On quadratic APN functions and dimensional dual hyperovals

Yves Edel
Department of Pure Mathematics and Computer Algebra
Ghent University
Krijgslaan 281, S22, B-9000 Ghent, Belgium

Abstract

In this paper we characterize the d-dimensional dual hyperovals in $PG(2d+1,2)$ that can be obtained by Yoshiara's construction [21] from quadratic APN functions and state a one-to-one correspondence between the extended affine equivalence classes of quadratic APN functions and the isomorphism classes of these dual hyperovals.

1 Introduction

Motivated by applications in cryptography, a lot of research has been done to construct functions which are "as nonlinear as possible" (see e.g. [7, 12] for a recent overview and references). One class of such functions are **almost perfect nonlinear (APN)** functions.

Definition 1. *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called **APN** if and only if for all $a \in \mathbb{F}_2^n \setminus \{0\}$ and $b \in \mathbb{F}_2^n$ the equation $f(x+a)+f(x) = b$ has at most two solutions. An APN function is called **quadratic** if, for every a, $B_f(a,x) := f(x+a)+f(x)+f(a)+f(0)$ is a linear function.*

Another important class of nonlinear functions are **almost bent (AB)** functions. AB functions can exist only if n is odd. It is well known that any AB function is also APN (see [6]), but not vice versa. However, for odd n, any quadratic APN function must be AB (see [8]).

APN functions have links to other mathematical objects. An APN function is equivalent to a binary error correcting $[2^n, 2^n-2n-1, 6]_2$ code, which is contained in the dual of the first order Reed-Muller code (see [8]).

There are also links to finite geometry [14, 16, 21]. In this paper we focus on the link with dual hyperovals, objects introduced by Huybrechts and Pasini [15]. The reader who is not familiar with projective geometries may wish to read section 2.1 first.

Definition 2. *A set $\mathcal{D}$ of d-dimensional subspaces of a projective geometry $PG(k,q)$, with $|\mathcal{D}| = 1+(q^{d+1}-1)/(q-1)$, is called a ($d$-dimensional) **dual hyperoval** if the intersection of any two distinct elements of $\mathcal{D}$ is a point and any three have an empty intersection.*

The projective geometry generated by the subspaces of $\mathcal{D}$ is called its ***ambient space****.*

The smallest space in which a d-dimensional dual hyperoval can exist is $PG(2d, q)$. Cooperstein and Thas [9] construct dual hyperovals in $PG(2d, 2)$ with the property $\bigcup_{D\in\mathcal{D}} D = PG(2d, 2) \setminus Y$, for some $(d-1)$-dimensional subspace Y. Del Fra [10] shows, that every hyperoval in $PG(2d, 2)$ is of this type.

In [21] Yoshiara gives the following construction of d-dimensional dual hyperovals $\mathcal{D}_f$ in $PG(2d+1, 2)$ using a quadratic APN function $f : \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$

$$\mathcal{D}_f := \{D_a | a \in \mathbb{F}_2^{d+1}\} \text{ with } D_a := \{(x, B_f(a, x)) | 0 \neq x \in \mathbb{F}_2^{d+1}\}. \tag{1}$$

Here $B_f(a, x) = f(x + a) + f(x) + f(a) + f(0)$ as defined in Definition 1.

He proves that the dual hyperoval obtained from the APN function from [11] is not isomorphic to the known dual hyperovals. Moreover he states that Taniguchi's d-dimensional dual hyperovals in $PG(2d+1, 2)$ [18, 20] that can not be obtained in this way from an APN function.

In this paper we characterize the d-dimensional dual hyperovals in $PG(2d+1, 2)$ that can be obtained by Yoshiara's construction.

Definition 3. *A d-dimensional dual hyperoval $\mathcal{D}$ in $PG(2d+1, 2)$ is an* ***APN-dual hyperoval*** *if and only if the following hold:*

1. *There is a d-dimensional subspace Y such that $Y \cap \bigcup_{D\in\mathcal{D}} D = \emptyset$.*
2. *For any mutually different $A, B, C \in \mathcal{D}$ we have that*

$$(A \cap B) + (B \cap C) + (C \cap A) \in Y,$$

where for distinct points a and b of $PG(2d+1, 2)$, we denote by $a + b$ the point on the line joining a and b distinct from a and b.

