Revisiting some results on APN and algebraic immune functions

Claude Carlet,
Universities of Bergen, Norway and Paris 8, France.

E-mail: claude.carlet@gmail.com

Abstract

We push a little further the study of two characterizations of almost perfect nonlinear (APN) functions introduced in our recent monograph. We state open problems about them, and we revisit in their perspective a well-known result from Dobbertin on APN exponents. This leads us to new results about APN power functions and more general APN polynomials with coefficients in a subfield $\mathbb{F}_{2^k}$, which ease the research of such functions and of differentially uniform functions, and simplifies the related proofs by avoiding tedious calculations. In a second part, we give slightly simpler proofs than in the same monograph, of two known results on Boolean functions, one of which deserves to be better known but needed clarification, and the other needed correction.

1 Introduction

New characterizations of almost perfect nonlinear (APN) functions have been recently given in the book [7], which will be a common reference for the present paper. We state related open problems and we make more explicit the condition involved in one of the problems. We revisit the Dobbertin result saying that a power function $F(x) = x^d$ over $\mathbb{F}_{2^n}$ has necessarily an exponent d such that $\gcd(d, 2^n - 1)$ equals 1 if n is odd and 3 if n is even. Considering this result with the viewpoint of the second characterization allows us to guess a new property: if an APN polynomial function $F(x)$ over $\mathbb{F}_{2^n}$ has all its coefficients in a subfield $\mathbb{F}_{2^k}$ such that $\frac{n}{k}$ is odd, then for every nonzero $a \in \mathbb{F}_{2^k}$ and every $b \in \mathbb{F}_{2^k}$, the solutions of the equation $F(x)+F(x+a) = b$ all belong to $\mathbb{F}_{2^k}$, if they exist. We shall show that this allows simplifying some proofs dealing with specific APN functions.

We also revisit two other results on Boolean and vectorial functions which are essential in the state-of-the-art on Boolean functions for cryptography too, but need their proofs to be clarified and completed in the case of the first one, and to have some inaccuracies corrected (as well as the statement) in the case

of the second one. Such corrections are given in the recent book [7]; we give here slightly simpler proofs.

2 Preliminaries

For every positive integer n, we call n-variable Boolean function any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We call the set $supp(f) = \{x \in \mathbb{F}_2^n; f(x) = 1\}$ the support of such function f, and the size of this support its Hamming weight, denoted by $w_H(f)$. The Hamming distance between two functions equals the Hamming weight of their sum. Any n-variable Boolean function admits a unique algebraic normal form (ANF): denoting $x = (x_1, \ldots, x_n)$, we have $f(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$, where $a_I \in \mathbb{F}_2$. The global degree of this ANF is called the algebraic degree of f and is denoted by $d_{alg}(f)$. The function d_{alg} satisfies the relation $d_{alg}(fg) \leq d_{alg}(f) + d_{alg}(g)$, where $(fg)(x)$ is defined as equal to $f(x)g(x)$. A function is affine if and only if its algebraic degree is at most 1. The nonlinearity $nl(f)$ of a Boolean function f equals the minimum distance between f and affine functions.

Definition 1 *We call annihilator of an n-variable Boolean function f any n-variable Boolean function g such that $fg = 0$. The algebraic immunity of f equals then the minimum algebraic degree of the nonzero annihilators of f and of the nonzero annihilators of its complement $f + 1$.*

Given another positive integer m, we call (n, m)-function (or vectorial function if we do not specify the numbers n and m of input and output bits), any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. Such functions are also called S-boxes, when they are used as substitution boxes in block ciphers. The ANF of such function is defined the same way as for Boolean functions, with the only difference that $a_I \in \mathbb{F}_2^m$. The algebraic degree of such F equals the maximum algebraic degree of its coordinate functions.

Definition 2 *[15, 21, 16] Let n, m, δ be positive integers. An (n, m)-function F is called* differentially δ-uniform *if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. The minimum of those values δ having such property, that is, the maximum number of solutions of such equations, is denoted by δ_F and is called the* differential uniformity *of F.*

When we speak of differentially uniform functions without specifying the value of δ, this implies that the unspecified value of δ is small.

Definition 3 *[21, 1, 17] An (n, n)-function F is called* almost perfect nonlinear *(*APN*) if it is differentially 2-uniform, that is, if for every $a \in \mathbb{F}_2^n \setminus \{0_n\}$ and every $b \in \mathbb{F}_2^n$, the equation $D_aF(x) := F(x) + F(x + a) = b$ has 0 or 2 solutions (*i.e. $|\{D_aF(x), x \in \mathbb{F}_2^n\}| = 2^{n-1}$*). Equivalently, for distinct elements x, y, z, t of $\mathbb{F}_2^n$, the equality $x + y + z + t = 0$ implies $F(x) + F(y) + F(z) + F(t) \neq 0$, that is, the restriction of F to any 2-dimensional flat (*i.e. affine plane*) of $\mathbb{F}_2^n$ is non-affine.*

3 Characterizations of APN-ness and consequences

APN functions and more general differentially uniform functions play a central role in the framework of block ciphers, in conventional cryptography. They are their only nonlinear parts, and are then (in relation with the diffusion layers) the main actors in their security. Nyberg's studies on them facilitated the invention by Daemen and Rijmen of the standard in civil symmetric cryptography, the AES. The classical characterizations of APN and differentially uniform functions (for instance by the Walsh transform or the numbers of solutions of some systems of equations) are recalled comprehensively in [7]. Some new characterizations are given in this same monograph. Let us recall and study them a little more in detail. This will lead us to open problems and to a new result.

3.1 Characterization by the degrees of univariate polynomials

The vector space $\mathbb{F}_2^n$ can be endowed with the structure of the field $\mathbb{F}_{2^n}$, since this field is an n-dimensional vector space over $\mathbb{F}_2$. Then every (n,n)-function (and more generally, every (n,m)-function where m divides n) can be uniquely represented by its univariate representation:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i \in \mathbb{F}_{2^n}[x]/(x^{2^n}+x). \tag{1}$$

The algebraic degree of such function F equals the maximum Hamming weight of the binary expansion of the exponents i such that $\delta_i \neq 0$. All known APN functions are expressed in this representation and it is an open problem to find an infinite class of APN functions represented in the vector space $\mathbb{F}_2^n$, for instance by its ANF, without endowing it with the structure of the field $\mathbb{F}_{2^n}$ and without using the structure of a subfield $\mathbb{F}_{2^r}$ where r would be a large divisor of n.

It is observed in [7] that:

Proposition 1 *Any (n,n)-function F, given in univariate form, is APN if and only if, for every $a \in \mathbb{F}_{2^n}^*$ and every $b \in \mathbb{F}_{2^n}$, the univariate polynomial $\gcd(x^{2^n}+x, F(x)+F(x+a)+b)$ has degree at most 2, and more precisely, has degree 0 or 2.*

The reason why this is true is simple: $x^{2^n}+x$ splits completely over $\mathbb{F}_{2^n}$ and its roots, all simple, are all the elements of $\mathbb{F}_{2^n}$; the polynomial $F(x)+F(x+a)+b$ has then a number of zeros in $\mathbb{F}_{2^n}$ equal to the degree of its gcd with $x^{2^n}+x$. Hence, F is differentially δ-uniform if and only if, for every $a \in \mathbb{F}_{2^n}^*$ and every $b \in \mathbb{F}_{2^n}$, the polynomial $\gcd(x^{2^n}+x, F(x)+F(x+a)+b)$ has degree at most δ.

