A note on APN permutations in even dimension

M. Calderini[a], M. Sala[a], I. Villa[a]

[a]*Department of Mathematics, University of Trento, Via Sommarive 14, 38100 Povo (Trento), Italy*

Abstract

APN permutations in even dimension are vectorial Boolean functions that play a special role in the design of block ciphers. We study their properties, providing some general results and some applications to the low-dimension cases. In particular, we prove that none of their components can be quadratic. For an APN vectorial Boolean function (in even dimension) with all cubic components we prove the existence of a component having a large number of balanced derivatives. Using these restrictions, we obtain the first theoretical proof of the non-existence of APN permutations in dimension 4. Moreover, we derive some contraints on APN permutations in dimension 6.

Keywords: Permutation, Boolean functions, Almost Perfect Nonlinear, Partially bent.
MSC: 94A60, 06E30, 20B40.

1. Introduction

A block cipher is a cryptographic primitive that allows the encryption/decryption of fixed-length messages once a secret key has been shared (called the *session key*). Given a fixed key, a block cipher can be viewed as a permutation on the message space. For its performance, a block cipher is designed as the composition of many efficient transformations, called *rounds*. In any round, a *round key* is derived from the session key and acts on the message space, sometimes on the whole space (as in translation-based ciphers [10], such as the AES [14] or the SERPENT [4]), sometimes on portions thereof (as in Feistel ciphers [17]). The action of a round key is traditionally a translation, that is, any (portion of the) message is viewed as a binary vector and is summed with the round key (or XORed, in computer science language). These traditional ciphers are the most common and include some notable Feistel ciphers, such as DES [18], Camellia [1] and Kasumi [16], and all translation-based ciphers, but some alternative actions of the round keys can be found even in block ciphers which have been used in practice, such as IDEA [21], SAFER [25] and GOST [15]. Efficiency reasons explain why in traditional ciphers all-but-one round components are affine maps, being the so-called *S-box* the only exception, and the latter is then called the *non-linear component* of the cipher.

Email addresses: marco.calderini@unitn.it (M. Calderini), maxsalacodes@gmail.com (M. Sala), irene1villa@gmail.com (I. Villa)

If also the S-boxes would be affine maps, the block cipher would be trivial to break. Unsurprisingly, the most effective attacks to traditional block ciphers start from the study of their S-boxes and their non-linear behavior, as explained below. In particular, the so-called *differential cryptanalysis* [5] has proved especially effective. The most basic version of this attack successfully applies when two plaintexts with a (known) fixed difference lead after the last-but-one round to outputs whose difference takes a (known) value with a probability significantly higher than the average. To minimize the success probability of this attack, the theory of vectorial Boolean functions ([12]) has identified an ideal property for the involved S-box, that is, to be an Almost Perfect Nonlinear function (or APN for short). Relevant definitions and properties of APN functions can be found in Section 2. It is important to note that the APN functions used in translation-based ciphers have to be bijective, that is, they must be permutations. In the case of the ciphers AES and SERPENT the S-boxes used are not APN. As regards AES, there is no known example of an 8-bit APN permutation, while for SERPENT there does not exist a 4-bit APN permutation.
However, in Feistel ciphers is not necessary that the S-boxes are invertible (not even in DES), although they are in some, like in Kasumi. In Kasumi the S-boxes are APN permutation, as they are defined over an odd dimensional space.

Although much is known for APN permutations in odd dimension, implementative reasons make a case for the use of APN functions in even dimension, especially when the dimension is a power of 2. Unfortunately, little is known at present for these cases and what is known relies heavily on computer checking:

- It is known that there is no APN permutation in dimension 4 (the first non-trivial case), but the proof relies on extensive computations providing no theoretical insight on the reasons behind their non-existence.

- It is known that there is at least one APN permutation with dimension 6, called the Dillon's permutation ([7]). Interestingly, prior to [7] it was conjectured that no APN permutations in even dimension could exist, since nobody could find any example [20].

- It is known that any cubic APN permutation in dimension 6 must be CCZ-equivalent to the Dillon's permutation, which is itself CCZ-equivalent to a quadratic function, but again this proof is of a purely computational nature [22].

- All computationally-found APN permutations in dimension 6 lack a quadratic component, again with no hint to as why [22].

- Very little is known on a putative APN permutation in dimension 8 or higher.

In this paper we present some advances in the theoretical understanding of properties for APN permutations of even dimension. After having provided some notation and preliminaries in Section 2, we claim the following main results:

- in Section 3, any APN permutation must lack a partially-bent component; this implies that it must also lack a quadratic component;

- in Section 4, any cubic APN function (not necessarily a permutation) must have a component with a large number of balanced derivatives; moreover, we classify cubic Boolean functions in dimension 4 according to their number of balanced derivatives;

- in Section 5, we derive two immediate consequences of our previous results; the first relates to dimension 4 and is the first-ever theoretical proof of the non-existence of an APN permutation; the second relates to dimension 6 and is the theoretical explanation of the component degrees for all known APN permutations.

