Quadratic APN functions as subspaces of alternating bilinear forms

Yves Edel[*]
Department of Mathematics
Ghent University, Krijgslaan 281, S22
B-9000 Ghent, Belgium

In this note we illuminate and apply the equivalence of quadratic APN functions to certain subspaces of alternating bilinear forms. These subspaces can be characterized by the rank-distance of the dual subspace, or equivalently, as the subspaces of $\bigwedge^2 \mathbb{F}_2^m$ avoiding the variety of elements of rank 2. Or, in the geometric language, as subspaces external (or skew) to the line Grassmannian.

1 Introduction

Definition 1. *Let $\mathbb{F}_p$ be the finite field with p elements, p prime. A function*

$$F : \mathbb{F}_p^m \to \mathbb{F}_p^n$$

which satisfies, for all $0 \neq a \in \mathbb{F}_p^m$ and $b \in \mathbb{F}_p^n$,

$$|\{x \in \mathbb{F}_p^m \,|\, F(x+a) - F(x) = b\}| \leq d \tag{1}$$

with $d = 1$ is called **perfect nonlinear (PN)** *or* **planar**. *The function F is called* **almost perfect nonlinear (APN)** *if it satisfies the equation with $d = 2$.*

PN functions do not exist in even characteristic. Due to the existence of PN functions in odd characteristic, APN functions are mostly studied in characteristic 2 and the majority of papers on APN functions deals with the (extremal) case $m = n$. However there exist also some results in an even more general setting, obtained by replacing the

[*] The research of this author takes place within the project "Linear codes and cryptography" of the Research Foundation – Flanders (FWO) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-BCrypt.

vector spaces in Definition 1 by arbitrary abelian groups (see e.g. [25, 16]).

Let $b \in \mathbb{F}_p^n$. The functions

$$F_b : \mathbb{F}_p^m \to \mathbb{F}_p : \quad x \mapsto b \cdot F(x)$$

are called the **component functions** of F. These can be represented by polynomials in $\mathbb{F}_p[X_1, \ldots, X_m]$ (also called Boolean functions, in the case $p = 2$). What is referred to as the **(algebraic) degree of an APN function** is the maximum of the algebraic degrees $d^\circ(F_b)$ among all component functions of F reduced modulo $X_i^p - X_i$.

Quadratic APN functions are APN functions of degree 2. We will restrict ourselves to the case $p = 2$ and mainly to quadratic APN functions.

APN functions have relations to other objects in mathematics. There is the, meanwhile classical, equivalence to binary error correcting codes of length 2^m and dimension $m + n + 1$, containing the first order Reed-Muller Code and with dual distance 6 (see [12]). This is the code C_F as defined here in Equation (5).

An other example is the equivalence of quadratic APN functions with a subclass of dimensional dual hyperovals and semibiplanes. These behave, to some extent, very similar as PN functions, spreads and translation planes in odd characteristic. This link also proved to be useful (see e.g. [16, 2, 20, 25, 32, 33]).

In this note we want to draw the attention to a further, less exploited, link of quadratic APN functions. Modulo affine functions, a quadratic function, in the above defined sense, is equivalent to a subspace of alternating bilinear forms (this will be made more explicit later). These are classical and long studied objects. The APN condition (Equation (1)) translates straightforward in terms of these subspaces (as used en passant by Nakagawa and Yoshiara [30, 34], see also [21]). Suitably stated this fits seamless in the theory of association schemes of alternating bilinear forms due to Delsarte and Goethals [17]. After introducing some notations in the next section, we point out this link in more detail, and then give, as application, some results on the structure of quadratic APN functions, which were valuable for the computer based classification of the quadratic APN functions $F : \mathbb{F}_2^6 \to \mathbb{F}_2^6$. Also alternative arguments for some results on quadratic APN functions are given.

Finally, as a further application of this link, we will see that quadratic APN functions are equivalent to some already investigated objects in multilinear algebra, namely subspaces of $\bigwedge^2 \mathbb{F}_2^m$ avoiding the variety of elements of rank 2. Or in geometric language, to external (or skew) subspaces to the line Grassmannian for $q = 2$. The known constructions of these objects (as far as aware to the author) turn out to be equivalent to the Gold-function.

APN functions have attracted some interest in the last years and several new quadratic APN functions have been found. This thus leads to new examples of such subspaces. On the other hand, the link with alternating forms and related structures may also prove to be useful in the other direction, for the further development of APN functions, such as the link with codes, PN functions and dual dimensional hyperovals already did.

