

On the linear structures of Balanced functions and quadratic APN functions

A. Musukwa and M. Sala

University of Trento, Via Sommarive, 14, 38123 Povo, Trento, Italy
 {augustinemusukwa, maxsalacodes}@gmail.com

Abstract

The set of linear structures of most known balanced Boolean functions is non-trivial. In this paper, some balanced Boolean functions whose set of linear structures is trivial are constructed. We show that any APN function in even dimension must have a component whose set of linear structures is trivial. We determine a general form for the number of bent components in quadratic APN functions in even dimension and some bounds on the number are produced. We also count bent components in any quadratic power functions.

Keywords: Boolean functions; linear space; APN functions; bent functions

MSC 2010: 06E30, 94A60, 14G50

1 Introduction

Balancedness is an important property which is sometimes required in Boolean functions since it is often desirable for cryptographic primitives to be unbiased in output. By recognising such importance, a lot of papers have been written on construction of balanced functions with cryptographic properties (see for example [7, 10, 12, 17]). One cryptographic property which is mostly considered in constructing such functions is nonlinearity. However, in this study we are interested in something different. We would like to consider the set of linear structures of balanced functions. In this paper, the set of linear structures of a Boolean function is called linear space. We believe that most known balanced functions do have non-trivial linear space. A typical example of a balanced function with non-trivial linear space is $g(x_1, \dots, x_{n-1}) + x_n$, where n is positive integer. It is a well-known balanced function and its linear space clearly includes the nonzero vector $(0, \dots, 0, 1)$. In this paper we construct some balanced functions whose linear spaces are trivial and in some cases we give a lower bound on their nonlinearities.

The nonlinearity and differential uniformity of a vectorial Boolean function (a mapping from \mathbb{F}_2^n to \mathbb{F}_2^m) are properties which are used to measure the resistance of a function towards linear and differential attacks, respectively. APN and AB functions provide optimal resistance against the said attacks. This gives a justification as to why there are many studies regarding APN and also AB functions. In this paper, we show that the linear spaces of some components of an APN function in even dimension must be trivial. In particular, we show that the dimension of the linear space of any component in APN permutation is at most 1. Some results on properties of quadratic APN functions are studied.

It is well-known that in any quadratic APN functions there are some bent components. So we provide a general form of the number of bent components in quadratic APN. From [15], we know that there are at most $2^n - 2^{n/2}$ bent components in any function from \mathbb{F}_2^n to itself. This motivated the authors to count bent components for any quadratic power function and so a comparison with quadratic power APN is made.

This paper is organised as follows. In Section 2, known results are reported. In Section 3, some balanced functions are constructed and in Section 4 we provide conditions which help to determine whether the balanced functions constructed in Section 3 have trivial linear space. In Section 5, we show that there is component in any APN function in even dimension whose linear space is trivial and we also present a general form for the number of bent components in any quadratic APN functions. In Section 6, we count bent components in any quadratic power functions.

2 Preliminaries

In this section, some definitions and well-known results are reported and for details, the reader is referred to [1, 5, 8, 13, 18].

The field of two elements, 0 and 1, is denoted by \mathbb{F} . A vector in the vector space \mathbb{F}^n is denoted by v . A vector whose i th coordinate is 1 and 0 elsewhere is denoted by e_i . We use ordinary addition $+$ instead of XOR \oplus . For any set A , its size is denoted by $|A|$.

A *Boolean function* (B.f.) is any function f from \mathbb{F}^n to \mathbb{F} and a *vectorial Boolean function* (v.B.f.) is any function F from \mathbb{F}^n to \mathbb{F}^m , with $n, m \in \mathbb{N}$. However, in this paper we consider v.B.f.'s from \mathbb{F}^n to \mathbb{F}^n . The B.f.'s in algebraic normal form, which is the n -variable polynomial representation over \mathbb{F} , is given by $f(x_1, \dots, x_n) = \sum_{I \subseteq \mathcal{P}} a_I (\prod_{i \in I} x_i)$, where $\mathcal{P} = \{1, \dots, n\}$ and $a_I \in \mathbb{F}$. The *algebraic degree* or simply *degree* of f (denoted by $\deg(f)$) is $\max_{I \subseteq \mathcal{P}} \{|I| \mid a_I \neq 0\}$. The set of all B.f.'s on n variables is denoted by B_n .

A B.f. f is *linear* if $\deg(f) = 1$ and $f(0) = 0$, *affine* if $\deg(f) \leq 1$, *quadratic* if $\deg(f) = 2$ and *cubic* if $\deg(f) = 3$. The set of all affine functions is denoted by A_n . Given a v.B.f. $F = (f_1, \dots, f_n)$, the functions f_1, \dots, f_n are called *coordinate functions* and the functions $\lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$ and “ \cdot ” denoting dot product, are called a *components* of F and we denote $\lambda \cdot F$ by F_λ . A v.B.f. F is said to be a *permutation* if and only if all its components are balanced. The degree of a v.B.f. F is given by $\deg(F) = \max_{\lambda \neq 0 \in \mathbb{F}^n} \{\deg(F_\lambda)\}$. If all components of a v.B.f. F are quadratic, we say that F is *pure quadratic*.

The *Hamming weight* of f is given by $w(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$. A function f is *balanced* if $w(f) = 2^{n-1}$. The *distance* between f and g is $d(f, g) = w(f + g)$ and the *nonlinearity* of f is $\mathcal{N}(f) = \min_{\omega \in A_n} d(f, \omega)$.

For $m < n$, if f is in B_n but depends only on m variables, then its restriction to these m variables is denoted by $f|_{\mathbb{F}^m}$. Clearly, $f|_{\mathbb{F}^m} \in B_m$.

The next result can be found in [13] on page 372.

Proposition 1. *If $g(x_1, \dots, x_{n-1})$ is an arbitrary B.f. on $n - 1$ variables, with a positive integer $n > 1$, then $f = g(x_1, \dots, x_{n-1}) + x_n$ is balanced.*

The *Walsh transform* of a B.f. f is defined as the function W_f from \mathbb{F}^n to \mathbb{Z} :

$$W_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x) + a \cdot x},$$

for all $a \in \mathbb{F}^n$. The set $\{W_f(a) \mid a \in \mathbb{F}^n\}$ is called the *Walsh spectrum* of a B.f. f . The *Walsh spectrum* of a v.B.f F is given by $\{W_{F_\lambda}(a) \mid a \in \mathbb{F}^n, \lambda \neq 0 \in \mathbb{F}^n\}$. Define $\mathcal{F}(f)$ as

$$\mathcal{F}(f) = W_f(0) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} = 2^n - 2w(f).$$

Note that f is balanced if and only if $\mathcal{F}(f) = 0$.

The nonlinearity of a function f can be written in terms of Walsh transform as

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}^n} |W_f(a)|.$$

The nonlinearity of a v.B.f F is defined as

$$\mathcal{N}(F) = \min_{\lambda \neq 0 \in \mathbb{F}^n} \mathcal{N}(F_\lambda).$$

It well-known that for every B.f. $f \in B_n$, with n even, $\mathcal{N}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. A function $f \in B_n$ is said to be *bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and this can happen only in even dimension. Note that the lowest possible value for $W_f(a)$, with $a \in \mathbb{F}^n$, is $2^{\frac{n}{2}}$ and this bound is achieved only for bent functions.

For n odd, a B.f. f is called *semi-bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$. In other words, f is semi-bent if, for all $a \in \mathbb{F}^n$, $W_f(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}$. Semi-bent functions are sometimes defined in even dimension. For n even, we say a function f is semi-bent if, for all $a \in \mathbb{F}^n$, $W_f(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$. A v.B.f. F in odd dimension is *almost-bent* (AB) if all its components are semi-bent.

A B.f. is called *plateaued* if its Walsh transform takes at most three values: 0 and $\pm\mu$ where μ is some positive integer, called the *amplitude* of the plateaued function. So clearly bent and semi-bent functions are plateaued.

We define the (*first-order*) *derivative* of f at a by $D_a f(x) = f(x+a) + f(x)$. A derivative of f at 0 is the trivial derivative and at any other point, $a \neq 0 \in \mathbb{F}^n$, we simply say a derivative. An element $a \in \mathbb{F}^n$ is called a *linear structure* of f if $D_a f$ is constant, and we denote the set of all linear structures of f by $V(f)$. The set $V(f)$ is called the *linear space* of f . We say the linear space is *trivial* if it contains zero vector only and *non-trivial* otherwise.

Theorem 2. *A B.f. f on n variables is bent if and only if $D_a f$ is balanced for any nonzero $a \in \mathbb{F}^n$.*

Two B.f.'s $f, g : \mathbb{F}^n \rightarrow \mathbb{F}$ are said to be *affine equivalent* if there exist an affinity $\varphi : \mathbb{F}^n \rightarrow \mathbb{F}^n$ such that $f = g \circ \varphi$. This relation is denoted by \sim_A and written as $f \sim_A g$. Observe that the relation \sim_A is equivalence relation. For $i \in \{1, \dots, n\}$ and $l \in A_{n-1}$, a *basic affinity* of \mathbb{F}^n maps $x_i \mapsto x_i + l(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ and fixes all other coordinates.

Proposition 3. *Let $f, g \in B_n$ be such that $f \sim_A g$. Then $w(f) = w(g)$ and so f is balanced if and only if g is balanced.*

Remark 4. *From Proposition 3 and applying the fact that $\mathcal{F}(f) = 2^n - 2w(f)$, we can easily deduce that if $f \sim_A g$ then $\mathcal{F}(f) = \mathcal{F}(g)$, that is, $\mathcal{F}(f)$ is invariant under affine equivalence.*

Theorem 5. *Let $f \in B_n$ be quadratic. Then*

- (i) $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $k \leq \lfloor \frac{n-1}{2} \rfloor$ if f is balanced,
(ii) $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $k \leq \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$ if f is unbalanced.