2. Preliminaries

We will denote by $\mathbb{F}_2$ the finite field with two elements. Let $m \geq 1$, in the sequel we consider Boolean function f from $(\mathbb{F}_2)^m$ to $\mathbb{F}_2$ and only vectorial Boolean function F from $(\mathbb{F}_2)^m$ to $(\mathbb{F}_2)^m$. Without loss of generality we will assume $f(0) = 0$ ($F(0) = 0$).
We denote the *derivative* of f in the direction of $a \in (\mathbb{F}_2)^m$ by $D_a f(x) = f(x+a) + f(x)$ and the *image* of f by $\mathrm{Im}(f) = \{f(x) \mid x \in (\mathbb{F}_2)^m\}$ (similarly for vectorial Boolean functions).
Let $\lambda \in (\mathbb{F}_2)^m$, we denote by F_λ the *component* $\sum_{i=1}^{m} \lambda_i f_i$ of F, where $f_1, \ldots, f_m$ are the coordinate functions of F. Note that for a vectorial Boolean function F we have $D_a F_\lambda = (D_a F)_\lambda$.

Let f be a Boolean function, if $\deg(f) = 0,1,2,3$, then f is, respectively, *constant*, *linear*, *quadratic*, *cubic*. Let F be a vectorial Boolean function, we say that F is *quadratic* if $\max_{\lambda \neq 0}\{\deg(F_\lambda)\} = 2$, *cubic* if $\max_{\lambda \neq 0}\{\deg(F_\lambda)\} = 3$. If all non-zero components of F are quadratic then we say that F is a *pure quadratic*. If all non-zero components of F are cubic then we say that F is a *pure cubic*.

Definition 2.1. *Let F be a vectorial Boolean function, for any $a, b \in (\mathbb{F}_2)^m$ we define*

$$\delta_F(a,b) = |\{x \in (\mathbb{F}_2)^m \mid D_a F(x) = b\}|.$$

The differential uniformity *of F is*

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

Those functions with $\delta(F) = 2$ are said Almost Perfect Nonlinear (APN).

We denote by $\mathscr{F}(f)$ the following value related to the Fourier transform of a Boolean function f:

$$\mathscr{F}(f) = \sum_{x \in (\mathbb{F}_2)^m} (-1)^{f(x)} = 2^m - 2\mathrm{w}_H(f),$$

where $\mathrm{w}_H(f)$ is the Hamming weight of f, i.e. the number of x such that $f(x) = 1$. The function is said to be *balanced* if and only if $\mathscr{F}(f) = 0$.

A necessary condition for a vectorial Boolean function F to be APN was provided by Nyberg in [26]. This condition involves the derivatives of the components of F. It was proved by Berger *et al.* [3] that this condition is also sufficient.

Proposition 2.2 ([26, 3])**.** *Let F be a vectorial Boolean function. Then, for any non-zero $a \in (\mathbb{F}_2)^m$*

$$\sum_{\lambda \in (\mathbb{F}_2)^m} \mathscr{F}^2(D_a F_\lambda) \geq 2^{2m+1}.$$

Moreover, F is APN if and only if for all non-zero $a \in (\mathbb{F}_2)^m$

$$\sum_{\lambda \in (\mathbb{F}_2)^m} \mathscr{F}^2(D_a F_\lambda) = 2^{2m+1}.$$

We recall the following non-linearity measures for vectorial Boolean functions, as introduced in [10, 19]:

$$n_i(F) = |\{\lambda \in (\mathbb{F}_2)^m \setminus \{0\} \mid \deg(F_\lambda) = i\}|,$$

$$\hat{n}(F) = \max_{a \in (\mathbb{F}_2)^m \setminus \{0\}} |\{\lambda \in (\mathbb{F}_2)^m \setminus \{0\} \mid \deg(D_a F_\lambda) = 0\}|,$$

$$\overline{\delta}(F) = \max_{a \in (\mathbb{F}_2)^m \setminus \{0\}} \left(\min \left\{ \delta \in \mathbb{N} \mid |\mathrm{Im}(D_a F)| > \frac{2^{m-1}}{\delta} \right\} \right).$$

$\overline{\delta}(F)$ is the *weakly differential uniformity* of F. If $\overline{\delta}(F) = 2$ then F is said *weakly-APN*.
For a vectorial Boolean function we report the following result.

Theorem 2.3 ([10, 19])**.** *Let F be a vectorial Boolean function, then*

1) $\delta(F) \geq \overline{\delta}(F)$,
in particular if F is APN then it is weakly-APN.

2) *If F is weakly-APN, then $\hat{n}(F) \leq 1$,*
in particular F APN implies $\hat{n}(F) \leq 1$.

The following theorem is well-known.

Theorem 2.4 ([13])**.** *Let F be APN, then $n_1(F) = 0$.*

Theorem 2.4 cannot be extended to weakly-APN functions, since from the classification of bijective vectorial Boolean functions for m =4 there is one affine equivalent class of weakly-APN functions with $n_1 = 1$.

Finally we recall some results on quadratic and partially bent Boolean functions.
The following two results can be found in [24] Chapter 15.

Proposition 2.5 ([24])**.** *Every quadratic function is affinely equivalent to:*

- $x_1 x_2 + \cdots + x_{2l-1} x_{2l} + x_{2l+1}$ *(where $l \leq \frac{m-1}{2}$) if it is balanced,*

- $x_1x_2+\cdots+x_{2l-1}x_{2l}$ *(where $l \le m/2$) if it has weight smaller than* 2^{m-1},
- $x_1x_2+\cdots+x_{2l-1}x_{2l}+1$ *(where $l \le m/2$) if it has weight greater than* 2^{m-1}.

Denote by $V(f)=\{a \mid D_a f \text{ is constant}\}$ the set of *linear structures* of a Boolean function f. Observe that $V(f)$ is a vector subspace.