We conclude the introduction by giving an overview of the currently known quadratic APN functions $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ (as far as aware to the author). From the classical monomial APN functions, only the Gold functions are quadratic. All recently found new APN functions (except one [23]) are quadratic. For $m \leq 5$, every quadratic APN function is equivalent to a Gold function [28,5]. For $m = 6$, 13 non-equivalent quadratic APN functions were found by Dillon [18,6]. The author was able to verify by computer that these are indeed all non-isomorphic quadratic APN functions for $m = 6$. The classification in the non-quadratic case, however, still is an open problem. For $m = 7$, we know 16, and for $m = 8$, we know 22 non-isomorphic quadratic APN functions (see [23] for details). For larger m, there are some sporadic examples (see [22,23]) and several infinite series. Identifying the vector space $\mathbb{F}_2^m$ with the finite field $\mathbb{F}_{2^m}$, the series can be given as:

$F(x) =$	Reference and some of the conditions
x^{2^i+1}	$(i,m) = 1$, the Gold function [24]
$x^3 + tr(x^9)$	[9, Corollary 1]
$x^{2^s+1} + wx^{2^{ik}+2^{nk+s}}$	$m = 3k$, [8, Corollary 1], see also [1,2]
$x^{2^s+1} + wx^{2^{ik}+2^{nk+s}}$	$m = 4k$, [8, Theorem 2], see also [1,2]
$bx^{2^s+1} + b^{2^k}x^{2^{k+s}+2^k} + cx^{2^k+1} + \sum_{i=1}^{k-1} r_i x^{2^{i+k}+2^i}$	$m = 2k$, k, s odd [4, Theorem 1]
$ux^{2^{-k}+2^{k+s}} + u^{2^k}x^{2^s+1} + vx^{2^{k+s}+2^s}$	$m = 3k$, $(s, 3k) = 1$ [4, Theorem 3]
$u^{2^k}x^{2^{-k}+2^{k+s}} + ux^{2^s+1} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^{k+s}+2^s}$	$m = 3k$, $(s, 3k) = 1$ [3, Theorem 2.1]
$x^{2^{2i}+2^i} + bx^{2^k+1} + cx^{2^k(2^{2i}+2^i)}$	$m = 2k$, $(i,k) = 1$ [7, Corollary 1]
$x(x^{2^i} + x^{2^k} + cx^{2^{i+k}}) + x^{2^i}(c^{2^k}x^{2^k} + sx^{2^{i+k}}) + x^{2^{i+1}2^k}$	$m = 2k$, $(i,k) = 1$ [7, Corollary 2]

2 Notation and definitions

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$ be a function and F_b, $b \in \mathbb{F}_2^n$, its component functions, as defined in the introduction. The **Walsh coefficients** $\mathcal{W}_F(a,b)$ are defined as

$$\mathcal{W}_F(a,b) := \sum_{x \in \mathbb{F}_2^m} (-1)^{a \cdot x + F_b(x)} \in \mathbb{Z}, \quad a \in \mathbb{F}_2^m, b \in \mathbb{F}_2^n.$$

Then the **Walsh spectrum** $\mathcal{W}_F$, respectively the **extended Walsh spectrum** $\pm\mathcal{W}_F$, is defined as the multiset (denoted by $\{* \cdots *\}$):

$$\mathcal{W}_F := \{* \, \mathcal{W}_F(a,b) | \, a \in \mathbb{F}_2^m, b \in \mathbb{F}_2^n \, *\} \quad \text{resp.} \;\; \pm\mathcal{W}_F := \{* \, |\mathcal{W}_F(a,b)| \, | \, a \in \mathbb{F}_2^m, b \in \mathbb{F}_2^n \, *\}.$$

The values for $b = 0$ are frequently omitted in the definition of the Walsh spectra, but as $\mathcal{W}_F(0,0) = 2^m$ and $\mathcal{W}_F(a,0) = 0$, for $a \neq 0$, these two versions of the definition contain the same information.

The function F is called **bent** if

$$\max_{b\neq 0}\{|\mathcal{W}_F(a,b)|\} = 2^{m/2}$$

and **almost bent** (AB) if

$$\max_{b\neq 0}\{|\mathcal{W}_F(a,b)|\} = 2^{(m+1)/2}.$$

For $n > m/2$, there exist no bent functions [31]. Let $m = n$, then, for $(a,b) \neq (0,0)$, $|\mathcal{W}_F(a,b)| \leq 2^{(m+1)/2}$. AB functions are thus optimal in this sense, m then is necessarily odd and every AB function is APN [13]. For quadratic APN functions, m odd, also the converse is true [12]. For more background on Boolean and vectorial functions defined on $\mathbb{F}_2^m$, we refer to [10, 11].

There are several concepts of equivalence for APN functions. We call the set of points

$$G_F := \{(1, x, F(x)) | x \in \mathbb{F}_2^m\} \subset \mathrm{PG}(m+n, 2)$$

the **graph** of the function F and define the affine subspaces

$$X := \{(1, x, 0) | x \in \mathbb{F}_2^m\}, \quad Y := \{(1, 0, y) | y \in \mathbb{F}_2^n\} \subset \mathrm{PG}(m+n, 2).$$

Definition 2. *Two APN functions $F, F' : \mathbb{F}_2^m \to \mathbb{F}_2^n$ are called:*

- **CCZ-equivalent** *[12], if there is an automorphism of $PG(m+n,2)$ mapping G_F to $G_{F'}$,*

- **extended affine (EA) equivalent***, if there is an automorphism of $PG(m+n,2)$, fixing the subspace Y, and mapping G_F to $G_{F'}$,*

- **affine equivalent***, if there is an automorphism of $PG(m+n,2)$, fixing the subspaces X and Y, and mapping G_F to $G_{F'}$.*

On the affine points $(1, x, y)$, we can describe this 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 note on quadratic APN functions, EA-equivalence is the appropriate concept here.

