Matrix representations of vectorial boolean functions and eigenanalysis

Brandon Dravie, Jérémy Parriaux, Philippe Guillot, Gilles Millérioux

Matrix representations of vectorial Boolean functions and eigenanalysis

Brandon Dravie[1], Jérémy Parriaux[1], Philippe Guillot[2], and Gilles Millérioux[1]

[1] Université de Lorraine, CRAN, UMR 7039, ESSTIN, 2 rue Jean Lamour, Vandœuvre-lès-Nancy, 54506, France
CNRS, CRAN, UMR 7039, France
brandon.dravie@univ-lorraine.fr,jeremy.parriaux@gmail.com, gilles.millerioux@univ-lorraine.fr,
[2] Université Paris 8
Laboratoire Analyse, Géométrie et Applications, LAGA, UMR 7539, France
philippe.guillot@univ-paris8.fr

Abstract. This paper aims at giving a unified overview on the various representations of vectorial Boolean functions, namely the Walsh matrix, the correlation matrix and the adjacency matrix. A new representation called polynomial matrix is introduced. It is shown that those different representations are similar. For a vectorial Boolean function with the same number of inputs and outputs, an eigenanalysis of those representations is performed. It is shown how eigenvalues and eigenvectors are related to the structure of the graph associated to this function.

1 Introduction

Vectorial Boolean functions [1] play an important role in cryptography as nonlinear components of symmetric algorithms [2]. They are also used in control theory to model discrete dynamical systems [3]. This paper aims at giving a unified overview on various representations of vectorial Boolean functions. Usual existing representations are presented such as the Walsh matrix, the correlation matrix and the adjacency matrix (related to graph representations) [4] often used in the analysis of cryptographic properties. Besides, we introduce a new representation based on algebraic properties. We call this representation polynomial matrix.

It is shown that the representations describe the same function in different bases and the bases are given explicitly. Then, the relations between these representations are proved. For square matrices representing the vectorial Boolean functions, we perform the eigenanalysis. Deep connections are established between the eigenvalues of those matrices, their related eigenspaces and the structure of the graphs of the vectorial Boolean functions.

The results are general and could be useful for people concerned with theoretical aspects regarding vectorial Boolean functions and with practical applications too. They are interesting in particular for cryptographic purposes.

The layout is the following: In Section 2, the different expressions of Boolean functions are recalled. Section 3 is devoted to vectorial Boolean functions and the corresponding matrix representations. A new representation called the polynomial matrix is introduced. The link between matrix representations and graph theory is established. Finally, Section 4 is devoted to the eigenanalysis of the matrix representations of a vectorial Boolean function and the corresponding properties of its graph representation.

2 Boolean functions representations

This section provides necessary prerequisites. The reader may refer to [1] for details. New results are also presented here as important complements.
A Boolean function is a function from the vector space $\mathbb{F}_2^n$ to the set $\{0,1\}$. Depending on the context, the set $\{0,1\}$ is considered either as the two element field $\mathbb{F}_2$ $(1+1=0)$ or as a subset of the field $\mathbb{C}$ of complex number $1+1=2$. We call such a function a (n)–function. The various usual representations are the truthtable, the Fourier and the Walsh transform and the polynomial representation. These are recalled below. It is clear that the convenience of a specific representation depends on the properties it is expected to characterize.

2.1 Truthtable

The truthtable of a Boolean function is the 2^n–dimensional vector composed of all the values of the function. It expresses the function in the basis of the indicator functions defined for all $u \in \mathbb{F}_2^n$ by:

$$\delta_u : \begin{array}{c} \mathbb{F}_2^n \longrightarrow \{0,1\} \\ x \longmapsto \delta_u(x) = \begin{cases} 1 & \text{if} \quad x = u \\ 0 & \text{else} \end{cases} \end{array} \tag{1}$$

The expression of f in this basis is:

$$f = \sum_{u \in \mathbb{F}_2^n} f(u)\delta_u.$$

2.2 Fourier/Walsh transform

Let f be any complex valued function on $\mathbb{F}_2^n$. We denote by $\widehat{f}$ its Fourier transform, which is by definition the complex-valued mapping $\mathbb{F}_2^n \longrightarrow \mathbb{C}$ defined for $u \in \mathbb{F}_2^n$ by:

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

where $x \cdot u = x_0 u_0 + \cdots + x_{n-1} u_{n-1}$ is the dot product of the two vectors x and u. This transform is invertible and the inverse is given by:

$$\widehat{\widehat{f}} = 2^n f \tag{3}$$

The Fourier transform is an expression of f in the orthogonal basis of the so-called Walsh functions, defined for all $u \in \mathbb{F}_2^n$ by:

$$\chi_u : \begin{array}{ccc} \mathbb{F}_2^n & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \frac{1}{2^n}(-1)^{u \cdot x}. \end{array} \tag{4}$$

The expression of f in this basis is:

$$f = \sum_{u \in \mathbb{F}_2^n} \widehat{f}(u) \chi_u.$$

When f is represented by its truthtable vector, the Fourier transform (2) also admits a matrix expression:

$$\widehat{f} = Hf, \tag{5}$$

where H is the so-called Hadamard matrix whose coefficient at row $u \in \mathbb{F}_2^n$ and column $v \in \mathbb{F}_2^n$ is:

$$H_{u,v} = (-1)^{u \cdot v}. \tag{6}$$

The Hadamard matrix H is invertible and its inverse is given by:

$$H^{-1} = \frac{1}{2^n} H. \tag{7}$$

As a result, it holds that

$$f = \frac{1}{2^n} H \widehat{f}$$

When dealing with Boolean functions, it is better to use the Walsh transform that has nicer properties than the Fourier transform in most cases. The Walsh transform of a Boolean function f is the Fourier transform of its sign function f_χ where $f_\chi = (-1)^f = 1 - 2f$. The Walsh transform of f is the function $\widehat{f_\chi}$ defined by:

$$\widehat{f_\chi} : \begin{array}{ccc} \mathbb{F}_2^n & \longrightarrow & \mathbb{R} \\ u & \longmapsto & \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + x \cdot u} \end{array} \tag{8}$$

Let us recall the following theorem.

Theorem 1 (Parseval's equality (see [1])). *For any $\mathbb{C}$– valued function f on $\mathbb{F}_2^n$:*

$$\sum_{u \in \mathbb{F}_2^n} \left[\widehat{f}(u)\right]^2 = 2^n \sum_{x \in \mathbb{F}_2^n} [f(x)]^2 \tag{9}$$

When applied to the sign function of Boolean functions, the equality (9) turns into

$$\sum_{u \in \mathbb{F}_2^n} \left[\widehat{f_\chi}(u)\right]^2 = \left[\sum_{u \in \mathbb{F}_2^n} \widehat{f_\chi}(u)\right]^2 = 2^{2n} \tag{10}$$

2.3 Polynomial representations

This section is devoted to polynomial representations of (n)–functions. Two representations are presented: Algebraic Normal Form (ANF)(see [5]) and Numerical Normal Form (NNF) (see [6]).
Due to the equality, $\forall a \in \{0,1\}\,,\ a = a^2$, distinct polynomials may represent the same Boolean function. In order to obtain the uniqueness of the representation, we only consider the polynomials in the ring of multivariate polynomials whose exponents for each indeterminate are at most one.
Let a and b be two elements of $\mathbb{F}_2$, it holds that $a^b = 1$ if $b \leq a$ and $a^b = 0$ elsewhere.
Polynomial representations are expressions of the function in the so-called basis of monomials defined, for $u \in \mathbb{F}_2^n$, by:

$$\begin{array}{c} \mathbb{F}_2^n \longrightarrow \{0,1\} \\ x \longmapsto x^u \end{array} \tag{11}$$

where

$$x^u = x_0^{u_0} \cdots x_{n-1}^{u_{n-1}} \tag{12}$$

is called a monomial.