Remark 6. By Theorem 5, it can be easily deduced that if n is even then the dimension of the linear space of any quadratic function is even, and if n is odd then its dimension is also odd.

The following corollary can be easily proved.

Corollary 7. Let f be a quadratic B.f. on n variables and $c \in \mathbb{F}$. Then

1. for even n , f is bent if and only if

$$f \sim_A x_1x_2 + \cdots + x_{n-1}x_n + c$$

2. for even n , f is semi-bent if and only if $f \sim_A x_1x_2 + \cdots + x_{n-3}x_{n-2} + x_{n-1}$ or $f \sim_A x_1x_2 + \cdots + x_{n-3}x_{n-2} + c$.
3. for odd n , f is semi-bent if and only if $f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$ or $f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + c$.

Lemma 8 ([9]). Two unbalanced quadratic B.f. g and h on n variables are affine equivalent if and only if $w(g) = w(h)$ and $\mathcal{N}(g) = \mathcal{N}(h)$.

Theorem 9 ([6]). Let $f \in B_n$ be a quadratic function. Then, for $a \in \mathbb{F}^n$, we have $W_f(a) \in \{0, \pm 2^{\frac{n+k}{2}}\}$ and $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n+k}{2}-1}$, where $k = \dim V(f)$.

Definition 10. Define $\delta_F(a, b) = |\{x \in \mathbb{F}^n \mid D_a F(x) = b\}|$, for $a, b \in \mathbb{F}^n$ and v.B.f. F . The differential uniformity of F is $\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} \delta_F(a, b)$ and always satisfies $\delta(F) \geq 2$. We call a function with $\delta(F) = 2$ Almost Perfect Nonlinear (APN).

Next we look at another representation of v.B.f., known as *univariate polynomial representation*, which will be used in some sections. Consider the finite field \mathbb{F}_{2^n} consisting of 2^n elements. It is well-known that the set $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$ is a cyclic group which has $2^n - 1$ elements. An element in \mathbb{F}_{2^n} which is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$ is called a *primitive element*. It is well explained in [5] that the vector space \mathbb{F}^n can be endowed with the structure of the finite field \mathbb{F}_{2^n} . So any function F from \mathbb{F}_{2^n} into \mathbb{F}_{2^n} admits a unique univariate polynomial representation over \mathbb{F}_{2^n} , given as:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \quad (2.1)$$

where $\delta_i \in \mathbb{F}_{2^n}$ and the degree of F is at most $2^n - 1$. Given the binary expansion $i = \sum_{s=0}^{n-1} i_s 2^s$, define $w_2(i) = \sum_{s=0}^{n-1} i_s$. So F is a v.B.f. whose algebraic degree is given by $\max\{w_2(i) \mid 0 \leq i \leq 2^n - 1, \delta_i \neq 0\}$ (see [5]).

The (absolute) trace function $Tr : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is defined as

$$Tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}},$$

where $x \in \mathbb{F}_{2^n}$. For $\alpha \in \mathbb{F}_{2^n}$, a component F_α of F is defined as $F_\alpha(x) = Tr(\alpha F)$.

We call any function of the form $F(x) = x^d$, for some non negative integer d , a *power function* and if $d = 2^i + 2^j$, for some non negative integers i and j , with $i \neq j$, we say it is quadratic power function.

3 Balanced Boolean functions

In this section we determine some conditions for B.f.'s to be balanced and we also construct some balanced functions.

If a B.f. is expressed in some particular form, its weight can be obtained from the weights of other B.f.'s on vector spaces with lower dimension as we explain below. First, observe that any B.f. f on $n + 1$ variables can be expressed in the form

$$f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n). \quad (3.1)$$

We show that if the weights of the functions g and h on n variables are known, then the weight of a B.f. on $n + 1$ variables is obtained.

Theorem 11. *Let $f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$, with $f \in B_{n+1}$ and $g, h \in B_n$. Then*

- (i) $w(f) = w((g + h)|_{\mathbb{F}^n}) + w(h|_{\mathbb{F}^n})$,
- (ii) f is balanced if both $g + h$ and h are balanced,
- (iii) f is unbalanced if one in $\{g + h, h\}$ is balanced and the other is not.

Proof. In this proof we view h , g and $g + h$ as functions in B_n .

(i) Let $X = (x_1, \dots, x_n)$. We have

$$\begin{aligned} \mathcal{F}(f) &= \sum_{(X, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}} (-1)^{x_{n+1}g(X) + h(X)} \\ &= \sum_{X \in \mathbb{F}^n} (-1)^{g(X) + h(X)} + \sum_{X \in \mathbb{F}^n} (-1)^{h(X)} \\ &= \mathcal{F}(g + h) + \mathcal{F}(h) \end{aligned} \quad (3.2)$$

So

$$\begin{aligned} w(f) &= 2^n - \frac{1}{2}\mathcal{F}(f) \\ &= 2^n - \frac{1}{2}[\mathcal{F}(g + h) + \mathcal{F}(h)] \\ &= 2^n - \frac{1}{2}[2^n - 2w(g + h) + 2^n - 2w(h)] \\ &= w(g + h) + w(h). \end{aligned} \quad (3.3)$$

(ii) Observe that if $g + h$ and h are balanced, we have $\mathcal{F}(g + h) = \mathcal{F}(h) = 0$ which implies that $w(f) = 2^n$, by Equation (3.3).

(iii) Without loss of generality, suppose that $g + h$ is balanced while h not. Then $\mathcal{F}(g + h) = 0$ and $\mathcal{F}(h) \neq 0$. So, by Equation (3.3), we have $w(f) = 2^n - \frac{1}{2}\mathcal{F}(h) \neq 2^n$ since $\mathcal{F}(h) \neq 0$, and so f is unbalanced. \square

Our first two constructions of balanced B.f.'s are based on the well-known fact in the Proposition 1 and Theorem 11.

Proposition 12. *Let $f \sim_A x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_{n-1})$, where $g = \tilde{g}(x_1, \dots, x_{n-1}) + x_n$ and $h = \tilde{h}(x_1, \dots, x_{n-2}) + x_{n-1}$. Then f is balanced.*

Proof. By Proposition 1, both $g + h$ and h are balanced and so, applying Theorem 11, f is balanced. \square

Notice that the result which we present in the following proposition is partly an extension of Proposition 12.

Proposition 13. *Let $g_i = \tilde{g}_i(x_{i+1}, \dots, x_{n-i}) + x_{n-i+1}$ be a B.f. on $n - 2i + 1$ variables, with integer $n > 2$ and $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$, and define the two functions on n variables as:*

$$f_\ell \sim_A \sum_{i=1}^{\ell-1} x_i g_i + g_\ell \quad (3.4)$$

and

$$\bar{f}_\ell \sim_A \sum_{i=1}^{\ell} x_i g_i + c, \quad (3.5)$$

with $\ell \leq \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$. Then f_ℓ is balanced and \bar{f}_ℓ is unbalanced.

Proof. For a positive integer $t \leq \ell - 1$, define

$$h_t = \sum_{i=t}^{\ell-1} x_i g_i + g_\ell \quad \text{and} \quad \bar{h}_t = \sum_{i=t}^{\ell} x_i g_i + c,$$

with $c \in \mathbb{F}$. Since $\mathcal{F}(f_\ell)$ is invariant under affine equivalence (see Remark 4) then, by Equation 3.2, we obtain

$$\mathcal{F}(f_\ell) = \sum_{i=1}^{\ell-2} \mathcal{F}(g_i + h_{i+1}) + \mathcal{F}(g_{\ell-1} + g_\ell) + \mathcal{F}(g_\ell) \quad (3.6)$$

and

$$\mathcal{F}(\bar{f}_\ell) = \sum_{i=1}^{\ell-1} \mathcal{F}(g_i + \bar{h}_{i+1}) + \mathcal{F}(g_\ell + c) + \mathcal{F}(c). \quad (3.7)$$

We conclude by Proposition 1 that $g_i + h_{i+1}$, $g_i + \bar{h}_{i+1}$, $g_{\ell-1} + g_\ell$ and $g_\ell + c$ are all balanced. So it implies that

$$\mathcal{F}(g_\ell + c) = \mathcal{F}(g_{\ell-1} + g_\ell) = \mathcal{F}(g_i + h_{i+1}) = \mathcal{F}(g_i + \bar{h}_{i+1}) = 0.$$

It follows that Equation (3.6) becomes $\mathcal{F}(f_\ell) = 0$, implying that f_ℓ is balanced and Equation (3.7) becomes $\mathcal{F}(\bar{f}_\ell) = \mathcal{F}(c) \neq 0$ which implies that \bar{f}_ℓ is unbalanced. \square

Remark 14. *All the quadratic B.f.'s are a special case of the functions constructed in Proposition 13 since if we let $\tilde{g}_i = 0$, for all $1 \leq i \leq \ell$, we obtain their classification via affine equivalence as given in Theorem 5.*

Any B.f. can also be expressed in the form

$$f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n). \quad (3.8)$$

We call this form the *convolutional product* of g and h .

Next we completely classify the balanced cubic functions of the class $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, with $\deg(h), \deg(g) \leq 2$.

