Handling vectorial functions by means of their graph indicators

Claude Carlet,
University of Bergen, Norway; University of Paris 8, France.

E-mail: claude.carlet@gmail.com

Abstract

We characterize the ANF and the univariate representation of any vectorial function as parts of the ANF and bivariate representation of the Boolean function equal to its graph indicator. We show how this provides, when F is bijective, the expression of F^{-1} and/or allows deriving properties of F^{-1}. We illustrate this with examples and with a tight upper bound on the algebraic degree of F^{-1} by means of that of F. We characterize by the Fourier-Hadamard transform, by the ANF, and by the bivariate representation, that a given Boolean function is the graph indicator of a vectorial function. We also give characterizations of those Boolean functions that are affine equivalent to graph indicators. We express the graph indicators of the sum, product, composition and concatenation of vectorial functions by means of the graph indicators of the functions. We deduce from these results a characterization of the bijectivity of a generic (n, n)-function by the fact that some Boolean function, which appears as a part of the ANF (resp. the bivariate representation) of its graph indicator, is equal to constant function 1. We also address the injectivity of (n, m)-functions. Finally, we study the characterization of the almost perfect nonlinearity of vectorial functions by means of their graph indicators.

1 Introduction

The graphs of functions play an important role in coding theory: a code (i.e. a set of vectors of a same length n over some finite field $\mathbb{F}_q$), linear (that is, having the structure of a vector space) or not, is called systematic if, up to a reordering of the codeword coordinates, it has the form of the graph $\mathcal{G}_F = \{(x, F(x)); x \in \mathbb{F}_q^k\}$ of a function F from $\mathbb{F}_q^k$ to $\mathbb{F}_q^{n-k}$ for some k (equal to the dimension when the code is linear). All linear codes are systematic and most important nonlinear codes such as the Kerdock, Preparata and Delsarte-Goethals codes are systematic [12]. Graphs also play a significant role in symmetric cryptography, in the diffusion layers and substitution boxes of block

ciphers. This role is essentially hidden in the latter case, but it is actual. For instance, the Walsh transform of a vectorial function F, which plays a central role in the determination of its nonlinearity, equals by definition the Fourier-Hadamard transform of the indicator (i.e. characteristic function) of its graph $\mathcal{G}_F = \{(x, F(x));\ x \in \mathbb{F}_2^n\}$ (that we call the graph indicator of the function). The CCZ equivalence of vectorial functions is also defined by means of their graphs, see e.g. [5]. A notion of algebraic immunity of vectorial functions is directly related to graph indicators as well, see [1, 6]. The important notion of almost perfect nonlinearity is naturally defined by means of the graphs of functions. And graph indicators play roles in recent advances of cryptography, such as counter-measures against side channel attacks; see for instance, in [13, 8, 10, 9], the leakage squeezing method and the related codes, called complementary information set (CIS) codes. Moreover, looking at these graphs helps simplifying some studies on vectorial functions. For instance, the graph of a permutation and the graph of its compositional inverse are equal, up to variable swap; the indicators are then the same function up to this swap, while computing the expression of the compositional inverse of a permutation from that of the function is complex (there are only few known classes of permutation polynomials whose compositional inverses are also known).

As we can see, it seems then useful to consider with more attention the graph indicators of vectorial functions. In fact, we shall see that it is often profitable to view (n, m)-functions through their graph indicators. This increases the number of variables from n to $n + m$, but it replaces the study of a vectorial function by that of a Boolean function. In terms of data complexity, the ANF of the graph indicator of an (n, m)-function involves 2^{n+m} bits and is then larger than the ANF of the function, which involves $m \cdot 2^n$ bits. The ratio is still larger for polynomial representations. This is the price to pay for having a representation including more information, as we shall show. It will be illustrated in this paper that we can recover the initial investment of calculating the ANF or the bivariate representation of the graph indicator, when we address compositional inverses (when they exist) and composition. Indeed, as we already mentioned, inversion just corresponds to a swap of variables in the graph indicator, and we shall see that composition can be implemented with graph indicators by simple additions and multiplications. Note that inversion and composition play central roles in block ciphers, since deciphering needs, for many ciphers, to invert functions, and composition is the main tool in iterative ciphers for reaching a sufficient confusion.

The paper is organized as follows. After preliminaries, we express in Section 3 the ANF and the numerical normal form (NNF) of the indicator $1_{\mathcal{G}_F}$ of the graph $\mathcal{G}_F = \{(x, F(x));\ x \in \mathbb{F}_2^n\}$ of any vectorial function F by means of the ANF and the NNF of (the coordinate functions of) the function. We also address the bivariate (polynomial) representation. We show that more information, directly exploitable, is contained in these representations of the graph indicator than in those of the function itself. When the function is bijective (i.e. one to one and onto), we characterize the ANF, respectively the univariate representation, of the compositional inverse as a part of the ANF of the

graph indicator (respectively, of its bivariate representation); this allows often to obtain an explicit (but maybe complex) expression of F^{-1}, without having to solve the equation $F(x) = y$ algebraically. We study this expression more in detail in the case of linear permutations. A lot of (future) work is probably feasible with this approach, revisiting the known (nonlinear) permutations. We study an example showing how this works in practice. Moreover, we observe that, even when $F^{-1}(y)$ cannot be explicitly calculated, results on F^{-1} can be directly deduced from the graph indicator approach; for instance, the inverse of a permutation of algebraic degree d has always algebraic degree at most $\left\lceil \frac{(d-1)n+2}{d} \right\rceil - 1$ (which equals $\lceil \frac{n}{2} \rceil$ for a quadratic permutation). We complete the section by studying more in detail the case of the multiplicative inverse functions, used as substitution box in the AES. In Section 4, we characterize by the Fourier-Hadamard transform, by the ANF and by the bivariate representation, the fact that a given $(n+m)$-variable Boolean function is the graph indicator of an (n,m)-function. We characterize in Section 5 the fact that a given $(n+m)$-variable Boolean function is affine equivalent to such graph indicator. We address in Section 6 the main operations (addition, multiplication, composition, concatenation, and an operation related to the so-called switching method) in terms of graph indicators. In Section 7, we obtain a rather simple characterization of bijectivity (which plays an important role in all domains, particularly in cryptography) by the fact that some Boolean function which appears as a part of its graph indicator equals the constant function 1. We specify the expression of this Boolean function by means of that of the function. In Section 8, we address injectivity and find three characterizations. In Section 9, we characterize the almost perfect nonlinearity property in two different ways by means of the graph indicator.

2 Preliminaries

In this paper, we denote the additions in $\mathbb{F}_2$ by $\oplus$ and those in $\mathbb{R}$ by $+$, so as to distinguish when the addition is made modulo 2 and when it is not. We shall simply use $+$ for the addition in $\mathbb{F}_2^n$ since there will never be ambiguity[1]. We shall denote by 0 the zero vector in any of the vector spaces over $\mathbb{F}_2$. We call n-variable Boolean function every function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and support of a Boolean function f the set $supp(f) = \{x \in \mathbb{F}_2^n;\ f(x) = 1\}$, while the support of a vector $x \in \mathbb{F}_2^n$ equals $\{i \in \{1, \ldots, n\}; x_i = 1\}$. The Hamming weight $w_H(f)$ of a Boolean function f (or of a vector) equals the size of its support. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n,m)-*function*s. Such function F being given, the n-*variable* Boolean functions $f_1, \ldots, f_m$, defined at every $x \in \mathbb{F}_2^n$ by $F(x) = (f_1(x), \ldots, f_m(x))$, are called the *coordinate functions* of F. When the numbers m and n are not specified, (n,m)-functions are called *vectorial Boolean functions* or simply *vectorial functions*. Those ones whose role is to

[1] Only additions modulo 2 will be performed, and since we shall sometimes identify $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, in which the addition is denoted by $+$, it seems natural to write $+$ as well in the case of $\mathbb{F}_2^n$.

ensure confusion in a block cipher are called *substitution boxes* (*S-boxes*). We refer to e.g. [4, 5] for a more complete state of the art.

Two vectorial functions F and G are called affine equivalent if there exist two affine permutations L over $\mathbb{F}_2^m$ and L' over $\mathbb{F}_2^n$ such that $G = L \circ F \circ L'$; they are called EA equivalent if there exists an affine function L from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ such that F and $G+L$ are affine equivalent; and they are called CCZ equivalent if their graphs $\mathcal{G}_F = \{(x, F(x));\ x \in \mathbb{F}_2^n\}$ and $\mathcal{G}_G = \{(x, G(x));\ x \in \mathbb{F}_2^n\}$ are affine equivalent in the sense that one is the image of the other by an affine permutation over $\mathbb{F}_2^{n+m}$. These three notions of equivalence are by increasing order of generality.

Among the classical representations of Boolean functions and of vectorial functions are the *truth-table* in the case of Boolean functions and the *look-up table* (LUT) in the case of vectorial functions. Both are the table of all pairs of an element of $\mathbb{F}_2^n$ (an ordering of $\mathbb{F}_2^n$ being fixed) and of the value of the function at this input. The *algebraic normal form* (in brief the *ANF*), which contains a little more information directly usable on the cryptographic strengths of functions, is the unique n-variable multivariate polynomial representation of the form

$$f(x) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I \, x^I, \tag{1}$$

where a_I belongs to $\mathbb{F}_2$ in the case of Boolean functions and to $\mathbb{F}_2^m$ in the case of (n,m)-functions (and where "x^I" is a notation that we shall use all along this paper). Note that we can deduce the ANF of the i-th coordinate function of F by replacing in (1) each coefficient $a_I \in \mathbb{F}_2^m$ by its i-th coordinate.
The degree of the ANF shall be denoted by $d_{alg}(f)$ (resp. $d_{alg}(F)$); it is called the *algebraic degree* of the function and equals $\max\{|I|;\ a_I \neq 0\}$, where $|I|$ denotes the size of I (with the convention that the zero function has algebraic degree 0). This makes sense thanks to the existence and uniqueness of the ANF. Note that the algebraic degree of an (n,m)-function F equals the maximal algebraic degree of its coordinate functions. It also equals the maximal algebraic degree of its *component functions*, that is, of the nonzero linear combinations over $\mathbb{F}_2$ of the coordinate functions, *i.e.* the functions of the form $v \cdot F$, where $v \in \mathbb{F}_2^m \setminus \{0\}$ and "$\cdot$" is an inner product in $\mathbb{F}_2^m$. It is an affine invariant (that is, its value does not change when we compose F, on the right or on the left, by an affine automorphism). We have:

$$f(x) = \bigoplus_{I \subseteq supp(x)} a_I, \tag{2}$$

which is valid for Boolean and vectorial functions, and where $supp(x)$ denotes the support of x.
The converse is also true: for all $I \subseteq \{1, \ldots, n\}$, we have:

$$a_I = \bigoplus_{x \in \mathbb{F}_2^n;\ supp(x) \subseteq I} f(x), \tag{3}$$

for f Boolean or vectorial. According to Relation (3), we have the well known property (see [12, 4]):

Proposition 1 *An n-variable Boolean function f satisfies $d_{alg}(f) = n$ if and only if $w_H(f)$ is odd.*

We call *quadratic* the functions of algebraic degree at most 2.
The ANF, because it lives in characteristic 2, is rather unsuitable for working on those cryptographic parameters which live in characteristic 0 (such as the Hamming weight, the nonlinearity), and on some other notions such as the almost perfect nonlinearity (see below). A representation similar to the ANF, see e.g. [4], but over the reals (over $\mathbb{Z}$ when dealing with Boolean functions) contains all the information given by the ANF and lives in characteristic 0. It is called the *numerical normal form* (NNF). Every pseudo-Boolean function φ (from $\mathbb{F}_2^n$ to $\mathbb{R}$), and in particular, every Boolean function considered as valued in $\{0,1\} \subset \mathbb{Z}$, has a unique representation in the form

$$f(x) = \sum_{I \subseteq \{1,\ldots,n\}} \lambda_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq \{1,\ldots,n\}} \lambda_I \, x^I; \quad \lambda_I \in \mathbb{R}, \tag{4}$$

($\lambda_I \in \mathbb{Z}$ if f is integer-valued), where the addition is in $\mathbb{R}$.

The ANF of vectorial functions and the NNF of their coordinate functions are not always convenient for designing functions satisfying the desired cryptographic criteria. The so-called *univariate representation* of an (n,n)-function is in some cases a more successful representation, obtained after identification between the vector space $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$: the latter, being an n-dimensional vector space over $\mathbb{F}_2$, it can be endowed with a basis $(e_1, \ldots, e_n)$ and x is then represented by $\sum_{j=1}^{n} x_j e_j$ that we still denote by x. Then (see e.g. [5]) there is a unique representation of F in the form

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

with $a_i \in \mathbb{F}_{2^n}$. This representation can be obtained by Lagrange's interpolation, which in this framework can be simplified as follows: since the function x^{2^n-1} takes value 1 at any nonzero input and the *Dirac (or Kronecker)* function over $\mathbb{F}_{2^n}$ (i.e. $\delta_0(x) = \begin{cases} 1 \text{ if } x = 0 \\ 0 \text{ otherwise} \end{cases}$) equals then $1 + x^{2^n-1}$, we have $F(x) = \sum_{a \in \mathbb{F}_{2^n}} F(a)(1 + (x+a)^{2^n-1})$. The algebraic degree of $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ equals the maximum 2-weight of the exponents i such that $a_i \neq 0$, where the 2-weight is the Hamming weight of the binary expansion (see e.g. [5]). If F is bijective as a function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^n}$, then $\sum_{i=0}^{2^n-1} a_i x^i$ is called a *permutation polynomial*.
Note that for every divisor m of n (for instance, for $m = 1$), an (n,m)-function can be viewed as a particular (n,n)-function, since $\mathbb{F}_{2^m}$ is a subfield of $\mathbb{F}_{2^n}$.
The equivalent of Proposition 1 for the univariate representation is:

Proposition 2 *For every (n,n)-function F, we have $\sum_{x\in\mathbb{F}_{2^n}} F(x) \neq 0$ if and only if $d_{alg}(F) = n$.*

Indeed, we have $\sum_{x\in\mathbb{F}_{2^n}} x^i = \begin{cases} 0 \text{ if } i \leq 2^n-2 \\ 1 \text{ if } i = 2^n-1 \end{cases}$.