Proposition 2.6 ([24]). *Any quadratic Boolean function f is balanced if and only if its restriction to $V(f)$ is not constant. If it is not balanced, then its weight equals* $2^{m-1} \pm 2^{\frac{m+k}{2}-1}$ *where k is the dimension of $V(f)$.*

Remark 2.7. *The proposition above implies that for any non-balanced quadratic Boolean function we have* $\mathscr{F}(f)=\pm 2^{\frac{m+k}{2}}$.

We report now the definition of partially bent function, which was introduced in [11].

Definition 2.8. *A Boolean function f is* partially bent *if there exists a linear subspace $\overline{V}(f)$ of $(\mathbb{F}_2)^m$ such that the restriction of f to $\overline{V}(f)$ is affine and the restriction of f to any complementary subspace U of $\overline{V}(f)$, $\overline{V}(f)\oplus U=(\mathbb{F}_2)^m$, is bent.*

Remark 2.9. *If f is partially bent, then f can be represented as a direct sum of the restricted functions, i.e., $f(y+z)=f(y)+f(z)$, for all $z\in\overline{V}(f)$ and $y\in U$. Moreover we can deduce from Proposition 2.5 that any quadratic function is partially bent.*

Remark 2.10. *If f is partially bent, the space $\overline{V}(f)$ is formed by the linear structures of f, which is $\overline{V}(f)=V(f)$. Indeed, let $a\in\overline{V}(f)\setminus\{0\}$ and $x\in(\mathbb{F}_2)^m$. Then $x=y+z$ for some $z\in\overline{V}(f)$ and $y\in U$. So, from Remark 2.9, we have*

$$D_af(x)=f(x+a)+f(x)=f(y+z+a)+f(y+z)=f(y)+f(z)+f(a)+f(y)+f(z)=f(a),$$

that implies $\overline{V}(f)\subseteq V(f)$.
Now, suppose that there exists $a\in V(f)\setminus\overline{V}(f)$. Without loss of generality $a\in U$. By definition $f_{|U}$ (the restriction of f to U) is bent. This implies $D_af_{|U}$ is balanced, but this is not possible as $D_af(x)=f(a)$ for all $x\in(\mathbb{F}_2)^m$. Then $\overline{V}(f)=V(f)$.
Moreover, since bent functions exist only in even dimension, $\dim(U)=m-\dim(V(f))$ *is even. Which implies that if m is even, the dimension of $V(f)$ is even. In particular $V(f)=\{0\}$ if and only if f is bent. This implies that if f is balanced and m is even then* $\dim(V(f))\geq 2$.

3. Properties of APN permutations

Our first result holds for any dimension and comes directly from the facts in previous section.

Theorem 3.1. *Let $m\geq 3$ and let F be an APN permutation of dimension m. There are only two cases:*

- $\hat{n}(F) = 0$, *which implies that for any* $\lambda \neq 0$ F_λ *is not partially bent and so* $n_1(F) = n_2(F) = 0$*;*
- $\hat{n}(F) = 1$, *for which it is possible that there is a* $\lambda \neq 0$ *such that* F_λ *is partially bent, and so* $n_1(F) = 0$ *and* $n_2(F) \geq 0$*.*

Proof. From Theorem 2.3 and Theorem 2.4 we have that $\hat{n}(F) \leq 1$ and $n_1(F) = 0$. If $\hat{n}(F) = 0$ then any non-zero component F_λ has $V(F_\lambda) = \{0\}$. This implies that if F_λ is partially bent, then F_λ is bent, see Remark 2.10, but it is not possible as F is a permutation.

If $\hat{n}(F) = 1$ then there exists F_λ with $V(F_\lambda) \neq \{0\}$, and it could be partially bent (in particular it could be quadratic). □

The condition on bijection for F is essential, otherwise the case $\hat{n} = 0$ may have bent components. As there are examples of quadratic APN permutations for any odd dimension, the previous theorem cannot be improved.

The case of an APN permutation F with m even is quite different and we will restrict to it from now on.

As shown in [27] there is no APN quadratic permutation over $(\mathbb{F}_2)^m$ for m even, that is $n_2(F) \leq 2^{m-1} - 1$. This result was extended by Nyberg [26] showing that an APN permutation F cannot have all components partially bent (for m even).

Moreover, in [2] the authors give some properties on the the components of a weakly-APN permutation in even dimension. In particular they study partially-bent and quadratic components, obtaining that the number of the quadratic components of a weakly-APN permutation can be at most $2^{m-2} - 1$ ([2] Proposition 4). As an APN function is weakly-APN, we have $n_2(F) \leq 2^{m-2} - 1$.

In the remainder of this section we will prove that *no component* of F is partially bent (quadratic).

We start with the following proposition.

Proposition 3.2. *Let F be an APN permutation over $(\mathbb{F}_2)^m$, with m even. If there are $a, \lambda \in (\mathbb{F}_2)^m \setminus \{0\}$ such that $D_a F_\lambda$ is constant, then $D_a F_\lambda = 1$.*

Proof. Suppose that there exist non-zero $a, \lambda \in (\mathbb{F}_2)^m$ such that $D_a F_\lambda = 0$. Without loss of generality we can suppose that $F_\lambda = f_1$, thus we have

$$\mathrm{Im}(D_a F) = \{(0, y_2, \ldots, y_m) \mid y_i \in \mathbb{F}_2\}.$$

Being F APN we have $|\mathrm{Im}(D_a F)| = 2^{m-1}$, so 0 has to lie in $\mathrm{Im}(D_a F)$, contradicting the fact that F is a permutation. □

Theorem 3.3. *Let F be an APN permutation over $(\mathbb{F}_2)^m$, with m even, then no non-zero component of F is partially bent.*