Theorem 15. *Let $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$ on $n + 1$ variables, with $\deg(h), \deg(g) \leq 2$, be cubic. Then f is balanced if and only if either both g and h are balanced or $g = h \circ \varphi + 1$, for some affinity φ and with both g and h unbalanced quadratic.*

Proof. Recall that $\mathcal{F}(g) = 2^n - 2w(g)$ and by Equation (3.2), we have $\mathcal{F}(f) = \mathcal{F}(g|_{\mathbb{F}^n}) + \mathcal{F}(h|_{\mathbb{F}^n})$. So f is balanced $\iff \mathcal{F}(f) = 0 \iff \mathcal{F}(g|_{\mathbb{F}^n}) = -\mathcal{F}(h|_{\mathbb{F}^n}) \iff 2^n - 2w(g|_{\mathbb{F}^n}) = -2^n + 2w(h|_{\mathbb{F}^n}) \iff w(g|_{\mathbb{F}^n}) + w(h|_{\mathbb{F}^n}) = 2^n \iff w(g|_{\mathbb{F}^n}) = 2^n - w(h|_{\mathbb{F}^n}) \iff w(g|_{\mathbb{F}^n}) = w(h|_{\mathbb{F}^n} + 1) \iff$ either both g and h are balanced or both g and h unbalanced quadratics related by $g = h \circ \varphi + 1$, for some affinity φ (see Lemma 8). \square

Observe that the forward direction of Theorem 15 holds in general but its converse might not be necessarily always true.

In the next result we construct balanced functions based on bent functions.

Proposition 16. *Let $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, with n even, be a B.f. on \mathbb{F}^{n+1} such that g and h are both bent. Then f is balanced if and only if $w(g) \neq w(h)$.*

Proof. Since $\mathcal{F}(g) = W_g(0) = \pm 2^{\frac{n}{2}}$, so any bent function on \mathbb{F}^n has the weight $2^{n-1} \pm 2^{\frac{n}{2}-1}$. Since $w(f) = w(g|_{\mathbb{F}^n}) + w(h|_{\mathbb{F}^n})$, so $w(f) = 2^n \pm 2^{\frac{n}{2}}$ if $w(g|_{\mathbb{F}^n}) = w(h|_{\mathbb{F}^n})$ and $w(f) = 2^n$ if $w(g|_{\mathbb{F}^n}) \neq w(h|_{\mathbb{F}^n})$. Hence f is balanced if and only if $w(g) \neq w(h)$. \square

Next we show that the balanced function in Proposition 16 [also for the unbalanced, that is, if $w(g) = w(h)$] are in fact plateaued.

Proposition 17. *Let $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, with n even, be a B.f. on \mathbb{F}^{n+1} such that g and h are both bent. Then f is a plateaued function.*

Proof. Let $\alpha = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$ and $z = (X, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$, where $X = (x_1, \dots, x_n)$. Then we have

$$\begin{aligned} W_f(\alpha) &= \sum_{z \in \mathbb{F}^{n+1}} (-1)^{f(z) + \alpha \cdot z} \\ &= \sum_{(x_{n+1}, X) \in \mathbb{F} \times \mathbb{F}^n} (-1)^{x_{n+1}g(X) + (1+x_{n+1})h(X) + a \cdot X + a_{n+1} \cdot x_{n+1}} \\ &= \sum_{X \in \mathbb{F}^n} (-1)^{h(X) + a \cdot X} + \sum_{X \in \mathbb{F}^n} (-1)^{g(X) + a \cdot X + a_{n+1}} \\ &= W_{h|_{\mathbb{F}^n}}(a) + (-1)^{a_{n+1}} W_{g|_{\mathbb{F}^n}}(a). \end{aligned} \tag{3.9}$$

Since g and h are bent then, for any $a \in \mathbb{F}^n$, the only possible values for $W_{h|_{\mathbb{F}^n}}(a)$ and $W_{g|_{\mathbb{F}^n}}(a)$ are $\pm 2^{\frac{n}{2}}$. So, for any $\alpha = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$, $W_f(\alpha)$ takes one of the values 0 or $\pm 2^{\frac{n}{2}+1}$. Hence f is plateaued. \square

4 Linear space of balanced Boolean functions

We present some conditions which help to determine whether a derivative of a B.f. is constant and we utilise them to check the balanced B.f.'s, constructed in Section 3, whose linear space is trivial.

Proposition 18. Let $f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$, where $g, h \in B_n$ and $f \in B_{n+1}$. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then

$$D_\lambda f \sim_A x_{n+1}D_a g + a_{n+1}g + D_a h.$$

Proof. Let $X = (x_1, \dots, x_n) \in \mathbb{F}^n$. Thus, we have $f = x_{n+1}g(X) + h(X)$. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. So

$$\begin{aligned} D_\lambda f &= (x_{n+1} + a_{n+1})g(X + a) + h(X + a) + x_{n+1}g(X) + h(X) \\ &= x_{n+1}[g(X + a) + g(X)] + a_{n+1}g(X + a) + h(X + a) + h(X) \\ &= x_{n+1}D_a g(X) + a_{n+1}[D_a g(X) + g(X)] + D_a h(X) \\ &\sim_A x_{n+1}D_a g(X) + a_{n+1}g(X) + D_a h(X). \quad (\text{apply } x_{n+1} \mapsto x_{n+1} + a_{n+1}) \quad \square \end{aligned}$$

For $f \in B_n$, we define the set which contains all $a \in \mathbb{F}^n$ such that $D_a f$ is balanced by $\Gamma(f)$, that is, $\Gamma(f) = \{a \in \mathbb{F}^n \mid D_a f \text{ is balanced}\}$ (see [4]).

We next show that the linear space of B.f. f and $\Gamma(f)$ are both invariant under affine equivalence.

Lemma 19. Let $g_1, g_2 \in B_n$ be such that $g_1 \sim_A g_2$. Then $|V(g_1)| = |V(g_2)|$ and $|\Gamma(g_1)| = |\Gamma(g_2)|$.

Proof. Let φ be the affinity of \mathbb{F}^n associated with invertible $M \in GL_n(\mathbb{F})$ and $w \in \mathbb{F}^n$, that is, $\varphi(y) = M \cdot y + w$, for all $y \in \mathbb{F}^n$. For $a \in \mathbb{F}^n$, we have

$$\begin{aligned} D_a g_1(x) &= D_a(g_2 \circ \varphi)(x) \\ &= g_2(\varphi(x + a)) + g_2(\varphi(x)) \\ &= g_2(M \cdot (x + a) + w) + g_2(\varphi(x)) \\ &= g_2(M \cdot x + M \cdot a + w) + g_2(\varphi(x)) \\ &= g_2(M \cdot a + \varphi(x)) + g_2(\varphi(x)) \\ &= D_{M \cdot a} g_2(\varphi(x)) = (D_{M \cdot a} g_2 \circ \varphi)(x). \end{aligned} \tag{4.1}$$

So it implies that $D_a g_1 = (D_{M \cdot a} g_2) \circ \varphi \sim_A D_{M \cdot a} g_2$. It follows by Proposition 3 that $w(D_a g_1) = w(D_{M \cdot a} g_2)$, so we conclude that $D_a g_1$ is balanced if and only if $D_{M \cdot a} g_2$ is balanced, $D_a g_1 = 0$ if and only if $D_{M \cdot a} g_2 \sim_A 0$, and $D_a g_1 = 1$ if and only if $D_{M \cdot a} g_2 \sim_A 1$. Hence we have $|V(g_1)| = |V(g_2)|$ and $|\Gamma(g_1)| = |\Gamma(g_2)|$. \square

Proposition 20. Let $f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$, where $g, h \in B_n$ and $f \in B_{n+1}$. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then $D_\lambda f = c$, with $c \in \mathbb{F}$ (i.e., $D_\lambda f$ is constant) if and only if $D_a g = 0$ and $D_a h = a_{n+1}g + c$.

Proof. $D_\lambda f = c$, with $c \in \mathbb{F}$ (i.e., $D_\lambda f$ is constant) if and only if

$$x_{n+1}D_a g + a_{n+1}g + D_a h = c$$

(see Proposition 18) if and only if $D_a g = 0$ and $D_a h = a_{n+1}g + c$. \square

We can deduce from Proposition 20 that the following result holds.

Corollary 21. Let $f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$, where $g, h \in B_n$ are non-constant and $f \in B_{n+1}$. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then $D_\lambda f$ is non-constant if and only if one of the following happens:

(i) $D_ag \neq 0$,

(ii) $D_ag = 0$ and $D_ah \neq a_{n+1}g + c$, with $c \in \mathbb{F}$.

Proposition 22. *If $f = x_{n+1}g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$, with n even and g bent, then f has a trivial linear space.*

Proof. Suppose that g is a bent function and let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. By Proposition 18, we have $D_\lambda f \sim_A x_{n+1}D_ag + a_{n+1}g + D_ah$. Observe that when $\lambda = (0, 1)$ we have $D_\lambda f \sim_A g$ which is a non-constant function since g is bent. If we show that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \times \{0\}) \times \mathbb{F}$, then we are done. Since g is bent then D_ag is balanced (i.e. nonzero), for any $a \in \mathbb{F}^n \setminus \{0\}$, and so we conclude by Corollary 21(i) that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \times \{0\}) \times \mathbb{F}$. \square

In the next result, we apply Corollary 21 to show that some balanced functions constructed in Proposition 12 have trivial linear space.

Proposition 23. *Let f be as constructed in Proposition 12. If $n \geq 3$ is odd and \tilde{g} with restriction to \mathbb{F}^{n-1} is bent, then the linear space of f is trivial.*

Proof. Assume that \tilde{g} , with restriction to \mathbb{F}^{n-1} , is bent and let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. We know, by Proposition 18, that $D_\lambda f \sim_A x_{n+1}D_ag + a_{n+1}g + D_ah$. Observe that when $\lambda = (0, 1)$ we have $D_\lambda f \sim_A g$ which is clearly non-constant as \tilde{g} is bent. Now we remain to show that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. We know from Corollary 21 that if D_ag is nonzero then $D_\lambda f$ is non-constant. So we can simply show that D_ag is nonzero, for all $a \in \mathbb{F}^n \setminus \{0\}$.