For any vector u in $\mathbb{F}_2^n$, the support of u is defined by:

$$\mathrm{supp}(u) = \big\{ i \in \{1,\ldots,n\} \mid u_i \neq 0 \big\}.$$

Remark 1. When x and u are two n–dimensional binary vectors, the notation $x \preceq u$ means that the support of x is included in the support of u. The following equivalences holds:

$$x \preceq u \Longleftrightarrow u^x = 1 \Longleftrightarrow \forall i \in \{1,\ldots,n\}\,,\ x_i \leq u_i. \tag{13}$$

2.3.1 Algebraic Normal Form (ANF)

Let us recall a multivariate polynomial representation of Boolean functions called Algebraic Normal Form (ANF for short).

The ANF coefficients of a function f are, by definition, for $u \in \mathbb{F}_2^n$,

$$a_u = \sum_{x \in \mathbb{F}_2^n} f(x) u^x, \tag{14}$$

where the sum is performed in the two element field $\mathbb{F}_2$. They express the function f in the basis of monomials as:

$$\forall x \in \mathbb{F}_2^n,\ f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u. \tag{15}$$

2.3.2 Numerical Normal Form (NNF)

Let us recall another multivariate polynomial representation of Boolean functions called Numerical Normal Form (NNF for short).
Unlike the ANF, the coefficients of the polynomial do not lie in the two element field $\mathbb{F}_2$ but in the field $\mathbb{C}$ of complex numbers. Notice that such a polynomial may not correspond to a $\{0,1\}$ valued function.
The NNF coefficients of a complex valued function f are the complex coefficients of f expressed in the basis of monomial functions. They are defined by:

$$\widetilde{f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathrm{hw}(x)-\mathrm{hw}(u)} f(x) u^x = \sum_{x \in \mathbb{F}_2^n | x \preceq u} (-1)^{\mathrm{hw}(x)-\mathrm{hw}(u)} f(x),\ u \in \mathbb{F}_2^n$$

where hw denotes the Hamming weight function and the sum is performed in the field of complex numbers. The expression of f in the basis of monomials is:

$$\forall x \in \mathbb{F}_2^n,\ f(x) = \sum_{u \in \mathbb{F}_2^n} \tilde{f}(u) x^u = \sum_{u \in \mathbb{F}_2^n | u \preceq x} \tilde{f}(u) \tag{16}$$

Likewise for the Fourier transform, a matrix relation exists between a function f described by its truthtable and its NNF:

$$\widetilde{f} = Zf, \tag{17}$$

where Z is a 2^n dimensional square matrix whose coefficient at row $u \in \mathbb{F}_2^n$ and column $v \in \mathbb{F}_2^n$ is given by:

$$Z_{u,v} = (-1)^{\mathrm{hw}(v)-\mathrm{hw}(u)} u^v.$$

The matrix Z is invertible and the inverse is the so called *monomial matrix* defined by:

$$Z^{-1} = M \tag{18}$$

where the coefficient at row $x \in \mathbb{F}_2^n$ and column $u \in \mathbb{F}_2^n$ of M is given by $M_{x,u} = x^u$. As a result, one has $f = M\tilde{f}$.

3 Vectorial Boolean functions representations

A vectorial Boolean function is, by definition, a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. It can be considered as a vector of m (n)–functions. We call such a function an (n,m)–function. Vectorial Boolean functions have been extensively discussed in [7]. For any vectorial Boolean function f, it is possible to define different matrix representations denoted by A_f, C_f, W_f, and P_f. They are respectively named adjacency, correlation, Walsh and polynomial matrices. For brevity, the superscript of the matrices is omitted when the corresponding function is clear. Let f_e be the function defined by the truthtable of Table 1. This function is used throughout the rest of the paper to illustrate the results.

x	000 001 010 011 100 101 110 111
$f_e(x)$	010 100 001 101 010 101 010 110

Table 1: Truthtable of function f_e

3.1 Adjacency matrix

The adjacency matrix of f is denoted by A. It is the expression of f in the basis of the indicator functions $(\delta_u)_{u\in\mathbb{F}_2^n}$, defined by equation (1).

Definition 1 (Adjacency matrix). *Let f be an (n,m)–function. Its adjacency matrix A is a $2^n \times 2^m$ dimensional matrix for which each row indexed by $x \in \mathbb{F}_2^n$ is null except the coefficient at the column $y = f(x)$, which equals* 1.

For example, the adjacency matrix of f_e is:

$$A_{f_e} = \begin{pmatrix} 0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&1&0 \end{pmatrix}$$

The name *adjacency matrix* is inspired from graph theory [8]. When the number of inputs equals the number of outputs, the function can also be represented by a labeled directed graph $\mathcal{G}$ as defined below.

Definition 2 (Directed graph (see [8])). *A directed graph $\mathcal{G}$ is a couple (V,E) where V is the set of vertices and E is the set of arcs. An arc is an ordered pair of vertices also called directed edge.*

Hereafter, we only consider directed graphs. Thus, for brevity but without any ambiguity, we merely call them graphs. A graph is naturally associated to a (n,n)–function, where an arc relates an input of the function to its image as defined below.

Definition 3 (Graph associated to a function (see [9])). *Let f be an (n,n)–function. The graph associated to f is defined by the set of vertices $V = \mathbb{F}_2^n$ and the set of arcs E that are the ordered pairs $(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $y = f(x)$.*

Now, let us recall some graph theoretic terminology that is necessary in the further development. For each definition, the corresponding structure is illustrated for the function f_e in Figure 1.

Definition 4 (Graph related terminology (see [8])).

- *An edge is an unordered pair of distinct vertices of the graph,*
- *An arc is a directed edge, i.e an ordered pair of distinct vertices. An arrow shows the direction of the edge,*
- *A vertex x is said to be incident to a vertex y (or to be a preimage of a vertex y) if there is an arc from x to y. The vertex 111 is incident to 110,*
- *The in-degree of a vertex is the number of vertices incident to that vertex. The in-degree of vertex 000 is 0. The in-degree of vertex 010 is 3,*
- *The out-degree of a vertex is the number of vertices for which this vertex is incident to. The out-degree of each vertex is 1, including vertex 101,*
- *A path is a sequence of vertices $(x_0, \ldots, x_k)$ such that, for each vertex, there is an arc from x_i to x_{i+1}. The length of the path is the number of arcs involved in the sequence. The sequence $(110, 010, 001)$ is a path of length 2,*
- *A cycle is a path such that the starting vertex and the ending vertex are the same. The sequence $(010, 001, 100, 010)$ is a cycle of length 3,*
- *A junction is a vertex such that the in-degree is at least two. The multiplicity of the junction is equal to the in-degree minus one. The vertex 101 is a junction of multiplicity one. The vertex 010 is a junction of multiplicity two,*
- *The preimage set of a vertex is the set of vertices incident to that vertex. The preimage set of the junction 010 is $\{000, 110, 100\}$ and the preimage set of the junction 101 is $\{011, 101\}$,*
- *A sink is a vertex with at least one incident vertex and such that it is not incident to any other vertex but itself. Any sink defines a cycle of length one. The vertex 101 is a sink,*
- *A leaf is a vertex with no incident vertex. The vertices $000, 011$ and 111 are the leaves of the graph,*
- *A connected component is a set of vertices such that there is always a path (not necessarily directed) that relates any two vertices of that set. The set of vertices $\{111, 110, 000, 010, 100, 001\}$ corresponds to one connected component and the set of vertices $\{011, 101\}$ corresponds to another connected component.*

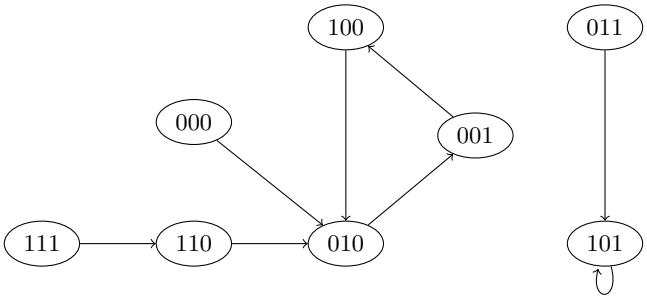

Fig. 1: Graph associated to the function f_e

The claims in the following Remarks 2, 3 and 4 are straightforward:

Remark 2.