If n is even, any $(n,n/2)$-function, viewed as a function from $\mathbb{F}_{2^{n/2}}^2$ to $\mathbb{F}_{2^{n/2}}$, can also be represented in bivariate form $\sum_{0\leq i,j\leq 2^{n/2}-1} a_{i,j}x^i y^j$, where $a_{i,j} \in \mathbb{F}_{2^{n/2}}$. We shall use the term of *polynomial representation* to globally denominate univariate and bivariate representations.

The *Fourier-Hadamard transform* of any pseudo-Boolean function φ (from $\mathbb{F}_2^n$ to $\mathbb{R}$) is the $\mathbb{R}$-linear mapping which maps φ to the function $\widehat{\varphi}$ defined on $\mathbb{F}_2^n$ by

$$\widehat{\varphi}(u) = \sum_{x\in\mathbb{F}_2^n} \varphi(x)\,(-1)^{u\cdot x}, \tag{5}$$

where "$\cdot$" is some chosen inner product in $\mathbb{F}_2^n$. It satisfies the so-called *inverse Fourier-Hadamard transform formula*: for all $a \in \mathbb{F}_2^n$, we have:

$$\sum_{u\in\mathbb{F}_2^n} \widehat{\varphi}(u)\,(-1)^{u\cdot a} = 2^n\varphi(a),$$

which proves that the Fourier-Hadamard transform is a bijection. And defining the convolutional product of two pseudo-Boolean functions φ and ψ as $(\varphi\otimes\psi)(x) = \sum_{a\in\mathbb{F}_2^n}\varphi(a)\psi(x+a)$, we have $\widehat{\varphi\otimes\psi} = \widehat{\varphi}\times\widehat{\psi}$.
If L is an $\mathbb{F}_2$-linear automorphism of $\mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$, and if L' is the adjoint operator of L^{-1}, defined by $L'(u)\cdot x = u\cdot L^{-1}(x)$ and whose matrix is the transpose of that of L^{-1}, the Fourier-Hadamard transform $\widehat{\varphi'}(u) = \sum_{x\in\mathbb{F}_2^n}\varphi'(x)\,(-1)^{u\cdot x}$ of the function $\varphi'(x) = \varphi(L(x)+a)$ is equal to $\sum_{x\in\mathbb{F}_2^n}\varphi(x)\,(-1)^{u\cdot L^{-1}(x+a)} = (-1)^{u\cdot L^{-1}(a)}\sum_{x\in\mathbb{F}_2^n}\varphi(x)\,(-1)^{L'(u)\cdot x} = (-1)^{L'(u)\cdot a}\,\widehat{\varphi}(L'(u))$.

Given an n-variable Boolean function f, we have two associated transforms: the Fourier-Hadamard transform of f, where f is then viewed as a function from $\mathbb{F}_2^n$ to $\{0,1\}$, and the *Walsh transform* of f which is the Fourier-Hadamard transform of the sign function $(-1)^f$:

$$W_f(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus u\cdot x}.$$

We have:

$$W_f = 2^n\,\delta_0 - 2\widehat{f}, \tag{6}$$

where δ_0 denotes the already encountered Dirac (or Kronecker) symbol over $\mathbb{F}_2^n$ (the ANF of $\delta_0(x)$ equals $\prod_{i=1}^n(x_i\oplus 1)$). There are relations between the coefficients λ_I of the NNF and the values of the Walsh transform, see e.g. [4].

For vectorial functions, we define the Walsh transform as follows, after choosing an inner product in $\mathbb{F}_2^n$ and an inner product in $\mathbb{F}_2^m$ (that we shall both denote

by "$\cdot$"):

$$W_F(u,v) = W_{v\cdot F}(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)\oplus u\cdot x};\ u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m.$$

An (n,n)-function F is called almost perfect nonlinear (APN) if, for every nonzero $a\in\mathbb{F}_2^n$ and every $b\in\mathbb{F}_2^n$, the equation $D_aF(x) = F(x)+F(x+a) = b$ has at most two solutions in $\mathbb{F}_2^n$, that is, has either two solutions or none (see [15, 2, 16, 7]). Function D_aF is called a *derivative* of F. APN functions contribute optimally to the resistance against differential attacks when they are used as S-boxes in block ciphers.

We call *graph indicator* of an (n,m)-function F the indicator (i.e. the characteristic function) $1_{\mathcal{G}_F}$ of the graph $\mathcal{G}_F = \{(x,F(x));\ x\in\mathbb{F}_2^n\}$. We have $1_{\mathcal{G}_F}(x,y) = 1$ if $F(x) = y$ and $1_{\mathcal{G}_F}(x,y) = 0$ otherwise. Note that for every $z\in\mathbb{F}_2^m$, the size $|F^{-1}(z)|$ of the pre-image of z by F equals the Hamming weight of the Boolean function $x\mapsto 1_{\mathcal{G}_F}(x,z)$ and that two (n,m)-functions F and G are equal to each other if and only if $1_{\mathcal{G}_F}(x,G(x))$ equals constant Boolean function 1; more precisely, the Hamming distance between F and G equals the complement to 2^n of the Hamming weight of $1_{\mathcal{G}_F}(x,G(x))$.
The Walsh transform of F equals the Fourier-Hadamard transform of $1_{\mathcal{G}_F}$, where the chosen inner product is $(x,y)\cdot(u,v) = x\cdot u\oplus y\cdot v$. Then, for all $(u,v)\neq(0,0)$, we have:

$$W_F(u,v) = -\frac{1}{2}W_{1_{\mathcal{G}_F}}(u,v),$$

and we have:

$$W_F(0,0) = 2^{2n-1} - \frac{1}{2}W_{1_{\mathcal{G}_F}}(0,0) = 2^n.$$

The nonlinearity of an (n,m)-function equals the minimum Hamming distance between its component functions $v\cdot F$, $v\neq 0$, $v\in\mathbb{F}_2^m$, and affine functions $a\cdot x\oplus\epsilon$, $a\in\mathbb{F}_2^n, \epsilon\in\mathbb{F}_2$. It equals $2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m, v\neq 0}|W_F(u,v)|$. Despite the relation between the Walsh transform of F and the Fourier-Hadamard transform of $1_{\mathcal{G}_F}$, the nonlinearity of F is not connected to the nonlinearity of $1_{\mathcal{G}_F}$, because of the case $u = v = 0$ which is excluded in the definition of the former and included in that of the latter; for $m\geq 2$, the nonlinearity of any graph indicator equals its Hamming weight 2^n because the nearest affine function is always the zero function.

Remark. The present paper focusses on the characterization by graph indicators of the properties of (n,m)-functions. It would be also interesting, *vice versa*, to study the properties of $1_{\mathcal{G}_F}$ by means of F. For instance, according to the so-called Xiao-Massey characterization of correlation immunity by the Fourier-Hadamard transform (see e.g. [4]), $1_{\mathcal{G}_F}$ is t-th order correlation immune if and only if $\widehat{1_{\mathcal{G}_F}}(u,v) = W_F(u,v)$ equals 0 for every non-zero $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^m$ of Hamming weight at most t. This is equivalent to the fact that $W_F(u,v) = 0$, for every (u,v) of Hamming weight at most t such that v is non-zero, that is, for every non-zero $v\in\mathbb{F}_2^m$, the component function $v\cdot F$ is $(t-w_H(v))$-th order

resilient. The study of such functions has been made for permutations (which play a role with respect to leakage squeezing, see the introduction) from the viewpoint of codes in [10]. The general case remains to be studied. Another example of possible study is that of the algebraic immunity of graph indicators, see [6]. □

3 ANF, NNF and bivariate representation of the graph indicator of a vectorial function

The purpose of this section is to express the two main representations of graph indicators (their ANF and their bivariate representation) by means of the corresponding representations of the vectorial functions, in a way as efficient as possible for future applications.

3.1 General case

3.1.1 ANF and NNF

Relation (3) applied to $1_{\mathcal{G}_F}$ gives that, for every $I \subseteq \{1,\dots,n\}$ and $J \subseteq \{1,\dots,m\}$, the coefficient of $x^I y^J$ in its ANF equals:

$$a_{I,J} = |\{x \in \mathbb{F}_2^n;\ supp(x) \subseteq I \text{ and } supp(F(x)) \subseteq J\}| \text{ [mod 2]}. \tag{7}$$

Note that, if F is monotone, in the sense that, for every $x, z \in \mathbb{F}_2^n$, the inclusion "$supp(x) \subseteq supp(z)$" implies the inclusion "$supp(F(x)) \subseteq supp(F(z))$", then for every $z \in \mathbb{F}_2^n$ and every $I \subseteq \{1,\dots,n\}$ and $J \subseteq \{1,\dots,m\}$ such that $I \subseteq supp(z)$ and $supp(F(z)) \subseteq J$, we have $a_{I,J} = |\{x \in \mathbb{F}_2^n;\ supp(x) \subseteq I\}|$ [mod 2] $= 2^{|I|}$ [mod 2] $= \begin{cases} 1 \text{ if } I = \emptyset \\ 0 \text{ otherwise.} \end{cases}$

But for general functions, Relation (7) is not quite easily exploitable. We shall give now a formula which sheds more light on the ANF of $1_{\mathcal{G}_F}$ (and allows to recover Relation (7)):

Proposition 3 *Let F be any (n,m)-function and let $f_1,\dots,f_m$ be its coordinate functions. We have:*

$$1_{\mathcal{G}_F}(x,y) = \prod_{j=1}^{m}(y_j \oplus f_j(x) \oplus 1) = \bigoplus_{J \subseteq \{1,\dots,m\}} \varphi_{F,J}(x)\, y^J, \tag{8}$$

where

$$\varphi_{F,J}(x) = \prod_{j \in J^c} (f_j(x) \oplus 1), \tag{9}$$

with $J^c = \{1,\dots,m\} \setminus J$.

Indeed, for every $y, y' \in \mathbb{F}_2^m$, we have $y = y'$ if and only if $\prod_{j=1}^m (y_j \oplus y'_j \oplus 1) = 1$. This, with $y' = F(x)$, proves the first assertion and the rest is straightforward.

We can see that the information contained in the ANF of $1_{\mathcal{G}_F}$ is more complete than that contained in the ANF of F, since all the products of the (complemented) coordinate functions of F appear in it. Of course, the ANF of F allows to deduce all the information on F, thanks to the uniqueness of the representation, but this information is not directly readable. We shall see much more in the sequel.
Relation (9) shows that a part of the ANF of $1_{\mathcal{G}_F}$, precisely the one corresponding to $|J| = m-1$, gives the knowledge of all coordinate functions of F:

Corollary 1 *Let $F = (f_1, \ldots, f_m)$ be any (n,m)-function. Then, for every $j \in \{1, \ldots, m\}$, the x-dependent coefficient of $y^{\{1,\ldots,m\}\setminus\{j\}}$ in the ANF of $1_{\mathcal{G}_F}(x,y)$ equals $f_j(x) \oplus 1$.*

The following decomposition of $1_{\mathcal{G}_F}(x,y)$, which is alternative to the one given in Proposition 3:

$$1_{\mathcal{G}_F}(x,y) = \bigoplus_{I \subseteq \{1,\ldots,n\}} \psi_{F,I}(y)\, x^I, \tag{10}$$

will play a role when dealing with composite functions $G \circ F$ in Subsection 6.3. Note that, as $\varphi_{F,J}$, function $\psi_{F,I}$ is (the ANF of) a Boolean function.

Let us now address the NNF of graph indicators, which can be used as we shall see, for checking properties such as APNness and injectivity. To calculate it, we can, according to Proposition 3, first calculate the NNF of the function $\varphi_j(x,y) = y_j \oplus f_j(x) \oplus 1$. This can be easily calculated as follows: the equality $\varphi_j(x,y) = y_j \oplus f_j(x) \oplus 1$ is equivalent to $(-1)^{\varphi_j(x,y)} = (-1)^{y_j \oplus f_j(x) \oplus 1} = -(-1)^{y_j}(-1)^{f_j(x)}$, that is, since $\varphi_j(x,y)$, y_j and $f_j(x)$ are Boolean, to $1 - 2\varphi_j(x,y) = -(1-2y_j)(1-2f_j(x))$. Hence, the NNF of $\varphi_j(x,y)$ equals $1 - f_j(x) + y_j(2f_j(x)-1)$. We deduce:

Proposition 4 *Let F be any (n,m)-function and let $f_1, \ldots, f_m$ be its coordinate functions (given by their NNF). The NNF of $1_{\mathcal{G}_F}(x,y)$ equals:*

$$\prod_{j=1}^{m} \big(1 - f_j(x) + y_j(2f_j(x)-1)\big) = \sum_{J \subseteq \{1,\ldots,m\}} \phi_{F,J}(x)\, y^J,$$

where

$$\phi_{F,J}(x) = \prod_{j \in J^c} (1 - f_j(x)) \prod_{j \in J} (2f_j(x) - 1), \tag{11}$$

with $J^c = \{1, \ldots, m\} \setminus J$.