Remark. This characterization is a direct translation of the definition, but it may give tools for proving APN-ness, thanks to the Euclidean algorithm, which eases the calculation of gcd's. Note moreover that if $F(x)$ is a power function over $\mathbb{F}_{2^n}$, that is, $F(x) = x^d$, then it is sufficient to check the condition for

$a = 1$, and all the coefficients obtained when applying the Euclidean algorithm belong to $\mathbb{F}_2$, which considerably simplifies the calculation and reduces the size of the necessary storage when computing. Unfortunately, after the searches made by Y. Edel (and unpublished), the next APN exponent candidates d are for n larger than or equal to 35; this seems to make the calculation of the gcd out of reach. However, this characterization may be an efficient way to search for new polynomial APN functions of low (polynomial) degrees.

Open problems. Find more direct proofs of the APN-ness of some of the known APN functions (see e.g. [3, 7]) by using this characterization. Find new APN functions thanks to it. ◇

Remark. Some other properties of a similar kind can be stated for APN functions and differentially δ-uniform functions. For instance, for every nonzero a, every b and every linear function L, the polynomial $\gcd(x^{2^n} + x, F(x) + L(x), F(x+a) + L(x+a) + b)$ has degree at most 2 (resp. δ). Indeed, there are at most 2 (resp. δ) solutions in $\mathbb{F}_{2^n}$ of the system of equations $F(x) + L(x) = F(x+a) + L(x+a) + b = 0$, since it implies $F(x) + F(x+a) = b + L(a)$.

3.2 Characterization by Boolean relations

Let us denote by δ_0 the Dirac (or Kronecker) symbol, that is, the Boolean function which takes value 1 at the input 0 and value 0 everywhere else. If $\mathbb{F}_2^n$ is viewed as a vector space, then we can write $\delta_0(x) = \prod_{i=1}^n (x_i + 1)$, and if we endow $\mathbb{F}_2^n$ with a structure of field, then we can write $\delta_0(x) = x^{2^n-1} + 1$.
By definition, an (n,n)-function is APN if and only if, for every nonzero $a \in \mathbb{F}_2^n$ and every $x \in \mathbb{F}_2^n$, the equality "$F(x) + F(x+a) + F(y) + F(y+a) = 0$" is equivalent to "$x + y = 0$ or $x + y + a = 0$". The two conditions "$x + y = 0$" and "$x + y + a = 0$" being exclusive of each other for $a \neq 0$, the Boolean function translating "$x + y = 0$ or $x + y + a = 0$" is $\delta_0(x+y) + \delta_0(x+y+a)$. We have then:

Proposition 2 *[7] Any (n,n)-function F is APN if and only if the Boolean function:*

$$\delta_0\Big(F(x) + F(x+a) + F(y) + F(y+a)\Big) + \delta_0\Big(x+y\Big) + \delta_0\Big(x+y+a\Big) \quad (2)$$

equals the zero function.

Equivalently, F is APN if and only if, denoting for every $a \neq 0$ by H_a any linear hyperplane excluding a, function D_aF is injective on H_a, that is:

$$1_{H_a}(x)\, 1_{H_a}(y)\, [\delta_0(F(x) + F(x+a) + F(y) + F(y+a)) + \delta_0(x+y)] \equiv 0.$$

These identities, when considered as multivariate polynomial equalities (that is, considering F represented by its ANF), need to be viewed in $\mathbb{F}_2[x,y]/(x_i^2 + x_i, y_i^2 + y_i; i = 1, \ldots, n)$.

They can also be considered as univariate identities in $\mathbb{F}_{2^n}[x,y]/(x^{2^n}+x, y^{2^n}+y)$, where $\delta_0(z) = 1+z^{2^n-1}$, and they need then to be reduced modulo $x^{2^n}+x$ and modulo $y^{2^n}+y$ before being checked as identically zero.

Remark. In the case of power functions, we have the same simplification as in Subsection 3.1. It is enough to check the APN property for $a = 1 \in \mathbb{F}_{2^n}$. Hence, $F(x) = x^d$ is APN if and only if:

$$\Big(x^d + (x+1)^d + y^d + (y+1)^d\Big)^{2^n-1} + \Big(x+y\Big)^{2^n-1} + \Big(x+y+1\Big)^{2^n-1} = 1 \pmod{x^{2^n}+x, y^{2^n}+y}. \quad (3)$$

Let us compare this way of addressing APN exponents with the classical method implementing the very definition of APN-ness. Let us take the example of Gold APN functions $F(x) = x^{2^j+1}$, where $\gcd(j,n) = 1$. Checking APN-ness with the classical method is very simple: we have $x^{2^j+1} + (x+1)^{2^j+1} = x^{2^j} + x + 1$ and the mapping $L_j : x \in \mathbb{F}_{2^n} \mapsto x^{2^j} + x$ is linear with kernel $\mathbb{F}_{2^n} \cap \mathbb{F}_{2^j} = \mathbb{F}_2$. The equation $L_j(x) = 1 + b$ has then at most 2 solutions for every b.
With Relation (3), we have $x^d + (x+1)^d + y^d + (y+1)^d = L_j(x+y)$ and we need first to calculate the univariate expression of $(L_j(x))^{2^n-1}$. It equals $x^{2^n-1}(1+x^{2^j-1})^{2^n-1}$ and $(1+x^{2^j-1})^{2^n-1}$ equals $\sum_{i=0}^{2^n-1} x^{i(2^j-1)}$. Since 2^j-1 is co-prime with 2^n-1, the multiplication of i by 2^j-1 in $\mathbb{Z}/(2^n-1)\mathbb{Z}$ is just a permutation over all exponents of x, so that $(1+x^{2^j-1})^{2^n-1}$ equals $(1+x)^{2^n-1}$. Hence we have $(L_j(x))^{2^n-1} = x^{2^n-1}(1+x)^{2^n-1} = (1+x)^{2^n-1} + 1 + x^{2^n-1} \pmod{x^{2^n}+x}$ and Relation (3) is then satisfied.
We see with this example that the characterization by Relation (3) may need more work to be implemented but also gives some different view, and we shall see in Subsections 3.4 and 3.5 that it gives explicit additional insight. Moreover, it may also have the advantage of giving a tool for discriminating APN exponent candidates, for instance by trying to find an expression by means of d of the coefficient of some monomial $x^k y^l$; the nullity of any such coefficient gives a necessary condition for APN-ness, the difficulty coming from the reduction modulo $x^{2^n}+x$ and $y^{2^n}+y$ in (3). ◇

Open problem: determine other infinite classes of pairs (n,d) such that the expression $\Big(x^d+(x+1)^d+y^d+(y+1)^d\Big)^{2^n-1}$ can be transformed modulo $x^{2^n}+x$ and $y^{2^n}+y$ into $\sum_{i=1}^{2^n-1}(x+y)^{ik} + (x+y)^{2^n-1}$ for some k co-prime with 2^n-1 (the exponents d will be automatically APN). ◇

3.3 Another related open problem

The open problem above is connected to the following one:

Open problem: determine all the exponents d such that $\delta_0(x^d+(x+1)^d+y^d+(y+1)^d)$ depends only on $x+y$, that is, $\delta_0(x^d+(x+1)^d+(x+y)^d+(x+y+1)^d)$

is a Boolean function of y, independent of x. $\diamond$

Note that this is a necessary condition for APN-ness since, for an APN exponent, we have that $\delta_0(x^d+(x+1)^d+y^d+(y+1)^d)$ equals 1 if $x+y \in \mathbb{F}_2$ and equals 0 otherwise. It is not a sufficient condition since some non-APN exponents satisfy it, for instance the Gold exponents $d = 2^j+1$ where $\gcd(j,n) > 1$. Note also that some exponents d do not have this property. Take for instance $d = 7$, then $x^d + (x+1)^d = x^6+x^5+x^4+x^3+x^2+x+1$ and $x^d+(x+1)^d+(x+y)^d+(x+y+1)^d = x^4(y^2+y)+x^2(y^4+y)+x(y^4+y^2)+y^6+y^5+y^4+y^3+y^2+y$. Then $\delta_0(x^d+(x+1)^d+(x+y)^d+(x+y+1)^d)$ does not depend only on y, since there exists $x \neq 0$ such that the expressions $x^4(y^2+y)+x^2(y^4+y)+x(y^4+y^2)+y^6+y^5+y^4+y^3+y^2+y$ and $y^6+y^5+y^4+y^3+y^2+y$ do not vanish simultaneously.

Let us give now a necessary and sufficient condition for the property involved in the open problem above to be satisfied by d. By binomial expansion and according to Lucas' theorem [13, page 404] (which states that $\binom{i}{j}$ is odd if and only if $j \preceq i$), we have $x^d+(x+1)^d = \sum_{0 \preceq i \prec d} x^i$, where $i \prec d$ means that $i \preceq d$ and $i \neq d$, where $i \preceq d$ means that the binary expansion of i is covered by that of d (*i.e.* has support included in its support). Therefore $x^d+(x+1)^d+(x+y)^d+(x+y+1)^d = \sum_{0 \prec i \prec d}(x^i+(x+y)^i) = \sum_{0 \preceq j \prec i \prec d} x^j y^{i-j}$. Note that all these monomials $x^j y^{i-j}$ are pairwise distinct and that:
- for $y = 0$, each monomial cancels since each $i-j$ is strictly positive,
- for $y = 1$, the monomials cancel each others, since, for each $j \prec d$ such that the Hamming weight $w_2(j)$ of the binary expansion of j is lower than or equal to $w_2(d)-2$ (condition implied by $i \prec d$ and $j \prec i$ above), there is an even number of possible i such that $i \prec d$ and $j \prec i$.
This is in both cases coherent with the fact that $x^d+(x+1)^d+(x+y)^d+(x+y+1)^d$ is identically null for these two values of y. And we have the following characterization:

Proposition 3 *Let n be any positive integer and let $d \in \mathbb{Z}/(2^n-1)\mathbb{Z}$. Then the function $\delta_0(x^d+(x+1)^d+y^d+(y+1)^d)$ depends only on $x+y$ if and only if, for every $y \in \mathbb{F}_{2^n}$ (or equivalently, for every $y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$), the polynomial in x equal to $\sum_{0 \preceq j \prec d}(\sum_{j \prec i \prec d} y^{i-j})\, x^j$ is either identically null or has no zero, and d is an APN exponent if and only if, for every $y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, this same polynomial has no zero.*

There are at least three ways to study such conditions:

- study the corresponding equation, for every $y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$,
- raise $\sum_{j \prec d}(\sum_{j \prec i \prec d} y^{i-j})\, x^j$ to the (2^n-1)-th power and reduce modulo $x^{2^n}+x$ (and either considering y as a second variable and reducing also modulo $y^{2^n}+y$, or considering y as an element of $\mathbb{F}_{2^n}$ and visiting all its possible values),

- express that, for every $y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$:

$$\gcd\Big(\sum_{j \prec d}\big(\sum_{j \prec i \prec d} y^{i-j}\big)\, x^j, x^{2^n}+x\Big) = 1.$$

3.4 Dobbertin's result revisited

Recall Dobbertin's proof of the fact that if d is an APN exponent then $\gcd(d, 2^n-1)$ equals 1 if n is odd and equals 3 otherwise: any element in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ can be written in the form $\frac{x}{x+1}$, where $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$; then $\left(\frac{x}{x+1}\right)^d = 1$ implies that $x^d+(x+1)^d = 0$ and therefore $x^d+(x+1)^d = x^{2d}+(x+1)^{2d} = (x^2)^d+(x^2+1)^d$, and since $x \mapsto x^d$ is APN and $x \notin \mathbb{F}_2$, this gives $x^2 = x+1$, that is, $x \in (\mathbb{F}_4 \cap \mathbb{F}_{2^n}) \setminus \mathbb{F}_2$ and this proves that the set of elements $y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ such that $y^d = 1$ is empty for n odd and has 2 elements for n even. This proves the result.

A by-product is that the solutions of $x^d + (x+1)^d = 0$, if they exist, belong to $\mathbb{F}_4$ if n is even and to $\mathbb{F}_2$ if n is odd (in fact, they do not then exist). We shall generalize this below in Theorem 1.

Let us show how the congruence:

$$\delta_0(x^d + (x+1)^d + y^d + (y+1)^d) + \delta_0(x+y) + \delta_0(x+y+1)$$
$$\equiv 0 \ [\mathrm{mod}\ x^{2^n}+x,\ \mathrm{mod}\ y^{2^n}+y], \tag{4}$$

allows to show the property in another way. We will see that this more complex approach has the advantage of providing clues. Taking $y = x^2$ in (4) and using that we have $\delta_0(x^d + (x+1)^d + x^{2d} + (x+1)^{2d}) = \delta_0((x^d + (x+1)^d)(1 + x^d + (x+1)^d)) = \delta_0(x^d + (x+1)^d) + \delta_0(1 + x^d + (x+1)^d)$, we obtain:

$$\delta_0(x^d + (x+1)^d) + \delta_0(1 + x^d + (x+1)^d) + \delta_0(x+x^2) + \delta_0(x+x^2+1) \equiv 0$$
$$[\mathrm{mod}\ x^{2^n}+x]. \tag{5}$$

Moreover, applying (4) with $y = 0$, we have:

$$\delta_0(1 + x^d + (x+1)^d) + \delta_0(x) + \delta_0(x+1) \equiv 0 \ [\mathrm{mod}\ x^{2^n}+x]. \tag{6}$$

Relation (5) added with (6) gives then:

$$\delta_0(x^d + (x+1)^d) + \delta_0(x+x^2+1) \equiv 0 \ [\mathrm{mod}\ x^{2^n}+x], \tag{7}$$

since we have $\delta_0(x+x^2) = \delta_0(x(1+x)) = \delta_0(x) + \delta_0(x+1)$.
Relation (7) implies that $\left(\frac{x}{x+1}\right)^d$ equals 1 if and only if $x \in \mathbb{F}_{2^{\gcd(2,n)}} \setminus \mathbb{F}_2$ and this leads to the nice Dobbertin's idea of considering the relation $\left(\frac{x}{x+1}\right)^d = 1$, and it gives Dobbertin's result.

Note that if n is even, and if w is primitive in $\mathbb{F}_4$, then we have $w^d+(w+1)^d = 0$. We have again that the two solutions of $x^d + (x+1)^d = 0$ are in $\mathbb{F}_4$.