Our main result is a one-to-one correspondence between the extended affine equivalence classes of quadratic APN functions (see Definition 5) and the isomorphism classes of APN-dual hyperovals (see Definition 4):

Theorem 1. *For any quadratic APN function $f : \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$ the set $\mathcal{D}_f$ as defined in equation (1) is a d-dimensional APN-dual hyperoval and for any d-dimensional APN-dual hyperoval $\mathcal{D}$ we can construct a quadratic APN function $f_{\mathcal{D}} : \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$, such that:*

- *If f, f' are extended affine equivalent quadratic APN functions then $\mathcal{D}_f$ and $\mathcal{D}_{f'}$ are isomorphic dual hyperovals.*
- *If $d \geq 2$ and if two APN-dual hyperovals $\mathcal{D}$ and $\mathcal{D}'$ are isomorphic then $f_{\mathcal{D}}$ and $f_{\mathcal{D}'}$ are extended affine equivalent.*
- *We have that $\mathcal{D}$ is isomorphic to $\mathcal{D}_{f_{\mathcal{D}}}$ and for $d \geq 2$ that f is extended affine equivalent to $f_{\mathcal{D}_f}$.*

An immediate consequence is that every new quadratic APN function gives rise to a new dual hyperoval. The only "classical" APN functions that are quadratic are the Gold functions [13, 17]. In [21, Proposition 3.2] Yoshiara mentions that his dual hyperovals (see [19]) are equivalent to those obtained from the Gold functions and that those are the only known d-dimensional dual hyperovals in $PG(2d+1,2)$ which can arise from APN functions. The APN functions are classified up to $n = 5$ [2]. All quadratic APN functions in this range are equivalent to the Gold functions.

Recently progress has been made in finding new APN functions. We just mention results on quadratic APN functions which are proven to be inequivalent to the Gold functions and refer again to [7, 12] as a reference on further known APN functions.

There are three infinite families of quadratic APN functions [5, 4] (see also [1]). In [3, 12] more than 40 inequivalent quadratic APN functions for $n \leq 9$ can be found . And last but not least there is the sporadic APN binomial for $n = 10$ [11] used by Yoshiara [21].

In the next section we will introduce the needed notation and give some auxiliary results. In the last section we will prove Theorem 1.

2 Preparatory section

2.1 Some notation

Let q be a prime power, $\mathbb{F}_q$ the finite field with q elements, and $\mathbb{F}_q^l$ the l-dimensional vector space over $\mathbb{F}_q$.

A k-dimensional **projective geometry** over $\mathbb{F}_q$ ($PG(k,q)$ for short) can be defined using its underlying vector space $\mathbb{F}_q^{k+1}$. For $0 \leq m \leq k$, the **m-dimensional subspaces** of $PG(k,q)$ are the $(m+1)$-dimensional subspaces of $\mathbb{F}_q^{k+1}$. Observe the shift in the dimension. The 0-, 1-, respectively 2-dimensional subspaces of $PG(k,q)$ are called **points**, **lines** and **planes**.

Containment and intersection of subspaces of $PG(k,q)$ is defined by containment and intersection of the corresponding subspaces of the underlying vector space.

In this paper, we work in $PG(2d+1,2)$. The points of $PG(2d+1,2)$ are in one-to-one correspondence with the non-zero vectors of $\mathbb{F}_2^{2d+2}$ (as a 1-dimensional subspace of $\mathbb{F}_2^{2d+2}$ consists only of the zero vector and one non-zero vector). This also justifies the notion $a+b$ in Definition 3; the vector in $\mathbb{F}_2^{2d+2}$ corresponding to $a+b$ is the sum of the vectors corresponding to a and b.

The **automorphisms** of $PG(2d+1,2)$ correspond to the invertible linear maps from $\mathbb{F}_2^{2d+2}$ to $\mathbb{F}_2^{2d+2}$.

Frequently, we denote a point in $PG(2d+1,2)$ by a pair $(x,y) \in (\mathbb{F}_2^{d+1} \times \mathbb{F}_2^{d+1}) \setminus \{(0,0)\}$, by identifying $\mathbb{F}_2^{d+1} \times \mathbb{F}_2^{d+1}$ with $\mathbb{F}_2^{2d+2}$. The automorphisms then will be denoted as 2×2 block matrices with the blocks being $(d+1)\times(d+1)$ matrices over $\mathbb{F}_2$.