Remark. It is also possible to deduce the NNF from the ANF: starting from $1_{\mathcal{G}_F}(x,y) = \bigoplus_{I \subseteq \{1,\ldots,n\}, J \subseteq \{1,\ldots,m\}} a_{I,J}\, x^I y^J$, we can determine the (unique) coefficients $\lambda_{I,J} \in \mathbb{Z}$ such that $1_{\mathcal{G}_F}(x,y) = \sum_{I \subseteq \{1,\ldots,n\}, J \subseteq \{1,\ldots,m\}} \lambda_{I,J}\, x^I y^J$, by

writing:

$$1_{\mathcal{G}_F}(x,y) = \bigoplus_{I\subseteq\{1,\ldots,n\},J\subseteq\{1,\ldots,m\}} a_{I,J}\, x^I y^J \iff$$
$$(-1)^{1_{\mathcal{G}_F}(x,y)} = \prod_{I\subseteq\{1,\ldots,n\},J\subseteq\{1,\ldots,m\}} (-1)^{a_{I,J}\, x^I y^J} \iff$$
$$1 - 2\ 1_{\mathcal{G}_F}(x,y) = \prod_{I\subseteq\{1,\ldots,n\},J\subseteq\{1,\ldots,m\}} (1 - 2\ a_{I,J}\, x^I y^J) \qquad (12)$$

and expanding (12).
It is also possible to deduce the NNF of $1_{\mathcal{G}_F}$ from the Walsh transform of F: according to the results recalled in [4] as well, we have:

$$\lambda_{I,J} = 2^{-(n+m)}(-2)^{|I|+|J|} \sum_{\substack{u\in\mathbb{F}_2^n;\ I\subseteq supp(u)\\ v\in\mathbb{F}_2^m;\ J\subseteq supp(v)}} \widehat{1_{\mathcal{G}_F}}(u,v)$$
$$= 2^{-(n+m)}(-2)^{|I|+|J|} \sum_{\substack{u\in\mathbb{F}_2^n;\ I\subseteq supp(u)\\ v\in\mathbb{F}_2^m;\ J\subseteq supp(v)}} W_F(u,v). \qquad \square$$

3.1.2 Polynomial representation

We now address the bivariate representation of graph indicators. Given an (n,n)-function in univariate form, the graph indicator can be directly obtained, using the univariate representation of δ_0 seen in Section 2 and Lucas' theorem [12, page 404]:

Proposition 5 *Let F be any (n,n)-function given under its univariate representation. The bivariate representation of its graph indicator equals:*

$$1_{\mathcal{G}_F}(x,y) = 1 + (y + F(x))^{2^n-1} = 1 + \sum_{j=0}^{2^n-1} y^{2^n-1-j}(F(x))^j,$$

where this expression is calculated in $\mathbb{F}_{2^n}[x,y]/(x^{2^n}+x, y^{2^n}+y)$. Conversely, the univariate representation of $F(x)$ is obtained from $1_{\mathcal{G}_F}(x,y)$ as the x-dependent coefficient of y^{2^n-2}.

We shall write

$$1_{\mathcal{G}_F}(x,y) = \sum_{j=0}^{2^n-1} \varphi_{F,j}(x)\, y^j = \sum_{i=0}^{2^n-1} \psi_{F,i}(y)\, x^i. \qquad (13)$$

The reader should not confuse $\varphi_{F,j}$ and $\psi_{F,i}$ with the functions $\varphi_{F,J}$ of Proposition 3 and $\psi_{F,I}$ of Relation (10); the former are not even Boolean functions in general, except for $i,j \in \{0, 2^n-1\}$, while the latter are; the context and the second index will always specify unambiguously which function we are dealing with.

3.2 Case of a permutation

Assuming $m = n$, if F is a *permutation*, then we have:

$$1_{\mathcal{G}_F}(x, y) = 1_{\mathcal{G}_{F^{-1}}}(y, x), \tag{14}$$

where F^{-1} is the compositional inverse of F.

3.2.1 ANF

The coefficient of the monomial x^I in Relation (14) equals $\psi_{F,I}(y) = \varphi_{F^{-1},I}(y) = \prod_{i \in I^c}(f'_i(y) \oplus 1)$, where f'_i is the i-th coordinate function of F^{-1}. In particular:

Proposition 6 *Let F be any (n, n)-permutation. For every $i = 1, \ldots, n$, the i-th coordinate function f'_i of F^{-1} satisfies $f'_i(x) = \psi_{F,\{1,\ldots,n\}\setminus\{i\}}(y) \oplus 1$, where $\psi_{F,I}$ is defined by Relation (10).*

Hence, the knowledge of the ANF of $1_{\mathcal{G}_F}$ also gives direct information on F^{-1} while the ANF of F gives none. Proposition 6 provides an alternative way for calculating F^{-1}, without solving the equation $F(x) = y$ by algebraic methods. Of course, we need to know that F is a permutation, but there are methods which allow not solving equations, such as applying Hermite's criterion or using the characterization we shall obtain in Section 7.
Let us summarize, for future use. Relation (14) writes:

$$1_{\mathcal{G}_F}(x, y) = \prod_{j=1}^{n}(f_j(x) \oplus y_j \oplus 1) =$$

$$\bigoplus_{J \subseteq \{1,\ldots,m\}} y^J \prod_{j \in J^c}(f_j(x) \oplus 1) = \bigoplus_{I \subseteq \{1,\ldots,n\}} x^I \prod_{i \in I^c}(f'_i(y) \oplus 1) = \tag{15}$$

$$\prod_{i=1}^{n}(f'_i(y) \oplus x_i \oplus 1) = 1_{\mathcal{G}_{F^{-1}}}(y, x).$$

We shall see that F^{-1} plays an important role when dealing with composite functions $G \circ F$.

Remark. For any (n, m)-function F, we could consider the (m, n)-function F', playing the role of a pseudo-inverse of F, whose i-th coordinate function, for $i \in \{1, \ldots, n\}$, equals $\psi_{F,\{1,\ldots,n\}\setminus\{i\}} \oplus 1$, where $\psi_{F,I}$ is defined by Relation (10). When F is a permutation, then F' equals F^{-1}, according to Proposition 6. For general function F, considering such F' may or may not be of interest:
- It may happen that F' is constant (when, in the ANF of $1_{\mathcal{G}_F}(x, y)$, there is no term $x^I y^J$ with $|I| = n - 1$ and $|J| > 0$). This happens for instance when F is affine and there exist two pairs of complementary coordinate functions of F. Indeed, $f_{j_1} = f_{j_2} \oplus 1$ implies $(f_{j_1} \oplus 1)(f_{j_2} \oplus 1) = 0$, and for each term $x^I y^J$ with nonzero coefficient in $1_{\mathcal{G}_F}(x, y)$, the monomial x^I can come only from the products of at most $n-2$ coordinate functions of F and has then degree at most

$n-2$.
- Let $F=(f_1,\ldots,f_n,f_{n+1})$ be an $(n,n+1)$-function such that $\pi=(f_1,\ldots,f_n)$ is a permutation and f_{n+1} is the zero function. Let $f'_1,\ldots,f'_n$ be the coordinate functions of π^{-1}. Then we have, for every $x,y\in\mathbb{F}_2^n$ and $y_{n+1}\in\mathbb{F}_2$ that $1_{\mathcal{G}_F}(x,(y,y_{n+1}))=(y_{n+1}\oplus 1)\prod_{j=1}^n(y_j\oplus f_j(x)\oplus 1)=(y_{n+1}\oplus 1)\prod_{i=1}^n(x_i\oplus f'_i(y)\oplus 1)$ and $\psi_{F,\{1,\ldots,n\}\setminus\{i\}}(y,y_{n+1})\oplus 1$ equals $(y_{n+1}\oplus 1)(f'_i(y)\oplus 1)\oplus 1$. Then we have $F'(y,y_{n+1})=(y_{n+1}\oplus 1)\pi^{-1}(y)+y_{n+1}(1,\ldots,1)$. This is an extension of π^{-1} obtained by concatenating the look-up table of π^{-1} and the look-up table of the constant function $(1,\ldots,1)$.
- Take $F=(f_1,\ldots,f_{n-1})$ where the f_i's are the $n-1$ first coordinate functions of a permutation π, then for $x\in\mathbb{F}_2^n$ and $y\in\mathbb{F}_2^{n-1}$, we have $1_{\mathcal{G}_F}(x,y)=1_{\mathcal{G}_\pi}(x,(y,0))+1_{\mathcal{G}_\pi}(x,(y,1))=1_{\mathcal{G}_\pi}(x,(y,0))\oplus 1_{\mathcal{G}_\pi}(x,(y,1))=\prod_{i=1}^n(x_i\oplus f'_i(y,0)\oplus 1)\oplus\prod_{i=1}^n(x_i\oplus f'_i(y,1)\oplus 1)$. Then $\psi_{F,\{1,\ldots,n\}\setminus\{i\}}(y)\oplus 1$ equals $f'_i(y,0)\oplus f'_i(y,1)\oplus 1$, and $F'(y)$ equals the sum of $(1,\ldots,1)$ and of the restrictions of π^{-1} to the hyperplanes of equations $y_n=0$ and $y_n=1$.
- Let F be the monotone function such that, for every $j\in\{1,\ldots,n\}$, $f_j(x)=x^{I_j}$, where I_j is some subset of $\{1,\ldots,n\}$. Then $1_{\mathcal{G}_F}(x,y)=\prod_{j=1}^m(y_j\oplus x^{I_j}\oplus 1)$ and $\psi_{F,\{1,\ldots,n\}\setminus\{i\}}(y)\oplus 1$ equals:

$$1\oplus\bigoplus_{\substack{J\subseteq\{1,\ldots m\};\,\forall j\notin J,i\notin I_j\\ \text{and }\forall i'\neq i,\exists j\notin J;\,i'\in I_j}}\prod_{j\in J}(y_j\oplus 1).$$

We leave for future work the study of such functions and of other functions F' related to other "natural" classes of vectorial functions in ANF form. □

3.2.2 Polynomial representation

Assuming again that F is a permutation, we have:

$$1_{\mathcal{G}_F}(x,y)=1_{\mathcal{G}_{F^{-1}}}(y,x)=1+\sum_{j=0}^{2^n-1}x^{2^n-1-j}(F^{-1}(y))^j, \tag{16}$$

and we deduce:

Proposition 7 *Let F be an (n,n)-permutation. The univariate representation of $F^{-1}(y)$ equals the y-dependent coefficient of x^{2^n-2} in the bivariate representation of $1_{\mathcal{G}_F}(x,y)$.*

In the case of a power (i.e. monomial) function $F(x)=x^d$ over $\mathbb{F}_{2^n}$, with $\gcd(d,2^n-1)=1$, we have $1_{\mathcal{G}_F}(x,y)=1+\sum_{j=0}^{2^n-1}y^{2^n-1-j}x^{dj}$, and Proposition 7 only tells us that $F^{-1}(y)$ equals $y^{\frac{1}{d}}$ where $\frac{1}{d}$ is calculated in $\mathbb{Z}/(2^n-1)\mathbb{Z}$.

In the case of a linear permutation, represented by a linearized permutation polynomial $L(x)=\sum_{i=0}^{n-1}b_ix^{2^i}$, let us see that Proposition 7 allows to revisit a

well-known property, but also provides more information. The bivariate representation of $1_{\mathcal{G}_L}(x,y)$ equals $\sum_{j=0}^{2^n-1} y^{2^n-1-j}(\sum_{i=0}^{n-1} b_i x^{2^i})^j$. Writing the binary expansion of j in the form $j = \sum_{k\in J} 2^k$, with $J \subseteq \{0,\ldots,n-1\}$, we have $1_{\mathcal{G}_L}(x,y) = \sum_{J\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in J} 2^k} \prod_{k\in J}(\sum_{i=0}^{n-1} b_i^{2^k} x^{2^{k+i} \pmod n})$. Therefore, using Proposition 7, we can state:

Corollary 2 *Let $L(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$ be any linearized permutation polynomial over $\mathbb{F}_{2^n}$. Then we have:*

$$1_{\mathcal{G}_L}(x,y) = \sum_{J\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in J} 2^k} \sum_{\kappa\in\{0,\ldots,n-1\}^J} \left(\prod_{k\in J} b_{\kappa_k}^{2^k}\right) x^{\sum_{k\in J} 2^{k+\kappa_k} \pmod n},$$

and:

$$L^{-1}(y) = \sum_{J\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in J} 2^k} \sum_{\substack{\kappa\in\{0,\ldots,n-1\}^J \\ \sum_{k\in J} 2^{k+\kappa_k} \equiv 2^n-2 \pmod{2^n-1}}} \left(\prod_{k\in J} b_{\kappa_k}^{2^k}\right).$$

Note that for having $\sum_{k\in J} 2^{k+\kappa_k} \equiv 2^n - 2 \pmod{2^n-1}$, it is necessary that J has size $n-1$ (and that all the $k+\kappa_k \pmod n$ are distinct when k ranges over J), since $|J| \geq n-1$ is clearly necessary, and for $|J| = n$, that is, for $j = 2^n-1$, the exponent of y is 0 and the corresponding part in the whole polynomial $1_{\mathcal{G}_L}(x,y)$, that is, $1 + \sum_{j=0}^{2^n-1} x^{2^n-1-j}(L^{-1}(0))^j$ has no term in x^{2^n-2}, because $L^{-1}(0) = 0$. Since J has size $n-1$, the exponent of y is a power of 2 and the compositional inverse of a linearized permutation is then also a linearized polynomial, which is of course very well known. With Corollary 2, we have an explicit expression of $L^{-1}(y)$.

For general permutations, determining explicitly the compositional inverse is an open problem for a non-negligible part of known bijections. Let us give an example of how the graph indicator can be used:

Example. Dobbertin has shown that, for every m, the function $x^{2^{m+1}+1}+x^3+x$ is a permutation over $\mathbb{F}_{2^n}$, for $n = 2m+1$. We have, in $\mathbb{F}_2[x,y]/(x^{2^n}+x, y^{2^n}+y)$:

$$1_{\mathcal{G}_F}(x,y) = 1 + \sum_{j=0}^{2^n-1} y^{2^n-1-j}(x^{2^{m+1}+1} + x^3 + x)^j,$$

and denoting respectively by j_0 and j_1 the remainder and the quotient in the division of j by 2^m, we obtain:

$$1 + \sum_{j_0=0}^{2^m-1} \sum_{j_1=0}^{2^{m+1}-1} y^{2^m(2^{m+1}-j_1)-j_0-1}(x^{2^{m+1}+1} + x^3 + x)^{2^m j_1 + j_0} =$$

$$1 + \sum_{j_0=0}^{2^m-1} \sum_{j_1=0}^{2^{m+1}-1} y^{2^m(2^{m+1}-j_1)-j_0-1}(x^{3\cdot 2^m} + x^{2^m+1} + x^{2^m})^{j_1}(x^{2^{m+1}+1} + x^3 + x)^{j_0}.$$

This expression has degree $3\cdot 2^m(2^{m+1}-1)+(2^{m+1}+1)(2^m-1) = 2^{n+2}-2^{m+2}-1$ relative to x, and the only positive integers congruent with 2^n-2 modulo 2^n-1 and smaller than or equal to $2^{n+2}-2^{m+2}-1$ are 2^n-2, $2\cdot 2^n-3$ and $3\cdot 2^n-4$. Then, $F^{-1}(y)$ equals the sum of the y-dependent coefficients of $x^{2^m(2^{m+1}-1)+2^m-2}$, $x^{2^m(2\cdot 2^{m+1}-1)+2^m-3}$ and $x^{2^m(3\cdot 2^{m+1}-1)+2^m-4}$ in it. The expression is too complex for being given here, but it is explicit.