3.5 Extension of Dobbertin's result

Let us now see what gives this method if we replace y by x^{2^k} for some $k \geq 0$. This will lead us to a new result that we can prove more directly once we get the idea. We obtain from (4) that for every APN exponent d:

$$\delta_0(x^d + (x+1)^d + x^{2^k d} + (x+1)^{2^k d}) + \delta_0(x + x^{2^k}) + \delta_0(x + x^{2^k} + 1) \equiv 0 \ [\mathrm{mod}\ x^{2^n} + x].$$

Denoting $\gcd(k,n)$ by l, the equality $\delta_0(x^d + (x+1)^d + x^{2^k d} + (x+1)^{2^k d}) = 1$ is equivalent to $x^d + (x+1)^d = \left(x^d + (x+1)^d\right)^{2^k}$, that is, $x^d + (x+1)^d \in \mathbb{F}_{2^k} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^l}$ and we have then $\delta_0(x^d + (x+1)^d + x^{2^k d} + (x+1)^{2^k d}) = \sum_{u \in \mathbb{F}_{2^l}} \delta_0(x^d + (x+1)^d + u)$. Moreover:

- $\delta_0(x + x^{2^k}) = 1$ is equivalent to $x^{2^k} = x$, that is, $x \in \mathbb{F}_{2^l}$,
- if $\gcd(2k,n) = 2l$, then, since $x + x^{2^k}$ is linear, $\delta_0(x + x^{2^k} + 1) = 1$ is equivalent to $x \in w + \mathbb{F}_{2^l}$ where w is some fixed element of $\mathbb{F}_{2^{2l}} \setminus \mathbb{F}_{2^l}$ such that $w + w^{2^k} = 1$, and otherwise, we have $\gcd(2k,n) = l$ and $\delta_0(x + x^{2^k} + 1) = 1$ is impossible, since $x + x^{2^k} = 1$ implies $x + x^{2^{2k}} = 0$, that is, $x \in \mathbb{F}_{2^{2k}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^l}$ but then $x + x^{2^k} = 0$.

Then $\delta_0(x + x^{2^k}) + \delta_0(x + x^{2^k} + 1)$ equals the indicator of $\{0, w\} + \mathbb{F}_{2^l}$ if $\gcd(2k,n) = 2l$, and otherwise, it equals the indicator of $\mathbb{F}_{2^l}$.

1. if $l = 1$, then we obtain no information additional to Dobbertin's observation,
2. if $l > 1$ and $\gcd(2k,n) = \gcd(k,n) = l$ (that is, if $\frac{n}{l}$ is odd), then $\sum_{u \in \mathbb{F}_{2^l}} \delta_0(x^d + (x+1)^d + u)$ equals the indicator of $\mathbb{F}_{2^l}$; equivalently, for every $x \notin \mathbb{F}_{2^l}$, we have $x^d + (x+1)^d \notin \mathbb{F}_{2^l}$.
3. if $l > 1$ and $\gcd(2k,n) = 2\gcd(k,n) = 2l$ (ie $\frac{n}{l}$ is even), then $\sum_{u \in \mathbb{F}_{2^l}} \delta_0(x^d + (x+1)^d + u)$ equals the indicator of $\{0, w\} + \mathbb{F}_{2^l}$.

These observations lead in the next subsection to a new theorem, whose statement is very simple.

Open problem: find more expressions of y as a function of x, which would provide new results on APN functions. ◇

3.6 On APN polynomial functions with coefficients in a subfield

The observations of the previous subsection lead to the following theorem, which generalizes them, and whose proof can be given in a more direct way.

Theorem 1 *Let $n = kn'$ with n' odd, and let $F(x)$ be an APN power function over $\mathbb{F}_{2^n}$, or more generally an APN polynomial over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^k}$. For every $b \in \mathbb{F}_{2^k}$ and every nonzero $a \in \mathbb{F}_{2^k}$, the (two) solutions $x \in \mathbb{F}_{2^n}$ of $F(x) + F(x + a) = b$, if they exist, belong to $\mathbb{F}_{2^k}$, that is, moving from the extension field of degree k to that of degree kn' does not provide any new solution to the equation $F(x) + F(x + a) = b$.*

Proof. For every $x \in \mathbb{F}_{2^n}$, the relation $F(x)+F(x+a) = b$ implies $F(x)+F(x+a) = (F(x) + F(x + a))^{2^k} = F(x^{2^k}) + F(x^{2^k} + a)$, since a and b are elements of $\mathbb{F}_{2^k}$ and $F(x)$ is a polynomial with coefficients in $\mathbb{F}_{2^k}$. Then, function F being APN over $\mathbb{F}_{2^n}$, this implies either $x^{2^k} = x$, that is, $x \in \mathbb{F}_{2^k}$, or $x^{2^k} = x+a$ which implies $x^{2^{2k}} = (x^{2^k})^{2^k} = (x+a)^{2^k} = x$, that is $x \in \mathbb{F}_{2^{2k}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{\gcd(2k,n)}} = \mathbb{F}_{2^k}$ which makes $x^{2^k} = x + a$ impossible. □

This result had been missed[1] (even if they were close) by the authors of [2, Proposition 3] when they generalized Dobbertin's result. This illustrates how the more complex approach by (4) gives clues for properties that are not obvious to see.
Theorem 1 tells that, for any nonzero $a \in \mathbb{F}_{2^k}$, the derivative $x \mapsto D_aF(x) = F(x) + F(x + a)$ maps $\mathbb{F}_{2^k}$ to (a half of) $\mathbb{F}_{2^k}$ and maps $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ to (a half of) $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. Note that the restriction of F to $\mathbb{F}_{2^k}$ is an APN (k, k)-function (it is valued in $\mathbb{F}_{2^k}$ thanks to the fact that its coefficients are in $\mathbb{F}_{2^k}$). All this applies to the following known APN functions over $\mathbb{F}_{2^n}$ (see more in [7], in particular the references where these functions were introduced) and for the following values of k (for which it is interesting to see to which class of APN functions the restriction to $\mathbb{F}_{2^k}$ belongs):

- Gold APN functions x^{2^i+1}, where $\gcd(i, n) = 1$; k divisor of n (the restriction of this Gold function to $\mathbb{F}_{2^k}$ is a Gold function).
- Kasami APN functions $x^{4^i-2^i+1}$, where $\gcd(i, n) = 1$; k divisor of n (the restriction of this Kasami function to $\mathbb{F}_{2^k}$ is a Kasami function).
- The inverse function x^{2^n-2}, where n is odd; k divisor of n (the restriction of this inverse function to $\mathbb{F}_{2^k}$ is an inverse function).
- The Welch function x^{2^t+3}, $n = 2t + 1$; k (odd) divisor of n: writing $n = k(2r + 1)$, $k = 2l + 1$, we have $t = \frac{n-1}{2} = kr + l$ and for $x \in \mathbb{F}_{2^k}$, $x^{2^k} = x$ implies $x^{2^t+3} = x^{2^l+3}$ (the restriction of this Welch function to $\mathbb{F}_{2^k}$ is then a Welch function).
- Niho functions $x^{2^t+2^{\frac{t}{2}}-1}$ for t even and $x^{2^t+2^{\frac{3t+1}{2}}-1}$ for t odd, $n = 2t+1$: as above, writing $n = k(2r + 1)$, $k = 2l + 1$, we have $t = \frac{n-1}{2} = kr + l$

[1] Ref. [2, Proposition 3] gives the conclusion that either the two solutions belong to $\mathbb{F}_{2^k}$ or they satisfy $x^{2^k} + x = a$, but misses that under the conditions of Theorem 1, the latter case cancels.

and for $x \in \mathbb{F}_{2^k}$, $x^{2^k} = x$ implies for t even: $x^{2^t+2^{\frac{t}{2}}-1} = x^{2^l+2^{\frac{l}{2}}-1}$ if r and l are even and $x^{2^t+2^{\frac{t}{2}}-1} = x^{2^l+2^{\frac{k+l}{2}}-1} = x^{2^l+2^{\frac{3l+1}{2}}-1}$ if r and l are odd, and for t odd: $x^{2^t+2^{\frac{3t+1}{2}}-1} = x^{2^l+2^{\frac{3l+1}{2}}-1} = x^{2^l+2^{\frac{l}{2}}-1}$ for r even and l odd and $x^{2^t+2^{\frac{3t+1}{2}}-1} = x^{2^l+2^{\frac{3l+1}{2}}-1}$ for r odd and l even (the restriction of this Niho function to $\mathbb{F}_{2^k}$ is then always a Niho function).