Let $a = (\tilde{a}, a_n) \in \mathbb{F}^{n-1} \times \mathbb{F}$, where $\tilde{a} = (a_1, \dots, a_{n-1})$. If $\tilde{a} = (0, \dots, 0)$ and $a_n = 1$, then we have $D_ag = 1$ which is nonzero. If $a = (\tilde{a}, 1)$, with $\tilde{a} \in \mathbb{F}^{n-1} \setminus \{0\}$, we have $D_ag = D_{\tilde{a}}\tilde{g} + 1$ which must be nonzero as $D_{\tilde{a}}\tilde{g}$ is balanced because \tilde{g} is bent. If $a = (\tilde{a}, 0)$, with $\tilde{a} \in \mathbb{F}^{n-1} \setminus \{0\}$, we have $D_ag = D_{\tilde{a}}\tilde{g}$ which is balanced as \tilde{g} is bent. Thus, D_ag is nonzero, for all $a \in \mathbb{F}^n \setminus \{0\}$. Hence the linear space of f is trivial. \square

Notice that we can apply similar arguments as in the proof of Proposition 23 to show that the linear space for any function of the form given in Proposition 13, with \tilde{g}_1 bent, is trivial.

Example 24. *For any positive odd integer $n \geq 3$, a function of the form:*

$$f = x_{n+1}(x_1x_2 + \dots + x_{n-2}x_{n-1} + x_n) + h(x_1, \dots, x_{n-2}) + x_{n-1}$$

is balanced and its linear space is trivial.

Next we determine whether the linear space of any balanced cubic function of the form (3.8) [i.e., $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, with $\deg(g), \deg(h) \leq 2$] is trivial. From Theorem 15, we know that such functions are balanced if and only if either both g and h are balanced or $g = h \circ \varphi + 1$, for some unbalanced quadratics g and h , and an affinity φ .

Proposition 25. *Let $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$ on \mathbb{F}^{n+1} , with n even, be cubic such that g and h are quadratic bent related by $g = h \circ \varphi + 1$, for some affinity φ . Then the linear space of f is trivial.*

Proof. Suppose that both g and h , with restrictions to \mathbb{F}^n , are bent. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Observe that $f = x_{n+1}(g + h) + h$, and so f is cubic if and only if $g + h$ is a quadratic function. So we assume that $g + h$ is quadratic. By Proposition 18, we have $D_\lambda f \sim_A x_{n+1}D_a(g + h) + a_{n+1}(g + h) + D_a h$. Observe that when $\lambda = (1, 0)$ we have $D_\lambda f \sim_A g + h$ which is non-constant as we assumed that $g + h$ is quadratic.

Next we prove that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. By Corollary 21(i), we know that if $D_a(g + h) \neq 0$, then $D_\lambda f$ is non-constant. Now we show that $D_\lambda f$ is still non-constant if $D_a(g + h) = 0$, for some $a \in \mathbb{F}^n \setminus \{0\}$. Assume that $D_a(g + h) = 0$, for some $a \in \mathbb{F}^n \setminus \{0\}$. Then we have $D_\lambda f \sim_A a_{n+1}(g + h) + D_a h$. If $a_{n+1} = 0$ then $D_\lambda f \sim_A D_a h$, and so it is non-constant since $D_a h$ has to be balanced as h is bent. If $a_{n+1} = 1$ then $D_\lambda f \sim_A g + h + D_a h$ which is also non-constant since $g + h$ is a quadratic and $D_a h$ has degree 1 as it is balanced. \square

Remark 26. *Since the convolutional product of g and h can be reduced to $f = x_{n+1}(g + h) + h$, so either $\deg(f) = \deg(h)$ [this happens when $\deg(g + h) < \deg(h)$] or $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. Moreover, we can use Theorem 11, to deduce that $w(f) = w(g|_{\mathbb{F}^n}) + w(h|_{\mathbb{F}^n})$ and f is balanced if g and h are balanced.*

Finally, we determine some balanced functions constructed in Proposition 16 [i.e., $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, where g and h are both bent and $w(g) \neq w(h)$] which have trivial linear space.

Proposition 27. *Let $f = x_{n+1}g(x_1, \dots, x_n) + (1 + x_{n+1})h(x_1, \dots, x_n)$, with n even, be a B.f. on $n + 1$ variables such that g and h are both bent. Then the linear space of f is trivial if $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$.*

Proof. Recall that $D_\lambda f \sim_A x_{n+1}D_a(g + h) + a_{n+1}(g + h) + D_a h$, for $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$ (see Proposition 25). Observe that $f = x_{n+1}(g + h) + h$. We are given that $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. So it follows that $\deg(g + h) = \max\{\deg(g), \deg(h)\}$, implying that $g + h$ is non-constant since g and h are bent. When $\lambda = (0, 1)$, we have $D_\lambda f \sim_A g + h$ which is non-constant.

Now we prove that $D_\lambda f$, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$, is non-constant. If $D_a(g + h) \neq 0$, then $D_\lambda f$ is non-constant, by Corollary 21(i). Suppose that $D_b(g + h) = 0$, for some $b \in \mathbb{F}^n \setminus \{0\}$. We need to show that $D_\lambda f$ is still non-constant, for $\lambda = (b, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. In this case we have $D_\lambda f \sim_A a_{n+1}(g + h) + D_b h$. If $a_{n+1} = 0$ then we have $D_\lambda f \sim_A D_b h$ which is non-constant since $D_b h$ has to be balanced as h is bent. If $a_{n+1} = 1$ then we have $D_\lambda f \sim_A g + h + D_b h$. Since $\deg(g + h) = \max\{\deg(g), \deg(h)\}$, so we have $\deg(g + h) = \max\{\deg(g), \deg(h)\} > \deg(D_b h)$, implying that $\deg(D_\lambda f) = \deg(g + h) > \deg(D_b h)$. So $D_\lambda f$ must be non-constant. Hence the linear space of f is trivial. \square

Let $\alpha = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Observe that, from Equation (3.9), we obtain $|W_f(\alpha)| \leq |W_{g|_{\mathbb{F}^n}}| + |W_{h|_{\mathbb{F}^n}}|$. So it follow that the nonlinearity of f in Propositions 25 and 27 is

$$\begin{aligned}
\mathcal{N}(f) &= 2^n - \frac{1}{2} \max_{\alpha \in \mathbb{F}^{n+1}} |W_f(\alpha)| \\
&\geq 2^n - \frac{1}{2} \max_{\alpha \in \mathbb{F}^{n+1}} (|W_{g|_{\mathbb{F}^n}}| + |W_{h|_{\mathbb{F}^n}}|) \\
&\geq 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}^{n+1}} |W_{g|_{\mathbb{F}^n}}| + 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}^{n+1}} |W_{h|_{\mathbb{F}^n}}| \\
&= \mathcal{N}(g|_{\mathbb{F}^n}) + \mathcal{N}(h|_{\mathbb{F}^n})
\end{aligned} \tag{4.2}$$

This suggests a way of constructing B.f.'s with high nonlinearity. For instance, from the relation (4.2), we deduce that the nonlinearity of the balanced function f constructed in Propositions 25 and 27 is $\mathcal{N}(f) \geq 2^{N-1} - 2^{\frac{N-1}{2}}$, with $N = n + 1$.

Example 28. Let $g = x_1x_2 + x_3x_4 + 1$ and $h = x_1x_4 + x_2x_3$. The cubic function $f = x_5g + (1 + x_5)h$ is balanced and its linear space is trivial. It can be easily verified that $\mathcal{N}(f) = 12$, implying that f is semi-bent. Note that both g and h , with restriction to \mathbb{F}^4 , are bent related by $g = h \circ \varphi + 1$, where $\varphi = A(x_1, x_2, x_3, x_4)^T$, with

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

5 APN functions in even dimension

In this section we study the linear spaces of components of APN functions in even dimension. We show that, for any APN function, there must be a component with trivial linear space. We also provide a general form for the number of bent components in quadratic APN function and show bounds on their number.

5.1 Linear space for components of APN functions in even dimension

We first give some definitions and results which are crucial in studying the linear spaces of components of APN functions in even dimension.

Definition 29. A B.f. f on n variables is called a splitting function if we have $f \sim_A g(x_1, \dots, x_i) + h(x_{i+1}, \dots, x_n)$, for some positive integer i , $g \in B_i$ and $h \in B_{n-i}$. We say that i is a splitting number of f and $S(f)$ denotes the set of all splitting numbers of f . We define a splitting index of f as the number $\sigma(f) = \min S(f)$.

Remark 30. Let $f \in B_n$ be a splitting function. Then

1. i is a splitting number $\iff n - i$ is a splitting number,
2. clearly, $\sigma(f) \in \{1, \dots, \lfloor n/2 \rfloor\}$.

Lemma 31. Let $f \in B_n$. Then $\sigma(f) = 1$ if and only if $\dim V(f) \geq 1$.

Proof. Suppose that $\sigma(f) = 1$, that is, $f \sim_A \tilde{f} = g(x_1) + h(x_2, \dots, x_n)$. So we have $\tilde{f} = f \circ \varphi$, where $\varphi(y) = My + w$, for some $w \in \mathbb{F}^n$ and invertible $M \in GL_n(\mathbb{F})$. Clearly $D_{e_1}f$ is constant. By Equation (4.1) in the proof Lemma 19, we have $D_{e_1}\tilde{f} = (D_{Me_1}f) \circ \varphi$ and since $w(D_{e_1}\tilde{f}) = w(D_{Me_1}f)$ (see Proposition 3), so $(D_{Me_1}f) \circ \varphi$ must also be constant. Note that $Me_1 \neq 0$ since M is a linear isomorphism. Thus both 0 and Me_1 are in $V(f)$ which implies that $\dim V(f) \geq 1$.