Even if, for a given permutation F, it is not possible to obtain an explicit expression of F^{-1}, the ANF or the univariate representation of the graph indicator can give useful information on F^{-1}, which can be exploited in proofs. We give an example in the next subsection.

Remark. Similarly with what we did with the ANF, we could consider, when F is a non-necessarily bijective (n,n)-function, the (n,n)-function F' whose univariate representation equals the y-dependent coefficient of x^{2^n-2} in the bivariate representation of $1_{\mathcal{G}_F}(x,y)$. There are important cases where such function has no interest. For instance, let $F(x)=x^d$ be a power function. Then according to Proposition 5, we have $F'(y) = \sum_{\substack{j\in\{1,\ldots,2^n-2\}\\ dj\equiv -1 \pmod{2^n-1}}} y^{2^n-1-j} = \sum_{\substack{j\in\{1,\ldots,2^n-2\}\\ dj\equiv 1 \pmod{2^n-1}}} y^j$. If F is not a permutation, then $\gcd(d,2^n-1)$ is strictly larger than 1 and divides $dj \pmod{2^n-1}$ for every $j\in\{1,\ldots,2^n-2\}$. Hence, $F'(y)=0$. We leave open the question of determining classes of non-bijective functions F presenting interest from coding theoretic or cryptographic viewpoint, and for which F' would also present such interest. □

3.3 Algebraic degree of the compositional inverse of a permutation

Let us illustrate further the power of the approach by graph indicators, by proving a general property of the inverses of permutations. This property concerns the algebraic degree, which we shall handle by the ANF (we could also use the univariate representation, since the algebraic degree is directly readable on this representation as well). Applying Corollary 1 to $1_{\mathcal{G}_{F^{-1}}}(y,x) = 1_{\mathcal{G}_F}(x,y)$, we have $d_{alg}(F^{-1}) \leq d$ if and only if all terms x^Iy^J such that $|I| = n-1$ and $|J| > d$ in the ANF of $1_{\mathcal{G}_F}(x,y)$ have null coefficient, that is (since no term in $x^{\{1,\ldots,n\}}y^J$ exists with $|J|\geq 1$ in the ANF of $1_{\mathcal{G}_{F^{-1}}}(y,x)$): for every $J\subseteq\{1,\ldots,n\}$, we have that $|J|>d$ implies $d_{alg}(\prod_{j\in J^c}(f_j(x)\oplus 1)) \leq n-2$, or equivalently, by replacing J by its complement:

Proposition 8 *Let F be any (n,n)-permutation and let $f_1,\ldots,f_n$ be its coordinate functions. The algebraic degree of F^{-1} is bounded above by d if and only if, for all $J\subseteq\{1,\ldots,n\}$, we have:*

$$\Big(|J|\leq n-d-1\Big) \Longrightarrow \Big(d_{alg}\Big(\prod_{j\in J} f_j(x)\Big)\leq n-2\Big).$$

Moreover, using the right-hand side of Relation (15), if $d_{alg}(F^{-1}) \leq d$, then all the terms $x^I y^J$ such that $|I| \geq n-k$ and $|J| > kd$ in $1_{\mathcal{G}_F}(x,y) = 1_{\mathcal{G}_{F^{-1}}}(y,x)$ have null coefficient, since each product of at most k coordinate functions of F^{-1} has algebraic degree at most kd. Hence, using now the left-hand side of Relation (15), $|J| > kd$ implies $d_{alg}\left(\prod_{j\in J^c} f_j(x)\right) \leq n-k-1$. Changing J into its complement shows that, if $d_{alg}(F^{-1}) \leq d$, then:

$$|J| \leq n-kd-1 \Longrightarrow d_{alg}\left(\prod_{j\in J} f_j(x)\right) \leq n-k-1.$$

Changing now F into F^{-1}, taking $k = \lfloor \frac{n-2}{d} \rfloor$ (which is the largest value ensuring $n-kd-1 \geq 1$ and for which $n-k-1 = \left\lceil \frac{(d-1)n+2}{d} \right\rceil - 1$), and $|J| = 1$, we have then:

Corollary 3 *Let n and $1 \leq d \leq n-1$ be two positive integers. For every (n,n)-permutation F of algebraic degree at most d, we have:*

$$d_{alg}(F^{-1}) \leq \left\lceil \frac{(d-1)n+2}{d} \right\rceil - 1.$$

In particular, if F is quadratic, then $d_{alg}(F^{-1}) \leq \lceil \frac{n}{2} \rceil$.

This bound is tight since we know that the inverse of the Gold APN permutation x^{2^j+1}, with $\gcd(j,n) = 1$, n odd, has algebraic degree $\frac{n+1}{2}$, see [16], and since the inverse of an affine permutation ($d = 1$) is affine.

3.4 Graph indicator of the multiplicative inverse function

The power function x^{2^n-2} over $\mathbb{F}_{2^n}$ (used with $n = 8$ as an S-box in the AES) is called the multiplicative inverse function because, for $x \neq 0$, it takes value $\frac{1}{x}$. It is worth a special look. According to Proposition 5, we have $1_{\mathcal{G}_F}(x,y) = 1 + (y + x^{2^n-2})^{2^n-1} = 1 + \sum_{j=0}^{2^n-1} x^{(2^n-2)(2^n-1-j)} y^j$. Hence, using that, if the exponent of x is nonzero and divisible by 2^n-1, we can replace it with 2^n-1 and otherwise, we can replace it with the remainder in its division by 2^n-1, we obtain $1_{\mathcal{G}_F}(x,y) = 1 + x^{2^n-1} + \sum_{j=1}^{2^n-2} x^{(2^n-2)(2^n-1-j)} y^j + y^{2^n-1}$, that is,

$$1_{\mathcal{G}_F}(x,y) = x^{2^n-1} + y^{2^n-1} + \sum_{j=0}^{2^n-2} (xy)^j, \tag{17}$$

which has algebraic degree $2\,n-2$. We have $1_{\mathcal{G}_F}(x,y) = 1_{\mathcal{G}_F}(y,x)$, which is coherent with the involutivity of F and the coefficient of x^{2^n-2} equals y^{2^n-2}, which illustrates Proposition 7.

4 Characterizations of the graph indicators of vectorial functions

In this section, we want to characterize those $(n+m)$-variable Boolean functions which are the graph indicators of (n,m)-functions. We have at least three reasons why we are interested by such a characterization. Firstly, these functions do play a role as we have seen, and deserve then to be clearly identified. Secondly, we anticipate that the study of graph indicators may allow finding more properties of vectorial functions themselves and of their combinations in the rounds of block ciphers in the future (we have seen a preliminary illustration in Subsection 3.3). Thirdly, this will allow us to characterize in Section 7 the graph indicators of permutations.

4.1 Characterization by the Fourier-Hadamard transform

A Boolean function h over $\mathbb{F}_2^n \times \mathbb{F}_2^m$ is the graph indicator of an (n,m)-function if and only if, for every $x \in \mathbb{F}_2^n$, there exists exactly one $y \in \mathbb{F}_2^m$ such that $h(x,y)=1$. This can be characterized by the Fourier-Hadamard transform:

Proposition 9 *Let n and m be any positive integers. A Boolean function h over $\mathbb{F}_2^n \times \mathbb{F}_2^m$ is the graph indicator of an (n,m)-function if and only if, for all $u \in \mathbb{F}_2^n$, its Fourier-Hadamard transform satisfies:*

$$\widehat{h}(u,0) = 2^n \, \delta_0(u).$$

Proof. For every $a, x \in \mathbb{F}_2^n$, the sum $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(a+x)}$ equals 2^n if $x=a$ and 0 otherwise. Then, the number of y such that $h(a,y)=1$ equals $2^{-n}\sum_{u,x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} h(x,y)(-1)^{u\cdot(a+x)} = 2^{-n}\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot a}\widehat{h}(u,0)$. Hence, h is the graph indicator of an (n,m)-function if and only if, for all $a \in \mathbb{F}_2^n$, its Fourier-Hadamard transform satisfies $\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot a}\widehat{h}(u,0) = 2^n$. This is equivalent to saying that the function $u \in \mathbb{F}_2^n \mapsto \widehat{h}(u,0)$ has for Fourier-Hadamard transform the constant function 2^n. Since this constant function equals the Fourier-Hadamard transform of $u \in \mathbb{F}_2^n \mapsto 2^n\delta_0(u)$, this proves the result, by the bijectivity of the Fourier-Hadamard transform. □

Denoting by F the (n,m)-function whose h is the graph indicator, $\widehat{h}$ equals the Walsh transform of F, and satisfies then also that, for all $a \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m$:

$$\sum_{u\in\mathbb{F}_2^n} \widehat{h}(u,v)(-1)^{a\cdot u} = 2^n(-1)^{v\cdot F(a)} \in \{-2^n, 2^n\}.$$

4.2 Characterization by the ANF

Let us use again that a function h is the indicator of the graph of some (n,m)-function if and only if, for every $x \in \mathbb{F}_2^n$, the Boolean function $y \mapsto h(x,y)$ is an atomic function (i.e. the indicator of a singleton), but characterize this by

means of the ANF. Any atomic function of y has the form $\prod_{j=1}^{m}(y_j \oplus \epsilon_j) = \bigoplus_{J\subseteq\{1,\ldots,m\}} \left(\prod_{j\in J^c} \epsilon_j\right) y^J$, where ϵ_j equals the coefficient of $y^{\{1,\ldots,m\}\setminus\{j\}}$. By uniqueness of the ANF, a Boolean function $g(y)$ given by its ANF $g(y) = \bigoplus_{J\subseteq\{1,\ldots,m\}} a_J\, y^J$, $a_J \in \mathbb{F}_2$, is then atomic if and only if, for every $J \subseteq \{1,\ldots,m\}$, we have $a_J = \prod_{j\in J^c} a_{\{1,\ldots,m\}\setminus\{j\}} = \prod_{\substack{K\subseteq\{1,\ldots,m\}\\ |K|=m-1, J\subseteq K}} a_K$ (with $a_{\{1,\ldots,m\}} = 1$). We deduce:

Proposition 10 *Let $h(x,y)$ be any $(n+m)$-variable Boolean function given by its ANF:*

$$h(x,y) = \bigoplus_{I\subseteq\{1,\ldots,n\}, J\subseteq\{1,\ldots,m\}} a_{I,J}\, x^I y^J = \bigoplus_{J\subseteq\{1,\ldots,m\}} h_{\varphi,J}(x)\, y^J.$$

Then, h is the indicator of the graph of some (n,m)-function if and only if, for all $J \subseteq \{1,\ldots,m\}$, we have:

$$h_{\varphi,J} = \prod_{\substack{K\subseteq\{1,\ldots,m\}\\ |K|=m-1, J\subseteq K}} h_{\varphi,K},$$

and the function $h_{\varphi,\{1,\ldots,m\}}$ equals constant function 1.

According to Proposition 3, the j-th coordinate function of the (n,m)-function F whose graph indicator equals h equals $f_j(x) = h_{\varphi,\{1,\ldots,m\}\setminus\{j\}} \oplus 1$.

4.3 Characterization by the bivariate representation

We shall similarly characterize by means of the bivariate representation the fact that a $2n$-variable function h is the indicator of the graph of some (n,n)-function. Given $x \in \mathbb{F}_{2^n}$, the Boolean function $y \mapsto h(x,y)$ is an atomic function if and only if it has the form $1+(y+u)^{2^n-1} = 1+\sum_{j=0}^{2^n-1} y^{2^n-1-j}u^j$. By uniqueness of the representation and u being the coefficient of y^{2^n-2}, a Boolean function $g(y)$ given by its univariate representation $g(y) = \sum_{j=0}^{2^n-1} a_j y^j$, $a_j \in \mathbb{F}_{2^n}$, is atomic if and only if: 1) $a_0 = 1 + (a_{2^n-2})^{2^n-1}$, 2) for every $j = 1,\ldots,2^n-2$, we have $a_{2^n-1-j} = (a_{2^n-2})^j$, and 3) $a_{2^n-1} = 1$. We deduce:

Proposition 11 *Let $h(x,y)$ be any $(n+m)$-variable Boolean function given by its bivariate form:*

$$h(x,y) = \sum_{i,j\in\{0,\ldots,2^n-1\}} a_{i,j}\, x^i y^j = \sum_{j\in\{0,\ldots,2^n-1\}} h_{\varphi,j}(x)\, y^j;\ a_{i,j} \in \mathbb{F}_{2^n}.$$

Then, h is the indicator of the graph of some (n,n)-function if and only if:

1) $h_{\varphi,0} = 1 + (h_{\varphi,2^n-2})^{2^n-1}$,
2) $\forall\, j \in \{1,\ldots,2^n-2\}$, $h_{\varphi,2^n-1-j} = (h_{\varphi,2^n-2})^j$,
3) $\forall x \in \mathbb{F}_{2^n}$, $h_{\varphi,2^n-1}(x) = 1$.

According to Proposition 5, the (n,n)-function F whose graph indicator equals h equals the x-dependent coefficient of y^{2^n-2} in $h(x,y)$.

5 Characterization of the Boolean functions affine equivalent to graph indicators

We need to characterize the functions $h(x,y)$ which are affine equivalent to a graph indicator because the affine equivalence of graph indicators corresponds to the important CCZ equivalence notion (see [7, 3]) recalled in Section 2. Proposition 9 is easily extended by affine equivalence:

Proposition 12 *Let n and m be any positive integers. A Boolean function h over $\mathbb{F}_2^n \times \mathbb{F}_2^m$ is affinely equivalent to the graph indicator of an (n,m)-function if and only if there exists an n-dimensional vector space on which its Fourier-Hadamard transform equals 0, except at the 0 point where it takes value 2^n.*

Indeed, according to what is recalled in Section 2 about the Fourier-Hadamard transform, if L is an $\mathbb{F}_2$-linear automorphism of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ and $a \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, and if L' is the adjoint operator of L^{-1} and $h'(x) = h(L(x)+a)$, we have $\widehat{h'}(u,v) = (-1)^{L'(u,v)\cdot a}\,\widehat{\varphi}(L'(u,v))$. The condition of Proposition 12 is then necessary (the n-dimensional space being $L'^{-1}(\mathbb{F}_2^n \times \{0\})$. Conversely, if the condition is satisfied, then up to affine equivalence, we may assume that this n-dimensional vector space equals $\mathbb{F}_2^n \times \{0\}$ and the condition is sufficient.