- The Dobbertin function $x^{2^{4k}+2^{3k}+2^{2k}+2^k-1}$, where $n = 5k$ (the restriction of this Dobbertin function to $\mathbb{F}_{2^k}$ is the cube function, which is a particular Gold function and a particular Kasami function; this is the only case where the restriction is not in the same class as the (n, n)-function).

- $F(x) = x^{2^i+1} + (x^{2^i} + x)\, tr_n(x^{2^i+1} + x)$, where $n > 3$ is odd, $\gcd(n, i) = 1$ and $tr_n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$; k divisor of n (the restriction is similar to the original function because n' being odd, we have for $x \in \mathbb{F}_{2^k}$ that $tr_n(x^{2^i+1} + x) = tr_k(x^{2^i+1} + x)$).

- For n odd, $m \,|\, n$, $m \neq n$ and $\gcd(n, i) = 1$, the (n, n)-function:

$$x^{2^i+1} + tr_m^n(x^{2^i+1}) + x^{2^i} tr_m^n(x) + x\ tr_m^n(x)^{2^i} +$$
$$[tr_m^n(x)^{2^i+1} + tr_m^n(x^{2^i+1}) + tr_m^n(x)]^{\frac{1}{2^i+1}}(x^{2^i} + tr_m^n(x)^{2^i} + 1) +$$
$$[tr_m^n(x)^{2^i+1} + tr_m^n(x^{2^i+1}) + tr_m^n(x)]^{\frac{2^i}{2^i+1}}(x + tr_m^n(x))$$

  where tr_m^n denotes the trace function $tr_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$; k divisor of n (it is here difficult to say if the restriction is similar to the original function).

- $F(x) = x^{2^i+1} + (x^{2^i} + x + 1)\, tr_n(x^{2^i+1})$, where $n \geq 4$ is even and $\gcd(n, i) = 1$; k divisor of n (the restriction is similar to the original function).

- For n even and divisible by 3, the function $F(x)$ equal to

$$[x + tr_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + tr_n(x)\, tr_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})]^{2^i+1},$$

  where $\gcd(n, i) = 1$; k divisor of n (the restriction is similar to the original function).

- $x^3 + tr_n(x^9)$ (the restriction is similar to the original function).

There are other cases of APN functions (see [7]) that we do not detail because making explicit the conditions for the coefficients to belong to $\mathbb{F}_{2^k}$ would take too much room.

Counter-examples to Theorem 1 when F has coefficients outside $\mathbb{F}_{2^k}$ are for instance with functions $u\,F(x)$ where F has its coefficients in $\mathbb{F}_{2^k}$ and $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

Remark. After obtaining the result of Theorem 1, the author learned of the existence of [24], which proves this result in a more complex way for the sole Dobbertin function and for $k = \frac{n}{5}$. This same reference deduces that, for $n = 5k$ odd, modifying over $\mathbb{F}_{2^k}$ the Dobbertin (n, n)-function by replacing its value by that of any differentially 4-uniform (resp. 6-uniform) permutation G gives a differentially 4-uniform (resp. 6-uniform) function. We have in fact a more general result. $\diamond$

Corollary 1 *Let $n = kn'$ with n' odd, and let $F(x)$ be any APN polynomial over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^k}$ and let G be any function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^k}$. The function:*

$$H : x \mapsto \begin{cases} G(x) \text{ if } x \in \mathbb{F}_{2^k} \\ F(x) \text{ if } x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k} \end{cases} \tag{8}$$

is differentially $\max(4, \delta_G)$*-uniform.*

This corollary is a direct consequence of Theorem 1 above and from [5, Theorem 4.1]. For making our paper self-contained, let us give an explicit proof. For every $a \in \mathbb{F}_{2^k}^*$, given $b \in \mathbb{F}_{2^k}$, we have, according to Theorem 1: $|\{x \in \mathbb{F}_{2^n}; H(x) + H(x+a) = b\}| = |\{x \in \mathbb{F}_{2^k}; G(x)+G(x+a) = b\}| \leq \delta_G$, and given $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we have, since D_aG is valued in $\mathbb{F}_{2^k}$: $|\{x \in \mathbb{F}_{2^n}; H(x) + H(x+a) = b\}| = |\{x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}; F(x) + F(x+a) = b\}| \leq 2$; the equation $H(x) + H(x+a) = b$ has then at most δ_G solutions in $\mathbb{F}_{2^n}$, whatever is b. For every $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, given $b \in \mathbb{F}_{2^n}$, we have $|\{x \in \mathbb{F}_{2^n}; H(x)+H(x+a) = b\}| = |\{x \in \mathbb{F}_{2^k}; G(x)+F(x+a) = b\}| + |\{x \in a+\mathbb{F}_{2^k}; F(x)+G(x+a) = b\}| + |\{x \in \mathbb{F}_{2^n} \setminus (\mathbb{F}_{2^k} \cup (a+\mathbb{F}_{2^k})); F(x) + F(x+a) = b\}| = 2|\{x \in \mathbb{F}_{2^k}; G(x) + F(x+a) = b\}| + |\{x \in \mathbb{F}_{2^n} \setminus (\mathbb{F}_{2^k} \cup (a + \mathbb{F}_{2^k})); F(x)+F(x+a) = b\}| \leq 2|\{x \in \mathbb{F}_{2^k}; G(x)+F(x+a) = b\}|+2$. The relation $G(x)+F(x+a) = b$ for $x \in \mathbb{F}_{2^k}$ implies $F(x+a) \in b+\mathbb{F}_{2^k}$. Hence, if the equation $G(x)+F(x+a) = b$ has (at least) two distinct solutions in $\mathbb{F}_{2^k}$, say x and $x+u$, where $u \in \mathbb{F}_{2^k}^*$, then we have $D_uF(x+a) \in \mathbb{F}_{2^k}$, a contradiction with Theorem 1, since $x+a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. We deduce that $|\{x \in \mathbb{F}_{2^k}; G(x) + F(x+a) = b\}| \leq 1$ and $|\{x \in \mathbb{F}_{2^n}; H(x) + H(x+a) = b\}| \leq 4$.
This completes the proof.