Conversely, suppose that $\dim V(f) \geq 1$, that is, $\exists a \neq 0 \in V(f)$ such that $D_af = c$, with $c \in \mathbb{F}$. We can take the \mathbb{F} -linear isomorphism E of \mathbb{F}^n that sends $e_1 \mapsto Ee_1 = a$ so that we have $\tilde{f} = f \circ E$ and thus,

$$D_{e_1}\tilde{f} = (D_{Ee_1}f) \circ E = (D_af) \circ E = (c) \circ E = c$$

which implies that $D_{e_1}\tilde{f}$ is constant. Since we have $D_{e_1}\tilde{f} = c$, so we can write $\tilde{f} = cx_1 + h(x_2, \dots, x_n)$. Hence $\sigma(f) = 1$ as $f \sim_A \tilde{f}$. \square

Remark 32. If $g(x_1, \dots, x_s)$, with a positive integer $s < n$, is in B_n then we have $w(g) = 2^{n-s}w(g|_{\mathbb{F}^s})$.

The preceding remark is useful in the following.

Lemma 33. Let $f \in B_n$, with n even. If $\sigma(f) = 1$, then $|\Gamma(f)| \leq 2^n - 4$.

Proof. Suppose $f \in \mathbb{F}^n$ has $\sigma(f) = 1$, that is, $f \sim_A \tilde{f} = cx_1 + h(x_2, \dots, x_n)$, with $c \in \mathbb{F}$. By Lemma 19, we have $|\Gamma(f)| = |\Gamma(\tilde{f})|$, so we can simply consider $|\Gamma(\tilde{f})|$. It is clear that 0 and e_1 are both not in $\Gamma(\tilde{f})$ since $D_0\tilde{f} = 0$ and $D_{e_1}\tilde{f} = c$. Suppose that these are the only ones, that is, $|\Gamma(\tilde{f})| = 2^n - 2$. This implies that, for all $a \in \mathbb{F}^n \setminus \{0, e_1\}$, $D_a\tilde{f}$ is balanced.

Let $W = \langle e_2, \dots, e_n \rangle$ and denote $W^* = W \setminus \{0\}$. Clearly, W^* is contained in $\mathbb{F}^n \setminus \{0, e_1\}$, that is, $W^* \subset \Gamma(\tilde{f})$. So, for all $a \in W^*$, $D_a\tilde{f}$ is balanced. It is clear that $W \simeq \mathbb{F}^{n-1}$. Observe that, for any $a = (0, b) \in \{0\} \times (\mathbb{F}^{n-1} \setminus \{0\}) = W^*$, we have $D_a\tilde{f} = D_bh$ as the first coordinate of a is 0. Since $D_a\tilde{f}$ does not depend on x_1 then, by Remark 32, we have $2^{n-1} = w(D_a\tilde{f}) = w(D_bh) = 2w(D_bh|_{\mathbb{F}^{n-1}}) \implies w(D_bh|_{\mathbb{F}^{n-1}}) = 2^{n-2}$, that is, $D_bh|_{\mathbb{F}^{n-1}}$ is balanced, for all $b \in \mathbb{F}^{n-1} \setminus \{0\}$. This implies that h , with restriction to \mathbb{F}^{n-1} , is bent (see Theorem 2).

But $n-1$ is odd as n is even, so it implies that we have a bent function on \mathbb{F} -vector space of odd dimension, which is impossible. Thus, the assumption that $|\Gamma(\tilde{f})| = 2^n - 2$ is false, and so we can say $|\Gamma(\tilde{f})| \leq 2^n - 3$.

Suppose that $d \in \mathbb{F}^n \setminus \{0, e_1\}$ is the other nonzero element such that $D_d\tilde{f}$ is unbalanced. So $D_{d+e_1}\tilde{f}(x) = D_{e_1}\tilde{f}(x) + D_d\tilde{f}(x+e_1) = c + D_d\tilde{f}(x+e_1) = (c + D_d\tilde{f}(x)) \circ \varphi$, for $c \in \mathbb{F}$ and $\varphi(y) = Iy + e_1$, with I as an identity in $GL_n(\mathbb{F})$. That is, $D_{d+e_1}\tilde{f}(x) \sim_A D_d\tilde{f}(x) + c$. Since $D_d\tilde{f}(x)$ is unbalanced then $D_d\tilde{f}(x) + c$ must be unbalanced, implying that $D_{d+e_1}\tilde{f}(x)$ is also unbalanced. That is, $\{0, e_1, d, d+e_1\} \not\subset \Gamma(\tilde{f})$. Hence we have $|\Gamma(\tilde{f})| \leq 2^n - 4$. \square

Next we state a well-known result for characterization of APN function.

Theorem 34 ([1]). Let F be a v.B.f. from \mathbb{F}^n into \mathbb{F}^n . Then

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a(F_\lambda)) \geq 2^{2n+1}(2^n - 1). \quad (5.1)$$

Moreover, F is APN if and only if equality holds.

In the next results we discuss about the linear space for components of an APN function in even dimension.

Theorem 35. Let a v.B.f. F from \mathbb{F}^n to itself, with n even, be APN. Then there is $\lambda \neq 0 \in \mathbb{F}^n$ such that the linear space of F_λ is trivial.

Proof. Since, by Lemma 31, a B.f. has a nonzero linear structure if and only if its splitting index is 1, so we simply show that for any APN function F it is impossible to have $\sigma(F_\lambda) = 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$.

Suppose, by contradiction, that F is APN and $\sigma(F_\lambda) = 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$. By Lemma 33, we can suppose that, for any $\lambda \neq 0 \in \mathbb{F}^n$, there are nonzero v , u and w not in $\Gamma(F_\lambda)$ such that D_vF_λ is constant, D_uF_λ and D_wF_λ are both unbalanced. So we have

$\mathcal{F}^2(D_0F_\lambda) = \mathcal{F}^2(D_vF_\lambda) = 2^{2n}$, and both $\mathcal{F}^2(D_uF_\lambda)$ and $\mathcal{F}^2(D_wF_\lambda)$ are nonzero positive integers (recall that, for any B.f. f , $\mathcal{F}(f) = 0$ if and only if f is balanced). Thus, we have

$$\begin{aligned} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda) &\geq \mathcal{F}^2(D_0F_\lambda) + \mathcal{F}^2(D_vF_\lambda) + \mathcal{F}^2(D_uF_\lambda) + \mathcal{F}^2(D_wF_\lambda) \\ &= 2^{2n} + 2^{2n} + \mathcal{F}^2(D_uF_\lambda) + \mathcal{F}^2(D_wF_\lambda) > 2^{2n+1} \end{aligned}$$

from which we deduce that

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda) > 2^{2n+1}(2^n - 1).$$

Thus, by Theorem 34, it is impossible for F to be an APN function. So it follows that if F is an APN function in even dimension then there is a component whose linear space is trivial. \square

Proposition 36 ([4]). *Let F be an APN permutation over \mathbb{F}^n , with n even. If there are $\lambda \neq 0, a \neq 0 \in \mathbb{F}^n$ such that D_aF_λ is constant, then $D_aF_\lambda = 1$.*

In the next result we talk about the maximum possible dimension for linear spaces of components of APN permutation.

Theorem 37. *If F is an APN permutation over \mathbb{F}^n , with n even, then $\dim V(F_\lambda) \leq 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$.*

Proof. Suppose, by contradiction, that there is $\mu \neq 0 \in \mathbb{F}^n$ such that $\dim V(F_\mu) > 1$. It follows that $V(F_\mu)$ contains at least three nonzero elements. Let $a, b \in V(F_\mu)$ be nonzero and distinct. Then, by Proposition 36, we have $D_aF_\lambda = D_bF_\lambda = 1$. Clearly, $a + b$ is also a nonzero element in $V(F_\mu)$ different from a and b . Note that $D_{a+b}F_\mu(x) = D_aF_\mu(x) + D_bF_\mu(x + a)$, $x \in \mathbb{F}^n$. By Equation (4.1) in the proof Lemma 3, $D_bF_\mu(x + a) = (D_{Ib}F_\mu) \circ \varphi \sim_A D_bF_\mu$, with $\varphi(x) = Ix + a$ and I being the identity matrix of $GL_n(\mathbb{F})$. Since $D_bF_\mu = 1$, so we must have $D_bF_\mu(x + a) = 1$. Thus, $D_{a+b}F_\mu(x) = 0$, which is impossible by Proposition 36. Thus, we must have $\dim V(F_\lambda) \leq 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$. \square

5.2 Quadratic APN functions

A quadratic v.B.f. from \mathbb{F}^n to itself is denoted by Q , the linear space $V(Q_\lambda)$ of a component Q_λ is denoted by V_λ and we let $V_\lambda^* = V_\lambda \setminus \{0\}$. It is well-known that any APN function cannot contain linear components, so we assume that Q is pure quadratic. For quadratic functions, it is clear from Theorem 5 that we have trivial linear space if and only if the function is bent. So, by Theorem 35, any quadratic APN functions must have some bent components. In this subsection we are mainly counting how many bent components are in quadratic APN functions.

First we prove a result which relates the dimensions of linear spaces for components of Q to quadratic APN functions.

Proposition 38. *For any quadratic $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$, we have*

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} (2^{\dim V_\lambda} - 1) \geq 2^n - 1. \quad (5.2)$$

Moreover, equality holds if and only if Q is APN.