It seems difficult to extend the characterization of Proposition 10 or that of Proposition 11 by affine equivalence in an efficient way. Of course, we could write "there exists an affine automorphism L such that $h \circ L$ is a graph indicator" and use for instance that $(h \circ L)_{\varphi,J}(x) = \bigoplus_{supp(y)\subseteq J} h(L(x,y))$ for deducing a characterization from Proposition 10, but getting rid of "there exists" seems difficult.

Another characterization is possible, that is more complex but gives more information. According to Proposition 3, for every (n,m)-function F, function $1_{\mathcal{G}_F}(x,y)$ factorizes into the product of the m Boolean functions $h_j(x,y) = y_j \oplus f_j(x) \oplus 1$ which are $\mathbb{F}_2$-linearly independent. Denoting by e_j the j-th vector of the canonical basis of $\mathbb{F}_2^m$, we have $W_{h_j}(u,v) = \sum_{x\in\mathbb{F}_2^n, y\in\mathbb{F}_2^m} (-1)^{y_j\oplus f_j(x)\oplus 1\oplus u\cdot x\oplus v\cdot y} = -\Big(\sum_{x\in\mathbb{F}_2^n}(-1)^{f_j(x)\oplus u\cdot x}\Big)\Big(\sum_{y\in\mathbb{F}_2^m}(-1)^{y_j\oplus v\cdot y}\Big) = \begin{cases} -2^n\, W_{f_j}(u) \text{ if } v = e_j \\ 0 \text{ otherwise.} \end{cases}$. Hence, the Walsh transforms of these m functions have their supports included in parallel n-dimensional affine spaces A_j (of equation $v = e_j$) which are such that each element of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ can be expressed uniquely in the form $\sum_{j=1}^m a_j$ with $a_j \in A_j$. We shall say that the A_j's uniquely generate $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathbb{F}_2$-linearly.
Let L be an $\mathbb{F}_2$-linear automorphism of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ and L' the adjoint operator of L^{-1}. The images by L' of the affine spaces $\mathbb{F}_2^n \times \{e_j\}$ are parallel n-dimensional

affine spaces that uniquely generate $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathbb{F}_2$-linearly. Then, according to what is recalled above, if $h(x,y)$ is affine equivalent to the graph indicator of F, its ANF factorizes into the product of m Boolean functions whose Walsh supports are parallel n-dimensional affine spaces uniquely generating $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathbb{F}_2$-linearly.
Conversely, assume that an $(n+m)$-variable Boolean function h equals the product of n Boolean functions, each of which has for Walsh support an n-dimensional affine space, and that these affine spaces are parallel and uniquely generate $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathbb{F}_2$-linearly. Then there exists a linear automorphism which maps these n-dimensional affine spaces to the spaces $\mathbb{F}_2^n \times \{e_j\}$. Since it is easily seen that any $(n+m)$-variable Boolean function having $\mathbb{F}_2^n \times \{e_j\}$ for Walsh support has the form $y_j \oplus f_j(x) \oplus 1$, we deduce:

Proposition 13 *Any $(n+m)$-variable Boolean function is affine equivalent to the graph indicator of a function if and only if it equals the product of n Boolean functions, each of which has for Walsh support an n-dimensional affine space and these affine spaces are parallel and uniquely generate $\mathbb{F}_2^n \times \mathbb{F}_2^m$, $\mathbb{F}_2$-linearly.*

6 Graph indicators of sums, products, compositions and concatenations of vectorial functions

We can apply Proposition 3 or 5 to $F * G$, where $*$ is some binary operation, to deduce the expression of the ANF or of the polynomial representation of $1_{\mathcal{G}_{F*G}}$, by means of the corresponding representations of F and G. It may be also useful to have such an expression by means of the corresponding representations of $1_{\mathcal{G}_F}$ and $1_{\mathcal{G}_G}$. We address this below for the main operations and modifications on vectorial functions.

6.1 Sums of functions

According to Proposition 3, given two (n,m)-functions F and G, we have $1_{\mathcal{G}_{F+G}}(x,y) = \prod_{j=1}^{m}(y_j \oplus f_j(x) \oplus g_j(x) \oplus 1)$, where the f_j's and the g_j's are the coordinate functions of F and G, respectively. The ANF of $1_{\mathcal{G}_{F+G}}(x,y)$ (that we shall denote the same way as the function itself, as it is usual) writes then:

$$1_{\mathcal{G}_{F+G}}(x,y) = 1_{\mathcal{G}_F}(x, y+G(x)) = 1_{\mathcal{G}_G}(x, y+F(x)), \tag{18}$$

where $1_{\mathcal{G}_F}, 1_{\mathcal{G}_G}, F$ and G stand here also for the ANF of the functions. But this does not give $1_{\mathcal{G}_{F+G}}$ by means of $1_{\mathcal{G}_F}$ and $1_{\mathcal{G}_G}$, and it involves compositions of functions, which are more complex to calculate/compute than additions and multiplications. Let us then use another approach.
Relation (18) corresponds to expressing that the equality $F(x)+G(x)=y$ is equivalent to $F(x) = y+G(x)$ and to $G(x) = y+F(x)$. This same equality is also equivalent to "$\exists z \in \mathbb{F}_2^n; F(x)=z$ and $G(x)=y+z$". Then, since $F(x)=z$

cannot be true simultaneously for a same x and two different z, we deduce:

$$1_{\mathcal{G}_{F+G}}(x,y) = \sum_{z\in\mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,z)1_{\mathcal{G}_G}(x,y+z) = \bigoplus_{z\in\mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,z)1_{\mathcal{G}_G}(x,y+z), \quad (19)$$

and since we have here a sum modulo 2, we can replace these indicator functions by their ANF or by their univariate representation.

Remark. Relation (19) replaces the complexity of a composition by that of a multiplication combined with a sum of 2^n terms. This represents a considerable gain. □

Remark. It seems that the case of a direct sum of functions (i.e. when F and G depend on disjoint variables) is not significantly simpler than the general case of a sum. □

6.1.1 Graph indicator of a derivative

The derivatives $D_aF(x) = F(x)+F(x+a)$ of vectorial functions play an important role, in particular for APN functions. Let us then apply the result above to derivatives. We have, using that, for any Boolean functions f and g, we have $fg = \frac{f+g-(f\oplus g)}{2}$:

$$\begin{aligned} 1_{\mathcal{G}_{D_aF}}(x,y) &= \sum_{z\in\mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,z)1_{\mathcal{G}_F}(x+a,y+z) \\ &= \sum_{z\in\mathbb{F}_2^n} \frac{1_{\mathcal{G}_F}(x,z) + 1_{\mathcal{G}_F}(x+a,y+z) - D_{(a,z)}1_{\mathcal{G}_F}(x,y)}{2} \\ &= 1 - \frac{1}{2}\sum_{z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y), \end{aligned} \quad (20)$$

where $D_{(a,z)}1_{\mathcal{G}_F}(x,y) = 1_{\mathcal{G}_F}(x,y) \oplus 1_{\mathcal{G}_F}(x+a,y+z)$. We shall exploit this in Section 9).

6.2 Products of functions

The situation with the product is slightly more tricky than with the sum, because of the zero absorbance. Let F and G be two (n,n)-functions, that we shall take valued in $\mathbb{F}_{2^n}$ so as to be able to multiply their outputs, and let their graph indicators be therefore in bivariate form. According to Proposition 5, we have $1_{\mathcal{G}_{FG}}(x,y) = 1 + (y + F(x)G(x))^{2^n-1}$. For every x such that $G(x) \neq 0$, we have $(G(x))^{2^n-1} = 1$ and dividing $(y + F(x)G(x))^{2^n-1}$ by $(G(x))^{2^n-1}$ gives $1_{\mathcal{G}_{FG}}(x,y) = 1 + [y(G(x))^{2^n-2} + F(x)]^{2^n-1}$. The bivariate representation of $1_{\mathcal{G}_{F+G}}(x,y)$ writes then:

$$1_{\mathcal{G}_{FG}}(x,y) = (G(x))^{2^n-1}1_{\mathcal{G}_F}(x, y(G(x))^{2^n-2}) + ((G(x))^{2^n-1}+1)(1+y^{2^n-1}).$$

Here again, this does not give $1_{\mathcal{G}_{FG}}$ by means of $1_{\mathcal{G}_F}$ and $1_{\mathcal{G}_G}$, and it involves compositions of functions. It is possible to get rid of compositions but it seems difficult to completely avoid the use of $F(x)$ and $G(x)$. The relation $F(x)G(x) = y$ when $G(x) \neq 0$ is equivalent to "$\exists z \in \mathbb{F}_{2^n}^*; G(x) = z$ and $F(x) = yz^{2^n-2}$" and we have:

$$1_{\mathcal{G}_{FG}}(x,y) = (G(x))^{2^n-1} \sum_{z \in \mathbb{F}_{2^n}^*} 1_{\mathcal{G}_F}(x, yz^{2^n-2}) 1_{\mathcal{G}_G}(x,z) + ((G(x))^{2^n-1}+1)(1+y^{2^n-1}).$$

6.3 Composition of functions

We now study the graph indicators of composite functions $G \circ F$. Composition plays a central role in block ciphers, since these are iterative, and the whole cipher is the composition of all the transformations performed by the rounds. An (n,m)-function $F(x)$ being given (by its ANF or by its univariate representation) and an (m,r)-function $G(y)$ being given by the indicator $1_{\mathcal{G}_G}(y,z)$ of its graph (which can be represented by its ANF or by its bivariate representation), the equality $(G \circ F)(x) = G(F(x))$ results in:

$$1_{\mathcal{G}_{G\circ F}}(x,z) = 1_{\mathcal{G}_G}(F(x),z);\ x \in \mathbb{F}_2^n, z \in \mathbb{F}_2^r. \tag{21}$$

But here again, Relation (21) still involves a composition, which is complex to calculate. Moreover, this hybrid expression using $1_{\mathcal{G}_G}$ and F instead of $1_{\mathcal{G}_G}$ and $1_{\mathcal{G}_F}$ is not easily iterable while in block ciphers, composition is iterated. So let us address the case where we are given the ANF of $1_{\mathcal{G}_F}$ rather than that of $F(x)$. The equation of the support of $1_{\mathcal{G}_{G\circ F}}(x,z)$ can be obtained by the elimination of y from the two equations $1_{\mathcal{G}_F}(x,y) = 1$ and $1_{\mathcal{G}_G}(y,z) = 1$. This can be handled easily, similarly to what we did with addition in Subsection 6.1. Indeed, for every x, there is exactly one y such that $1_{\mathcal{G}_F}(x,y) = 1$, and this gives the possibility of expressing $1_{\mathcal{G}_{G\circ F}}(x,z)$ by addition in $\mathbb{Z}$ or in $\mathbb{F}_2$, and multiplication:

$$1_{\mathcal{G}_{G\circ F}}(x,z) = \sum_{y \in \mathbb{F}_2^m} 1_{\mathcal{G}_F}(x,y) 1_{\mathcal{G}_G}(y,z) = \bigoplus_{y \in \mathbb{F}_2^m} 1_{\mathcal{G}_F}(x,y) 1_{\mathcal{G}_G}(y,z). \tag{22}$$

Remark. If F is identity, then since $1_{\mathcal{G}_F}(x,y)$ equals 1 if $y = x$ and equals 0 otherwise, this formula gives correctly $1_{\mathcal{G}_{G\circ F}}(x,z) = 1_{\mathcal{G}_G}(x,z)$ and if G is identity it gives also $1_{\mathcal{G}_{G\circ F}}(x,z) = 1_{\mathcal{G}_F}(x,z)$. □

Remark. Here also, replacing the complexity of a composition by that of a multiplication combined with a sum of 2^n terms represents a considerable gain. Moreover, Relation (22) can be interpreted, thanks to Proposition 1, in a rather efficient way: $1_{\mathcal{G}_{G\circ F}}(x,z)$ equals 1 if and only if the Boolean function $y \mapsto 1_{\mathcal{G}_F}(x,y) 1_{\mathcal{G}_G}(y,z)$ has algebraic degree m. □

6.3.1 ANF

According to Relation (22) and using Relations (8) and (10) and Proposition 1, we have:

$$\begin{aligned} 1_{\mathcal{G}_{G\circ F}}(x,z) &= \bigoplus_{\substack{I\subseteq\{1,\ldots,n\}\\K\subseteq\{1,\ldots,r\}}} x^I z^K \left(\bigoplus_{y\in\mathbb{F}_2^n} \left(\psi_{F,I}(y)\varphi_{G,K}(y)\right)\right) \\ &= \bigoplus_{\substack{I\subseteq\{1,\ldots,n\},K\subseteq\{1,\ldots,r\};\\ d_{alg}\left(\psi_{F,I}(y)\prod_{k\in K^c}(g_k\oplus 1)\right)=m}} x^I z^K, \end{aligned} \tag{23}$$

where $K^c = \{1,\ldots,r\}\setminus K$ and the g_k's are the coordinate functions of G. Note that Relation (23) simplifies when F is a permutation: we have then

$$\begin{aligned} 1_{\mathcal{G}_{G\circ F}}(x,z) &= \bigoplus_{\substack{I\subseteq\{1,\ldots,n\}\\K\subseteq\{1,\ldots,r\}}} x^I z^K \left(\bigoplus_{y\in\mathbb{F}_2^n} \left(\prod_{i\in I^c}(f_i'\oplus 1)\prod_{k\in K^c}(g_k\oplus 1)\right)\right) \\ &= \bigoplus_{\substack{I\subseteq\{1,\ldots,n\},K\subseteq\{1,\ldots,r\};\\ d_{alg}\left(\prod_{i\in I^c}(f_i'\oplus 1)\prod_{k\in K^c}(g_k\oplus 1)\right)=n}} x^I z^K, \end{aligned}$$

where $I^c = \{1,\ldots,n\}\setminus I$ and the f_i''s are the coordinate functions of F^{-1}.