We call a function $B : \mathbb{F}_2^{d+1} \times \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$ **symmetric** if $B(x,y) = B(y,x)$, **symplectic** if $B(x,x) = 0$ and **bilinear** if $B(x+x',y) = B(x',y) + B(x',y)$

and $B(x, y + y') = B(x, y) + B(x, y')$.

The frequently used function $B_f(x, y) := f(x + y) + f(x) + f(y) + f(0)$ is symmetric and symplectic. If f is quadratic then by definition B_f is also bilinear.

2.2 Auxiliary results

The following property of dual hyperovals follows from a simple counting argument:

Proposition 1. *Let $\mathcal{D}$ be a dual hyperoval. For any point $P \in \bigcup_{D\in\mathcal{D}} D$ there is exactly one pair $D \neq D' \in \mathcal{D}$ such that $P = D \cap D'$.*

The next proposition shows that the notion of APN-dual hyperovals (Definition 3) is well defined.

Proposition 2. *Let $\mathcal{D}$ be a dual hyperoval and $A, B, C \in \mathcal{D}$ mutually different. Then*

1. *the points $c := A \cap B$, $a := B \cap C$ and $b := C \cap A$ are not collinear,*
2. *the point $P(A, B, C) := a + b + c$ is the (unique) point in the plane $\langle a, b, c\rangle$ which is on none of the lines ab, bc and ca.*

Proof. 1: If a, b, c would be collinear, then, as $a, b \in C$ and C is a subspace, we have that also $c \in C$. Repeating this argument for A, B shows that the whole line is in $A \cap B \cap C$, a contradiction to the definition of a dual hyperoval.

2: From 1. we see that $P(A, B, C)$ lies in the Fano plane $\langle a, b, c\rangle$. The statement follows by direct verification. □

Lemma 1. *If f is a quadratic APN function, then $\mathcal{D}_f$ is a d-dimensional APN-dual hyperoval. If $d \geq 2$ then the ambient space of $\mathcal{D}_f$ is $PG(2d + 1, 2)$.*

Proof. That $\mathcal{D}_f$ is a dual hyperoval is [21, Theorem 2.1 (1)]. The result concerning the ambient space is [21, Proposition 2.2].

It only remains to prove the simple fact that $\mathcal{D}_f$ is an APN-dual hyperoval. By definition there are no points in the subspace $Y = \{(0, y)|y \in \mathbb{F}_2^{d+1} \setminus \{0\}\}$. Direct verification shows that $D_a \cap D_b = (a + b, B_f(a, b))$.

$$(D_a \cap D_b) + (D_b \cap D_c) + (D_c \cap D_a) = (0, B_f(a, b) + B_f(b, c) + B_f(c, a)) \quad (2)$$

Hence $\mathcal{D}_f$ is an APN-dual hyperoval with respect to Y. □

Lemma 2. *If f is a quadratic function and $\mathcal{D}_f$ is a dual hyperoval, then f is APN.*

Proof. Assume f is not APN but $\mathcal{D}_f$ is a dual hyperoval. Then there is some $a \neq 0$, and some b, such that $B_f(x, a) = f(x+a)+f(a)+f(a)+f(0) = b$ has more than two solutions, say $x = u, v, w$. Then the point $(a, B_f(x, a)) \in D_u \cap D_v \cap D_w$ for three mutually different u, v, w, contradicting Proposition 1. □

Lemma 3. *Let $d \geq 2$ and $\mathcal{D}$ be an APN-dual hyperoval constructed from an APN function f using (1) (so $\mathcal{D} = \mathcal{D}_f$). Then the subspace Y of the APN-dual hyperoval in Definition 3 is uniquely determined.*

Proof. Let $\mathcal{P}_f := \{P(A,B,C)|A,B,C \in \mathcal{D}_f \text{ mutually different}\}$. In (2) we have shown, that $\mathcal{P}_f = \{(0, B_f(a,b) + B_f(b,c) + B_f(c,a))|a \neq b \neq c \in \mathbb{F}_2^{d+1}\}$. Using that B_f is a symmetric, symplectic and bilinear function we see that

$$B_f(a,b) + B_f(b,c) + B_f(c,a) = B_f(a+c,b) + B_f(c,a) = B_f(a+c,a+b).$$

So we have $\mathcal{P}_f = \{(0, B_f(u,v))|u,v \in \mathbb{F}_2^{d+1} \setminus \{0\}\}$.