Proof. Since $\mathcal{F}^2(D_0Q_\lambda) = 2^{2n}$, so we have

$$\begin{aligned}
\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda) &= \sum_{\lambda \neq 0 \in \mathbb{F}^n} [\mathcal{F}^2(D_0Q_\lambda) + \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda)] \\
&= \sum_{\lambda \neq 0 \in \mathbb{F}^n} [2^{2n} + \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda)] \\
&= 2^{2n}(2^n - 1) + \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda). \tag{5.3}
\end{aligned}$$

By Theorem 34 and Equation (5.3), we deduce that

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda) \geq 2^{2n}(2^n - 1) \tag{5.4}$$

and equality holds if and only if Q is APN.

For any quadratic Q , $\deg(D_aQ_\lambda) = 0$ if $a \in V_\lambda$ and $\deg(D_aQ_\lambda) = 1$ if $a \notin V_\lambda$. So we have $\mathcal{F}^2(D_aQ_\lambda) = 2^{2n}$ if $a \in V_\lambda$ and $\mathcal{F}^2(D_aQ_\lambda) = 0$ if $a \notin V_\lambda$. Thus, we have

$$\begin{aligned}
\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{F}^2(D_aQ_\lambda) &= \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in V_\lambda^*} \mathcal{F}^2(D_aQ_\lambda) \\
&= \sum_{\lambda \neq 0 \in \mathbb{F}^n} 2^{2n}|V_\lambda^*| \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} (2^{\dim V_\lambda} - 1). \tag{5.5}
\end{aligned}$$

We deduce, from the relation (5.4) and Equation (5.5), that

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} (2^{\dim V_\lambda} - 1) \geq 2^n - 1$$

and equality holds if and only if Q is APN. \square

It can be easily shown that for any quadratic B.f. f in odd dimension we have $\dim V(f) \geq 1$ and equality holds when f is a semi-bent. This implies that the equality in the relation (5.2) happens when Q is an AB function. Since in odd dimension all quadratic functions have non-trivial linear space, then all components of any quadratic APN function in odd dimension have non-trivial linear space. Thus, it implies that the result in Theorem 35 cannot be extended to APN function in odd dimension.

Now we focus on quadratic v.B.f. in even dimension. From Theorem 5, it is clear that any quadratic B.f. in even dimension has a splitting index 1 or 2. By Corollary 7, we deduce that quadratic is bent if and only if the splitting index is 2.

Definition 39. For any quadratic Q , define

$$\Delta_i = \{\lambda \in \mathbb{F}^n \mid \lambda \neq 0, \sigma(Q_\lambda) = i\}, \quad N = |\Delta_1| \quad \text{and} \quad B = |\Delta_2|.$$

Remark 40. From Definition 39, N is the number of non-bent components and B is the number of bent components in Q and so we have $N + B = 2^n - 1$.

Nyberg in [14], proved that bent functions exist only from \mathbb{F}^n to \mathbb{F}^m , with $m \leq n/2$, so it well-known that no v.B.f. from \mathbb{F}^n to itself is bent.

Remark 41. *The maximum number of bent components in any v.B.f. from \mathbb{F}^n to itself is $2^n - 2^{\frac{n}{2}}$ (see [15]). So $0 \leq B \leq 2^n - 2^{\frac{n}{2}}$. In [16], no plateaued APN function has the maximum number of bent components. It is well-known that quadratic functions are plateaued.*

In the next result we wish to determine B when Q is an APN function and contains only bent and semi-bent components.

Proposition 42. *Let a quadratic $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$, with n even, be such that Q_λ , with $\lambda \neq 0$, is bent or semi-bent. Then Q is APN if and only if there are exactly $\frac{2}{3}(2^n - 1)$ bent components.*

Proof. For any quadratic APN Q , by Theorem 35, we conclude that $B > 0$, that is, some components of Q must be bent (as we require that the linear space of some components must be trivial). Since n is even, so $\dim V_\lambda$ is even (see Remark 6). From Theorem 5 and Corollary 7, we can deduce that $\dim V_\lambda = 0$ if and only if Q_λ is bent. That is, $\dim V_\lambda \neq 0$ if $\lambda \in \Delta_1$ and $\dim V_\lambda = 0$ if $\lambda \in \Delta_2$. For any quadratic APN Q , by Proposition 38, we must have

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} (2^{\dim V_\lambda} - 1) = 2^n - 1. \quad (5.6)$$

Since $\dim V_\lambda = 0$ if $\lambda \in \Delta_2$, then Equation (5.6) can be reduced to

$$\sum_{\lambda \in \Delta_1} (2^{\dim V_\lambda} - 1) = 2^n - 1. \quad (5.7)$$

That is, Q is APN if and only if Equation (5.7) holds.

If Q is such that Q_λ , with $\lambda \neq 0$, is bent or semi-bent, then N is the number of semi-bent (i.e., $\dim V_\lambda = 2$, for any $\lambda \in \Delta_1$). Thus, Equation (5.7) is true if and only if $(2^2 - 1)|\Delta_1| = 3N = 2^n - 1 \iff N = (2^n - 1)/3$. Since $N + B = 2^n - 1$, so $B = 2(2^n - 1)/3$. \square

It follows from Proposition 42 that any quadratic APN function in even dimension with the set $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$ as its Walsh spectrum has $2(2^n - 1)/3$ bent components. It is well-known that the Walsh spectrum of any Gold function in even dimension is $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$, so any Gold function has $2(2^n - 1)/3$ bent components.

Theorem 43. *Let a quadratic $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$, with n even, be APN. Then*

$$2(2^n - 1)/3 \leq B \leq 2^n - 2^{n/2} - 2,$$

where $B = 2(2^n - 1)/3 + 4t$, for some integer $t \geq 0$.

Proof. Suppose that Q is APN. Since the dimension of the linear space of any quadratic in even dimension is even (see Remark 6), so it follows that for any Q_λ , with $\lambda \in \Delta_1$, we have $\dim V_\lambda \geq 2$. If, for any $\lambda \in \Delta_1$, Q_λ is semi-bent then we are in Proposition 42, that is, $B = 2(2^n - 1)/3$. If some components are neither bent nor semi-bent, then we must have $B > 2(2^n - 1)/3$ for Equation (5.7) to be satisfied.

If Q has a component Q_μ , with $\mu \in \Delta_1$, which is not semi-bent, then $\dim V_\mu = 2k$, for some $k \geq 2$. So, for Equation (5.7) to be satisfied, the presence of Q_μ in Q has to increase the number of bent components by

$$\frac{2^{2k} - 1}{2^2 - 1} - 1 = \frac{2^{2k} - 4}{3} = 4 \left(\frac{2^{2k-2} - 1}{3} \right)$$

which clearly is divisible by 4. So it follows that $B = 2(2^n - 1)/3 + 4t$, for some integer $t \geq 0$.

By Remark 41, we have $B \leq 2^n - 2^{n/2}$. Now we show that it not possible to have $B = 2^n - 2^{n/2}$. For some $t \geq 0$, we have $B = 2(2^n - 1)/3 + 4t = 2[(2^n - 1)/3 + 2t] \not\equiv 0 \pmod{4}$ since $(2^n - 1)/3 + 2t$ is odd. Thus, $B \neq 2^n - 2^{n/2}$ since $2^n - 2^{n/2} \equiv 0 \pmod{4}$. Hence we must have $B \leq 2^n - 2^{n/2} - 2$. \square

For any quadratic APN Q in demension 4, by Theorem 43, we only have one possibility, that is, $B = 10$ (this satisfies Proposition 42). We state this result in following.

Corollary 44. *A pure quadratic $Q : \mathbb{F}^4 \rightarrow \mathbb{F}^4$ is APN if and only if $B = 10$.*

Not long time ago, only quadratic APN functions with $B = 2(2^n - 1)/3$ were known. From Proposition 42, such functions contain only bent and semi-bent components. As noted earlier Gold functions are example of such functions. It had been conjectured that all quadratic APN functions are equivalent to Gold functions (i.e., all quadratic APN functions have the same number of bent components) until Dillon in 2006 gave an example of quadratic APN with different number of bent components and inequivalent to Gold functions. The Dillon's Example:

$$F(x) = x^3 + z^{11}x^5 + z^{13}x^9 + x^{17} + z^{11}x^{33} + x^{48}$$

is defined over \mathbb{F}_{2^6} , with z primitive. Using MAGMA, we found that F has 46 bent components. That is, it is an example of quadratic APN with $B = 2(2^n - 1)/3 + 4$ (i.e., $t = 1$ by Theorem 43). Also by computer search, we found the function:

$$G(x) = x^3 + z^{53}x^{10} + z^{41}x^{18} + z^{59}x^{33} + z^{43}x^{34} + z^{31}x^{48}$$

over \mathbb{F}_{2^6} , with z primitive, which has the same number of bent components as F , the Dillon's Example. From Theorem 43, we deduce that, in dimension 6, all the possibilities for the number of bent components in any quadratic APN function are: 42, 46, 50 and 54. So far we only know the existence of quadratic APN functions with 42 (Gold functions and others) and 46 (Dillon's example) bent components but we are uncertain whether those with 50 and 54 exists.