This property provides some interesting differentially 4-uniform functions H, such as the functions of the form $x \mapsto \begin{cases} uF(x) \text{ if } x \in \mathbb{F}_{2^k} \\ F(x) \text{ if } x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k} \end{cases}$, where $u \in \mathbb{F}_{2^k} \setminus \mathbb{F}_2$.
Moreover, if:

1. G is APN,
2. for every $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, $x \in \mathbb{F}_{2^k}$ and $y \in \mathbb{F}_{2^n} \setminus (\mathbb{F}_{2^k} \cup (a + \mathbb{F}_{2^k}))$, we have $G(x) + F(x + a) \neq F(y) + F(y + a)$,

then H is APN.
Note that, by the definition of APN-ness (more precisely, according to the property "for distinct elements x, y, z, t of $\mathbb{F}_2^n$, the equality $x + y + z + t = 0$ implies

$F(x)+F(y)+F(z)+F(t)\neq 0$", in Definition 3), taking for G the restriction of F to $\mathbb{F}_{2^k}$ satisfies the condition; indeed, for $a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$, $x\in\mathbb{F}_{2^k}$ and $y\in\mathbb{F}_{2^n}\setminus(\mathbb{F}_{2^k}\cup(a+\mathbb{F}_{2^k}))$, the elements $x, x+a, y, y+a$ are all distinct and they sum to 0. This is coherent since F is APN on $\mathbb{F}_{2^n}$. We do not know if, for some $k<n$ such that $k|n$ and some APN polynomial F over $\mathbb{F}_{2^n}$ with coefficients in $\mathbb{F}_{2^k}$, the condition can be satisfied by a function G different from the restriction of F to $\mathbb{F}_{2^k}$. In fact, we do not know an example of two APN functions differing on a strict subfield, only (which is equivalent, thanks to the invariance of APN-ness under affine equivalence, to knowing an example of two APN functions differing on a k-dimensional vector subspace of $\mathbb{F}_{2^n}$, only, where k is a strict divisor of n and is then at most $\frac{n}{2}$). This is related to the question of the minimum Hamming distance between APN functions studied in [4], where is shown that the minimum nonzero Hamming distance between a given APN function F and all the other APN functions is at least $\frac{\min_{b,\beta\in\mathbb{F}_{2^n}}|\{a\in\mathbb{F}_{2^n};\exists x\in\mathbb{F}_{2^n};D_aF(x)+F(a+\beta)=b\}|}{3}+1$. For instance, the minimum nonzero Hamming distance between the cube function $F(x)=x^3$ and all the other APN functions is at least $\frac{2^{n-1}-2^{\frac{n}{2}}+2}{3}$; hence, the double condition 1-2 above is never satisfied when F is the cube function and $n\geq 6$. We conjecture that, for every APN (n,n)-function F with $n\geq 7$ and every $b,\beta\in\mathbb{F}_{2^n}$, we have $|\{a\in\mathbb{F}_{2^n};\exists x\in\mathbb{F}_{2^n};D_aF(x)+F(a+\beta)=b\}|\geq 3\cdot 2^{\frac{n}{2}}$ (this is true for all the values computed in [4, Table II]) and the double condition 1-2 above is never satisfied.

Note also that taking F and G bijective makes H bijective too. Indeed, since the coefficients of F are in $\mathbb{F}_{2^k}$, we have $F(\mathbb{F}_{2^k})\subseteq\mathbb{F}_{2^k}$ and then $F(\mathbb{F}_{2^k})=\mathbb{F}_{2^k}$, and then $F(\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k})=\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$.

Note finally that, given an APN polynomial $G(x)$ over $\mathbb{F}_{2^n}$ having some coefficients outside $\mathbb{F}_{2^k}$, the function:

$$H':x\mapsto\begin{cases}F(x)\text{ if }x\in\mathbb{F}_{2^k}\\ G(x)\text{ if }x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}\end{cases}$$

is in general not differentially 4-uniform. For instance, taking for $F(x)$ an APN power function and for $G(x)$ the function $uF(x)$ with $u\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^k}$ provides counter-examples. Of course, if all the coefficients of G are in $\mathbb{F}_{2^k}$, then we are in the situation of (8) with F and G swapped, since the restriction of F to $\mathbb{F}_{2^k}$ is valued in $\mathbb{F}_{2^k}$ and APN; then H' is differentially 4-uniform.

4 Algebraic immunity and higher order nonlinearity

In the framework of stream ciphers in conventional cryptography, a major event in the history of Boolean functions is the invention of algebraic attacks (AA). These attacks, which use the existence of low algebraic degree annihilators of the filter or combiner function f in a stream cipher or of its complement $f+1$, were devastating for several stream ciphers used at that time, and they obliged

the designers of stream ciphers to use Boolean functions in more variables than before their invention, which consequently posed a problem (which is not completely resolved nowadays) regarding the speed of these ciphers. We refer to [7] for more details.
It took five years before an infinite class of functions could be found in [8], satisfying all the necessary classical criteria (balancedness, a high algebraic degree and a high nonlinearity; more precisely, a good tradeoff between these three parameters) and also satisfying the new criterion resulting from this invention, which is to have a large algebraic immunity (AI).
Meanwhile, a bound between the AI and the nonlinearity was found in [9]:

$$nl(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}$$

and more general bounds between the AI and another parameter called the higher order nonlinearity were found.
Given two positive integers $r \leq n$ and an n-variable Boolean function f, the rth-order nonlinearity of f, denoted by $nl_r(f)$ (the notation being simplified into $nl(f)$ in the case of $r = 1$, that is, in the case of the nonlinearity as we defined it in Section 2), equals the minimum Hamming distance between f and those Boolean functions of algebraic degree at most r. The first bound on the higher order nonlinearity was found in [6] and writes:

$$nl_r(f) \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i} \tag{9}$$

and a second bound (which improves upon (9) for low values of r) has been found in [14] and writes:

$$nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1} \binom{n-r}{i}. \tag{10}$$

Finally in [11] was found a result implying all the bounds previously obtained, and can then be considered as their generalization (even if it did not provide more bounds). The proofs in [11] and in the other papers [9, 10, 12] written by the same author on the same subject, had parts that were insufficiently argumented, and some made unnecessary assumptions. In [7], the results and the proofs have been clarified. To complete the clarification, let us give slightly simplified and completed versions of these proofs, and see what is essential for proving (9) and (10) and what is not and can be considered as (interesting) complements.

Lobanov's approach in [11] is based on the next proposition.

Proposition 4 *[11, 12] For any n-variable Boolean functions f, h and any integers $0 \leq k, l \leq n$, denoting by $An_k(h)$ the vector space of the annihilators of algebraic degree at most k of h and by $\dim(An_k(h))$ its dimension, we have:*

$$d_H(f,h) \geq \dim(An_k(h)) - \dim(An_k(f)) + \dim(An_l(h+1)) - \dim(An_l(f+1)).$$

Moreover, if $d \leq AI(f)$, then we have:

$$d_H(f,h) \geq \dim(An_{d-1}(h)) + \dim(An_{d-1}(h+1)). \tag{11}$$

Proof. Let us consider the equations

$$\sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| \leq k}} a_I \prod_{i \in I} x_i = 0 \quad (E_{x,k})$$

in the $\sum_{i=0}^{k} \binom{n}{i}$ unknowns $a_I \in \mathbb{F}_2$, expressing that a given Boolean function g of (unknown) ANF $\sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| \leq k}} a_I \prod_{i \in I} x_i$ vanishes at $x = (x_1, \ldots, x_n)$. Let us select the maximum possible number of linearly $\mathbb{F}_2$-independent equations $E_{x,k}$, with $x \in supp(f)$. This number equals the rank of the system, that is, $2^n - \dim(An_k(f))$. Among these equations, there exist at least $\dim(An_k(h)) - \dim(An_k(f))$ of them which are linearly independent from the equations $E_{x,k}$, $x \in supp(h)$, and there are then at least $\dim(An_k(h)) - \dim(An_k(f))$ elements in $supp(f) \setminus supp(h)$. We can apply this to $f+1$ and $h+1$ as well, with l in the place of k. This gives the first inequality. Moreover, if $d \leq AI(f)$, then $\dim(An_{d-1}(f)) = \dim(An_{d-1}(f+1)) = 0$. This completes the proof. □