The subspace Y contains $\mathcal{P}_f$. If there would be another d-dimensional subspace Y' with this property, we would have $\mathcal{P}_f \subseteq Y \cap Y'$, a $(d-1)$-dimensional space. As the elements of $\mathcal{D}_f$ are defined as $D_a := \{(x, B_f(a,x))|x \neq 0 \in \mathbb{F}_2^m\}$ this would imply that the ambient space of $\mathcal{D}_f$ is PG(2d,2), contradicting Lemma 1. □

Dual hyperovals are sets of subspaces in $PG(k,q)$. Isomorphy is defined in the natural way.

Definition 4. *Two dual hyperovals in $PG(k,q)$ are called **isomorphic** if there is an automorphism of $PG(k,q)$ that maps one to the other.*

There are several concepts of equivalence for APN functions. We call the set of points $G_f := \{(1,x,f(x))|x \in \mathbb{F}_{2^n}\} \subset PG(2n,2)$ the **graph** of the function f and define the affine subspaces $X := \{(1,x,0)|x \in \mathbb{F}_{2^n}\}$, $Y := \{(1,0,y)|y \in \mathbb{F}_{2^n}\} \subset PG(2n,2)$.

Definition 5. *Two APN functions $f,g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called:*

- ***CCZ-equivalent**, if there is an automorphism of $PG(2n,2)$ mapping G_f to G_g,*
- ***extended affine (EA) equivalent**, if there is an automorphism of $PG(2n,2)$, fixing the subspace Y, which maps G_f to G_g,*
- ***affine equivalent**, if there is an automorphism of $PG(2n,2)$, fixing the subspaces X and Y, which maps G_f to G_g.*

On the affine points $(1,x,y)$ we can describe the automorphism by

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}.$$

We have EA-equivalence if and only if $B = 0$, and affine equivalence if and only if $B = C = 0$.

Affine equivalent functions are also EA-equivalent. EA-equivalent functions are also CCZ-equivalent. The algebraic degree of an APN function is an invariant under EA-equivalence but not under CCZ-equivalence. As we will focus in this article on quadratic APN functions (i.e. functions of algebraic degree 2), EA-equivalence is the appropriate concept here.

An other frequently found definition of EA-equivalence is the following; f and g are called EA-equivalent if there exist invertible affine mappings A_1, A_2 and a linear (or affine) mapping L such that

$$g(x) = A_2 f(A_1(x)) + L(x).$$

This definition is equivalent with the one given above as we can identify

$$A_1(x) = A^{-1}(x+u), \quad A_2(y) = D(y) + v + CA^{-1}u \quad \text{and} \quad L(x) = CA^{-1}x.$$

Lemma 4. *If f, g are EA-equivalent quadratic APN functions, then the dual hyperovals $\mathcal{D} := \mathcal{D}_f$ and $\mathcal{D}' := \mathcal{D}_g$ are isomorphic.*

If the EA-equivalence is given by the mapping

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} \tag{3}$$

the isomorphism of the dual hyperovals is given by:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Proof. We will use the following identity:

$$f(a+b+c)+f(a+b)+f(a+c)+f(b+c)+f(a)+f(b)+f(c)+f(0) = 0 \tag{4}$$

This is the bilinearity of B_f, i.e. $B_f(a+b,c) = B_f(a,c)+B_f(b,c)$, expanded as in Definition 1.

We rewrite the subspaces $D'_a = \{(x, g(x+a)+g(x)+g(a)+g(0)) | x \neq 0 \in \mathbb{F}_2^n\} \in \mathcal{D}'$ in terms of f. As f and g are EA-equivalent with equivalence relation (3) we can write $g(x) = CA^{-1}(x+u) + Df(A^{-1}(x+u)) + v$ and hence

$$\begin{aligned} & g(x+a)+g(a)+g(x)+g(0) = \\ & \qquad CA^{-1}(x+a+u) + Df(A^{-1}(x+a+u)) + \\ & \qquad CA^{-1}(a+u) + Df(A^{-1}(a+u)) + \\ & \qquad CA^{-1}(x+u) + Df(A^{-1}(x+u)) + \\ & \qquad CA^{-1}u + Df(A^{-1}u) \\ = \;& D(\, f(A^{-1}(x+u)) + f(A^{-1}(x+a+u)) + f(A^{-1}(a+u)) + f(A^{-1}u)\,) \\ = \;& D(\, f(A^{-1}(x+a)) + f(A^{-1}x) + f(A^{-1}a) + f(0)\,). \quad \text{(using (4))} \end{aligned}$$

Thus we have shown that

$$D'_a = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} D_{A^{-1}a}$$

□

The bilinear function $B_f(u,v) = f(x+a)+f(x)+f(a)+f(0)$ does not uniquely determine f but only the EA-equivalence class of f. This is due to the fact that in characteristic 2 the quadratic form is not uniquely determined by its bilinear form.