We wish to remark that, although it is known that there are CCZ-equivalent APN functions which are not EA-equivalent, for quadratic APN functions with $m = n$, EA- and CCZ-equivalence coincide for all APN functions the author was able to test (i.e. the functions F mentioned in the introduction with $m \leq 10$).

An other frequently found definition of EA-equivalence is the following: F and F' are called EA-equivalent if there exist affine bijections A_1, A_2 and a linear (or affine) map L such that

$$F' = A_2 \circ F \circ A_1 + L.$$

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

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

3 Alternating bilinear forms and APN functions

3.1 Alternating bilinear forms

A bilinear map $B : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ is called an **alternating bilinear form** if for any $x \in \mathbb{F}_2^m$, $B(x, x) = 0$. This implies that $B(x, y) = B(y, x)$. The alternating bilinear maps form an $\binom{m}{2}$-dimensional vector space which we will denote by $\mathbb{A}_m$ or $\mathbb{A}$ for short.

Coordinatize by choosing some basis $e_1, \ldots, e_m$ of $\mathbb{F}_2^m$. By abuse of notation, denote also the matrix representing $B \in \mathbb{A}$ by $B = (b_{i,j})$, with $b_{i,j} := B(e_i, e_j)$. Define a scalar product on $\mathbb{A}$ by

$$\langle A, B \rangle := \sum_{i<j} a_{i,j} b_{i,j}.$$

For a subspace $\mathcal{B} \subseteq \mathbb{A}$, define the dual subspace $\mathcal{B}^\perp$, as usual, as

$$\mathcal{B}^\perp := \{A \in \mathbb{A} \mid \langle A, B \rangle = 0 \text{ for all } B \in \mathcal{B}\}.$$

Use the codimension of the radical of the map B, hence the rank of the matrix B, as a weight function on $\mathbb{A}$ (all elements of $\mathbb{A}$ have even rank) and define the corresponding **(rank-)distance** as

$$d(A, B) := \mathsf{rank}(A - B) \text{ for } A, B \in \mathbb{A}.$$

The alternating bilinear forms, together with this distance form an association scheme. We quote some consequences and refer to the original work of Delsarte and Goethals for the details [17].

Let $k := \lfloor m/2 \rfloor$. For a subset $\mathcal{B} \subseteq \mathbb{A}_m$, define the **distance distribution $\mathbf{a}(\mathcal{B})$** by:

$$\mathbf{a}(\mathcal{B}) = \mathbf{a} = (a_0, \ldots, a_k), \quad |\mathcal{B}| a_i := |\{(A, B) \in \mathcal{B} \times \mathcal{B} \mid d(A, B) = 2i\}|.$$

For subspaces $\mathcal{B}$, the distance distribution $\mathbf{a}$ equals the **rank distribution**, i.e.

$$a_i := |\{B \in \mathcal{B} \mid \mathsf{rank}(B) = 2i\}|.$$

The **P-transform** $\mathbf{a}P$ of $\mathbf{a}$ is defined as

$$\mathbf{a}P := \mathbf{a}' = (a'_0, \dots, a'_k), \quad a'_j = \sum_{i=0}^{k} a_i P_j(i), \tag{2}$$

where $P_{i,j} = P_j(i)$ are the **generalised Krawtchouk polynomials**:

$$P_j(x) := \sum_{l=0}^{j} (-1)^{j-l} 4^{\binom{j-l}{2}} \begin{bmatrix} k-l \\ k-j \end{bmatrix}_4 \begin{bmatrix} k-x \\ l \end{bmatrix}_4 c^l, \qquad \text{with } c := 2^{m(m-1)/(2k)},$$

and

$$\begin{bmatrix} x \\ k \end{bmatrix}_b := \prod_{i=0}^{k-1} \frac{b^x - b^i}{b^k - b^i}$$

are the b**-nary Gaussian coefficients**.

Theorem 3 ([17, Theorem 2]). *The P-transform $\mathbf{a}P$ of the distance distribution of any subset $\mathcal{B} \subseteq \mathbb{A}_m$ is nonnegative, i.e.*

$$(\mathbf{a}P)_j \geq 0, \quad j = 0, \dots, k := \lfloor m/2 \rfloor.$$

Theorem 4 ([17, Theorem 3]). *Let $\mathcal{B} \subseteq \mathbb{A}$ be a subspace and let $\mathbf{a}'$ be the distance distribution of $\mathcal{B}^\perp$, then*

$$|\mathcal{B}|\mathbf{a}' = \mathbf{a}P.$$

We say that a subset $\mathcal{B} \subseteq \mathbb{A}$ has **(rank-)distance** d if $d(A, B) \geq d$ holds for any $A \neq B \in \mathcal{B}$. Alternating bilinear forms have even rank, especially $d = 2\delta$. (Delsarte and Goethals call such a $\mathcal{B} \in \mathbb{A}_m$ an (m, δ)-set in [17].) There is an analog of the Singleton bound for these sets.