Lobanov then notes that, if $k \geq l$, then the mapping $\phi_{k,l} : (g_1, g_2) \mapsto g_1 + g_2$ is linear from the Cartesian product $An_k(h) \times An_l(h+1)$ to the vector space $B_{k,l}(h) = \{g \in \mathcal{BF}_n;\ d_{alg}(g) \leq k \text{ and } d_{alg}(hg) \leq l\}$, because we have that $(g_1+g_2)h = g_2$. Moreover, he observes that if we compose $\phi_{k,l}$ with the mapping $g \in B_{k,l}(h) \mapsto ((1+h)g, hg) \in An_k(h) \times An_l(h+1)$, we obtain the identity. Hence, $\phi_{k,l}$ is an $\mathbb{F}_2$-linear isomorphism, and we have then:

$$\big(k \geq l\big) \Rightarrow \Big(\dim(An_k(h)) + \dim(An_l(h+1)) = \dim B_{k,l}(h)\Big). \tag{12}$$

Proofs of Bounds (9) and (10) are then deduced as follows: Bound (11) and Relation (12) imply that, for every n-variable Boolean function f and every positive integer $r \leq n$, we have:

$$nl_r(f) \geq \min_{h \in \mathcal{BF}_n, d_{alg}(h) \leq r} \dim(B_{AI(f)-1, AI(f)-1}(h)). \tag{13}$$

Restricting ourselves without loss of generality to the case $d_{alg}(h) = r$, we have, for every k:

- $\dim(B_{k,k}(h)) \geq 2\sum_{i=0}^{k-r} \binom{n-r}{i}$. Indeed, let $\prod_{i \in I} x_i$ be a monomial of degree r in the ANF of h. Then all the n-variable functions of the form

$hg_1 + (h+1)g_2$ where g_1, g_2 have algebraic degree at most $k-r$ and depend only on variables $x_i, i \notin I$, belong to $B_{k,k}(h)$, since $hg_1 + (h+1)g_2$ has algebraic degree at most k and $h(hg_1 + (h+1)g_2) = hg_1$ has algebraic degree at most k as well. Moreover, all these functions are distinct, because the linear mapping $(g_1, g_2) \mapsto hg_1 + (h+1)g_2$ has trivial kernel, since $hg_1 + (h+1)g_2 = 0$ implies $hg_1 = (h+1)g_2 = 0$, because the two functions hg_1 and $(h+1)g_2$ have disjoint supports, and this implies $g_1 = g_2 = 0$ because g_1 and g_2 depend only on variables $x_i, i \notin I$, and then the ANF of hg_1 contains $g_1 \prod_{i \in I} x_i$ and the ANF of $(h+1)g_2$ contains $g_2 \prod_{i \in I} x_i$. We have then that (13) implies (9),

- similarly, $\dim(B_{k,k}(h)) \geq \sum_{i=0}^{k-r} \binom{n}{i} + \sum_{i=k-2r+1}^{k-r} \binom{n-r}{i}$, because, if $\prod_{i \in I} x_i$ is a monomial of degree r in the ANF of h, then all n-variable functions of the form $g_1 + hg_2$ where g_1, g_2 have algebraic degree at most $k-r$ and g_2 depends only on variables $x_i, i \notin I$, and has only monomials of degree at least $k-2r+1$, belong to $B_{k,k}(h)$ and are distinct since the linear mapping $(g_1, g_2) \mapsto g_1 + hg_2$ has trivial kernel. We have then that (13) implies (10).

Open problem: deduce other bounds from Relation (13). ◇

Other interesting results in Lobanov's papers, whose proofs also needed to be completed (which was done in [7]), are as follows (we also present here the proofs in a simplified way).

Proposition 5 *[11] If, for some $k < \lceil \frac{n}{2} \rceil$, the equations $E_{x,k}$, $x \in supp(f)$, are $\mathbb{F}_2$-linearly independent, then $f+1$ has no nonzero annihilator of algebraic degree at most k.*

Proof. Suppose there exists a nonzero annihilator g of algebraic degree at most k of $f+1$. We have then $supp(g) \subseteq supp(f)$. Since all the equations $E_{x,k}$, $x \in supp(f)$, are $\mathbb{F}_2$-linearly independent, all those corresponding to $x \in supp(g)$ are $\mathbb{F}_2$-linearly independent, and for every choice of $(b_x)_{x \in supp(g)} \in \mathbb{F}_2^{w_H(g)}$, the system of the linear equations $E_{x,k} = b_x$ for x ranging over $supp(g)$ has a solution. In particular, for every $u \in supp(g)$, there exists g' of algebraic degree at most k such that $gg' = \delta_u$ (the Dirac symbol at u, *i.e.* the indicator function of the singleton $\{u\}$), a contradiction with $d_{alg}(gg') \leq d_{alg}(g) + d_{alg}(g') \leq 2k < n$. □

In [11] is deduced the folllowing proposition, which shows in a way the optimality of Lobanov's results: assuming that the algebraic degree of h is at most $\lceil \frac{n}{2} \rceil$, he proves the following proposition, which does not need in fact the assumption $d_{alg}(h) \leq \lceil \frac{n}{2} \rceil$:

Proposition 6 *Let n be any positive integer. For every $d \leq \lceil \frac{n}{2} \rceil$ and every function h such that $\dim(An_{d-1}(h)) + \dim(An_{d-1}(h+1)) > 0$, there exists f for which Bound (11) is an equality and such that $AI(f) \geq d$.*

Proof. Let C_1 (resp. C_0) be a maximal subset of $supp(h)$ (resp. $supp(h+1)$) such that the corresponding equations $E_{x,d-1}$, for $x \in supp(h)$ (resp. $x \in supp(h+1)$), are $\mathbb{F}_2$-linearly independent. We have $|C_1| = \sum_{i=0}^{d-1} \binom{n}{i} - \dim(An_{d-1}(h))$ and $|C_0| = \sum_{i=0}^{d-1} \binom{n}{i} - \dim(An_{d-1}(h+1))$. According to Proposition 5 applied to the indicator function 1_{C_1} (resp. 1_{C_0}) and with $k = d-1$, the ranks of the systems of equations $E_{x,d-1}$, where $x \notin C_1$, respectively, $x \notin C_0$, are both equal to $\sum_{i=0}^{d-1} \binom{n}{i}$. Since C_0 is included in the complement of C_1, there exists outside $C_1 \cup C_0$, a subset C_0' of size $\sum_{i=0}^{d-1} \binom{n}{i} - |C_0| = \dim(An_{d-1}(h+1))$ such that the equations $E_{x,d-1}$, $x \in C_0 \cup C_0'$, are $\mathbb{F}_2$-linearly independent. Since C_1 is included in the complement of C_0, there exists outside $C_1 \cup C_0$, a subset C_1' of size $\sum_{i=0}^{d-1} \binom{n}{i} - |C_1| = \dim(An_{d-1}(h))$ such that the equations $(E_{x,d-1})$, $x \in C_1 \cup C_1'$, are $\mathbb{F}_2$-linearly independent. Since C_0 and C_1 were taken maximal, we have $C_1' \subseteq supp(h+1)$ and $C_0' \subseteq supp(h)$. The function $f = h + 1_{C_0'} + 1_{C_1'}$ satisfies $d_H(f,h) = \dim(An_{d-1}(h)) + \dim(An_{d-1}(h+1))$. And we have $AI(f) \geq d$, since the rank of the system of equations $E_{x,d-1}$, $x \in supp(f)$, is larger than or equal to $|C_1| + |C_1'| = \sum_{i=0}^{d-1} \binom{n}{i}$ and therefore, the rank of the system of equations $E_{x,d-1}$ where $x \in supp(f)$ equals $\sum_{i=0}^{d-1} \binom{n}{i}$ and similarly the rank of the system of equations $E_{x,d-1}$ where $x \notin supp(f)$ equals $\sum_{i=0}^{d-1} \binom{n}{i}$. □

