.: Crooked maps in $\mathbb{F}_{2^n}$. Finite Fields Appl. **13**(3) (2007) 713–726
25. Edel, Y.: On quadratic APN functions and dimensional dual hyperovals. http://www.mathi.uni-heidelberg.de/ yves/Papers/APNdho.html
26. Brinkmann, M., Leander, G.: On the classification of APN functions up to dimension five. Des., Codes, Cryptogr. **1–3** (2008) 273–288
27. Dillon, J.F.: slides from invited talk "APN Polynomials–An Update", given at "The 9th International Conference on Finite Fields and their Applications", held at University College Dublin. http://mathsci.ucd.ie/ gmg/Fq9Talks/Dillon.pdf (2009)

28. Janwa, H., Wilson, R.M.: Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in $\mathrm{char}.\ 2$ and some applications to cyclic codes. In: Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993). Volume 673 of Lecture Notes in Comput. Sci. Springer, Berlin (1993) 180–194
29. Jedlicka, D.: APN monomials over $\mathrm{GF}(2^n)$ for infinitely many n. Finite Fields Appl. **13**(4) (2007) 1006–1028
30. Hernando, F., McGuire, G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. arXiv:0903.2016v3 (2009)