Proof. Suppose that F_λ is partially bent, for some $\lambda \in (\mathbb{F}_2)^m \setminus \{0\}$. From Remark 2.10 and being F a permutation, we have that the space of the linear structure of F_λ has at least dimension 2. Let a_1 and a_2 be two distinct non-zero vectors of $V(F_\lambda)$. Let $x \in (\mathbb{F}_2)^m$, from Proposition 3.2 and Remark

2.10 we have $D_{a_1}F_\lambda(x) = F_\lambda(a_1) = 1$ and $D_{a_2}F_\lambda(x) = F_\lambda(a_2) = 1$. This implies $a_1 + a_2 \in V(F_\lambda)$, $a_1 + a_2 \neq 0$ and

$$D_{a_1+a_2}F_\lambda(x) = F_\lambda(a_1 + a_2) = F_\lambda(a_1) + F_\lambda(a_2) = 0 \quad \text{(for all } x \in (\mathbb{F}_2)^m\text{)}.$$

But $D_{a_1+a_2}F_\lambda = 0$ contradicts Proposition 3.2. □

Corollary 3.4. *Let F be an APN permutation over $(\mathbb{F}_2)^m$, for m even. Then $n_2(F) = 0$.*

Remark 3.5. *As observed by C. Carlet and L. Budaghyan in a private communication, Theorem 3.3 cannot be extended to the non-existence of plateaued components, since Dillon's APN permutation does have some.*

Remark 3.6. *Let f be a bent Boolean function and ℓ be a linear Boolean function. Then $f + \ell$ is bent. Indeed, let $a \in (\mathbb{F}_2)^m \setminus \{0\}$. Thus we have*

$$D_a(f + \ell)(x) = D_a f(x) + D_a \ell(x) = D_a f(x) + c,$$

where $c \in \mathbb{F}_2$. As $D_a f$ is balanced, then $D_a(f + \ell)$ is balanced. This implies that $f + \ell$ is bent. Moreover, we immediately have that if f is partially bent and ℓ is a linear Boolean function, then $f + \ell$ is partially bent.

We recall that two functions F and F' are called EA-equivalent if there are an affine mapping L and function G affinely equivalent to F, such that $F' = G + L$.
From Remark 3.6 we obtain the following.

Proposition 3.7. *Let F be a vectorial Boolean function with partially bent components. If F' is EA-equivalent to F, then F' has partially bent components.*

Proof. $F' = G + L$ for some G affine equivalent to F and L affine map of $(\mathbb{F}_2)^m$. Thus the component λ of F' is $F'_\lambda = G_\lambda + L_\lambda$ for all $\lambda \in (\mathbb{F}_2)^m$. As F has a partially bent component, then also G has a partially bent component (it is affine equivalent to F). Let G_λ be partially bent, then from Remark 3.6 we have that $G_\lambda + L_\lambda$ is partially bent. □

For m even and $\gcd(m, i) = 1$ the following two families of APN functions were constructed in [9], [8]

$$x^{2^i+1} + (x^{2^i} + x + 1)\mathrm{Tr}(x^{2^i+1}),$$
$$x^3 + \mathrm{Tr}(x^9) + (x^2 + x + 1)\mathrm{Tr}(x^3),$$

where $\mathrm{Tr}(x)$ denotes the trace function from $\mathbb{F}_{2^m}$ into $\mathbb{F}_2$. It was proven in [23] that the first one is not EA-equivalent to permutations and, at the best of our knowledge, a similar result is missing for the second one. However, both functions have quadratic components which implies, according to Corollary 3.4 and Proposition 3.7, that both of them are not EA-equivalent to permutations.
More generally, since EA-equivalence preserves partially bent components, then the following holds:

Corollary 3.8. *Let m be even and F be an APN function over $(\mathbb{F}_2)^m$ having a partially bent (quadratic) component. Then F is EA-inequivalent to any permutation.*

4. On cubics in even dimension

In this section we are interested in cubic Boolean functions and cubic vectorial Boolean functions.

Given a Boolean function f, we are interested in counting the number of its derivatives that are balanced, that is the cardinality of $\Gamma(f) = \{a \in (\mathbb{F}_2)^m \mid D_a f \text{ is balanced}\}$. Observe that if f is quadratic, then its derivatives can be either linear functions (which are balanced) or constant functions, which are non-balanced. For a cubic function, the situation is less obvious. The following theorem presents an estimate of Γ for a component of a pure-cubic APN function.

Theorem 4.1. *Let F be a cubic APN vectorial Boolean function over $(\mathbb{F}_2)^m$, with m even. Then there exists $\lambda \neq 0$ such that*

$$|\Gamma(F_\lambda)| \geq 2^m - 2^{m-2} - 1.$$

Proof. Consider any $a \in \mathbb{F}^m$, $a \neq 0$. For any component F_λ we are interested in the following integers: $\deg(D_aF_\lambda)$, where clearly $0 \leq \deg(D_aF_\lambda) \leq 2$, $\mathscr{F}(D_aF_\lambda)$, and $k_\lambda = \dim(V(D_aF_\lambda))$. We note that $k_\lambda \geq 2$, because $D_a(D_aF_\lambda) = 0$ and so D_aF_λ cannot be bent (see Remark 2.10). We can have the following cases:

1) $\deg(D_aF_\lambda) = 0$, then we have $D_aF_\lambda = 0, 1$ and so $\mathscr{F}(D_aF_\lambda) = \pm 2^m = \pm 2^{\frac{m+m}{2}}$.