Theorem 5 ([17, Theorem 4]). *Let $\mathcal{B} \subseteq \mathbb{A}_m$ be a set of distance $d = 2\delta$, then*

$$|\mathcal{B}| \leq c^{k-\delta+1}, \qquad \textit{with } c := 2^{m(m-1)/(2k)}, k := \lfloor m/2 \rfloor.$$

Sets attending this bound are called **maximal**.

Theorem 6 ([17, Theorem 5]). *Let $\mathcal{B} \subseteq \mathbb{A}_m$ be a maximal subspace, then $\mathcal{B}^\perp$ is also maximal and has distance $2k - d + 4$, $k := \lfloor m/2 \rfloor$.*

A base change in $\mathbb{F}_2^m$ induces a natural action of $\mathrm{GL}(m, 2)$ on $\mathbb{A}_m$:

$$g : \mathbb{A}_m \to \mathbb{A}_m : \ B \mapsto B^g, \ B^g(x, y) := B(gx, gy), \qquad \text{with } g \in \mathrm{GL}(m, 2).$$

The matrix of B^g is congruent to the matrix of B (i.e. $B^g = g^t B g$).

We call two subspaces $\mathcal{B}, \mathcal{B}' \subseteq \mathbb{A}$ **congruent** or **equivalent under the natural action of GL**$(m, 2)$ if there is a $g \in \mathrm{GL}(m, 2)$ such that $\mathcal{B}' = \{B^g \mid B \in \mathcal{B}\} =: \mathcal{B}^g$.

Let $f : \mathbb{F}_2^m \to \mathbb{F}_2$. The map

$$\Delta : f \mapsto B_f, \quad B_f(x,y) := f(x+y) + f(x) + f(y) + f(0) \tag{3}$$

maps the quadratic functions surjectively on $\mathbb{A}$ and its kernel consists of the affine functions.

Vice versa, let $B \in \mathbb{A}$ with associated matrix $(b_{i,j})$, then the quadratic function $g(x_1, \ldots, x_m) := \sum_{i<j} b_{i,j} x_i x_j$ has the property that $B_g = B$. This is the (uniquely determined) **hyperbolic quadratic form** associated with $B \in \mathbb{A}$. The hyperbolic quadratic form of B_f is obtained from f by applying $x_i^2 = x_i$ and deleting its affine part.

A quadratic function $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$ gives rise to a subspace $\mathcal{B}_F$ of $\mathbb{A}_m$. Define

$$\mathcal{B}_F := \{B_{F_b} \mid F_b \text{ a component function of } F\}.$$

We now can give the relation of the equivalence of functions and of alternating bilinear forms on the other hand (compare also with [30, Theorem 2]).

Lemma 7. *For quadratic functions, the following conditions are equivalent:*

- *F and F' are EA-equivalent,*
- *$\mathbb{B}_F$ and $\mathbb{B}_{F'}$ are congruent (resp. equivalent under the natural action of $GL(m,2)$).*

Proof. We just sketch the line of argument.

The functions F and F' are EA-equivalent if there is an affine bijection of the form

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

which maps the set $\{(x, F(x)) | x \in \mathbb{F}_2^n\}$ to the set $\{(x, F'(x)) | x \in \mathbb{F}_2^n\}$.

The matrix A corresponds to the natural action of $\mathrm{GL}(m,2)$. The matrix D is a basis change for the component functions, thus leaves the space spanned by the component functions invariant. The remaining map alters F' only by an affine function hence has no influence on the alternating bilinear form. □

3.2 Characterisation of quadratic APN functions

Let now F be a quadratic APN function. We want to express the APN condition in terms of the vector space $\mathcal{B}_F$. The map Δ (Equation (3)) appears, up to a constant shift, in the definition of APN. So this is a simple translation. As $B(a,a) = 0$ for any a and $B \in \mathbb{A}$, we have by Definition 1 that a quadratic function F is APN if and only if the (x,a) with $x = a$ are the only simultaneous zeros of all $B(a,x) \in \mathcal{B}_F$. As

$$B(a,x) = \sum_{i=1}^{m} \sum_{j=1}^{m} b_{i,j} a_i x_j = \sum_{i<j} b_{i,j}(a_i x_j + a_j x_i) = \langle B, B' \rangle, \text{ with } B' = (a_i x_j + a_j x_i)_{i,j}, \tag{4}$$

we have that F is APN if and only if $\mathcal{B}_F^\perp$ contains no non-zero B' of the form $B' = (a_i x_j + a_j x_i)_{i,j}$, hence no B' of rank 2.

We thus get a characterisation of APN functions in terms of subspaces of alternating bilinear forms, which is essentially the characterization used in [30, 34].