- the graph associated to an (n, n)–function is such that there is one and only one arrow starting from any of its vertices,
- the graph associated to a permutation contains neither leaf nor junctions,
- if a graph contains no leaf then it is the graph associated to a permutation and thus, it contains no junction,
- if a graph contains no junction then it is the graph associated to a permutation and thus, it contains no leaf.

Remark 3. As the set of vertices of the graph of a (n, n)–function is finite, the graph contains at least one cycle.

Remark 4. If there is no leaf, then the graph is a union of cycles and it contains no junction. Besides, each new leaf, either adds a new junction or increases the multiplicity of an existing junction by one. As a consequence, the number of leaves equals the sum of the multiplicities of the junctions.

3.2 Walsh/correlation matrix

Correlation matrices have been defined in [4]. They are related to Walsh matrices by a mere normalization coefficient.

Definition 5 (see [7]). *The Walsh matrix of an (n, m)–function is the $2^m \times 2^n$ dimensional matrix W whose coefficients are defined at indexes $u \in \mathbb{F}_2^m$ and $v \in \mathbb{F}_2^n$ by:*

$$W_{u,v} = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot f(x) + v \cdot x}. \tag{19}$$

For all $u \in \mathbb{F}_2^m$ and all $v \in \mathbb{F}_2^n$, the coefficient $W_{u,v}$ is the number of times the Boolean function $x \longmapsto u \cdot f(x)$ equals the linear Boolean function $x \longmapsto v \cdot x$, minus the number of times they differ.

For example, the Walsh matrix of the function f_e is:

$$W_{f_e} = \begin{pmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & -2 & -2 & 6 & -2 \\ 0 & -4 & 0 & -4 & 4 & 0 & -4 & 0 \\ -6 & -2 & 2 & -2 & 2 & -2 & 2 & -2 \\ 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & -2 & -2 & -2 & 6 \\ -4 & 0 & -4 & 0 & 0 & 4 & 0 & -4 \\ -2 & -6 & -2 & 2 & -2 & 2 & -2 & 2 \end{pmatrix}$$

The row $u \in \mathbb{F}_2^m$ of the matrix W is the Walsh transform of the linear combinations of the coordinates of f defined by $x \longmapsto u \cdot f(x)$, $x \in \mathbb{F}_2^n$. The list of the coefficients of the Walsh matrix of a function is called the spectrum of the function.

Definition 6 (see [4]). *The correlation matrix of a (n,m)–function f is:*

$$C_f = 2^{-n} W_f. \tag{20}$$

Let us recall important results used further and which have been published in [10].
We are given an (n,m)–function g and a random variable $X \in \mathbb{F}_2^n$ whose value is described by the probability law $p : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ that expresses the probability $p(x)$ that $X = x$. We are concerned with inferring the probability law $q : \mathbb{F}_2^m \longrightarrow \mathbb{R}$ that describes the random variable $Y \in \mathbb{F}_2^m$ defined by $Y = g(X)$, q being defined by $q(y) = \Pr[g(X) = y]$. Without any ambiguity, the notation p (respectively q) refers either to the function or to the 2^n (respectively 2^m) column vectors whose coordinate index $x \in \mathbb{F}_2^n$ (respectively $y \in \mathbb{F}_2^m$) has the value $p(x)$ (respectively $q(y)$).

Proposition 1 (see [10]). *Let g be an (n,m)–function and X be a random variable described by the probability law p. Then the probability law q of the random variable $Y = g(X)$ is given by:*

$$q = H^{-1} C_g H p. \tag{21}$$

Remark 5. Let $\widehat{p}$ and $\widehat{q}$ be the respective Fourier transform of p and q as defined in Proposition 1. It is also shown in [10] that

$$\widehat{q} = C_g \widehat{p} \tag{22}$$

3.3 Reduced Walsh/correlation matrix

The reduced Walsh matrix is defined as follows.

Definition 7 (Reduced Walsh matrix). *For a Walsh matrix W of dimension $2^m \times 2^n$, its reduced matrix $W^\star$ of dimension $(2^m - 1) \times (2^n - 1)$ is the matrix deduced from W, where the first row and the first column have been removed.*

$$W^\star = \begin{pmatrix} W_{1,1} & \cdots & W_{1,2^n-1} \\ \vdots & & \vdots \\ W_{2^m-1,1} & \cdots & W_{2^m-1,2^n-1} \end{pmatrix}.$$

Remark 6. The same definition holds for the correlation matrix C.

It is interesting because it yields more homogeneous results. The purpose of the sequel is to show that no information on f is lost with the reduced matrix, except for constant functions.

First, let us note that the first row of the correlation matrix always equals the 2^n–dimensional vector $(2^n, 0, \ldots, 0)$. In the sequel, considerations on the first column are given.

Lemma 1. *Let f be an (n)–function. Then, the quantity $\sum_{u\in\mathbb{F}_2^n|u\neq 0}\widehat{f_\chi}(u)$ is null if and only if f is a constant function.*

Proof. It holds that:

$$\begin{aligned}\sum_{u\in\mathbb{F}_2^n|u\neq 0}\widehat{f_\chi}(u) &= \sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x} - \widehat{f_\chi}(0)\\ &= \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot x} - \widehat{f_\chi}(0)\\ &= 2^n f_\chi(0) - \widehat{f_\chi}(0).\end{aligned}$$

As $f_\chi(0)$ is ± 1, on one hand $2^n f_\chi(0) = \pm 2^n$, and on the other hand $\widehat{f_\chi}(0) = \sum_{x\in\mathbb{F}_2^n} f_\chi(x) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)} = \pm 2^n$ if and only f is constant. □

Lemma 2. *An (n)–function f can be uniquely recovered from its last 2^n-1 Walsh coefficients provided that it is not a constant function.*

Proof. Recovering f from $\widehat{f_\chi}$ by the inverse Fourier transform formula (3) requires the knowledge of the 2^n Walsh coefficients. The value $\widehat{f_\chi}(0)$ can be found using Parseval theorem (Theorem 1).

$$\sum_{u\in\mathbb{F}_2^n}\left[\widehat{f_\chi}(u)\right]^2 = \sum_{u\in\mathbb{F}_2^n}\widehat{f_\chi}(u)\cdot\sum_{v\in\mathbb{F}_2^n}\widehat{f_\chi}(v)$$

$$\widehat{f_\chi}(0)^2 + \sum_{u\in\mathbb{F}_2^n|u\neq 0}\left[\widehat{f_\chi}(u)\right]^2 = \widehat{f_\chi}(0)^2 + 2\widehat{f_\chi}(0)\sum_{u\in\mathbb{F}_2^n|u\neq 0}\widehat{f_\chi}(u) + \sum_{\substack{u\in\mathbb{F}_2^n|u\neq 0\\ v\in\mathbb{F}_2^n|v\neq 0}}\widehat{f_\chi}(u)\widehat{f_\chi}(v)$$

Then, as f is not constant, from Lemma 1, $\sum_{u\in\mathbb{F}_2^n|u\neq 0}\widehat{f_\chi}(u)$ is not null and $f_\chi(0)$ can be recovered by

$$\widehat{f_\chi}(0) = \frac{1}{2}\frac{\sum_{u\in\mathbb{F}_2^n|u\neq 0}\left[\widehat{f_\chi}(u)\right]^2 - \sum_{\substack{u\in\mathbb{F}_2^n|u\neq 0\\ v\in\mathbb{F}_2^n|v\neq 0}}\widehat{f_\chi}(v)}{\sum_{u\in\mathbb{F}_2^n|u\neq 0}\widehat{f_\chi}(u)}$$

Being known all the values of $\widehat{f_\chi}$, function f is recovered by the inverse Fourier transform (3). □

Finally, we have the following result.