2) $\deg(D_aF_\lambda) = 1$, then D_aF_λ is balanced and so $\mathscr{F}(D_aF_\lambda) = 0$.

3) $\deg(D_aF_\lambda) = 2$ and D_aF_λ is balanced, so $\mathscr{F}(D_aF_\lambda) = 0$.

4) $\deg(D_aF_\lambda) = 2$ and D_aF_λ is not balanced, so from Remark 2.7 we have $\mathscr{F}(D_aF_\lambda) = \pm 2^{\frac{m+k_\lambda}{2}}$.

Let $s_\lambda = \frac{m+k_\lambda}{2}$, noting that $k_\lambda \geq 2$, then $\frac{m}{2} + 1 \leq s_\lambda \leq m$. Observe that in case 1 and 4 we have $\mathscr{F}^2(D_aF_\lambda) = 2^{2s_\lambda}$, while in case 2 and 3 we have $\mathscr{F}^2(D_aF_\lambda) = 0$. Since $a \neq 0$ and $\mathscr{F}^2(D_aF_0) = 2^{2m}$, from Proposition 2.2, we have

$$\sum_{\lambda \neq 0} \mathscr{F}^2(D_aF_\lambda) = 2^{2m}.$$

We will now consider functions D_aF_λ, with λ and a varying freely in $(\mathbb{F}_2)^m \setminus \{0\}$.

Now let $\Delta_a = \{\lambda \neq 0 \mid \mathscr{F}(D_aF_\lambda) \neq 0\}$ and $\overline{\Delta_a} = \{\lambda \neq 0 \mid \mathscr{F}(D_aF_\lambda) = 0\}$, i.e. $\Delta_a \cup \overline{\Delta_a} = (\mathbb{F}_2)^m \setminus \{0\}$. Hence in our case we have

$$2^{2m} = \sum_{\lambda \neq 0} \mathscr{F}^2(D_aF_\lambda) = \sum_{\lambda \in \Delta_a} \mathscr{F}^2(D_aF_\lambda) = \sum_{\lambda \in \Delta_a} 2^{2s_\lambda}.$$

Since $s_\lambda \geq \frac{m}{2} + 1$, we have

$$2^{2m} \geq \sum_{\lambda \in \Delta_a} 2^{2(\frac{m}{2}+1)} = 2^{m+2}|\Delta_a|, \quad \text{and so } |\Delta_a| \leq 2^{m-2}.$$

We have thus proved that

$$|\Delta_a| \leq 2^{m-2} \text{ and } |\overline{\Delta_a}| \geq 2^m - 2^{m-2} - 1.$$

Note that $\Gamma(F_\lambda) = \{a \mid \mathscr{F}(D_a F_\lambda) = 0\}$. Assuming now that for all $\lambda \neq 0$ we have $|\Gamma(F_\lambda)| < 2^m - 2^{m-2} - 1$, we would have

$$(2^m - 1) \cdot (2^m - 2^{m-2} - 1) \leq \sum_{a \neq 0} |\overline{\Delta_a}| = \sum_{\lambda \neq 0} |\Gamma(F_\lambda|) < (2^m - 1) \cdot (2^m - 2^{m-2} - 1),$$

and this is impossible. Thus there exists $\lambda \neq 0$ such that $|\Gamma(F_\lambda)| \geq 2^m - 2^{m-2} - 1$. □

Observe that the previous theorem holds, when m is even, for any cubic APN function F such that $F : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$, even if F is not a permutation (and even if F is a pure-cubic).

It turns out that $\Gamma(f)$ suffers a strong constraint when we specialize to the case $m = 4$, as next theorem shows.

Theorem 4.2. *Let $f : (\mathbb{F}_2)^4 \to \mathbb{F}_2$ be a cubic Boolean function. Then*

$$|\Gamma(f)| = |\{a \mid \mathscr{F}(D_a f) = 0\}| < 11.$$

Proof. Suppose that $|\Gamma(f)| \geq 11$. Since $|\Gamma(f)| > 8$, $\Gamma(f)$ contains 4 linearly independent vectors. Without loss of generality we can assume e_1, e_2, e_3, e_4 (the standard basis) belong to $\Gamma(f)$. We will implicitly use in the remainder of this proof that $D_{e_1}(f)$,..., $D_{e_4}(f)$ are balanced for our f.

The Boolean function f can be written as $f = \mathrm{supp}_0(f) + \mathrm{supp}_1(f) + \mathrm{supp}_2(f) + \mathrm{supp}_3(f)$, where $\mathrm{supp}_i(f)$ contains only terms of degree i for $i = 1, 2, 3$. Note that $\mathrm{supp}_0(f) + \mathrm{supp}_1(f)$, that is, the linear part does not influence the balancedness of any derivative of f, and so we can consider $f = \mathrm{supp}_2(f) + \mathrm{supp}_3(f)$. We will find a contradiction depending on the following cases, which are characterized by the weight of $\mathrm{supp}_3(f)$, i.e. $|\mathrm{supp}_3(f)|$, which can only vary in $1 \leq |\mathrm{supp}_3(f)| \leq 4$ since $m = 4$ and $\deg(f) = 3$.
In the following cases we will write Boolean functions as polynomials that may contain squares, using the standard notation of viewing them implicitly in the quotient ring $\mathbb{F}_2[x_1, x_2, x_3, x_4]/\langle x_1^2 - x_1, \ldots, x_4^2 - x_4 \rangle$. Also, since we will apply affine transformations we will sometimes obtain a Boolean function g such that $g(0) = 1$. However, we will write that g is *equivalent* to g' if g is affine equivalent to either g' or $g' + 1$. This equivalence notion preserves balancedness and it is appropriate for our goals.