Lemma 8. *The following conditions are equivalent:*

- *F is a quadratic APN function,*
- *$\mathcal{B}_F^\perp$ contains no element of rank 2,*
- *the (rank-)distance of the subspace $\mathbb{B}_F^\perp \in \mathbb{A}$ is at least 4.*

3.3 Applications

Define the binary linear code C_F of length 2^m by the generator matrix

$$M_F := \begin{pmatrix} & 1 & \\ \cdots & x & \cdots \\ & F(x) & \end{pmatrix}, \quad x \in \mathbb{F}_2^m. \tag{5}$$

So C_F is the union of the cosets $F_b + \mathrm{RM}(1, m)$ of the first order Reed-Muller Code $\mathrm{RM}(1, m)$, where F_b, $b \in \mathbb{F}_2^n$, is any component function of F. Let F be a quadratic function. It is known that the weight distribution of $F_b + \mathrm{RM}(1, m)$ only depends on the rank of $\Delta F_b \in \mathbb{A}$.

Theorem 9 ([27, §15, Theorem 5]). *Let f be a quadratic function with $\mathsf{rank}(\Delta f) = 2h$. The weight distribution of the coset $f + RM(1, m)$ is*

$$A_{2^{m-1}-2^{m-h-1}} = A_{2^{m-1}+2^{m-h-1}} = 2^{2h} \;\; \textit{and} \;\; A_{2^{m-1}} = 2^{m+1} - 2^{2h+1}.$$

As $\mathcal{B}_F$ consists of the Δ-images of all component functions of F, the (rank-)distance distribution of the subspace $\mathcal{B}_F \subseteq \mathbb{A}$ determines the weight distribution of the linear code C_F and therefore also the extended Walsh spectrum of F. We have the following results.

Corollary 10. *Let $k := \lfloor m/2 \rfloor$, let $\mathbf{a}$ be the (rank-)distance distribution of B_F, $\mathbf{A}$ the distance distribution of C_F, and $\pm\mathcal{W}_F$ the extended Walsh spectrum of F. Then:*

$$A_i = \begin{cases} 1 & \textit{for } i = 0, 2^m, \\ 2^{2m+1} - \sum_{h=0}^{k} a_h 2^{2h+1} & \textit{for } i = 2^{m-1}, \\ a_h 2^{2h} & \textit{for } i = 2^{m-1} \pm 2^{m-h-1}, \quad h = 1, \ldots, k, \\ 0 & \textit{otherwise.} \end{cases}$$

$$\pm\mathcal{W}_F = \{ * \, i^{\nu_i} \, * \} \textit{ with } \nu_i = \begin{cases} 1 & \textit{for } i = 2^m, \\ 2^{2m} - \sum_{h=0}^{k} a_h 2^{2h} & \textit{for } i = 0, \\ a_h 2^{2h} & \textit{for } i = 2^{m-h}, \quad h = 1, \ldots, k, \\ 0 & \textit{otherwise.} \end{cases}$$

We now investigate the possible (rank-)distance distributions of quadratic APN functions F for $m = n$, and as well the true dimension m' of B_F (the dimension of the code C_F thus is $1 + m + m'$). By construction, $m' \leq m$ and we will see that $m = m'$. This is known in general, i.e. also for non-quadratic APN functions [12, Corollary 1.i]. The proof of [12] relies, however, on a non-trivial coding-theoretical result. We use that $B_F^{\perp}$ has, by Lemma 8, (rank-)distance at least 4.

Firstly consider the case m odd. The space $\mathcal{B}_F^{\perp}$ has dimension $\binom{m}{2} - m'$. Theorem 5 shows that $m' = m$ and, as then the bound is met with equality, we have that $\mathcal{B}_F^{\perp}$ is maximal. Theorem 6 states that every non-zero element of $\mathcal{B}_F^{\perp}$ has maximal possible rank $m - 1$. Using Corollary 10, we see that F is AB. We thus have an alternative argument for the the main statement of Theorem 8 of [12].

Corollary 11. *Let m be odd. Every quadratic APN function $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is almost bent (AB).*

Now let $m = 2k$. Theorem 5 shows that $m' = m - 1$ or $m' = m$. The case $m' = m - 1$ can not appear for subspaces, for $m > 2$, due to a result of Cooperstein ([14, Theorem 6.1], see the explanation in Section 3.4 below).

Alternatively we can argue that in the case $m' = m - 1$, we have that $\mathcal{B}_F^{\perp}$ is maximal and, again by Theorem 6, every non-zero element of $\mathcal{B}_F^{\perp}$ has maximal possible rank m. Using Corollary 10, we see that F is bent. This is only possible for $m - 1 = m' \leq m/2$ (see Section 2). Thus for $m > 2$, we must have that $m' = m$. We assume in the following that we are in this case.