Proposition 2. *An (n,m)–function can be uniquely recovered from its reduced Walsh matrix provided that it is not a constant function.*

Proof. Let f be an (n,m)–function. The rows of its matrix W are the Walsh transforms of all the linear combinations of its coordinate functions. It suffices to

reconstruct these coordinate functions to retrieve the function f. From Lemma 2, when f is not a constant (n)– function, it is possible to recover a coordinate of f from the $2^n - 1$ Walsh coefficients of this coordinate.
Now, assume that f is not constant. Then there exists a coordinate function f^j which is not constant. If there is a coordinate function f^i which is constant, then there is a row in the matrix W which is the Walsh transform of $f^i + f^j$ where the sum is performed modulo 2. The function $f^i + f^j$ is not constant and so, Lemma 2 applies. Let $g = f^i + f^j$. If f^i is $x \longmapsto 0$ then $\widehat{g_\chi} = \widehat{f^j_\chi}$, and if f^i is $x \longmapsto 1$ then, $\widehat{g_\chi} = -\widehat{f^j_\chi}$. Therefore, it is always possible to determine whether f^i is the constant function $x \longmapsto 0$ or the constant function $x \longmapsto 1$ provided that there is at least one non constant coordinate function.
As a conclusion, when an (n, m)–function f is not constant, all its coordinate functions can be recovered from the reduced Walsh matrix of f (and so the correlation matrix) and then f can be entirely recovered. □

3.4 Polynomial matrices

The extension of the NNF to an (n, m)–function gives rise to a $2^m \times 2^n$ dimensional matrix denoted with P. We call it the *polynomial matrix* of f, and the entry at row indexed by $u \in \mathbb{F}_2^m$ and column indexed by $v \in \mathbb{F}_2^n$ is defined by:

$$P_{u,v} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathrm{hw}(x)-\mathrm{hw}(v)} f(x)^u v^x.$$

Note that the rows indexed by $u \in \mathbb{F}_2^n$ for which $\mathrm{hw}(u) = 1$ correspond to the NNF of a coordinate function of f. The matrix P expresses f in the basis of the polynomials, $x \longmapsto (-1)^{\mathrm{hw}(x)-\mathrm{hw}(v)} v^x$, $v \in \mathbb{F}_2^n$. For example, the polynomial matrix of f_e is

$$P_{f_e} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

In the same way as the ANF can be obtained by performing a modulo two reduction of the NNF, we can define a modulo two reduction of the polynomial matrix P.

3.5 Reduced Polynomial matrix

Likewise for correlation matrix, we define the reduced form P^* of a polynomial matrix P associated to an (n, m)–function f. Assuming that f is not constant, we will prove that f can be recovered given the coefficients of $P^\star$.

Definition 8 (Reduced polynomial matrix). *For any polynomial matrix P of dimension $2^m \times 2^n$, its reduced matrix $P^\star$ of dimension $(2^m-1)\times(2^n-1)$ is the matrix deduced from P, where the first row and column have been removed.*

$$P^\star = \begin{pmatrix} P_{1,1} & \cdots & P_{1,2^n-1} \\ \vdots & & \vdots \\ P_{2^m-1,1} & \cdots & P_{2^m-1,2^n-1} \end{pmatrix}$$

The following lemma is similar to Parseval's identity, and is based on the fact that for any $\{0,1\}$ valued function f, one has $\sum_{x\in\mathbb{F}_2^n} f(x) = \sum_{x\in\mathbb{F}_2^n} f^2(x)$.

Lemma 3 (see [11]).
If f is a Boolean (n)–function then,

$$\sum_{x\in\mathbb{F}_2^n} f(x) = \sum_{x\in\mathbb{F}_2^n}\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} \tilde{f}(u)\tilde{f}(v)x^u x^v. \tag{23}$$

The next lemma expresses orthogonality between monomial functions.

Lemma 4 (see [11]). *Let $s,u\in\mathbb{F}_2^n$ then,*

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^n} (-1)^{\mathrm{hw}(x)} x^s u^x &= \sum_{x\in\mathbb{F}_2^n \mid s\preceq x\preceq u} (-1)^{\mathrm{hw}(x)} \\ &= \begin{cases} (-1)^{\mathrm{hw}(u)} & \text{if } s=u \\ 0 & \text{else} \end{cases}\end{aligned}$$

In particular, for $s=0$, $\sum_{x\in\mathbb{F}_2^n} (-1)^{\mathrm{hw}(x)} u^x = \begin{cases} 1 & \text{if } u=0 \\ 0 & \text{else.} \end{cases}$

As a straightforward consequence of Lemma 4 and relation (16), the following remark holds.

Remark 7. A Boolean function f is constant if and only if, for all nonzero vector $u\in\mathbb{F}_2^n$, $\tilde{f}(u)=0$.

Remark 8. From Lemma 2, it can be inferred whether a Boolean function is a constant function or not, given its 2^n-1 Walsh coefficients at the nonzero vectors.

The following result acts as a counterpart of Lemma 1 for NNF.

Proposition 3. *The Boolean function f is non constant if and only if the quantity* $\sum_{u\in\mathbb{F}_2^n \mid u\neq 0} \tilde{f}(u) 2^{-\mathrm{hw}(u)}$ *is non null.*

Proof. The following equalities hold:

$$\begin{aligned}\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{-\operatorname{hw}(u)} &= -\tilde{f}(0)+\sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n|x\preceq u}(-1)^{\operatorname{hw}(u)-\operatorname{hw}(x)}f(x)2^{-\operatorname{hw}(u)}\\ &= -\tilde{f}(0)+\sum_{x\in\mathbb{F}_2^n}(-1)^{\operatorname{hw}(x)}f(x)\sum_{u\in\mathbb{F}_2^n|u\succeq x}\left(-\frac{1}{2}\right)^{\operatorname{hw}(u)}\end{aligned}$$

For all vector $x\in\mathbb{F}_2^n$, the consideration of terms u whose weight is greater than $\operatorname{hw}(x)$ gives

$$\begin{aligned}\sum_{u\in\mathbb{F}_2^n|u\succeq x}\left(-\frac{1}{2}\right)^{\operatorname{hw}(u)} &= \sum_{j=0}^{n-\operatorname{hw}(x)}\binom{n-\operatorname{hw}(x)}{j}\left(-\frac{1}{2}\right)^{\operatorname{hw}(x)+j}\\ &= \left(-\frac{1}{2}\right)^{\operatorname{hw}(x)}\left(\frac{1}{2}\right)^{n-\operatorname{hw}(x)}\\ &= (-1)^{\operatorname{hw}(x)}\left(\frac{1}{2}\right)^{n}\end{aligned}$$

Then, noting that $\tilde{f}(0)=f(0)$, it follows that:

$$\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{-\operatorname{hw}(u)} = -f(0)+\left(\frac{1}{2}\right)^n\sum_{x\in\mathbb{F}_2^n}f(x).$$