Relation (22) can be iterated to the composition of r functions $G_1,\ldots,G_r$ where G_t is from $\mathbb{F}_2^{m_{t-1}}$ to $\mathbb{F}_2^{m_t}$: for $x\in\mathbb{F}_2^{m_0}$ and $z\in\mathbb{F}_2^{m_r}$, we have:

$$1_{\mathcal{G}_{G_r\circ\cdots\circ G_1}}(x,z) =$$

$$\bigoplus_{\substack{(y_1,\ldots,y_{r-1})\in\\ \mathbb{F}_2^{m_1}\times\cdots\times\mathbb{F}_2^{m_{r-1}}}} \left(1_{\mathcal{G}_{G_1}}(x,y_1)\left(\prod_{t=2}^{r-1} 1_{\mathcal{G}_{G_t}}(y_{t-1},y_t)\right)1_{\mathcal{G}_{G_r}}(y_{r-1},z)\right). \tag{24}$$

6.3.2 Polynomial representation

We restrict ourselves here to $n=m=r$. According to Relations (13) and (22), we have:

$$1_{\mathcal{G}_{G\circ F}}(x,z) = \sum_{i=0}^{2^n-1}\sum_{k=0}^{2^n-1}\left(\sum_{y\in\mathbb{F}_2^n}\psi_{F,i}(y)\varphi_{G,k}(y)\right)x^i z^k.$$

Assuming again that F is an (n,n)-permutation, we have, according to Proposition 5 and Relations (16) and (22), that:

$$1_{\mathcal{G}_{G\circ F}}(x,z) =$$

$$\sum_{i=0}^{2^n-1}\left(\sum_{y\in\mathbb{F}_{2^n}}(F^{-1}(y))^i\right)x^{2^n-1-i} + \sum_{k=0}^{2^n-1}\left(\sum_{y\in\mathbb{F}_{2^n}}(G(y))^k\right)z^{2^n-1-k} +$$

$$\sum_{i,k\in\{0,\ldots,2^n-1\}} \left(\sum_{y\in\mathbb{F}_{2^n}} (F^{-1}(y))^i (G(y))^k \right) x^{2^n-1-i} z^{2^n-1-k}.$$

We have $\sum_{i=0}^{2^n-1} \left(\sum_{y\in\mathbb{F}_{2^n}} (F^{-1}(y))^i \right) x^{2^n-1-i} = \sum_{y\in\mathbb{F}_{2^n}} (1+1_{\mathcal{G}_F}(x,y)) = 1$ and $\sum_{k=0}^{2^n-1} \left(\sum_{y\in\mathbb{F}_{2^n}} (G(y))^k \right) z^{2^n-1-k} = \sum_{y\in\mathbb{F}_{2^n}} (1+1_{\mathcal{G}_G}(y,z)) = |G^{-1}(z)| \pmod 2$. Hence, according Proposition 2:

$$1_{\mathcal{G}_{G\circ F}}(x,z) = 1 + |G^{-1}(z)| \pmod 2 + \sum_{\substack{i,k\in\{0,\ldots,2^n-1\} \\ d_{alg}((F^{-1}(y))^i (G(y))^k)=n}} x^{2^n-1-i} z^{2^n-1-k}.$$

6.4 Concatenated functions

Concatenation plays a central role in block ciphers, since their S-boxes, for instance the $(128,128)$-function used in the AES, are most often, for reasons of speed, the concatenations of small S-boxes ($(8,8)$-functions in the case of the AES).
The concatenation $F=(F_1,\ldots,F_k)$ of (n,m)-functions $F_1,\ldots,F_k$ is defined as

$$F : (x^{(1)},\ldots,x^{(k)}) \in (\mathbb{F}_2^n)^k \mapsto (F_1(x^{(1)}),\ldots,F_k(x^{(k)})) \in (\mathbb{F}_2^m)^k.$$

Graph indicators behave very simply with respect to it. Indeed, since we have $F(x^{(1)},\ldots,x^{(k)}) = (y^{(1)},\ldots,y^{(k)})$ if and only if $\forall i=1,\ldots,k,\ F_i(x^{(i)}) = y^{(i)}$, we have then:

$$1_{\mathcal{G}_F}((x^{(1)},\ldots,x^{(k)}),(y^{(1)},\ldots,y^{(k)})) = \prod_{i=1}^{k} 1_{\mathcal{G}_{F_i}}(x^{(i)},y^{(i)}). \tag{25}$$

Note the similarity with the relation:

$$W_F((u^{(1)},\ldots,u^{(k)}),(v^{(1)},\ldots,v^{(k)})) = \prod_{i=1}^{k} W_{F_i}(u^{(i)},v^{(i)}),$$

which is also true (note however that the fact that $x^{(1)},\ldots,x^{(k)}$ have no coordinate in common is necessary for the latter relation and not for the former).
In the S-boxes of block ciphers, the functions $F_i(x^{(i)})$ will be given in practice in univariate form, with $x^{(i)} \in \mathbb{F}_{2^n}$. According to Proposition 5, Expression (25) gives then:

$$1_{\mathcal{G}_F}((x^{(1)},\ldots,x^{(k)}),(y^{(1)},\ldots,y^{(k)})) =$$
$$\prod_{i=1}^{k} \left(1 + \left(y^{(i)} + F_i(x^{(i)}) \right)^{2^n-1} \right) =$$
$$\sum_{L\subseteq\{1,\ldots,k\}} \left(\prod_{i\in L} \left(y^{(i)} + F_i(x^{(i)}) \right)^{2^n-1} \right) =$$

$$\sum_{L\subseteq\{1,\ldots,k\}}\sum_{\lambda\in\{0,\ldots,2^n-1\}^L}\left(\prod_{i\in L}\left((y^{(i)})^{2^n-1-\lambda_i}(F_i(x^{(i)}))^{\lambda_i}\right)\right). \tag{26}$$

For each F_i which is a permutation, we can change F_i into F_i^{-1} while exchanging $x^{(i)}$ and $y^{(i)}$.
In the case where each F_i equals the multiplicative inverse function, then, starting again from Relation (25) and using Relation (17), we obtain:

$$1_{\mathcal{G}_F}((x^{(1)},\ldots,x^{(k)}),(y^{(1)},\ldots,y^{(k)})) =$$

$$\prod_{i=1}^{k}\left((x^{(i)})^{2^n-1}+(y^{(i)})^{2^n-1}+\sum_{j=0}^{2^n-2}(x^{(i)}y^{(i)})^j\right) =$$

$$\sum_{L\subseteq\{1,\ldots,k\}}\sum_{\lambda\in\{0,\ldots,2^n-2\}^L}\left(\prod_{i\in L^c}\left((x^{(i)})^{2^n-1}+(y^{(i)})^{2^n-1}\right)\prod_{i\in L}\left((x^{(i)}y^{(i)})^{\lambda_i}\right)\right). \tag{27}$$

6.4.1 Composing a function obtained by concatenation by another function

In the model of block cipher called substitution-permutation network (SPN), a round is made of a global S-box (often made by the concatenation of smaller S-boxes, see above), followed by a diffusion layer (which is most often a linear permutation, for reasons of speed), followed by the addition of the round key. Looking at two rounds leads then to considering a function which is the composition of a function $F=(F_1,\ldots,F_k)$ equal to the concatenation of small S-boxes F_i, and of a function G equal to an affine automorphism composed with a global S-box. Using Relation (26) and that $1_{\mathcal{G}_{G\circ F}}(x,z)$ equals 1 if and only if the Boolean function $y\mapsto 1_{\mathcal{G}_F}(x,y)1_{\mathcal{G}_G}(y,z)$ has algebraic degree $m=kn$, and expressing $1_{\mathcal{G}_G}((y^{(1)},\ldots,y^{(k)}),z)$ in the form:

$$\sum_{K\subseteq\{1,\ldots,r\}}\varphi_{G,K}(y^{(1)},\ldots,y^{(k)})z^K,$$

we deduce the expression:

$$1_{\mathcal{G}_{G\circ F}}((x^{(1)},\ldots,x^{(k)}),z) =$$

$$\sum_{\substack{L\subseteq\{1,\ldots,k\},K\subseteq\{1,\ldots,r\},\lambda\in\{0,\ldots,2^n-2\}^L\\ d_{alg}\left(h_{L,K,\lambda}\right)=kn}}\left(\prod_{i\in L}(F_i(x^{(i)}))^{\lambda_i}\right)z^K,$$

where

$$h_{L,K,\lambda}(y)=\left(\prod_{i\in L}\left((y^{(i)})^{2^n-1-\lambda_i}\right)\right)\varphi_{G,K}(y^{(1)},\ldots,y^{(k)}).$$

In the case where each F_i equals the multiplicative inverse function, using Relation (27) and again that $1_{\mathcal{G}_{G\circ F}}(x,z)$ equals 1 if and only if the Boolean function $y \mapsto 1_{\mathcal{G}_F}(x,y)1_{\mathcal{G}_G}(y,z)$ has algebraic degree $m = kn$, we obtain:

$$1_{\mathcal{G}_{G\circ F}}((x^{(1)},\ldots,x^{(k)}),z) =$$

$$\sum_{\substack{L\subseteq\{1,\ldots,k\},K\subseteq\{1,\ldots,r\},\lambda\in\{0,\ldots,2^n-2\}^L,b\in\{0,1\}^{L^c}\\ d_{alg}\left(h_{L,K,\lambda,b}\right)=kn}} \left(\prod_{i\in L^c}(x^{(i)})^{(2^n-1)\,(1-b_i)}\prod_{i\in L}(x^{(i)})^{\lambda_i}\right) z^K,$$

where

$$h_{L,K,\lambda,b}(y) = \left(\prod_{i\in L^c}(y^{(i)})^{(2^n-1)\,b_i}\prod_{i\in L}(y^{(i)})^{\lambda_i}\right)\varphi_{G,K}(y^{(1)},\ldots,y^{(k)}).$$

6.5 Functions obtained by the switching method

The switching method has been used to construct new APN functions from known ones [11]. It consists of adding a Boolean function to an (n,n)-function (in univariate form). Up to affine equivalence, this is equivalent to modifying one of the coordinate functions of the vectorial function. This latter viewpoint generalizes to (n,m)-functions. So let $F = (f_1,\ldots,f_m)$ be any (n,m)-function and let f be any n-variable Boolean function. Let us denote by F_f the (n,m)-function whose last coordinate equals $f_m \oplus f$ and whose other coordinates are kept unchanged, and by F' the $(n,m-1)$-function obtained from F by discarding its last coordinate. Then, denoting $y' = (y_1,\ldots,y_{m-1})$, it is straightforward to see, either by using Proposition 3 or by checking separately each case $f(x) = 0$ and $f(x) = 1$ and using that if $1_{\mathcal{G}_{F'}}(x,y') = 0$ then $1_{\mathcal{G}_F}(x,y) = 0$, that:

$$1_{\mathcal{G}_{F_f}}(x,y) = 1_{\mathcal{G}_F}(x,y) \oplus f(x)\,1_{\mathcal{G}_{F'}}(x,y'). \tag{28}$$

7 Characterizing bijectivity by means of graph indicators

Bijectivity is needed in many situations of cryptography and coding (it plays in fact a role in all domains where vectorial functions are used). For instance, in SPN, the S-boxes must be bijective; in leakage squeezing and in the related CIS codes, the function used must be bijective; and the so-called threshold implementation with uniformity (see [14]) of an (n,n)-permutation is an (nk,nk)-permutation.
An (n,n)-function F is bijective if and only if $1_{\mathcal{G}_F}(y,x)$ is the indicator of the graph of a function.

7.1 Characterization by the Fourier-Hadamard transform

Proposition 9 applied to $1_{\mathcal{G}_F}(y,x)$ gives the well-known:

Proposition 14 *Let n be any positive integer. An (n,n)-function is bijective if and only if, for all $v \in \mathbb{F}_2^n$, the Fourier-Hadamard transform of its graph indicator satisfies:*

$$\widehat{1_{\mathcal{G}_F}}(0,v) = 2^n\,\delta_0(v).$$

7.2 Characterization by the ANF

The characterization of the graph indicators of functions in Proposition 10 allows characterizing the graph indicators of permutations. We write $h(x,y) = \sum_{J\subseteq\{1,\ldots,n\}} h_{\varphi,J}(x)\,y^J = \sum_{I\subseteq\{1,\ldots,n\}} h_{\psi,I}(y)\,x^I$ (so that if $h = 1_{\mathcal{G}_F}$, then $h_{\varphi,J} = \varphi_{F,J}$ and $h_{\psi,I} = \psi_{F,I}$). Then we know that h is the graph indicator of an (n,m)-function if and only if, for all $J \subseteq \{1,\ldots,n\}$, we have:

$$h_{\varphi,J} = \prod_{\substack{K\subseteq\{1,\ldots,n\}\\ |K|=n-1, J\subseteq K}} h_{\varphi,K},$$

and $h_{\varphi,\{1,\ldots,n\}}$ equals the constant function 1. This double condition being assumed satisfied, h is then the graph indicator of a permutation if and only if, for all $I \subseteq \{1,\ldots,n\}$, we have:

$$h_{\psi,I} = \prod_{\substack{K\subseteq\{1,\ldots,n\}\\ |K|=n-1, I\subseteq K}} h_{\psi,K},$$

and $h_{\psi,\{1,\ldots,n\}}$ equals the constant function 1. In fact, the second condition suffices. Indeed, $h_{\psi,\{1,\ldots,n\}}(y)$ being the y-dependent coefficient of $x^{\{1,\ldots,n\}}$ in $1_{\mathcal{G}_F}(x,y)$, the fact that it equals the constant function 1 translates, according to Proposition 1, that for every $y \in \mathbb{F}_2^n$, the size of $F^{-1}(y)$ is odd and this is sufficient for F to be a permutation.