One example of quadratic functions F which always exists are the Gold functions. The weight distribution of C_F is known. We will call it the **classical distribution**. For $m = 2k$, the classical distribution is (see [19]):

$$A_i = \begin{cases} 1 & \text{for } i = 0, 2^m, \\ 2(2^m-1)(2^{m-2}+1) & \text{for } i = 2^{m-1}, \\ \frac{2^m-1}{3}2^{m+1} & \text{for } i = 2^{m-1} \pm 2^{k-1}, \\ \frac{2^m-1}{3}2^{m-2} & \text{for } i = 2^{m-1} \pm 2^{k}, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

The distribution $\mathbf{a}$ of the alternating bilinear forms in $\mathcal{B}_F$ is, by Corollary 10:

$$a_h = \begin{cases} 1 & \text{for } h = 0, \\ \frac{2}{3}(2^m-1) & \text{for } h = k, \\ \frac{1}{3}(2^m-1) & \text{for } h = k-1, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

3.3.1 P-Transform for APN, $m = 2k$ even

For an n-dimensional subspace, the distribution $\mathbf{a}$ fulfils:

$$\sum_{j=0}^{k} a_j = 2^n, \quad a_0 = 1. \tag{8}$$

We transform Equation (2) for $i = 1$:

$$\begin{aligned}
a'_1 &= \frac{1}{2^n}(\mathbf{a}P)_1 := \sum_{i=0}^{k} a_i \sum_{j=0}^{1} (-1)^{1-j} 4^{\binom{1-j}{2}} \begin{bmatrix} k-j \\ k-1 \end{bmatrix}_4 \begin{bmatrix} k-i \\ j \end{bmatrix}_4 2^{(m-1)\cdot j} \\
&= \frac{1}{2^n} \sum_{i=0}^{k} a_i (- \begin{bmatrix} k \\ k-1 \end{bmatrix}_4 + \begin{bmatrix} k-i \\ 1 \end{bmatrix}_4 2^{m-1}) \\
&= \frac{1}{2^n} \sum_{i=0}^{k} a_i (-(4^k-1)/3 + 2^{m-1}(4^{k-i}-1)/3) \\
&\overset{(8)}{=} \frac{1}{2^n 3}(-2^n(4^k-1) + 2^{m-1}((4^k-1) + \sum_{i=1}^{k-1} a_i (4^{k-i}-1))) \\
&= \frac{1}{3}((2^{m-1-n}-1)(4^k-1) + 2^{m-1-n} \sum_{i=1}^{k-1} a_i (4^{k-i}-1)).
\end{aligned}$$

For B_F, with F being a quadratic APN function, we have $a'_1 = 0$ and $n = m = 2k > 2$. The above equation simplifies to

$$a_{k-1} = \frac{1}{3}(4^k - 1 - \sum_{i=1}^{k-2} a_i (4^{k-i}-1)). \tag{9}$$

The value a_k is minimal (by Equation (8)) if $\sum_{i=1}^{k-1} a_i$ is maximal. By Equation (9), this is the case if a_{k-1} is as large as possible, hence if $a_i = 0$ for $0 < i < k-1$. Then $a_{k-1} = (4^k-1)/3$, hence the weight distribution is the classical distribution.

The value a_k is larger than the number of elements in an $(m-1)$-dimensional subspace, thus there is always a basis of B_F consisting of elements of full rank.

Let $Y \subset \mathcal{B}_F$ be the set of the a_k elements of rank m (i.e. the image of the set of component functions which are bent). Assume Y contains an r-dimensional subspace Z, but no $(r+1)$-dimensional subspace. We count the points of $Y \setminus Z$. The $(r+1)$-dimensional subspaces through Z in (the m-dimensional vector space) $\mathcal{B}_F$ partition the points of $\mathcal{B}_F \setminus Z$ and thus also the points of Y not in Z. There are $2^{m-r} - 1$ such $(r+1)$-dimensional subspaces. Each contains at least one non-zero point not in Y, hence at most $2^r - 1$ points of $Y \setminus Z$. Hence,

$$|Y \setminus Z| \leq (2^{r-1}-1)(2^{m-r}-1) \quad \Leftrightarrow \quad |Y| \leq (2^r - 1)2^{m-r}. \tag{10}$$

Thus we have shown the following result.

Lemma 12. *Let $Y \subset \mathcal{B}_F$ be the set of elements of rank m. If $|Y| > 2^m - 2^{m-r}$, then Y contains an $(r+1)$-dimensional subspace.*

Here, $a_n \geq \frac{2}{3}(2^m - 1) = 2^m - 1 - \sum_{j=0}^{k-1} 2^{2j} > 2^m - 2^{m-1}$, so we summarise:

Corollary 13.

- *Y contains at least a 2-dimensional subspace,*
- *Y contains a basis of $\mathcal{B}_F$,*
- *$|\mathcal{B}_F \setminus Y| \geq 2^{m/2}$.*

The last item is again due to the already mentioned result of Cooperstein, resp. due to the non-existence of bent functions with $n > m/2$.

An other way to get the first item is by observing that a cap in $\mathrm{PG}(B_f) = \mathrm{PG}(m-1, 2)$ contains at most 2^{m-1} points, hence Y is no cap, thus contains a (projective) line.