In [19], some quadratic APN functions in dimension 8 with Walsh spectrum $\{-64, -32, -16, 0, 16, 32, 64\}$ (which is different from the Walsh spectrum of Gold function) are found. These functions are further classified in terms of their distribution of Walsh coefficients and two classes are found. One class has 487 functions and the other one has 12 functions. In a class of 487 functions, we considered the function:

$$\begin{aligned} G'(x) = & z^{249}x^{192} + z^{24}x^{160} + z^{210}x^{144} + z^{69}x^{136} + z^{46}x^{132} + z^{164}x^{130} + z^{43}x^{129} \\ & + z^{31}x^{96} + z^{30}x^{80} + z^{115}x^{72} + z^{228}x^{68} + z^{16}x^{66} + z^{228}x^{65} + z^{217}x^{48} \\ & + z^9x^{40} + z^{251}x^{36} + z^{151}x^{34} + z^{77}x^{33} + z^{189}x^{24} + z^{109}x^{20} + z^{191}x^{18} \\ & + z^{249}x^{17} + z^{175}x^{12} + z^{130}x^{10} + z^{91}x^9 + z^{59}x^6 + z^{60}x^5 + z^{121}x^3 \end{aligned}$$

and by checking with MAGMA, we found that it contains $2(2^8 - 1)/3 + 4 = 174$ bent components (i.e., $t = 1$ by Theorem 43) and in the other class, we considered the function:

$$\begin{aligned} G''(x) = & z^{130}x^{192} + z^{160}x^{160} + z^{117}x^{144} + z^{230}x^{136} + z^{228}x^{132} + z^{162}x^{130} \\ & + z^{25}x^{129} + z^{79}x^{96} + z^{204}x^{80} + z^{83}x^{72} + z^{159}x^{68} + z^{234}x^{66} + z^{36}x^{65} \\ & + z^{67}x^{48} + z^{151}x^{40} + z^{17}x^{36} + z^{81}x^{34} + z^{52}x^{33} + z^9x^{24} + z^{116}x^{20} \\ & + z^{102}x^{18} + z^{97}x^{17} + z^{74}x^{12} + z^{48}x^{10} + z^{144}x^9 + z^{58}x^6 + z^{146}x^5 + z^{123}x^3 \end{aligned}$$

which was found to have $2(2^8 - 1)/3 + 8 = 178$ bent components (i.e., $t = 2$ by Theorem 43). Thus, in dimension 8, we only know the existence of quadratic APN functions with 170, 174 and 178 bent components and it is yet to be known whether quadratic APN functions having $B = 2(2^8 - 1)/3 + 4t$, with $3 \leq t \leq 17$, bent components exist.

Proposition 45. *Let $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$ be APN with $B = 2(2^n - 1)/3 + 4t$, for some positive integer t , as described in Theorem 43. Then*

$$\mathcal{N}(Q) = \begin{cases} 2^{n-1} - 2^{n/2} & \text{if } t = 0, n \geq 4 \\ 2^{n-1} - 2^{n/2+1} & \text{if } 1 \leq t \leq 4, n \geq 6 \end{cases}$$

Proof. We first need to recall from Remark 6, that for any quadratic B.f. on n variables, with even n , the dimension k of its linear space is even and the Walsh spectrum is $\{0, 2^{(n+k)/2}\}$.

If $t = 0$ then, by Proposition 42, all components of Q are bent and semi-bent, that is, the Walsh spectrum of Q is $\{0, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$. So clearly, by Corollary 9, $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2}$.

To prove that $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2+1}$ if $1 \leq t \leq 4$, we need to show that for this range of t we have $\dim V_\lambda \in \{0, 2, 4\}$, for all $\lambda \neq 0 \in \mathbb{F}^n$, that is, Walsh spectrum of Q is $\{0, \pm 2^{(n+4)/2}, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$.

It is clear from Theorem 43 that for $t \geq 1$, we have $B > 2(2^n - 1)/3$, and so Proposition 42 allows us to conclude that there must be $\lambda \neq 0 \in \mathbb{F}^n$ such that $\dim V_\lambda > 2$. We claim that if $1 \leq t \leq 4$, then we have $\dim V_\lambda \in \{0, 2, 4\}$, for $\lambda \neq 0 \in \mathbb{F}^n$. Suppose, by contradiction, that there is $\mu \neq 0 \in \mathbb{F}^n$ such that $\dim V_\mu = 6$. Then, as noted in the proof of Theorem 43, the presence of Q_μ increases the number of bent components by

$$4 \left(\frac{2^{6-2} - 1}{3} \right) = 4(5),$$

implying that $B \geq 2(2^n - 1)/3 + 4(5)$. So it follows that if, for some $\lambda \neq 0 \in \mathbb{F}^n$, $\dim V_\lambda = 6$, then we have $t \geq 5$. This implies that, if $1 \leq t \leq 4$, then we must have $\dim V_\lambda \in \{0, 2, 4\}$, for all $\lambda \neq 0 \in \mathbb{F}^n$. So in this case the Walsh spectrum of Q is $\{0, \pm 2^{(n+4)/2}, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$ from which we deduce that $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2+1}$. \square

From Proposition 45, it seems like the nonlinearity of any quadratic APN function decreases as the number of bent components increases and it is the highest when the number of bent components is at the lowest possible.

6 Quadratic power functions

Pott et al. in [15] say that the question to determine all monomial bent functions $Tr(\alpha x^d)$ on \mathbb{F}_{2^n} , with $\alpha \in \mathbb{F}_{2^n}^*$ and n even, has attracted quite a lot of research interest. In this section we study the Walsh spectrum and enumerate bent components for any quadratic power functions. Recall that a function $F = x^d$ is a quadratic power functions if $d = 2^j + 2^i$, with $i \neq j$ and $j > i \geq 0$. It is well-known that a function with the power $d = 2^i(2^{j-i} + 1)$ is affine equivalent to the one with power $d' = 2^{j-i} + 1$. So we simply consider the power $2^k + 1$, for some positive integer k . For a function F , we denote its image by $\text{Im}(F)$.

We denote the greatest common divisor integers m and m' by (m, m') . We begin with the following well-known result which can be found in [11].

Lemma 46. *For any positive integers n and k , we have*

$$(a) \quad (2^n - 1, 2^k - 1) = 2^{(n,k)} - 1,$$

$$(b) \quad (2^n - 1, 2^k + 1) = \begin{cases} 1 & \text{if } n/(n,k) \text{ is odd,} \\ 2^{(n,k)} + 1 & \text{if } n/(n,k) \text{ is even.} \end{cases}$$

Theorem 47. *Let $F(x) = x^{2^k+1}$ be a function in $\mathbb{F}_{2^n}[x]$, with even n and some integer $k \geq 1$. Let $m = (n, k)$, $s = (n, 2k)$ and $e = 1$ if n/m is odd and $e = 2^m + 1$ if n/m is even. Then*

- (a) F is an e -to-1 function,
- (b) F_α is bent if and only if $\alpha \notin \text{Im}(F)$.
- (c) the number of bent components for F is $\frac{(e-1)(2^n-1)}{e}$,
- (d) the Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$, and $\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$ if $e = 2^m + 1$.

Proof. Let $S = \text{Im}(F) \setminus \{0\} = \{\xi^{2^k+1} \mid \xi \in \mathbb{F}_{2^n}^*\}$. It can be easily shown that S is a multiplicative subgroup of $\mathbb{F}_{2^n}^*$.

- (a) Clearly, F maps $\mathbb{F}_{2^n}^*$ onto S . So we only need to show that S has the order $(2^n - 1)/e$. Now we need to find the order of S . First observe that every element ζ in S satisfies $\zeta^{(2^n-1)/e} = 1$, where $e = (2^n - 1, 2^k + 1)$. By Lemma 46, $e = 1$ if n/m is odd and $e = 2^m + 1$ if n/m is even. If ν is a primitive element in \mathbb{F}_{2^n} , then the order of ν^{2^k+1} is $\text{ord}(\nu^{2^k+1}) = \text{ord}(\nu^e) = (2^n - 1)/e$. Clearly, ν^{2^k+1} has the highest order in S . It is well-known that $\mathbb{F}_{2^n}^*$ is cyclic group, so S being a subgroup must be cyclic with ν^{2^k+1} as a generator. Thus, it follows that the order of S is $(2^n - 1)/e$, implying that F is an e -to-1 function.
- (b) It is equivalent to show that F_α is non-bent if and only if $\alpha \in \text{Im}(F)$. F_α is bent if its linear space is trivial, so we need to prove that the dimension of the linear space of F_α is non-trivial, that is, $\dim V_\alpha \geq 1$ if and only if $\alpha \in \text{Im}(F)$.