Lemma 5. *Given a symmetric, symplectic and bilinear function $B(u,v) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ we can construct a quadratic function g such that $B(u,v) = B_g(u,v)$. If we start from $B(u,v) = B_f(u,v)$, then g is EA-equivalent to f.*

If quadratic functions f, g have the same bilinear function, they are EA-equivalent.

Proof. The argument may look more familiar if we apply it to the component functions. Choose a basis of $\mathbb{F}_2^n$ over $\mathbb{F}_2$. Let $B^{(i)}(u,v) : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ the restriction of $B(u,v)$ to the i-th coordinate.

We would like to find a $g^{(i)}$ such that

$$B^{(i)}(u,v) = g^{(i)}(u+v) + g^{(i)}(u) + g^{(i)}(v) + g^{(i)}(0). \tag{5}$$

So, essentially, we want to reconstruct the quadratic form $g^{(i)}$ from the symplectic bilinear form $B^{(i)}$. But as we are in characteristic 2 the quadratic form is not uniquely determined by its bilinear form. We represent $B^{(i)}$ as a matrix $C^{(i)}$ with entries $c^{(i)}_{j,k}$ with respect to our chosen basis, so

$$B^{(i)}(u,v) = u^t C^{(i)} v, \text{ with } c^{(i)}_{j,k} = c^{(i)}_{k,j} \text{ and } c^{(i)}_{j,j} = 0.$$

Then the $g^{(i)}$ fulfilling equation (5) are

$$g^{(i)}_{d,e}(x) := \sum_{j<k} c^{(i)}_{j,k} x_j x_k + \sum_j d^{(i)}_j x_j^2 + e^{(i)}\,.$$

Choose $g := g_{0,0}$.

Let $f = g_{d,e}$ for some choice of the $d^{(i)}_j, e^{(i)} \in \mathbb{F}_2$. As $x_j \in \mathbb{F}_2$ we have that $x_j^2 = x_j$. So any choice of the $d^{(i)}_j, e^{(i)}$ gives an APN function which is EA-equivalent to g as

$$\begin{pmatrix} x \\ g_{d,e}(x) \end{pmatrix} = \begin{pmatrix} I & 0 \\ d & I \end{pmatrix} \begin{pmatrix} x \\ g(x) \end{pmatrix} + \begin{pmatrix} 0 \\ e \end{pmatrix}.$$

Two quadratic APN functions having the same bilinear function are EA equivalent to the same g, hence EA equivalent to one another. □

3 Proof of Theorem 1

We have defined the $\mathcal{D}_f$ associated with the quadratic APN function f in equation (1). In Lemma 1 we have shown that $\mathcal{D}_f$ is a d-dimensional APN-dual hyperoval. In Lemma 4 we have shown that EA-equivalent APN-functions f, g yield isomorphic dual hyperovals $\mathcal{D}_f$ and $\mathcal{D}_g$. This proves the direction from the quadratic APN function to the APN-dual hyperoval of Theorem 1.

In the remainder of this section we will show the opposite direction. Firstly, we describe the outline of the proof.

In Subsection 3.1, given an APN-dual hyperoval $\mathcal{D}$, we construct a symmetric, symplectic and bilinear function $B_{\mathcal{D}}$, such that applying the construction of a dual hyperoval as in equation (1) with this bilinear function leads to a dual hyperoval isomorphic to $\mathcal{D}$.

By Lemma 5 the bilinear function $B_{\mathcal{D}}$ gives rise to a quadratic function $f_{\mathcal{D}}$, which is APN by Lemma 2. In particular we have that $\mathcal{D}_{f_{\mathcal{D}}}$ is isomorphic to $\mathcal{D}$ as claimed in the theorem.

In subsection 3.2 we will show that if we start from isomorphic APN-dual hyperovals $\mathcal{D}$ and $\mathcal{D}'$, this construction gives us EA-equivalent APN functions $f_{\mathcal{D}}$ and $f_{\mathcal{D}'}$.

This proves Theorem 1.