Open problem: deduce corollaries from these two propositions. ◇

5 Higher order nonlinearity and resistance to FAA

Shortly after the invention of algebraic attacks were found the fast algebraic attacks (FAA), which put an additional threat. The evaluation of the parameter $\min\{d_{alg}(g) + d_{alg}(fg);\ g \neq 0\}$, which is the main ingredient in the parameters quantifying the resistance to FAA (called fast algebraic complexity, FAC, and fast algebraic immunity, FAI, see [7]), is expensive in time. A nice result was found in [23] which showed that, for this parameter to have a sufficiently large value, the functions need to lie at large Hamming distance from low algebraic degree Boolean functions. This property is beneficial for a designer, since it allows him/her to avoid some constructions of Boolean functions which would inevitably be weak against fast algebraic attacks. It showed in particular that a construction from bent functions provided in [22] to further improve the nonlinearity of the function proposed in [8] was not satisfactory (while the function from [8] itself is satisfactory from this viewpoint as well). But as shown in [7], the proof in [23] has several shortcomings and the result itself seems false. In the present section, we briefly recall the corrected proof and take this opportunity to present it in a slightly simpler way. We refer to [7] for more details.

Theorem 2 *For any positive integer n and any non-negative integer $r \leq n$, let f be any n-variable function and $k = \min\{d_{alg}(g) + d_{alg}(fg);\ g \neq 0\}$. We have*

then:

$$nl_r(f) \geq \sum_{i=0}^{\lfloor \frac{k-r-1}{2} \rfloor} \binom{n}{i}.$$

Proof. We prove the result by contradiction and suppose then that $nl_r(f) < \sum_{i=0}^{\lfloor \frac{k-r-1}{2} \rfloor} \binom{n}{i}$. By definition, there exists a Boolean function h of algebraic degree at most r whose Hamming distance $w_H(f+h)$ to f equals $nl_r(f)$. The system of the $w_H(f+h)$ equations $E_{x,\lfloor \frac{k-r-1}{2} \rfloor}$ (see Section 4), where $x \in supp(f+h)$, has rank smaller than or equal to its number of equations and then strictly smaller than $\sum_{i=0}^{\lfloor \frac{k-r-1}{2} \rfloor} \binom{n}{i}$. There exists then a nonzero annihilator g of $f+h$ whose algebraic degree is at most $\lfloor \frac{k-r-1}{2} \rfloor$. We have then $fg = hg$ with $g \neq 0$ and $d_{alg}(g) + d_{alg}(fg) = d_{alg}(g) + d_{alg}(hg) \leq 2 \lfloor \frac{k-r-1}{2} \rfloor + r < k$, a contradiction. □

Acknowledgement: We thank Sihem Mesnager for useful indications.

References

[1] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science* 765, pp. 65-76, 1994.

[2] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions. *IEEE Transactions on Information Theory* 52 (9), pp. 4160-4170, 2006.

[3] L. Budaghyan. *Construction and Analysis of Cryptographic Functions*. 168 pages. Springer 2014, ISBN 978-3-319-12990-7

[4] L. Budaghyan, C. Carlet, T. Helleseth, N. S. Kaleyski. On the Distance Between APN Functions. *IEEE Transactions on Information Theory* 66(9), pp. 5742-5753, 2020.

[5] M. Calderini. Differentially low uniform permutations from known 4-uniform functions. *Designs, Codes and Cryptography*, pp.1-20, 2020.

[6] C. Carlet. On the higher order nonlinearities of algebraic immune functions. *Proceedings of CRYPTO 2006, Lecture Notes in Computer Science* 4117, pp. 584-601, 2006.

[7] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 562 pages, 2021.

[8] C. Carlet and K. Feng. An infinite class of balanced functions with optimum algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. *Proceedings of ASIACRYPT 2008, Lecture Notes in Computer Science* 5350, pp. 425-440, 2008.

[9] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2005/441, 2005.

[10] M. Lobanov. Exact relation between nonlinearity and algebraic immunity. *Discrete Mathematics and Applications* 16 (5), pp. 453-460, 2006.

[11] M. Lobanov. Tight bounds between algebraic immunity and nonlinearities of high orders. *NATO Science for Peace and Security Series - D: Information and Communication Security*, Vol 18: Boolean Functions in Cryptology and Information Security, IOS Press, pp. 296-306, 2008 and *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2007/444, 2007 and *Journal of Applied and Industrial Mathematics* 3 (3), pp. 367-376, 2009 (title: Exact relations between nonlinearity and algebraic immunity) and private communication.

[12] M. Lobanov. A method for obtaining lower bounds on the higher order nonlinearity. *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2013/332, 2013.

[13] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, North Holland. 1977.

[14] S. Mesnager. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. *IEEE Transactions on Information Theory* 54 (8), pp. 3656-3662, 2008. Preliminary version available in *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2007/117, 2007.

[15] K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT 1991, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[16] K. Nyberg. On the construction of highly nonlinear permutations. *Proceedings of EUROCRYPT 1992, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.

[17] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.

[18] K. Nyberg. New bent mappings suitable for fast implementation. *Proceedings of Fast Software Encryption FSE 1993, Lecture Notes in Computer Science* 809, pp. 179-184, 1994.

[19] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption FSE 1994, Lecture Notes in Computer Science* 1008, pp. 111-130, 1995.

[20] K. Nyberg. Multidimensional Walsh transform and a characterization of bent functions. *Proceedings of the IEEE Information Theory Workshop ITW 2007*, Bergen, Norway, pp. 1-4, 2007.

[21] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. *Journal of Cryptology* 8(1), pp. 27-37, 1995, (extended version of the *Proceedings of CRYPT0' 92, Lecture Notes in Computer Science* 740, pp. 566-574, 1993).

[22] Z. Tu and Y. Deng. A conjecture on binary string and its applications on constructing Boolean functions of optimal algebraic immunity. *Designs, Codes and Cryptography* 60 (1), pp. 1-14, 2011.

[23] Q. Wang and T. Johansson. A note on fast algebraic attacks and higher order nonlinearities. *Proceedings of Information Security and Cryptology INSCRYPT 2010, Lecture Notes in Computer Science* 6584, pp. 84-98, 2010.

[24] Y. Wang, W.G. Zhang and Z. Zha. Low differentially uniform permutations from Dobbertin APN function over $\mathbb{F}_{2^n}$. Preprint, 2021, https://arxiv.org/abs/2103.10687 .