i) $|\mathrm{supp}_3(f)| = 4$

$$f(x) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + \sum_{i<j} \beta_{ij} x_i x_j.$$

We have already assumed that the standard basis belongs to $\Gamma(f)$, so $\Gamma(f)$ contains all vectors of weight 1. There are other 7 vectors in $\Gamma(f)$ and in $(\mathbb{F}_2)^4$ there are five vectors of weight 3 or 4. Thus in $\Gamma(f)$ there is at least a vector of weight 2. A permutation of the coordinates will not change our situation, that is, Γ will still contain the vectors with the prescribed weights, and so without loss of generality we can assume that $(1100) \in \Gamma$. If we derive f in the direction of e_1 we obtain

$$\begin{aligned} D_{e_1} f(x) =& x_2x_3 + x_2x_4 + x_3x_4 + \sum_{j \neq 1} \beta_{1j}x_j \\ =& (x_2 + x_3 + \beta_{14})(x_3 + x_4 + \beta_{12}) + (1 + \beta_{12} + \beta_{13} + \beta_{14})x_3 + \beta_{12}\beta_{14}, \end{aligned}$$

that is equivalent to $x_1x_2 + (1 + \beta_{12} + \beta_{13} + \beta_{14})x_3$. From Proposition 2.5 we have that $D_{e_1} f$ is balanced if and only if $\beta_{12} + \beta_{13} + \beta_{14} = 0$.

Similarly from the derivative $D_{e_2} f$ we get that $\beta_{12} + \beta_{23} + \beta_{24} = 0$.
Now, if we derive the function in the direction of $a = (1100)$ we obtain

$$\begin{aligned} D_a f(x) =& x_1x_3 + x_2x_3 + x_3 + x_1x_4 + x_2x_4 + x_4 + x_3x_4 + x_3x_4 \\ &+ \beta_{12}(x_1 + x_2 + 1) + \beta_{13}x_3 + \beta_{14}x_4 + \beta_{23}x_3 + \beta_{24}x_4 \\ =& (x_1 + x_2 + 1 + \beta_{13} + \beta_{23})(x_3 + x_4 + \beta_{12}) \\ &+ x_4(\beta_{13} + \beta_{23} + \beta_{14} + \beta_{24}) + \beta_{12}(\beta_{13} + \beta_{23}), \end{aligned}$$

which is equivalent to $x_1x_2 + (\beta_{13} + \beta_{23} + \beta_{14} + \beta_{24})x_3$. The obtained Boolean function is balanced if and only if $\beta_{13} + \beta_{23} + \beta_{14} + \beta_{24} = 1$, which contradicts the previous conditions, since

$$0 + 0 = \beta_{12} + \beta_{13} + \beta_{14} + \beta_{12} + \beta_{23} + \beta_{24} = \beta_{13} + \beta_{23} + \beta_{14} + \beta_{24}.$$

ii) $|\mathrm{supp}_3(f)| = 3$

Without loss of generality we can consider

$$f(x) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + \sum_{i<j} \beta_{ij}x_ix_j.$$

Considering the derivative in the direction of e_2 we have

$$\begin{aligned} D_{e_2} f(x) =& x_1x_3 + x_1x_4 + \sum_{j \neq 2} \beta_{2j}x_j \\ =& (x_1 + \beta_{23})(x_3 + x_4 + \beta_{12}) + (\beta_{23} + \beta_{24})x_4 + \beta_{12}\beta_{23}. \end{aligned}$$

As before, from Proposition 2.5 we have $\beta_{23} + \beta_{24} = 1$. Similarly, we have $\beta_{23} + \beta_{34} = 1$ from $D_{e_3} f$, and $\beta_{24} + \beta_{34} = 1$ from $D_{e_4} f$. The three conditions on β_{ij}'s cannot simultaneously hold.

iii) $|\mathrm{supp}_3(f)| = 2$

In this case we can assume without loss of generality that f is given by

$$f(x) = x_1x_2x_3 + x_1x_2x_4 + \sum_{i<j} \beta_{ij}x_ix_j.$$

We will consider first its derivatives in the direction of the e_1, e_2, e_3 and, as usual, we will determine the conditions that preserve the linear part (Proposition 2.5 first case).

$$\begin{aligned}
D_{e_1} f(x) =& x_2x_3 + x_2x_4 + \sum_{j\neq 1} \beta_{1j}x_j \\
=& (x_2 + \beta_{13})(x_3 + x_4 + \beta_{12}) + (\beta_{13} + \beta_{14})x_4 + \beta_{12}\beta_{13},
\end{aligned}$$

then $\beta_{13} + \beta_{14} = 1$.
Similarly we have $\beta_{23} + \beta_{24} = 1$ from $D_{e_2} f$.
Deriving f in the direction of e_3 we have

$$\begin{aligned}
D_{e_3} f(x) =& x_1x_2 + \sum_{j} \beta_{3j}x_j \\
=& (x_1 + \beta_{23})(x_2 + \beta_{13}) + \beta_{34}x_4 + \beta_{13}\beta_{23}.
\end{aligned}$$

Then $\beta_{34} = 1$.