3.3.2 Example: $m = 6$

As an example, we have a look at the possible rank distributions of $\mathcal{B}_F$, for $F : \mathbb{F}_2^6 \to \mathbb{F}_2^6$ being a quadratic APN function. Equation (9) specialises to: $21 = 5a_1 + a_2$. Hence, choosing $0 \leq a_1 < 5$ leads to the following possible rank distributions $\mathbf{a}$:

$$(1,0,21,42), \quad (1,1,16,46), \quad (1,2,11,50), \quad (1,3,6,54), \quad (1,4,1,58).$$

From the third distribution on, a 3-dimensional subspace is guaranteed. The fifth distribution cannot occur by Corollary 13. Only the first two occur as distributions of one of the actual 13 non-isomorphic $\mathcal{B}_F$.

3.4 A link with $\bigwedge^2 \mathbb{F}_2^m$ and the line Grassmannian

There is a well-known equivalence between alternating bilinear forms on V and the **wedge-** or **external-product** $\bigwedge^2 V$. In general, $\bigwedge^k V$ is linked with the Grassmannians. Quadratic APN functions appear naturally, although not under this name, in this setting as we will see.

We refer to [28] for a more extensive short introduction on this topic. More details and proofs can be found in text books such as [29]. For the Grassmannians, see also [26, Chapter 24].

Let V be an m-dimensional vector space over $\mathbb{F}$. An element $u \in \bigwedge^k V$ is called **decomposable** if there exist $u_1, \dots, u_k \in V$ such that $u = u_1 \wedge \cdots \wedge u_k$ (i.e. if u can be written as a **pure** wedge-product). We have $u_1 \wedge \cdots \wedge u_k = 0$ if and only if $u_1, \dots, u_k$ are linearly dependent.

Let $Gr(k, V)$, resp. $Gr(k, m)$, denote the set of all k-dimensional subspaces of an m-dimensional vector space V. Let $U, U' \in Gr(k, m)$ be the subspaces generated by $u_1, \ldots, u_k$, resp. $u'_1, \ldots, u'_k$. Then $U = U'$ if and only if $u_1 \wedge \cdots \wedge u_k = \lambda(u'_1 \wedge \cdots \wedge u'_k)$ for some $\lambda \in \mathbb{F}$.

As a consequence, we have an injective embedding γ of $Gr(k, V)$ in the projective space with underlying vector space $\bigwedge^k V$:

$$\gamma : Gr(k, V) \to \mathrm{PG}(\bigwedge^k V).$$

Thus, $\gamma(Gr(k, m))$ consists of the decomposable elements of $\mathrm{PG}(\bigwedge^k V)$ and is a quadratic variety. The sets $Gr(k, m)$ are called the **Grassmannians** and $\gamma(Gr(k, m))$ the **Grassmannian variety**. As the 2-dimensional subspaces correspond to the projective lines, $\gamma(Gr(2, m))$ is frequently referred to as the **line-Grassmannian**. A subspace U is called an **external subspace** or **skew** to G if $U \cap G$ is zero (or empty if using the projective notation).

The general linear group $\mathrm{GL}(V)$ induces a natural action on $\bigwedge^k V$ by $u_1 \wedge \cdots \wedge u_k \mapsto g(u_1) \wedge \cdots \wedge g(u_k)$. The induced operation is a subgroup of the group of collineations of $\mathrm{PG}(\bigwedge^k V)$, stabilising the Grassmannian variety.

As mentioned, there is a well-known equivalence between alternating bilinear forms on V and $\bigwedge^2 V$. We therefore also can speak of the rank of elements in $\bigwedge^2 V$. The decomposable elements of $\bigwedge^2 V$ are the rank-2-elements. For example, the rank 2 form $B' = (a_i x_j + a_j x_i)_{i,j}$ appearing in the characterising Equation (4) corresponds to the pure element $a \wedge x$.

The natural action is a transitive operation on the elements of the same rank of $\bigwedge^2 V$.

The line-Grassmannian consists of the decomposable elements in $\bigwedge^2 V$, thus the Lemmata 7 and 8 give, by identifying $\mathcal{B}_F^{\perp}$ with some $(\binom{m}{2} - n)$-dimensional subspace of $\bigwedge^2 \mathbb{F}_2^m$ the following alternative characterisations of quadratic APN functions.

Corollary 14. *The following objects are equivalent:*

- *a quadratic APN function $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$,*
- *an $(\binom{m}{2} - n)$-dimensional subspace $U \in \bigwedge^2 \mathbb{F}_2^m$ containing no decomposable element,*
- *an $(\binom{m}{2} - n - 1)$-dimensional subspace $[U] \in PG(\bigwedge^2 \mathbb{F}_2^m)$, skew to the line-Grassmannian.*

The EA-equivalence classes of quadratic APN functions are in one-to-one correspondence with the orbits, under the natural action of $GL(m, 2)$, of the $(\binom{m}{2} - n)$-dimensional subspaces in $\bigwedge^2 \mathbb{F}_2^m$ (resp. $(\binom{m}{2} - n - 1)$-dimensional subspaces in $PG(\bigwedge^2 \mathbb{F}_2^m)$), fulfilling the above conditions.