Thus, the following equivalence holds:

$$\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{-\operatorname{hw}(u)}=0 \iff \sum_{x\in\mathbb{F}_2^n}f(x)=2^n f(0).$$

It is thereby proved that f is a constant Boolean function if and only if the value $\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{-\operatorname{hw}(u)}$ is null. □

Proposition 4. *Let f be a non constant Boolean (n)–function such that all the NNF coefficients are known except $\tilde{f}(0)$. Then f can be entirely recovered.*

Proof. The proof is constructive. Being known the NNF coefficients, the function f can be recovered from (16). In the sequel, it is shown how $\tilde{f}(0)$ can be expressed from other NNF coefficients. On one hand, from equality (16), it holds that

$$\sum_{x\in\mathbb{F}_2^n}f(x)=\sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n|x\succeq u}\tilde{f}(u)=\sum_{u\in\mathbb{F}_2^n}\tilde{f}(u)\sum_{x\in\mathbb{F}_2^n|x\succeq u}1=\sum_{u\in\mathbb{F}_2^n}\tilde{f}(u)\ 2^{n-\operatorname{hw}(u)}$$

and then

$$\sum_{x\in\mathbb{F}_2^n}f(x)=2^n\tilde{f}(0)+\sum_{u\in\mathbb{F}_2^n|u\neq 0}2^{n-\operatorname{hw}(u)}\tilde{f}(u) \tag{24}$$

On the other hand, relation (23) leads to:

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^n} f(x) &= \sum_{x\in\mathbb{F}_2^n}\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} \tilde{f}(u)\tilde{f}(v)x^u x^v \\ &= \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} \tilde{f}(u)\tilde{f}(v)\sum_{x\in\mathbb{F}_2^n} x^u x^v \\ &= \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} \tilde{f}(u)\tilde{f}(v)\sum_{x\in\mathbb{F}_2^n|x\succeq(u\vee v)} 1 \\ &= \sum_{u,v\in\mathbb{F}_2^n} \tilde{f}(u)\tilde{f}(v)\ 2^{n-\mathrm{hw}(u\vee v)}\end{aligned}$$

and then

$$\sum_{x\in\mathbb{F}_2^n} f(x) = 2^n\tilde{f}(0)+2\tilde{f}(0)\left[\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{n-\mathrm{hw}(u)}\right]+\sum_{\substack{u\in\mathbb{F}_2^n|u\neq 0\\ v\in\mathbb{F}_2^n|v\neq 0}}\tilde{f}(u)\tilde{f}(v)2^{n-\mathrm{hw}(u\vee v)} \quad (25)$$

Then, from relations (24) and (25), and in virtue of Proposition 3, it follows that:

$$\tilde{f}(0) = \frac{1}{2^{n+1}}\frac{\sum_{u\in\mathbb{F}_2^n|u\neq 0} 2^{n-\mathrm{hw}(u)}\tilde{f}(u) - \sum_{\substack{u\in\mathbb{F}_2^n|u\neq 0\\ v\in\mathbb{F}_2^n|v\neq 0}}\tilde{f}(u)\tilde{f}(v)2^{n-\mathrm{hw}(u\vee v)}}{\sum_{u\in\mathbb{F}_2^n|u\neq 0}\tilde{f}(u)2^{-\mathrm{hw}(u)}},$$

which completes the proof. □

We are now able to prove that the reduced matrix $P^\star$ is sufficient to get the whole polynomial matrix P.

Proposition 5. *An (n,m)–function can be recovered from its reduced polynomial matrix coefficients, provided that it is not a constant function.*

Proof. Recall that the coefficient $P_{u,v}$ of P is the value at vector v of the NNF of the function $x \longmapsto f(x)^u$. Hence, for all $u \in \mathbb{F}_2^n$ such that $\mathrm{hw}(u) = 1$, the coefficients of the row indexed by u of P correspond to the NNF values of the coordinate function f^u of f.
As f is not a constant function, it admits at least one non constant coordinate function f^u, where u is a vector of weight 1. From Remark 7, the non constant coordinates admit at least one nonzero NNF coefficient $\widetilde{f^u}(v) \neq 0$ where v is a nonzero vector in $\mathbb{F}_2^n$. Thus, from Proposition 4, the coordinate function f^u can be entirely recovered. It remains to recover the constant coordinates. They are characterized by a null row indexed by a vector of weight 1 in the reduced matrix $P^\star$. Let f^w such a constant coordinate of f, where $\mathrm{hw}(w) = 1$, and $g = f^u \cdot f^w$.

The NNF coefficients of g correspond to the row of $P^\star$ indexed by $u+w$, and one has:

$$\begin{aligned}\widetilde{g}(v) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{\mathrm{hw}(v)-\mathrm{hw}(x)} f^u(x) f^w(x) v^x \\ &= \begin{cases} \widetilde{f^u}(v) & \text{if } f^w \equiv 1 \\ 0 & \text{if } f^w \equiv 0 \end{cases}\end{aligned}$$

Hence the constant coordinate function of f can be recovered, which completes the proof. □

3.6 Similarity relations between the matrix representations

We prove in this subsection, for $m = n$, similarity relations that relate the polynomial matrix P, the correlation matrix $C = 2^{-n}W$ and the adjacency matrix A (with complex coefficients). We also show that, when the coefficients of the adjacency matrix A and of the polynomial matrix P are considered in $\mathbb{F}_2$, there exists a similarity transform that relates them. This relation allows to simplify the analysis of the eigenstructures of these matrices. This is typically the case for the issue addressed in Section 4.

The result below allows to relate the correlation matrix (or the Walsh matrix) of a function to the adjacency matrix of its graph.

Proposition 6. *Let f be an (n,n)–function, then its adjacency matrix A and its correlation matrix C are related by:*

$$A = H^{-1}\,{}^tCH, \tag{26}$$

where the matrix ${}^tC$ is the transpose of C and H is the Hadamard matrix (see (6)*).*

Proof. We show that (26) holds when both right and left hand sides are applied to the vectors of the canonical basis. Let e_x be the vector such that its x^{th} coordinate is 1 and the other components are zero. As a consequence, this vector can be interpreted as probability distribution. In view of Proposition 1, the vector $q = HCH^{-1}e_x$ is a probability vector and all its components equal zero except the component $y = f(x)$. This implies that the coefficients of the column x of HCH^{-1} are all zero except the one at row y. Therefore, for all $x, y \in \mathbb{F}_2^n$, the coefficient at row y and column x of HCH^{-1} is 1 if $x = f(y)$ and zero elsewhere. By definition, this is the transpose of the adjacency matrix. We recall that H is a symmetric matrix. Therefore, $H^{-1}\,{}^tCH$ is the adjacency matrix of f. □

The result below allows to relate the polynomial matrix of a function to the adjacency matrix of its graph.