The collected conditions are

$$\beta_{14} = \beta_{13} + 1,\, \beta_{24} = \beta_{23} + 1,\, \beta_{34} = 1.$$

Let $a \in \mathbb{F}^m$, $a = (\gamma, \gamma+1, \xi, \xi+1)$ with $\gamma, \xi \in \mathbb{F}_2$. Consider the derivative in the direction of a.

$$\begin{aligned}
D_a f(x) =& (\xi x_1x_2 + (\gamma+1)x_1x_3 + (\gamma+1)\xi x_1 + \gamma x_2x_3 + \gamma\xi x_2 + \gamma(\gamma+1)x_3 + \gamma(\gamma+1)\xi) \\
& + ((\xi+1)x_1x_2 + (\gamma+1)x_1x_4 + (\gamma+1)(\xi+1)x_1 \\
& + \gamma x_2x_4 + \gamma(\xi+1)x_2 + \gamma(\gamma+1)x_4 + \gamma(\gamma+1)(\xi+1)) \\
& + \beta_{12}((\gamma+1)x_1 + \gamma x_2 + \gamma(\gamma+1)) + \beta_{13}(\xi x_1 + \gamma x_3 + \gamma\xi) \\
& + (1+\beta_{13})((\xi+1)x_1 + \gamma x_4 + \gamma(\xi+1)) + \beta_{23}(\xi x_2 + (\gamma+1)x_3 + (\gamma+1)\xi) \\
& + (1+\beta_{23})((\xi+1)x_2 + (\gamma+1)x_4 + (\gamma+1)(\xi+1)) \\
& + ((\xi+1)x_3 + \xi x_4 + \xi(\xi+1)) \\
=& ((\gamma+1)x_1 + \gamma x_2 + \gamma\beta_{13} + (\gamma+1)\beta_{23} + \xi + 1)\cdot \\
& \cdot (x_3 + x_4 + \gamma x_1 + (\gamma+1)x_2 + \xi + \beta_{12} + (\gamma+1)\beta_{13} + \gamma\beta_{23}) + (constants)
\end{aligned}$$

For any values of (γ, ξ), $D_a f$ is equivalent to x_1x_2, which is not balanced. Then there are 4 distinct vectors such that the derivatives are not balanced.

Now consider the vector $\bar{a} = (1100)$. This is different from the four vectors above and the derivative in a is

$$\begin{aligned} D_{\bar{a}} f(x) =& x_1x_3 + x_2x_3 + x_3 + x_1x_4 + x_2x_4 + x_4 + \beta_{12}(x_1 + x_2 + 1) \\ & + \beta_{13}x_3 + (1+\beta_{13})x_4 + \beta_{23}x_3 + (1+\beta_{23})x_4 \\ =& (x_3 + x_4 + \beta_{12})(x_1 + x_2 + 1 + \beta_{13} + \beta_{23}) + \beta_{12}(\beta_{13} + \beta_{23}). \end{aligned}$$

The last expression is equivalent to x_1x_2, which is not balanced. So we have found five non-balanced derivates and therefore $|\Gamma(f)| < 11$.

iv) $|\mathrm{supp}_3(f)| = 1$

In this last case we can assume

$$f(x) = x_1x_2x_3 + \sum_{i<j} \beta_{ij}x_ix_j.$$

From the derivative in e_1 we have

$$\begin{aligned} D_{e_1} f(x) =& x_2x_3 + \sum_{j\neq 1} \beta_{1j}x_j \\ =& (x_2 + \beta_{13})(x_3 + \beta_{12}) + \beta_{14}x_4 + \beta_{12}\beta_{13}, \end{aligned}$$

so $\beta_{14} = 1$.
We can obtain similarly $\beta_{24} = 1$ and $\beta_{34} = 1$ from the derivatives $D_{e_2} f$ and $D_{e_3} f$ respectively.
As in the previous case we want to find more than four (not-null) elements that give unbalanced derivatives.
Let us consider $a \neq 0$, $a = (a_1, a_2, a_3, a_4)$, with $a_1 + a_2 + a_3 = 0$ and $(a_1, a_2, a_3) \neq (0,0,0)$. Since in f the first three variables take the same role, we can assume without loss of generality that $a_3 = 0$, so $a_1 = a_2 = 1$. Now let us consider the derivative of f with respect to $a = (1\ 1\ 0\ a_4)$.

$$\begin{aligned} D_a f(x) =& x_1x_3 + x_2x_3 + x_3 + \beta_{12}(x_1 + x_2 + 1) \\ & + x_3(\beta_{13} + \beta_{23} + a_4) + (x_4 + a_4x_1) + (x_4 + a_4x_2) = \\ =& (x_3 + \beta_{12} + a_4) \cdot (x_1 + x_2 + 1 + \beta_{13} + \beta_{23} + a_4) \\ & + (\beta_{12} + a_4)(1 + \beta_{13} + \beta_{23} + a_4). \end{aligned}$$

The obtained function is equivalent to x_1x_2, so it is not balanced. Therefore there are at least 6 elements for which $D_a f$ is not balanced and so $\Gamma(f)$<10.

The analysis of the previous cases has shown the following:

- if $\mathrm{supp}_3(f) = 4$ then $\Gamma(f) < 10$,

- if $\text{supp}_3(f) = 3$ then $\Gamma(f) < 10$,
- if $\text{supp}_3(f) = 2$ then $\Gamma(f) < 11$,
- if $\text{supp}_3(f) = 1$ then $\Gamma(f) < 10$.

We can conclude that for any f we certainly have $\Gamma < 11$. □

5. Consequences in low dimensions

In this section we discuss some consequences of our previous results.

m=4

There are two immediate non-existence results for the case $m = 4$. The first holds also for non-bijective functions.