Theorem 1 *Let F be an (n,n)-function and*

$$1_{\mathcal{G}_F}(x,y) = \bigoplus_{I,J\subseteq\{1,\ldots,n\}} a_{I,J}\,x^I y^J = \bigoplus_{I\subseteq\{1,\ldots,n\}} \psi_{F,I}(y)\,x^I.$$

Then, F is a permutation if and only if the function $\psi_{F,\{1,\ldots,n\}}$ equals constant function 1. Moreover, we have then for all $I \subseteq \{1,\ldots,n\}$:

$$\psi_{F,I} = \prod_{\substack{K\subseteq\{1,\ldots,n\}\\ |K|=n-1, I\subseteq K}} \psi_{F,K}$$

Remark. This characterization by a single n-variable Boolean function is conceptually simple and therefore appealing. The expression of the ANF of $\psi_{F,\{1,\ldots,n\}}(y)$ by means of the coefficients of the ANF of the coordinate functions $f_j(x)$; $j = 1,\ldots,n$, can be deduced from the decomposition given by Proposition 3, after expanding each product $\prod_{j\in J^c}(f_j(x)\oplus 1)$ and keeping only the coefficient of its term $x^{\{1,\ldots,n\}}$. We shall study below more in detail the case where $F(x)$ is given in polynomial form, which is slightly simpler. □

7.3 Characterization by the bivariate representation

According to Proposition 11, an $(n+m)$-variable Boolean function $h(x,y) = \sum_{i,j\in\{0,\ldots,2^n-1\}} a_{i,j}\, x^i y^j = \sum_{j\in\{0,\ldots,2^n-1\}} h_{\varphi,j}(x)\, y^j;\ a_{i,j} \in \mathbb{F}_{2^n}$, is the graph indicator of an (n,n)-function if and only if:

$$\begin{aligned}
&1)\ h_{\varphi,0} = 1 + (h_{\varphi,2^n-2})^{2^n-1},\\
&2)\ \forall\, j \in \{1,\ldots,2^n-2\},\ h_{\varphi,2^n-1-j} = (h_{\varphi,2^n-2})^j,\\
&3)\ h_{\varphi,2^n-1} = 1.
\end{aligned}$$

Writing $h(x,y) = \sum_{i\in\{0,\ldots,2^n-1\}} h_{\psi,i}(y)\, x^i$, we have then that h is the graph indicator of a permutation if and only if:

$$\begin{aligned}
&1)\ h_{\psi,0} = 1 + (h_{\psi,2^n-2})^{2^n-1},\\
&2)\ \forall\, i \in \{1,\ldots,2^n-2\},\ h_{\psi,2^n-1-i} = (h_{\psi,2^n-2})^i,\\
&3)\ h_{\psi,2^n-1} = 1.
\end{aligned}$$

Here again, knowing that h is a graph indicator, the last condition suffices (the proof is similar):

Theorem 2 *Let F be an (n,n)-function and*

$$1_{\mathcal{G}_F}(x,y) = \sum_{i,j\in\{0,\ldots,2^n-1\}} a_{i,j}\, x^i y^j = \sum_{i=0}^{2^n-1} \psi_{F,i}(y)\, x^i;\ a_{i,j} \in \mathbb{F}_{2^n}.$$

Then, F is a permutation if and only if the function $\psi_{F,2^n-1}$ equals constant function 1. Moreover, we have then:

$$\begin{aligned}
&1)\ \psi_{F,0} = 1 + (\psi_{F,2^n-2})^{2^n-1},\\
&2)\ \forall\, i \in \{1,\ldots,2^n-2\},\ \psi_{F,2^n-1-i} = (\psi_{F,2^n-2})^i.
\end{aligned}$$

According to Proposition 5, we have:

$$1_{\mathcal{G}_F}(x,y) = 1 + \sum_{K\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in K} 2^k} \prod_{k\in K} (F(x))^{2^k}.$$

Writing $F(x) = \sum_{r=0}^{2^n-2} a_r x^r$ (without loss of generality, since we know that F can be a permutation only if it has algebraic degree strictly less than n), we have then:

$$1_{\mathcal{G}_F}(x,y) =$$

$$1 + \sum_{K\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in K} 2^k} \prod_{k\in K} \left(\sum_{r=0}^{2^n-2} a_r^{2^k} x^{2^k r \pmod{2^n-1}} \right) =$$

$$1 + \sum_{K\subseteq\{0,\ldots,n-1\}} y^{2^n-1-\sum_{k\in K} 2^k} a_0^{\sum_{k\in K} 2^k} +$$

$$\sum_{\substack{K\subseteq\{0,\ldots,n-1\}\\ b\in\{0,\ldots,2^n-2\}^K,\, b\neq 0,\ldots,0}} y^{2^n-1-\sum_{k\in K}2^k}\left(\prod_{k\in K} a_{b_k}^{2^k}\right) x^{\lambda_{K,b}},$$

where $\{0,\ldots,2^n-2\}^K$ denotes the set of sequences $b=(b_k)_{k\in K}$ valued in $\{0,\ldots,2^n-2\}$ and indexed in K, and $\lambda_{K,b}$ equals $\sum_{k\in K}2^k b_k \pmod{2^n-1}$ if 2^n-1 does not divide $\sum_{k\in K}2^k b_k$, and equals 2^n-1 otherwise. We deduce:

$$\psi_{F,2^n-1}(y)=\sum_{\substack{K\subseteq\{0,\ldots,n-1\},b\in\{0,\ldots,2^n-2\}^K\\ b\neq 0,\ldots,0 \text{ and } \sum_{k\in K}2^k b_k\equiv 0 \,[\mathrm{mod}\ 2^n-1]}}\left(\prod_{k\in K} a_{b_k}^{2^k}\right) y^{2^n-1-\sum_{k\in K}2^k}.$$

Corollary 4 *Let $F(x)=\sum_{r=0}^{2^n-2}a_r x^r$; $a_r\in\mathbb{F}_{2^n}$, be any (n,n)-function. Then F is bijective if and only if, for all $K\subsetneq\{0,\ldots,n-1\}$, we have:*

$$\sum_{\substack{b\in\{0,\ldots,2^n-2\}^K, b\neq 0,\ldots,0\\ \sum_{k\in K}2^k b_k\equiv 0\,[mod\ 2^n-1]}}\left(\prod_{k\in K} a_{b_k}^{2^k}\right)=0,$$

and:

$$\sum_{\substack{b\in\{0,\ldots,2^n-2\}^{\{0,\cdots,n-1\}}\\ b\neq 0,\ldots,0 \ and\ \sum_{k=0}^{n-1}2^k b_k\equiv 0\,[mod\ 2^n-1]}}\left(\prod_{k=0}^{n-1} a_{b_k}^{2^k}\right)=1.$$

Remark. A permutation polynomial is called *complete* if the polynomial $F(x)+x$ is also a permutation polynomial. Complete polynomials are useful in many domains of applied mathematics (*e.g.* in the construction of bent functions). Theorem 2 provides a characterization of complete polynomials among permutation polynomials, by applying it to $F(x)+x$. Writing a program and checking the condition with a computer for a given function F in a small number of variables is easy. Determining the mathematical condition to be satisfied by F is more complex. Applying Proposition 5 to $F(x)+x$, using Lucas' theorem, denoting by $k\preceq i$ the fact that the binary expansion of i covers that of k and using the definition of $\varphi_{F,j}$ given after Proposition 5, we have $1_{\mathcal{G}_{F(x)+x}}(x,y)=1+(y+x+F(x))^{2^n-1}=1+\sum_{j=0}^{2^n-1}y^{2^n-1-j}(x+F(x))^j=1+\sum_{j=0}^{2^n-1}\sum_{k\preceq j}y^{2^n-1-j}x^{j-k}F(x)^k=1+\sum_{j=0}^{2^n-1}\sum_{k\preceq j}y^{2^n-1-j}x^{j-k}\varphi_{F,2^n-1-k}(x)$. Then, a permutation $F(x)=\sum_{r=0}^{2^n-2}a_r x^r$ is complete if and only if the coefficient of x^{2^n-1} in this expression equals the constant function 1.
An alternate way is to use Relation (19) and to use that $\sum_{z\in\mathbb{F}_{2^n}}z^k$ equals 1 if k is nonzero and is divisible by 2^n-1, and 0 otherwise, but this results in the same kind of calculations. □

7.4 Characterization up to CCZ equivalence

The two main parameters, see e.g. [5], that one wishes to optimize when choosing S-boxes for block ciphers – the nonlinearity (which should be large), and the

differential uniformity (which should be small) – are preserved by CCZ equivalence and are in fact properties of their graph indicators. Since bijectivity is needed in many cases, it is then important to be able to determine whether a $2n$-variable Boolean function (equal to a graph indicator or not) is affine equivalent to the graph indicator of a permutation.
We could try to combine the results of Section 5 with those of Subsections 7.2 and 7.3, but we saw in Section 5 that it seems already difficult to characterize by the ANF and by the polynomial representation the functions affine equivalent to graph indicators, not speaking of bijectivity. The characterization of Subsection 7.1 by the Fourier-Hadamard transform behaves better. Propositions 12 and 14 give:

Proposition 15 *A $(2n)$-variable Boolean function h is affine equivalent to the graph indicator of a permutation if and only if there exist two supplementary n-dimensional vector spaces (whose intersection is trivial and whose direct sum equals the whole space) on each of which the Fourier-Hadamard transform vanishes except at 0, where it takes value 2^n.*

Proposition 13 extends also nicely:

Proposition 16 *Any $(2n)$-variable Boolean function h is affine equivalent to the graph indicator of a permutation if and only if there exist two supplementary n-dimensional vector spaces E_1 and E_2 such that, for every $i = 1, 2$, function h equals the product of n Boolean functions having for Walsh supports cosets of E_i that uniquely generate $\mathbb{F}_2^n \times \mathbb{F}_2^n$, $\mathbb{F}_2$-linearly.*

8 Characterizing injectivity by means of graph indicators

We first observe that an (n, m)-function F (with $m \geq n$) is injective (i.e. one to one) if and only if there exists a subset E of $\mathbb{F}_2^m$ and an (m, n)-function G, such that, for every $x \in \mathbb{F}_2^n$ and every $y \in \mathbb{F}_2^m$, we have $1_{\mathcal{G}_F}(x, y) = 1_E(y)1_{\mathcal{G}_G}(y, x)$, and that this set E is unique. Indeed, the existence of E and G satisfying such equality is necessary since, taking for E the image set $Im(F)$ of F, for every $y \notin E$, this equality writes $0 = 0$, and for every $y \in E$, there is a unique $x \in \mathbb{F}_2^n$ such that $y = F(x)$, and denoting by G any function such that, for every $y \in E$, the value of $G(y)$ equals this unique x, the equality writes $1 = 1$. Conversely, if $1_{\mathcal{G}_F}(x, y) = 1_E(y)1_{\mathcal{G}_G}(y, x)$ for some set E and some (m, n)-function G, then for every $y \in E$, there exists a unique $x \in \mathbb{F}_2^n$ such that $y = F(x)$. Moreover, if $|E| < 2^n$ then there exists $x \in \mathbb{F}_2^n$ such that $1_{\mathcal{G}_F}(x, y) = 0$ for every $y \in \mathbb{F}_2^m$, a contradiction, hence $|E| = 2^n$ and $E = Im(F)$ (that is, E satisfying the condition is necessarily unique) and F is then injective.
When checking this condition, we can avoid visiting all the sets E of size 2^n since, when F is injective and E is its image set, we clearly have $1_E(y) = \bigoplus_{a \in \mathbb{F}_2^m} 1_{\mathcal{G}_F}(a, y)$. Hence:

Proposition 17 *Let $n \leq m$ and let F be any (n,m)-function. Then F is injective if and only if:*

$$1_{\mathcal{G}_F}(x,y) = \left(\bigoplus_{a \in \mathbb{F}_2^m} 1_{\mathcal{G}_F}(a,y) \right) 1_{\mathcal{G}_G}(y,x),$$

for some (m,n)-function G.

This characterization writes in a nicely simple way, but is in fact highly complex to check, because it needs to visit all (m,n)-functions. Let us then propose other, more practical, characterizations.
For every $y \in \mathbb{F}_2^m$, the sum $\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$ equals the size of $F^{-1}(y)$. If we have the NNF of $1_{\mathcal{G}_F}$, then we deduce that F is injective if and only if, for every $y \in \mathbb{F}_2^m$, we have[2] $\left(\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)\right)^2 = \sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$.
This has the advantage of being generalizable to k-to-1 functions in a strong sense (i.e. such that each preimage $F^{-1}(z)$ has size either 0 of k): the condition is then that, for all $y \in \mathbb{F}_2^n$, $\left(\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)\right)^2 = k \sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$.
Moreover, we have $\left(\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)\right)^2 \geq \sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$ for every (n,m)-function F and every $y \in \mathbb{F}_2^m$, with equality if and only if the function is Boolean, since the value of any sum $\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$ is an integer. Hence, F is injective if and only if we have $\sum_{y \in \mathbb{F}_2^m} \left(\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)\right)^2 = \sum_{y \in \mathbb{F}_2^m} \sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y)$, and therefore:

Proposition 18 *Let F be any (n,m)-function. Then, F is injective if and only if we have:*

$$\sum_{y \in \mathbb{F}_2^m} \left(\sum_{x \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x,y) \right)^2 = 2^n,$$

that is,

$$\sum_{x,x' \in \mathbb{F}_2^n} 1_{\mathcal{G}_F}(x', F(x)) = 2^n.$$

Note that this characterization does not generalize to k-to-1 functions, except for $k = 2$ when the size of each pre-image by F is necessarily even (such as in the case of a derivative; we shall exploit this in Section 9). Indeed, for every integer $k \geq 2$, there exist sequences of positive integers λ_i such that $\sum_i \lambda_i^2 = k \sum_i \lambda_i$ and $\exists i;\ \lambda_i \notin \{0,k\}$ (an example for $k = 2$ is 3,2,1,1,1).

Remark. Translating Proposition 18 by means of the NNF gives the condition $\sum_{x,x' \in \{0,1\}^n} \prod_{j=1}^m \left(1 - f_j(x) - f_j(x') + 2 f_j(x) f_j(x')\right) = 2^n$, that is,

[2] Note that, if $m = n$, this provides one more characterization of permutations.