Proposition 7. *Let f be an (n,n)–function, then, its polynomial matrix P and its adjacency matrix A are related by :*

$$P = M^{-1}AM. \tag{27}$$

where M is the monomial matrix defined by (18)*.*

Proof. As $M = Z^{-1}$, it must be shown that $PZ = ZA$. To this end, we show that each component of both matrices are equal. On one hand, the coefficient of ZA at row indexed by $u \in \mathbb{F}_2^n$ and column indexed by $v \in \mathbb{F}_2^n$ is:

$$\sum_{w \in \mathbb{F}_2^n} Z_{u,w} A_{w,v} = \sum_{w \in \mathbb{F}_2^n | v = f(w)} Z_{u,w}$$

On the other hand, the coefficient of PZ at row indexed by $u \in \mathbb{F}_2^n$ and column indexed by $v \in \mathbb{F}_2^n$ is:

$$\begin{aligned} \sum_{w \in \mathbb{F}_2^n} P_{u,w} Z_{w,v} &= \sum_{w \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} Z_{u,x} f(x)^w Z_{w,v} \\ &= \sum_{x \in \mathbb{F}_2^n} Z_{u,x} (-1)^{\mathrm{hw}(v)} \sum_{w \in \mathbb{F}_2^n} f(x)^w (-1)^{-\mathrm{hw}(w)} w^v \end{aligned}$$

In view of Lemma 4

$$\sum_{w \in \mathbb{F}_2^n} P_{u,w} Z_{w,v} = \sum_{x \in \mathbb{F}_2^n} Z_{u,x} (-1)^{\mathrm{hw}(v)} \underbrace{\sum_{w \in \mathbb{F}_2^n | v \preceq w \preceq f(x)} (-1)^{-\mathrm{hw}(w)}}_{\begin{cases} (-1)^{-\mathrm{hw}(v)} & \text{if } v = f(x) \\ 0 & \text{else} \end{cases}}$$

This shows that all entries of matrices PZ equal those of ZA. □

Remark 9. When they are reduced modulo 2, the entries of the matrices A and P can also be considered as elements on $\mathbb{F}_2$, and then Proposition 7 holds.

Considering Propositions 6 and 7 and taking into account the fact that a matrix and its transpose are similar, we conclude that $A, {}^tA, P$ and C are similar matrices.

3.7 Matrix representation and composition

It has been noted in [4] that the correlation matrix of the composition of two functions is the product of the correlation matrices of these functions. From Propositions 6 and 7, it is clear that this property holds for the adjacency matrix and for the polynomial matrix. As a result, the following proposition holds.

Proposition 8. *If f is a Boolean (n,m)–function and g is a (p,n)–function then, the matrix representations of the composition $f \circ g$, for the adjacency matrix A, correlation matrix C and polynomial matrix P, are given by:*

$$A_{f \circ g} = A_g A_f \tag{28}$$

$$C_{f \circ g} = C_f C_g \tag{29}$$

$$P_{f \circ g} = P_f P_g. \tag{30}$$

The following relations between matrix product and function composition also hold for reduced correlation and polynomial matrices.

Corollary 1. *If f is an (n,m)–function and g is a (p,n)–function then:*

$$C^\star_{f\circ g} = C^\star_f C^\star_g \tag{31}$$
$$P^\star_{f\circ g} = P^\star_f P^\star_g, \tag{32}$$

where $C^\star_f$ (resp. $P^\star_f$) denotes the reduced correlation (resp. the reduced polynomial) matrix of f.

Proof. This is a consequence of Proposition 8 and the fact that all the coefficients of the first row of the correlation and of the polynomial matrices are null except the coefficient of the first column. □

4 Eigenanalysis of the matrix representation

Let f be an (n,n)–function, the adjacency matrix A, the polynomial matrix P and the correlation matrix C are square matrices. This section is devoted to the eigenanalysis of these matrices. Due to the similarity relations, the eigenvalue analysis can be done on any of them. The study of the eigenvectors depends on the matrix under consideration. However, as the adjacency matrix has exactly one nonzero component equal to 1 per row, the study is easier on this matrix. As explained in Section 3.1, it is possible to associate a graph $\mathcal{G}$ to the function f. This section establishes connections between the eigenanalysis of the matrix representations of a vectorial Boolean function and its graph representation.
We show that the eigenvalues of the representation matrices are directly related to the number of cycles, to their length and to the number of leaves in the graph $\mathcal{G}$. It has been mentioned in Section 3.6 that, the adjacency matrix A can be considered either as a $\mathbb{C}$-valued matrix or an $\mathbb{F}_2$-valued matrix. The eigenanalysis below is performed in the field $\mathbb{C}$ of complex number, and thus, the eigenvectors are 2^n-dimensional complex vectors. Hence, each eigenvector can be indexed by the vertices of the graph $\mathcal{G}$ associated to the function f, since those vertices are elements of $\mathbb{F}_2^n$.
Section 4.1 is devoted to eigenvalues. In section 4.2, we show how to determine the corresponding eigenvectors of the adjacency matrix from the graph $\mathcal{G}$ of the function f.

4.1 Eigenvalues

Proposition 9. *The eigenvalues of the matrices A, P and C are either zero or roots of unity.*

Proof. Due to the similarity properties, the reasoning is performed for the adjacency matrix A, and the result still holds for the others matrices.

Let $\alpha \in \mathbb{C}$ be an eigenvalue of A and $v \in \mathbb{C}^n$ be an associated eigenvector, *i.e* $Av = \alpha v$. *Each row of* A *has only one nonzero coefficient which equals* 1.
From (28)*, for any integer* k, A^k *is the adjacency matrix of* f^k. *The sequence* $\left(A^k\right)_{k\in\mathbb{N}}$ *lies in a finite space and thus is ultimately periodic.*
Therefore, there exist two integers $i < j$ *such that* $A^i v = A^j v$ *and then,* $\alpha^i v - \alpha^j v = 0$. *It follows that* $\alpha^i(1-\alpha^{j-i})v = 0$, *which implies that either* $\alpha = 0$ *or* $1 - \alpha^{j-i} = 0$, *that is* α *is a root of unity.* □
The following proposition makes a connection between the eigenvalue zero and the leaves of the graph $\mathcal{G}$.

Proposition 10. *Let* f *be an* (n, n)*–function. Zero is an eigenvalue of the adjacency matrix* A *of* f *if and only if there exists a leaf in the graph* $\mathcal{G}$ *of* f.

Proof. By definition, if $x \in \{0,1\}^n$ is a leaf in the graph $\mathcal{G}$, then the column x of the adjacency matrix A is null. Let $e_x \in \{0,1\}^n$ be the vector whose components are all null except the one at row indexed by x which equals one. Thus, $Ae_x = 0$ and e_x is an eigenvector of the matrix A associated to the eigenvalue zero. Conversely, let $u \in \mathbb{C}^n$ be an eigenvector of A associated to the eigenvalue zero. Since each row of the adjacency matrix has exactly one nonzero coefficient, $Au = 0$ if and only if the columns of A whose indexes correspond to the nonzero components of the vector u are null, and the index of each null column of A indicates a leaf of the graph. That completes the proof. □

Remark 10. The proof of Proposition 10 gives a construction of eigenvectors related to the zero eigenvalue. There exists a simpler proof. Assuming that $x \in \{0,1\}^n$ is a leaf, the column x of the adjacency matrix A is null, which implies that the determinant of A is null too. Since this determinant equals the product of the eigenvalues, this means that 0 is an eigenvalue of A.
Conversely, if 0 is an eigenvalue of A, the kernel of the endomorphism associated to A is not reduced to zero. Thus, this endomorphism is not surjective, which indicates that the graph of f has a leaf.

Remark 11. If f is an (n, n)–function, let E_0 be the eigenspace of the eigenvectors associated to the eigenvalue zero of the adjacency matrix A of f. Then, the dimension of E_0 equals the number of leaves in the graph $\mathcal{G}$ of f.
If v is an eigenvector of the eigenvalue 0 for the adjacency matrix A then, $Av = 0$, and this is equivalent to $v_{f(x)} = 0$ for all $x \in \mathbb{F}_2^n$. Hence, it follows that the support of v is included in the set of the leaves of the graph and then E_0 is spanned by the vectors e_y as defined in the proof of Proposition 10 where y is a leaf of the graph.