Theorem 5.1. *Let $m = 4$ and F a pure cubic vectorial Boolean function. Then F is not APN.*

Proof. Suppose that F is APN. Then from Theorem 4.1 there exists a component F_λ such that $|\Gamma(F_\lambda)| \geq 11$. But Theorem 4.2 shows $\Gamma(F_\lambda) < 11$, since F_λ is cubic. □

As consequence we obtain our second result, which is the non-existence of APN permutations for $m = 4$.

Corollary 5.2. *There is no APN permutation for $m = 4$.*

Proof. Since F is invertible, then F is at most cubic. Since F is an APN, then $n_1(F) = 0$ (Theorem 2.4). Since F is an invertible APN, then $n_2(F) = 0$ (Corollary 3.4). Therefore, F is a pure cubic. But this contradicts Theorem 5.1. □

Observe that Theorem 5.1 and our previous result do no prevent the existence of quadratic or cubic APN's, which are known to exist (but of course they are not bijective). Indeed, in [6] they show (computationally) that there are exactly two APN functions in dimension 4 (up to EA-equivalence), one quadratic and one cubic. Theorem 5.1 shows that the latter, being a cubic APN, cannot be a pure cubic.

m=6

The first consequence of our previous result to dimension 6 is the following corollary.

Corollary 5.3. *Let F be an APN permutations in dimension* 6*, the the degrees of its non-zero components can be either* 3,4 *or* 5*.*

Proof. An invertible APN cannot have any quadratic component (Corollary 3.4), any linear component (Theorem 2.4) and any degree-6 component (because it's invertible). □

This is in accordance with experimental results by Langevin [22] and explains also because the degree of the components of Dillon's permutation are only 3 and 4 (although in principle there could be a component of degree 5).

Theorem 5.1 cannot be trivially extended to dimension 6, since pure cubic APN functions exist. Still, Theorem 4.1 applies and therefore any cubic APN must have a component with a large number of balanced derivatives, that is, with $\Gamma(F_\lambda) \geq 47$. However, for $m = 6$ this arises no contradiction, since there are cubics with $\Gamma(f) \geq 47$ and a suitable extension of Theorem 4.2 to the case $m = 6$ is missing.

We conclude this paper with noting that from the exam of the computational results presented in [22], we can derive a weaker version of Theorem 5.1 for $m = 6$.

Theorem 5.4. *Let $m = 6$ and F an invertible pure cubic. Then F is not APN.*

Acknowledgement

We would like to thank C. Carlet for useful discussions, and L. Budaghyan for nice observations and for pointing out the result of Corollary 3.8 for the case of quadratic components.

References

[1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms design and analysis. In *Selected Areas in Cryptography*, pages 39–56. Springer, 2001.

[2] R. Aragona, M. Calderini, D. Maccauro, and M. Sala. On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–14, 2016.

[3] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On Almost Perfect Nonlinear Functions Over $\mathbb{F}_2^n$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[4] E. Biham, R. Anderson, and L. Knudsen. SERPENT: A new block cipher proposal. In *Fast Software Encryption*, pages 222–238. Springer, 1998.

[5] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

[6] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49(1-3):273–288, 2008.

[7] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN permutation in dimension six. *Finite Fields: theory and applications*, 518:33–42, 2010.

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

[9] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[10] A. Caranti, F. Dalla Volta, and M. Sala. On some block ciphers and imprimitive groups. *Applicable Algebra in Engineering, Communication and Computing*, 20(5-6):229–350, 2009.

[11] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3(2):135–145, 1993.

[12] C. Carlet. Boolean functions for cryptography and error correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter 8, pages 257–397. Cambridge Univ. Press, 2010.

[13] C. Carlet. Vectorial boolean functions for cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter 9, pages 398–469. Cambridge Univ. Press, 2010.

[14] J. Daemen and V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[15] V. Dolmatov. GOST 28147-89: Encryption, decryption, and message authentication code (MAC) algorithms. Technical report, 2010. `http://tools.ietf.org/html/rfc5830`.

[16] ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms - Document 2: KASUMI Specification. Technical Report 3GPP TS 35.202 V10.0.0 (Release 10), 2011.

[17] H. Feistel, W. A. Notz, and J. L. Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(11):1545–1554, 1975.

[18] PUB FIPS. 46-3: Data Encryption Standard (DES). *National Institute of Standards and Technology*, pages 1–22, 1999. `http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf`.

[19] C. Fontanari, V. Pulice, A. Rimoldi, and M. Sala. On weakly APN functions and 4-bit S-Boxes. *Finite Fields and Their Applications*, 18(3):522–528, 2012.

[20] X.-D. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete Appl. Math.*, 154(2):313–325, 2006.

[21] X. Lai, J. L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. In *Advances in Cryptology-EUROCRYPT'91*, pages 17–38. 1991.

[22] P. Langevin, Z. Saygi, and E. Saygi. Classification of APN cubics in dimension 6 over GF(2). `http://langevin.univ-tln.fr/project/apn-6/apn-6.html`.

[23] Y. Li and M. Wang. The nonexistence of permutations EA-equivalent to certain AB functions. *IEEE Transactions on Information Theory*, 59(1):672–679, 2013.

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

[25] J. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. In *Fast Software Encryption*, pages 1–17. Springer, 1994.

[26] K. Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *Fast Software Encryption*, pages 111–130. Springer, 1995.

[27] J. Seberry, X.-M. Zhang, and Y. Zheng. Pitfalls in designing substitution boxes. In *Advances in Cryptology-CRYPTO'94*, pages 383–396. Springer, 1994.