$\sum_{x,x' \in \{0,1\}^n} \prod_{j=1}^{m} \Big(1 \oplus f_j(x) \oplus f_j(x')\Big) = 2^n$, which obviously characterizes injectivity. □

Let us see now what we can do with the ANF and the polynomial representation of $1_{\mathcal{G}_F}$. An (n,m)-function is injective if and only if, for every $y \in \mathbb{F}_2^m$, the Boolean function $x \mapsto 1_{\mathcal{G}_F}(x,y)$, which is the characteristic function of $F^{-1}(y)$, is either an atomic function or the zero function. We have seen that a Boolean function $g(x) = \bigoplus_{I \subseteq \{1,\ldots,n\}} a_I\, x^I$, $a_I \in \mathbb{F}_2$, is atomic if and only if, for every $I \subseteq \{1,\ldots,n\}$, we have $a_I = \prod_{i \in \{1,\ldots,n\} \setminus I} a_{\{1,\ldots,n\}\setminus\{i\}} = \prod_{\substack{K \subseteq \{1,\ldots,n\} \\ |K|=n-1, I \subseteq K}} a_K$ (and $a_{\{1,\ldots,n\}} = 1$). The same function is the zero function if and only if all its coefficients are zero, that is, the coefficients of degree $n-1$ are null and the others satisfy the same relation. We deduce:

Proposition 19 *Let F be an (n,m)-function F and*

$$1_{\mathcal{G}_F}(x,y) = \bigoplus_{I \subseteq \{1,\ldots,n\}, J \subseteq \{1,\ldots,m\}} a_{I,J}\, x^I y^J = \bigoplus_{I \subseteq \{1,\ldots,n\}} \psi_{F,I}(y)\, x^I.$$

Then, F is injective if and only if, for all $I \subsetneq \{1,\ldots,n\}$, we have:

$$\psi_{F,I} = \prod_{\substack{K \subseteq \{1,\ldots,n\} \\ |K|=n-1, I \subseteq K}} \psi_{F,K}$$

and $\psi_{F,\{1,\ldots,n\}} = 0$ implies $\psi_{F,I} = 0$, for all $I \subset \{1,\ldots,n\}$.

Similarly:

Proposition 20 *Let F be an (n,n)-function F and*

$$1_{\mathcal{G}_F}(x,y) = \sum_{i,j \in \{0,\ldots,2^n-1\}} a_{i,j}\, x^i y^j = \sum_{i \in \{0,\ldots,2^n-1\}} \psi_{F,i}(y)\, x^i.$$

Then, F is injective if and only if, for all $i \in \{1,\ldots,2^n-1\}$, we have:

$$\psi_{F,2^n-1-i} = (\psi_{F,2^n-2})^i$$

and $\psi_{F,2^n-1} = 0$ implies that $\psi_{F,i} = 0$, for all $i \in \{0,\ldots,2^n-2\}$.

9 Characterizing APNness by means of graph indicators

9.1 A first attempt

By definition (see Section 2), an (n,n)-function F is APN if and only if the multiset $\mathcal{G}_F + \mathcal{G}_F$ equals $2^n\,\{(0,0)\} \cup 2\,\Delta$, where Δ is a subset of $(\mathbb{F}_2^n \setminus \{0\}) \times \mathbb{F}_2^n$ and $2\,\Delta$ is the multiset whose value on Δ equals 2 and whose value elsewhere

equals 0. Let us translate this in terms of graph indicators. We denote by $\otimes$ the convolutional product. Viewing Boolean functions as pseudo-Boolean, that is, valued in $\mathbb{Z}$, we have, for univariate functions: $(f\otimes g)(x)=\sum_{a\in\mathbb{F}_2^n} f(a)g(x+a)$, and for bivariate functions: $(f\otimes g)(x,y)=\sum_{a,b\in\mathbb{F}_2^n} f(a,b)g(x+a,y+b)$, where these sums are calculated in $\mathbb{Z}$. The value at $(a,b)\in(\mathbb{F}_2^n\setminus\{0\})\times\mathbb{F}_2^n$ of the pseudo-Boolean function $1_{\mathcal{G}_F}\otimes 1_{\mathcal{G}_F}$ equals then the number of $(x,y)\in\mathcal{G}_F$ such that $(x+a,y+b)\in\mathcal{G}_F$. Then, denoting by γ_F the indicator of Δ (which is the notation used in [7]), we have:

Proposition 21 *Any (n,n)-function F is APN if and only if we have:*

$$1_{\mathcal{G}_F}\otimes 1_{\mathcal{G}_F}=2^n\cdot\delta_{(0,0)}+2\,\gamma_F, \tag{29}$$

where $\delta_{(0,0)}$ is the Dirac (or Kronecker) symbol and γ_F is a Boolean function over $\mathbb{F}_2^n\times\mathbb{F}_2^n$, equal to zero on $\{0\}\times\mathbb{F}_2^n$.

Remark. Using that the Fourier-Hadamard transform is $\mathbb{R}$-linear bijective, and applying the property seen in Section 2 that the Fourier-Hamard transform of the convolutional product of two pseudo-Boolean functions equals the product of their Fourier-Hadamard transforms, we deduce that any (n,n)-function F is APN if and only if we have $W_F^2=2^n+2\widehat{\gamma_F}$, where γ_F is a Boolean function; this revisits the result of [7, Lemma 4]. □

Let us see now if Proposition 21 can be used practically for checking APN-ness. In this proposition, $1_{\mathcal{G}_F}$ is seen as a pseudo-Boolean function. It is then not possible to replace it by its ANF nor by its univariate form, which both live in characteristic 2. If we wish to replace it by a polynomial representation, we can use the NNF. According to Propositions 4 and 21, we have that F is APN if and only if $\sum_{a,b\in\mathbb{F}_2^n}\prod_{j=1}^m\big(1+2b_jf_j(a)-b_j-f_j(a)\big)\prod_{j=1}^m\big(1+2(b_j+y_j-2b_jy_j)f_j(x+a)-(b_j+y_j-2b_jy_j)-f_j(x+a)\big)=2^n\cdot\delta_{(0,0)}(x,y)+2\gamma_F(x,y)$, where the additions when writing $f_j(x+a)$ are additions in $\mathbb{F}_2^n$, and the other additions/substractions are in $\mathbb{Z}$, and where γ_F is a Boolean function over $\mathbb{F}_2^n\times\mathbb{F}_2^n$, equal to zero on $\{0\}\times\mathbb{F}_2^n$. So, applying Proposition 21 and using the NNF leads to a characterization mixing sums in characteristic 2 and sums in characteristic 0, which is rather inconvenient.

Remark We know that F is APN if and only if $\sum_{u,v\in\mathbb{F}_2^n}W_F^4(u,v)=(3\cdot 2^n-2)2^{3n}$. We know that $W_F(u,v)=\widehat{1_{\mathcal{G}_F}}(u,v)=2^{2n-1}\delta_0(u,v)-\frac{1}{2}W_{1_{\mathcal{G}_F}}(u,v)$. Hence, $\sum_{u,v\in\mathbb{F}_2^n}W_F^4(u,v)=\frac{1}{16}\sum_{u,v\in\mathbb{F}_2^n}W_{1_{\mathcal{G}_F}}^4(u,v)-(2^{2n-1}-2^{n-1})^4+2^{4n-4}$ (indeed, $\widehat{1_{\mathcal{G}_F}}(0,0)=W_F(0,0)=2^n$ and $W_{1_{\mathcal{G}_F}}(0,0)=2^{2n-1}-2^{n-1}$). □

Remark. If F is APN and if we apply the switching method to it (see Subsection 6.5), Relation (28) writes: $1_{\mathcal{G}_{F_f}}(x,y)=(1-2f(x))1_{\mathcal{G}_F}(x,y)+f(x)\,1_{\mathcal{G}_{F'}}(x,y')$ (indeed, $1_{\mathcal{G}_F}(x,y)\,1_{\mathcal{G}_{F'}}(x,y')$ equals $1_{\mathcal{G}_F}(x,y)$). □

9.2 A second attempt

Let us apply the very definition of APNness (by the derivatives, see Section 2) and the expression of the graph indicators of derivatives given by Relation (20), which writes $1_{\mathcal{G}_{D_a F}}(x,y) = 1 - \frac{1}{2}\sum_{z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y)$, where the sum is in $\mathbb{Z}$. Since F is APN if and only if, for every nonzero $a \in \mathbb{F}_2^n$, the function $y \mapsto \sum_{x\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y)$ equals 2 times a Boolean function, and since $\sum_{x\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y)$ being even for every y, we have $\sum_{y\in\mathbb{F}_2^n}(\sum_{x\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y))^2 \geq 2\sum_{y\in\mathbb{F}_2^n}(\sum_{x\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y)) = 2\sum_{x,y\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y) = 2^{n+1}$, with equality if and only the function $y \mapsto \sum_{x\in\mathbb{F}_2^n} 1_{\mathcal{G}_{D_a F}}(x,y)$ equals 2 times a Boolean function, the condition becomes then $\sum_{y\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(1 - \frac{1}{2}\sum_{z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y))\right)^2 = 2^{n+1}$, that is, $\sum_{y\in\mathbb{F}_2^n}\left(2^{n+1} - \sum_{x,z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y)\right)^2 = 2^{n+3}$, that is, $2^{3n+2} - 2^{n+2}\sum_{x,y,z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y) + \sum_{y\in\mathbb{F}_2^n}\left(\sum_{x,z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y)\right)^2 = 2^{n+3}$. We have $\sum_{x,y,z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y) = 2\sum_{x,y\in\mathbb{F}_2^n}(1 - 1_{\mathcal{G}_{D_a F}}(x,y)) = 2^{2n+1} - 2^{n+1}$. We have then:

Proposition 22 *Let F be any (n,n)-function. Then F is APN if and ony if, for every nonzero $a \in \mathbb{F}_2^n$, we have:*

$$\sum_{y\in\mathbb{F}_2^n}\left(\sum_{x,z\in\mathbb{F}_2^n} D_{(a,z)}1_{\mathcal{G}_F}(x,y)\right)^2 = 2^{3n+2} - 2^{2n+3} + 2^{n+3}.$$

Note that here also, we have both kinds of additions, which is rather inconvenient: additions in characteristic 0 with the sums $\sum$ and an addition modulo 2 hidden in the notation $D_{(a,z)}1_{\mathcal{G}_F}(x,y)$.

Conclusion

We have studied the diverse representations of the graph indicators of vectorial functions in characteristic 2, and shown that, thanks to the information they provide on the functions, they constitute a useful tool. The size of such representations is larger than for the functions themselves, but we have shown that the benefit due to this increase of information is significant (for instance, in the case of a permutation, this provides the expressions of both the function and its compositional inverse), so that working with these indicators may be quite profitable. We have also characterized in different ways the representations of these graph indicators, and obtained original results on vectorial functions thanks to the study of these representations; for instance, we could show a tight bound on the algebraic degree of the inverse of a permutation. We have shown that all the main properties of vectorial functions (injectivity, bijectivity, APNness) can be characterized by the graph indicators. Some more work on them will be useful. We intend to study in particular more in detail the algebraic degree of composite functions by using this approach. We plan also to study the graph indicators

of those known permutations whose expression of the inverse is unknown, and to try deducing such expression for some of them. More characterizations (if possible by the ANF and the polynomial representation) of those $(2n)$-variable Boolean functions which are affine equivalent to the graph indicators of permutations would be also useful. And better characterizations of APNness would be quite interesting, as well as viewing the butterfly construction of [17] through representations of graph indicators. Studying the bentness and resiliency of vectorial functions may also take advantage of the approach by graph indicators. Secondary constructions of vectorial functions based on graph indicators may be also possible. Finally, we plan to study graph indicators in odd characteristic and to deduce a characterization of their bijectivity, which would probably lead to new results on planar functions.

References

[1] F. Armknecht and M. Krause. Constructing single- and multi-output boolean functions with maximal immunity. *Proceedings of ICALP 2006, Lecture Notes of Computer Science* 4052, pp. 180-191, 2006. See page 2.

[2] T. Beth and C. Ding, On almost perfect nonlinear permutations. *Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science* 765, pp. 65-76, 1994. See page 7.

[3] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Transactions on Information Theory* 52 (3), pp. 1141-1152, March 2006. See page 18.

[4] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397, 2010. See pages 4, 5, 6, 7, and 10.

[5] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469, 2010. See pages 2, 4, 5, and 28.

[6] C. Carlet. On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions. *NATO Science for Peace and Security Series, D: Information and Communication Security - Vol 23; Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pp. 104-116, 2009. See pages 2 and 8.

[7] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998. See pages 7, 18, and 32.

[8] C. Carlet, J. L. Danger, S. Guilley and H. Maghrebi. Leakage Squeezing of Order Two. *Proceedings of INDOCRYPT 2012, Lecture Notes in Computer Science* 7668, pp. 120-139, 2012. See page 2.

[9] C. Carlet, F. Freibert, S. Guilley, M. Kiermaier, J.-L. Kim and P. Solé. Higher-order CIS codes. *IEEE Transactions on Information Theory* 60(9), pp. 5283-5295, 2014. See page 2.

[10] C. Carlet, P. Gaborit, J.-L. Kim and P. Solé. A new class of codes for Boolean masking of cryptographic computations. *IEEE Transactions on Information Theory* 58 (9), pp. 6000-6011, 2012. See pages 2 and 8.

[11] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications* 3 (1), pp. 59-81, 2009. See page 25.

[12] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977. See pages 1, 5, and 10.

[13] M. Maghrebi, S. Guilley, and J.-L. Danger. Leakage Squeezing Countermeasure Against High-Order Attacks. *Proceedings of WISTP, Lecture Notes in Computer Science* 6633, pp. 208-223, 2011. See page 2.

[14] S. Nikova,V. Rijmen and M. Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *Journal of Cryptology* 24(2), pp. 292-321, 2011. See page 25.

[15] 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). See page 7.

[16] K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science* 765, pp. 55-64, 1994. See pages 7 and 15.

[17] L. Perrin, A. Udovenko, and A. Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem. *Proceedings of CRYPTO 2016, Lecture Notes in Computer Science* 9815, Part II, pp. 93-122, 2016 See page 34.