3.1 The construction of $f_{\mathcal{D}}$

3.1.1 Recovering the $(x, M_D x)$ representation

Let $\mathcal{D}$ be an APN-dual hyperoval and Y be the d-dimensional subspace of Definition 3.1.

As explained in section 2.1 we think of the points in $PG(2d+1,2)$ as pairs $(x,y) \in \mathbb{F}_2^{d+1} \times \mathbb{F}_2^{d+1} \setminus \{(0,0)\}$.

We may choose a basis (for the underlying vector space of) of $PG(2d+1,2)$ such that $Y = \{(0,y) | \, y \in \mathbb{F}_2^{d+1} \setminus \{0\}\}$. Then for any two different points (x,y) and (x',y') in $D \in \mathcal{D}$ we have $x \neq x'$, because D is a subspace and hence the sum of two points is in D but no point of D is in Y by Definition 3.1.

As $X := \{(x,0) | \, x \in \mathbb{F}_2^{d+1} \setminus \{0\}\}$ and D are both d-dimensional subspaces, the projection of D to X is X. So there exists for all $D \in \mathcal{D}$ a linear map $M_D : \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$ such that

$$D = \{(x, M_D x) | \, x \in \mathbb{F}_2^{d+1} \setminus \{0\}\}.$$

3.1.2 Indexing the $D \in \mathcal{D}$

Next choose one $D \in \mathcal{D}$ and name it D_0. Applying an automorphism of $PG(2d+1,2)$, stabilizing the subspace Y, we can achieve that $D_0 = \{(x,0) | \, x \in \mathbb{F}_2^{d+1} \setminus \{0\}\}$.

Now we index any $D \neq D_0 \in \mathcal{D}$ with the $a \in \mathbb{F}_2^{d+1} \setminus \{0\}$ determined by $(a,0) = D \cap D_0$ i.e. we **rename** this D to D_a.

By the dual hyperoval properties the indexing is well defined. Every D is uniquely indexed by an element of $\mathbb{F}_2^{d+1}$. Moreover, every element of $\mathbb{F}_2^{d+1}$ appears as an index, because $|\mathcal{D}| = 2^{d+1}$.

So we now have written

$$\mathcal{D} = \{D_a | a \in \mathbb{F}_2^{d+1}\} \text{ with } D_a = \{(x, M_a x) | x \in \mathbb{F}_2^{d+1} \setminus \{0\}\} \tag{6}$$

Observe that a is the (full) kernel of M_a, i.e. $M_a(a) = 0$.

The dual hyperoval given in (6) is isomorphic to the dual hyperoval from which we started, as we only applied basis transformations.

3.1.3 The symmetry $M_a(b) = M_b(a)$

Let $a \neq b \neq 0$. By definition we have $(a,0) = D_a \cap D_0$ and $(b,0) = D_b \cap D_0$. Using (6) we can express $D_a \cap D_b =: (u, M_a(u))$ as an element of D_a.

By Definition 3.2 we have $u = a + b$. Observing that a is the kernel of M_a we see that $D_a \cap D_b = (a+b, M_a(a+b)) = (a+b, M_a(b))$.

If we express $D_a \cap D_b$ as an element of D_b, we see with the same argument that $D_a \cap D_b = (a+b, M_b(a))$. In particular we have shown:

$$M_a(b) = M_b(a).$$

Using this identity we get linearity in the index, as:

$$M_{a+b}(x) = M_x(a+b) = M_x(a) + M_x(b) = M_a(x) + M_b(x) \tag{7}$$

This equation trivially holds if one of a and b is 0 or $a = b$.

So $M_a(x) =: B_{\mathcal{D}}(a,x) : \mathbb{F}_2^{d+1} \times \mathbb{F}_2^{d+1} \to \mathbb{F}_2^{d+1}$ is a symmetric symplectic bilinear function.

As already mentioned in the outline of the proof, it follows from Lemma 5 that there exists a quadratic function $f_{\mathcal{D}}$ with $B_{\mathcal{D}} = B_{f_{\mathcal{D}}}$. Then the construction of $\mathcal{D}_{f_{\mathcal{D}}}$ given in equation (1) shows that $\mathcal{D} = \mathcal{D}_{f_{\mathcal{D}}}$. By Lemma 2 $f_{\mathcal{D}}$ is APN.

This proves the first part.