A component F_α , with $\alpha \in \mathbb{F}_{2^n}$, is non-bent if there exists β in $\mathbb{F}_{2^n}^*$ such that $D_\beta F_\alpha$ is constant. Suppose that F_α , with $\alpha \in \mathbb{F}_{2^n}^*$, is non-bent and $D_\beta F_\alpha$ is constant, with $\beta \in \mathbb{F}_{2^n}$. So we have

$$\begin{aligned}
D_\beta F_\alpha(x) &= F_\alpha(x) + F_\alpha(x + \beta) = \text{Tr}(\alpha x^{2^k+1}) + \text{Tr}(\alpha(x + \beta)^{2^k+1}) \\
&= \text{Tr}(\alpha x^{2^k+1}) + \text{Tr}(\alpha(x^{2^k} + \beta^{2^k})(x + \beta)) \\
&= \text{Tr}(\alpha x^{2^k+1}) + \text{Tr}(\alpha(x^{2^k+1} + \beta x^{2^k} + \beta^{2^k}x + \beta^{2^k+1})) \\
&= \text{Tr}(\alpha \beta x^{2^k}) + \text{Tr}(\alpha \beta^{2^k} x) + \text{Tr}(\alpha \beta^{2^k+1}) \\
&= \text{Tr}((\alpha \beta + \alpha^{2^k} \beta^{2^k})x^{2^k}) + \text{Tr}(\alpha \beta^{2^k+1}). \tag{6.1}
\end{aligned}$$

Observe that $D_\beta F_\alpha$ is constant if and only if, in Equation (6.1), we have

$$\text{Tr}((\alpha \beta + \alpha^{2^k} \beta^{2^k})x^{2^k}) = 0.$$

This happens if and only if

$$\alpha \beta + \alpha^{2^k} \beta^{2^k} = \alpha \beta (1 + \alpha^{2^k-1} \beta^{2^{2k}-1}) = 0.$$

So either $\beta = 0$ or

$$\alpha^{2^k-1} \beta^{2^{2k}-1} = (\alpha \beta^\ell)^{2^k-1} = 1, \tag{6.2}$$

with $\ell = \frac{2^{2k}-1}{2^k-1} = 2^k + 1$. Suppose that ζ is a primitive element in \mathbb{F}_{2^n} . Then we can write $\alpha = \zeta^r$ and $\beta = \zeta^t$, for some integers r and t . So it follows that Equation (6.2) becomes $\zeta^{(r+t\ell)(2^k-1)} = 1$ which implies that

$$(r + t\ell)(2^k - 1) = r(2^k - 1) + t(2^{2k} - 1) = c(2^n - 1),$$

for some integer c . Thus, we have

$$r = \frac{c(2^n-1)}{2^k-1} - \frac{t(2^{2k}-1)}{2^k-1} = \frac{c(2^n-1)}{2^k-1} - t(2^k + 1) = e \left(\frac{c(2^n-1)}{e(2^k-1)} - \frac{t(2^k+1)}{e} \right).$$

Recall that $e = (2^n - 1, 2^k + 1)$. So all α 's which satisfy $(\alpha \beta^\ell)^{2^k-1} = 1$ must be those which satisfy $\alpha^{(2^n-1)/e} = 1$. These are elements whose orders are divisors of $(2^n - 1)/e$. It implies that $\alpha \in S$. Including $\alpha = 0$, it follows that F_α has a non-trivial linear space if and only if $\alpha \in \text{Im}(F)$.

- (c) By part (b), we deduce that the number of bent components is $2^n - |\text{Im}(F)|$. Since $|\text{Im}(F)| = 1 + |S| = 1 + (2^n - 1)/e$, then the number of bent components is

$$2^n - |\text{Im}(F)| = \frac{(e-1)(2^n-1)}{e}.$$

- (d) We first determine V_α , for any $\alpha \in \mathbb{F}_{2^n}^*$, and then use Theorem 9 to deduce the Walsh spectrum of F . In part (b), we showed that $V_\alpha = \{0\}$ if $\alpha \notin \text{Im}(F)$ (i.e., F_α is bent) and $|V_\alpha| > 1$ if $\alpha \in \text{Im}(F)$. For any $\alpha \in S = \text{Im}(F) \setminus \{0\}$, we also showed, in part (b), that $D_\beta F_\alpha$ is constant if either β is equal to 0 or satisfies $(\alpha \beta^{2^k+1})^{2^k-1} = 1$. Thus, we have $\beta^{2^{2k}-1} = (\alpha^{-1})^{2^k-1}$. If $\alpha = 1$, then $\beta \in \mathbb{F}_{2^s}^*$, with $s = (2k, n)$ and if $\alpha \neq 1$, then $\beta \in \mu \mathbb{F}_{2^s}^*$, where μ is ℓ -th root of α^{-1} . So it follows that $|V_\alpha| = 2^s$.

Given that $m = (n, k)$, by Lemma 46, we have $e = 1$ if n/m is odd and $e = 2^m + 1$ if n/m is even. If $e = 1$ then, by part (a), F is a permutation which implies that it has no bent components and so we have $|V_\alpha| = 2^s$, for all $\alpha \in \mathbb{F}_{2^n}^*$. This implies that its Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}\}$ (see Theorem 9). If $e = 2^m + 1$, then F contains bent components and as shown above, all the linear spaces of non-bent components have the same order 2^s , implying that the Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$.

□

Corollary 48. *Let $F(x) = x^{2^k+1}$ be a power polynomial in $\mathbb{F}_{2^n}[x]$, with positive integers n and $k \geq 1$ and let $e = (2^n - 1, 2^k + 1)$ and $s = (n, 2k)$. Then F is APN if and only if $e = 3$ and $s = 2$. Equivalently, F is APN if and only if there are exactly $2(2^n - 1)/3$ bent components and the rest semi-bent.*

Proof. By Theorem 47, there are $(2^n - 1)/e$ (non-trivial) non-bent components for F and their linear spaces have the same order 2^s . Since n is even then $s = 2t$, where $t = (k, n/2)$. Thus, by Proposition 38, F is APN if and only if

$$\left(\frac{2^n - 1}{e}\right)(2^s - 1) = 2^n - 1. \quad (6.3)$$

Since Equation (6.3) holds if and only if $e = 2^s - 1$, then we conclude that $(2^s - 1)|(2^k + 1)$. Since $t|s$ then $(2^t - 1)|(2^s - 1)$, implying that $(2^t - 1)|(2^k + 1)$. But also $(2^t - 1)|(2^k - 1)$ (recall that $t|k$), so it implies that we must have $t = 1$ as clearly $2^k - 1$ and $2^k + 1$ are relatively prime. Observe that $t = 1$ implies $s = 2$, so it follows that F is APN if and only if $s = 2$ and $e = 2^s - 1 = 3$. In other words, F is APN if and only if the number of bent components is exactly $2(2^n - 1)/3$ and the other components are semi-bent. □

From Theorem 47, we observe that a quadratic power function has some bent components if $e \geq 3$ and equality gives the lowest number of bent components we can get and also when F is APN. So we state this in the following.

Corollary 49. *If a quadratic power function, in even dimension, has some bent components, then they are at least $2(2^n - 1)/3$.*

Acknowledgement

The results in this paper appear in the first author's PhD thesis supervised by the second author.

References

- [1] Berger, T.-P., Canteaut, A., Charpin, P., Laigle-Chapuy, Y.: On almost perfect non-linear functions over \mathbb{F}_2^n . IEEE Trans. Inf. Theory **52**(9), (2006), 4160-4170.
- [2] Braeken, A., Borissov, Y., Nikova, S., Preneel B.: Classification of cubic $(n - 4)$ -resilient Boolean functions. IEEE Transactions on Information Theory **52**(4), (2006), 1670-1676.

- [3] Budaghyan, L., Helleseht, T., Li, N., Sun B.: Some Results on the Known Classes of Quadratic APN Functions. In: El Hajji, S., Nitaj, A., Souidi, E. (eds) Codes, Cryptology and Information Security, C2SI 2017, vol 10194, pp 3-16. Springer, Cham (2017).
- [4] Calderini, M., Sala, M., Villa I.: A note on APN permutations in even dimension, Finite Fields and Their Applications, **46**, (2017), 1-6.
- [5] Carlet, C.: Vectorial Boolean Functions for Cryptography. In Crama, Y., Peter L. Hammer, P.L. (eds.): *Boolean models and methods in mathematics, computer science and engineering*, vol 2, pp 398-470 Cambridge Univ. Press, Cambridge (2010).
- [6] Carlet, C.: Boolean functions for cryptography and error correcting codes. In Crama, Y. and Hammer, P.L. (Eds.): *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge, U.K.: Cambridge Univ. Press, (2010), pp. 257-397. Available at: <http://www.math.univ-paris13.fr/~carlet/pubs.html>
- [7] Chakrabarty K. and Hayes J.P.: Balanced Boolean functions, *IEEE Proc-Comput. Digit. Tech.*, 145, 1 (1998), 52-62.
- [8] Chee, S., Lee, S., Kim K.: Semi-bent Functions. In: Pieprzyk, J., Safavi-Naini, R. (eds.) Advances in Cryptology-ASIACRYPT'94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, vol 917, pp 107-118. Springer, Wollongong.(1994).
- [9] Cusick TW.: Affine equivalence of cubic homogeneous rotation symmetric functions. Inform Sci 181, (2011), 506-783.
- [10] Cusick, T. W., Cheon, Y.: Counting balanced Boolean functions in n variables with bounded degree, *Exp. Math.*, 16, 1, (2007), 101-105.
- [11] Erickson, M., Vazzana, A.: Introduction to number theory. Chapman & Hall/CRC, 1st edition, 2007.
- [12] Khoo, K., Gong, G.: New Construction for Balanced Boolean Functions with Very High Nonlinearity. *IEICE Trans. Fundamentals*, Vol.E90-A No.1 (2007), 29-35
- [13] MacWilliams, F.-J., Sloane, N.-J.-A.: The Theory of Error-Correcting Codes. Elsevier, New York (1977).
- [14] Nyberg, K.: Perfect non-linear S-boxes. In: *Proceedings of EUROCRYPT'91*, Lecture Notes in Computer Science 547, pp. 378-386, 1992.
- [15] Pott, A., Pasalic, E., Muratović-Ribić, A., Bajrić S.: On the Maximum Number of Bent Components of Vectorial Functions. *IEEE Transactions on Information Theory* **64**(1), (2018), 403-411.
- [16] Mesnager, S., Zhang, F., Tang, C., Zhou, Y.: Further study on the maximum number of bent components of vectorial functions. CoRR, abs/1801.06542, (2018).
- [17] Seberry J., Zhang XM., Zheng Y. Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics. In: Stinson D.R. (Eds) *Advances in Cryptology-CRYPTO 93. CRYPTO'1993*. Lecture Notes in Computer Science, 773, (1994). Springer, Berlin, Heidelberg.
- [18] Wu, C., Feng, D.: Boolean Functions and Their Applications in Cryptography. Springer, New York (2016).

- [19] Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Crypt. 73(27), (2014), 587-600.