Remark 12. The eigenvectors defined in the proof of Proposition 10 shows that eigenvectors can be interpreted as functions. Indeed, let f be an (n, n)–function and g an (n)–function. If $g \circ f = 0$ then the truthtable of g is an eigenvector for the eigenvalue 0 of A_f. Conversely, assume that g is an eigenvector of A_f associated to the eigenvalue 0 such that all its components are either zero or one then, $g \circ f = 0$.

Note that whenever the eigenvectors of the adjacency matrix of f associated to 0 are obtained as explained in the proof of Proposition 10, we can determine all the Boolean functions g for which Remark 12 applies. They are the set of all linear combinations with $\{0,1\}$ coefficients of the eigenvectors associated to 0. There is not any other one. Hence, if there are ℓ leaves in the graph $\mathcal{G}$, there are exactly 2^ℓ (n)–functions g such that $g \circ f = 0$.

We are now interested in nonzero eigenvalues. From Proposition 9, those eigenvalues are roots of unity.

Proposition 11. *Let f be an (n,n)–function, α be a nonzero eigenvalue of the adjacency matrix of f and let v be an eigenvector for the eigenvalue α. Let ℓ be the order of α and $x \in \{0,1\}^n$ be a n-dimensional binary vector. If the component v_x of vector v is nonzero, then the length of the ultimate cycle of the connected component of the graph $\mathcal{G}$ that contains x is multiple of ℓ.*

Proof. Let $x \in \{0,1\}^n$. By definition of the adjacency matrix of f and as v is an eigenvector for the eigenvalue α, one has $v_{f(x)} = \alpha v_x$. By induction, for all integer k:

$$v_{f^k(x)} = \alpha^k v_x. \tag{33}$$

By iterating enough the function f from the vector x, the vertex $f^i(x)$ falls into the ultimate cycle of the connected component of x as illustrated in Figure 2. Thus, there exists an integer i such that $f^i(x)$ belongs to this cycle. Let ℓ' be its length. By assumption, $f^{\ell'+i}(x) = f^i(x)$. From relation (33), $\alpha^{\ell'+i} v_x = \alpha^i v_x$. As v_x is assumed to be nonzero, $\alpha^{\ell'} = 1$ and this proves that ℓ' is multiple of ℓ. □

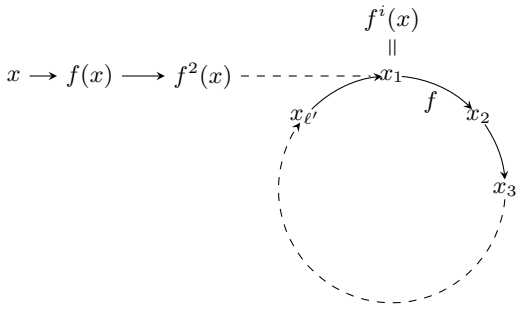

Fig. 2: The vertex x of the connected component is connected to its ultimate cycle by a path of length i whose elements are the iteration of the (n,n)–function f on the vertex x. This path is $\big(x, f(x), f^2(x), \ldots, f^i(x) = x_1\big)$.

Now, let us deal with the dimension of the eigenspaces. Let us denote by E_α the eigenspace associated to the eigenvalue α of the adjacency matrix of the (n,n)–function f. As stated at the beginning of Section 4, each eigenvector v

associated to α can be indexed by the vertices of the graph $\mathcal{G}$. Thus, the support of v is defined as:

$$\mathrm{supp}(v) = \{x \in \mathbb{F}_2^n \mid v_x \neq 0\}$$

Proposition 12. *Let α be a nonzero eigenvalue of the adjacency matrix of the (n,n)–function f and $\mathcal{C}$ be a connected component of the graph $\mathcal{G}$ whose ultimate cycle length is multiple of the order of α. Then, the subspace of E_α of the vectors whose support is included in $\mathcal{C}$ is of dimension 1.*

Proof. Let us choose any fixed vertex x_1 in $\mathcal{C}$. For all vertices x in $\mathcal{C}$, there exist two integers i and j such that $f^i(x) = f^j(x_1)$. Let w be the 2^n–dimensional complex vector whose components are defined, for all $x \in \{0,1\}^n$ by:

$$w_x = \begin{cases} 0 & \text{if } x \notin \mathcal{C}, \\ \alpha^{j-i} & \text{if } x \in \mathcal{C}, \text{ where } i \text{ and } j \text{ are defined as above.} \end{cases}$$

By construction, w is a nonzero eigenvector associated to the eigenvalue α whose support is included in $\mathcal{C}$, and thus, the subspace of E_α whose support is included in $\mathcal{C}$ is of dimension at least 1.
Now, let x and y be two vertices in $\mathcal{C}$, and i and j two integers such that $f^i(x) = f^j(y)$. From relation (33), for each eigenvector u for the eigenvalue α whose support is included in $\mathcal{C}$, one has: $u_{f^i(x)} = \alpha^i u_x = u_{f^j(y)} = \alpha^j u_y$. And thus

$$u_y = \alpha^{i-j} u_x.$$

Hence $u_x \neq 0$ for all $x \in \mathcal{C}$, and the support of u is $\mathcal{C}$. Let v be another such eigenvector for the eigenvalue α and let $\lambda = v_x/u_x$. From the above relation, one obtains:

$$v_y = \alpha^{i-j} v_x = \lambda \alpha^{i-j} u_x = \lambda u_y.$$

Thus, for all vertices $y \in \mathcal{C}$, one has $v_y/u_y = \lambda$. As a consequence, the vectors u and v are proportional and this shows that the subspace of E_α of vectors whose support is included in $\mathcal{C}$ is of dimension 1. □

The following proposition gives the dimension of the eigenspace E_α.

Proposition 13. *Let α be a nonzero eigenvalue of the adjacency matrix of an (n,n)–function. The dimension of the vectorspace E_α equals the number of cycles in the graph $\mathcal{G}$ whose length are multiple of the order of α.*

Proof. Let $\mathcal{C}_1, \ldots, \mathcal{C}_k$ be the k connected components that involve a cycle of length multiple of the order of α. For $i \in \{1, \ldots, k\}$, let H_i be the vector space of vectors whose support are included in $\mathcal{C}_i$. From Proposition 12, the vector spaces $E_\alpha \cap H_i$ are all 1 dimensional. On the other hand, theses spaces are pairwise complementary as the support of their vectors are disjoint. From Proposition 11, they span E_α and this achieves the proof. □

According to Remark 3, there always exists a cycle in the graph and thus 1 is always an eigenvalue of the adjacency matrix.

Corollary 2. *Let f be an (n,n)–function. The function f is an involution if and only if the eigenvalues of its adjacency matrix are either -1 or 1.*

Proof. An involution is an invertible function. Hence, there are no leaf in the associated graph. Besides, all the vertices belong to a cycle of length one or two. According to Propositions 10 and 13, the only admissible eigenvalues are -1 and 1. □

4.2 Eigenvectors

In this section, we are interested in identifying the eigenvectors associated to the eigenvalues for the adjacency matrix A, the polynomial matrix P and the correlation matrix C. Unlike eigenvalues, eigenvectors are basis-dependent. Due to Proposition 7, eigenvectors of P and C are easily deduced from eigenvectors of the adjacency matrix A. For each matrix, there is a natural way to derive a basis of the eigenspaces from the graph of the function.

4.2.1 Eigenvectors of the adjacency matrix A

The following proposition shows that the eigenvectors of the adjacency matrix A corresponding to the zero eigenvalue are deduced from the junctions of the graph $\mathcal{G}$ of the function f.