Cooperstein [14] investigates subspaces $U \in \bigwedge^2 \mathbb{F}_q^m$ skew to the sets of all elements with bounded rank. In [14, Theorem 6.1], it is stated that, for $m > 2$, subspaces skew to the set of elements of rank 2 (so the APN case for $q = 2$) have dimension at most $\binom{m}{2} - m$. This strengthens Theorem 5 for even m under the stronger assumption that the skew set is a subspace and is the alternative argument mentioned in the discussion on the true dimension of the image space of an APN function above.

Also an example for such an extremal subspace is given. By comparing the alternative geometrical construction, given in [15], with the remarks in the appendix of [21], it can be seen that this example corresponds, for $q = 2$, to Gold's APN function x^3.

References

[1] J. Bierbrauer. A family of crooked functions. *Designs, Codes and Cryptography*, 50:235–241, 2009.

[2] J. Bierbrauer. New semifields, PN and APN functions. *Designs, Codes and Cryptography*, 54(3):189–200, 2010.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire. A few more quadratic APN functions. *http://arxiv.org/pdf/0804.4799*, 2008.

[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[5] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49(1-3):273–288, 2005.

[6] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan. APN polynomials and related codes. *Journal of Combinatorics, Information and System Sciences*, 34(1-4):135–159, 2009.

[7] L. Budaghyan and C. Carlet. Classes of Quadratic APN trinomials and Hexanomials and Related Structures. *IEEE Transactions on Information Theory*, 54(8):2354–2357, 2008.

[8] L. Budaghyan, C. Carlet, and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[9] L. Budaghyan, C. Carlet, and G. Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[10] C. Carlet. *Boolean Methods and Models*, chapter Boolean functions for cryptography and error correcting codes. Cambridge University Press, to appear.

[11] C. Carlet. *Boolean Methods and Models*, chapter Vectorial Boolean functions for cryptography. Cambridge University Press, to appear.

[12] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

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

[14] B. N. Cooperstein. External flats to varieties in $\mathrm{PG}(\bigwedge^2(V))$ over finite fields. *Geometriae Dedicata*, 69(3):223–235, 1998.

[15] A. Cossidente and A. Siciliano. On tangent spaces and external flats to Grassmannians of lines over finite fields. *Linear Algebra and its Applications*, 347:81–89, 2002.

[16] R. S. Coulter and M. Henderson. A class of functions and their application in constructing semi-biplanes and association schemes. *Discrete Mathematics*, 202(1):21–32, 1999.

[17] P. Delsarte and J. M. Goethals. Alternating bilinear forms over $\mathrm{GF}(q)$. *Journal of Combinatorial Theory. Series A*, pages 26–50, 1975.

[18] J. F. Dillon. slides from talk given at "Polynomials over Finite Fields and Applications", held at Banff International Research Station, 2006.

[19] J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. *Finite Fields and Their Applications*, 10:342–389, 2004.

[20] Y. Edel. On quadratic APN functions and dimensional dual hyperovals. *Designs, Codes and Cryptography*, 57(1):35–44, 2010.

[21] Y. Edel. On some representations of quadratic APN functions and dimensional dual hyperovals. *RIMS Kôkyûroku*, 1687:118–130, 5 2010.

[22] Y. Edel, G. Kyureghyan, and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52 (2):744 – 747, 2006.

[23] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[24] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation function. *IEEE Transactions on Information Theory*, 14:154–156, 1968.

[25] F. Göloğlu and A. Pott. Almost perfect nonlinear functions: A possible geometric approach. In S. Nikova, B. Preneel, L. Storme, and J. A. Thas, editors, *Proceedings*

of the Contact Forum Coding Theory and Cryptography II *at The Royal Flemish Academy of Belgium for Science and the Arts 2007*, pages 75–100, Brussels, Belgium, September 21, 2007.

[26] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries.* Clarendon Press, Oxford, 1991.

[27] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[28] J. Maks and J. Simonis. Optimal subcodes of second order Reed-Muller codes and maximal linear spaces of bivectors of maximal rank. *Designs, Codes and Cryptography*, 21(1-3):165–180, 2000. Special issue dedicated to Dr. Jaap Seidel on the occasion of his 80th birthday (Oisterwijk, 1999).

[29] M. Marcus. *Finite Dimensional Multilinear Algebra*, volume I+II. Marcel Dekker, 1973.

[30] N. Nakagawa. On the number of generalized quadratic APN functions. Slides for Fq9: `http://mathsci.ucd.ie/~gmg/Fq9Talks/Nakagawa.pdf`.

[31] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in cryptology–EUROCRYPT '91 (Brighton, 1991)*, pages 378–386, Berlin, 1991. Springer.

[32] S. Yoshiara. Dimensional dual hyperovals associated with quadratic APN functions. *Innovations in Incidence Geometry*, 8:147–169, 2008.

[33] S. Yoshiara. Notes on APN functions, semibiplanes and dimensional dual hyperovals. *Designs, Codes and Cryptography*, 56(2-3):197–218, 2010.

[34] S. Yoshiara. Notes on split dimensional dual hyperovals. Manuscript.