3.2 The equivalence

We have shown in (7) that M_u is additive in the index u. This implies, that the mapping ϕ_u with

$$\phi_u \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} I & 0 \\ M_u & I \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

is a automorphism of $\mathcal{D}$ mapping D_a to D_{a+u}.

The group $\{\phi_u | u \in \mathbb{F}_2^{d+1}\}$ is a transitive subgroup of the automorphism group of $\mathcal{D}$, hence the choice of D_0 in Section 3.1.2 has no effect on the bilinear function $B_{\mathcal{D}}$.

Now consider two isomorphic APN-dual hyperovals $\mathcal{D}$ and $\mathcal{D}'$. We may assume that both $\mathcal{D}$ and $\mathcal{D}'$ are already of the form of equation (6). As $\mathcal{D}$ has a transitive automorphism group we can assume that the isomorphism ψ mapping $\mathcal{D}$ to $\mathcal{D}'$, maps D_0 to D'_0, i.e. ψ fixes the subspace $X = D_0 = D'_0$.

We already have shown, that both dual hyperovals can be constructed from an APN function. By Lemma 3 the subspace Y is uniquely determined. Hence the isomorphism ψ also has to fix the subspace Y. So the isomorphism ψ mapping $\mathcal{D}$ to $\mathcal{D}'$ is given by

$$\psi \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

By Lemma 4 we can find an APN function g, EA-equivalent to $f_{\mathcal{D}}$, such that $\mathcal{D}_g = \mathcal{D}'$. Hence the bilinear functions B_g and $B_{\mathcal{D}'}$ are the same. By Lemma 5 we see that g and $f_{\mathcal{D}'}$ are EA-equivalent.

So we have that $f_{\mathcal{D}}$ and $f_{\mathcal{D}'}$ are EA-equivalent APN functions.

This proves the second statement and concludes the proof of Theorem 1.

Acknowledgements

The research of the 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.

References

[1] J. Bierbrauer, A family of crooked functions. *Des. Codes Cryptogr.*, **50** (2009), 235–241.

[2] M. Brinkmann and G. Leander, On the classification of APN functions up to dimension five. *Des. Codes Cryptogr.*, **49** (2008), 273–288.

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

[4] L. Budaghyan, C. Carlet and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Inform. Theory*, **54** (2008), 4218–4229.

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

[6] 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 Comput. Sci., New York, 1995, Springer-Verlag, 356–365.

[7] C. Carlet, Vectorial Boolean functions for cryptography. In *Boolean Methods and Models*, Y. Crama and P. Hammer eds., Cambridge University Press, to appear.

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

[9] B. N. Cooperstein and J. A. Thas, On generalized k-arcs in $PG(2n, q)$. *Ann. Comb.*, (2001) 141–152.

[10] A. Del Fra, On d-dimensional dual hyperovals. *Geom. Dedicata*, **79** (2000) 157–178.

[11] 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), 744–747.

[12] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, **3** (2009), 59–81.

[13] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation function. *IEEE Trans. Inform. Theory*, **14** (1968), 154–156.

[14] F. Göloglu and A. Pott, Almost Perfect Nonlinear Functions: A possible geometric approach. In *Proceedings of the contact forum Coding Theory and Cryptography II.*, Royal Flemish Academy of Belgium for Science and the Arts, (2008), 75–100.

[15] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces. *Bull. Belg. Math. Soc. Simon Stevin*, **5** (1998), 341–353.

[16] N. Nakagawa and S. Yoshiara, A Construction of Differentially 4-Uniform Functions from Commutative Semifields of Characteristic 2. *Lecture Notes in Comput. Sci.*, **4547** (2007), 134-146.

[17] K. Nyberg, Differentially uniform mappings for cryptography. In *Advances in Cryptography. EUROCRYPT'93*, vol. 765 of Lecture Notes in Comput. Sci., New York, 1994, Springer-Verlag, 55–64.

[18] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even. *European J. Combin.*, **26** (2005) 95–99.

[19] S. Yoshiara, Dimensional dual arcs a survey. In *Finite Geometires, Groups, and Computation*, A. Hulpke, B. Liebler, T. Penttila, and A. Seress eds., Walter de Gruyter, Berlin-New York, 2006, 247–266.

[20] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals. *European J. Combin.*, **28** (2007) 674–684.

[21] S. Yoshiara, Dimensional dual hyperovals associated with quadratic APN functions. *Innov. Incidence Geom.*, **8** (2008), 147–169.