Proposition 14. *Assume that the vertex y is a junction of the (n,n)–function f and let x_1 and x_2 be two incident vertices of this junction. Let e_{x_1} (respectively e_{x_2}) be the 2^n-dimensional vector such that all its components are null except the one at coordinate x_1 (respectively x_2) which equals 1. Then, the vector $e = e_{x_1} - e_{x_2}$ is an eigenvector of the matrix ${}^tA$ for the eigenvalue 0.*

Proof. By assumption, the equality $f(x_1) = f(x_2)$ holds. Let $y = f(x_1)$ and e_y the 2^n-dimensional vector such that all its components equal 0, except the coordinate y which equals 1. One has $e_y = {}^tAe_{x_1}$ and $e_y = {}^tAe_{x_2}$. Thus, ${}^tA(e_{x_1} - e_{x_2}) = 0$ which completes the proof. □

Remark 13. According to Remark 4, from each junction of multiplicity k in $\mathcal{G}$, it is possible to get k independent eigenvectors of ${}^tA$ for the eigenvalue 0.

Remark 14. Conversely, if v is an eigenvector of ${}^tA$ for the eigenvalue 0, then the support of v is included in the set of preimages of junctions in the graph $\mathcal{G}$ of f.

Proposition 15. *Let $\mathcal{L} = (x_0, \ldots, x_{\ell-1})$ be a cycle of length ℓ of the graph $\mathcal{G}$ associated to an (n,n)–function, and α be a ℓ^{th} root of unity. Then, for i in $\{0, \ldots, \ell-1\}$, the complex number α^i is an eigenvalue of the adjacency matrix A. For every $i \in \{0, 1, \ldots, \ell-1\}$, an eigenvector v of α^i associated to the transpose matrix ${}^tA$ of A is given by:*

$$v_{x_j} = \begin{cases} \alpha^{i(\ell-j)} & \text{if } x_j \in \mathcal{L} \\ 0 & \text{elsewhere.} \end{cases} \tag{34}$$

Proof. It suffices to show that each vector $v = (v_x)_{x\in\mathbb{F}_2^n}$ defined by (34) is an eigenvector for α^i.
Let w be the vector defined by $w = {}^tAv$. One has $w_x = \sum_{y\in\mathbb{F}_2^n} A_{y,x}v_y = \sum_{y\in\mathbb{F}_2^n,\, x=f(y)} v_y$.
It must be shown that $w = \alpha^i v$. To this end, the two following cases are distinguished:

- if $x \notin \mathcal{L}$, then there is no element $y \in \mathcal{L}$ such that $x = f(y)$. As a result, $\sum_{y\in\mathbb{F}_2^n,\, x=f(y)} v_y = 0$ and then $w_x = 0$. Besides, from (34), one has $v_x = 0$ and then $w_x = \alpha^i v_x$,
- if $x = x_j \in \mathcal{L}$, then one has $w_{x_j} = v_{x_{j-1}}$ that is, $w_{f(x_{j-1})} = v_{x_{j-1}}$. By assumption, $v_{x_{j-1}} = \alpha^{i(l-j+1)} = \alpha^i\alpha^{i(l-j)} = \alpha^i v_{x_j}$ and then $w_x = \alpha^i v_x$ for all $x \in \mathcal{L}$.

As a consequence, the equality $w = Av = \alpha^i v$ holds in both cases. □

Proposition 16. *The trace of the adjacency matrix of f is the number of cycles of length one.*

Proof. According to Proposition 15, from each cycle of length ℓ, we can derive an ℓ^{th} root of unity as eigenvalue. The other eigenvalue is 0. The sum of all the ℓ^{th} roots of the unity equals zero except when $\ell = 1$. In this latter case, it equals one. □

Remark 15. As the trace is invariant under similarities, Proposition 16 also holds for polynomial and correlation matrices.

Remark 16. The result of Proposition 16 can be proved by noting that for $x \in \mathbb{F}_2^n$, the coefficient $A_{x,x}$ belonging to the main diagonal of the adjacency matrix A equals 1 if and only if the vector $f(x) = x$. Then the result holds, as the trace of a matrix is the sum of the main diagonal coefficients.

As an example, we show how to derive the eigenstructures of A_{f_e} based on the graph of Figure 1.
According to Proposition 14, the four eigenvectors associated to 0 are related to:

- the junction 010 with preimage set $\{000, 100, 110\}$ and thus multiplicity two,
- the junction 101 with preimage set $\{011, 101\}$ and thus multiplicity one.

The eigenvectors are denoted by a_0, a_1, a_2, a_3 and can be derived as follows.

$$a_0 = e_{x_1} - e_{x_5} = \begin{pmatrix} 1\\0\\0\\0\\-1\\0\\0\\0 \end{pmatrix}, \qquad a_1 = e_{x_1} - e_{x_7} = \begin{pmatrix} 1\\0\\0\\0\\0\\0\\-1\\0 \end{pmatrix}$$

$$a_2 = e_{x_5} - e_{x_7} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \qquad a_3 = e_{x_4} - e_{x_6} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

According to Proposition 15, due to the cycle $(101, 101)$, the following vectors are eigenvectors for the eigenvalues 1.

$$a_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad a_5 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

These two eigenvectors are obtained from the cycles of length one and three respectively in the graph.
According to Proposition 15, the following eigenvectors exist and are respectively associated to the eigenvalues $\jmath$ and $\jmath^2$, where $\jmath = \dfrac{1 + \imath\sqrt{3}}{2}$ is a primitive cube root of unity.

$$a_6 = \begin{pmatrix} 0 \\ \jmath \\ \jmath^2 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; a_7 = \begin{pmatrix} 0 \\ \jmath^2 \\ \jmath \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The eigenvectors of the correlation and polynomial matrices can be respectively obtained by applying the Hadamard matrix H given by (6) and the monomial matrix M given by (18) to the vectors a_0, a_1, a_2, a_3, a_4, a_5, a_6.
It is shown in the sequel that, from the eigenvectors of the adjacency matrix A, the change of basis of Proposition 6 and of Proposition 7 can be used to determine respectively the eigenspaces of the correlation matrix C and the polynomial matrix P.

4.2.2 Eigenvectors of the correlation matrix C

From (26), the eigenvectors of C can be deduced from those of ${}^tA$. If v is an eigenvector for ${}^tA$, then, due to (5), the Fourier transform of v, denoted by

$\widehat{v} = Hv$ is an eigenvector of the Walsh matrix W and so of the correlation matrix C. Therefore:

$$\forall y \in \mathbb{F}_2^n,\ \widehat{v}_y = \sum_{x \in \mathbb{F}_2^n} v_x (-1)^{x \cdot y}. \tag{35}$$

If v is an eigenvector of ${}^tA$ associated to the eigenvalue 0, then from Remark 14, the support of v is included in the set of preimages of the junctions in the graph $\mathcal{G}$.

Due to Equation (20), the eigenvalues of the Walsh matrix W are merely the eigenvalues of the ones of the correlation matrix C times 2^n. Thus, the eigenvectors are the same.

4.2.3 Eigenvectors of the polynomial matrix P

The eigenvectors of the polynomial matrix P can also be deduced from those of the adjacency matrix A by applying (27). If v is an eigenvector of A then $\widetilde{v} = Zv$ is an eigenvector of P. Therefore:

$$\forall y \in \mathbb{F}_2^n,\ \widetilde{v}_y = \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathrm{hw}(x) - \mathrm{hw}(y)} y^x v_x.$$

In the case when v is an eigenvector of A associated to the eigenvalue 0, the support of v is included in the set of the leaves of the graph $\mathcal{G}$.

5 Conclusion

In this paper, a unified overview on the various representations of vectorial Boolean functions, namely the Walsh matrix, the correlation matrix and the adjacency matrix, has been given. A new representation called polynomial matrix has been introduced with an interest when dealing with algebraic properties. It has been shown that those different representations are similar.
Then, an eigenanalysis of those representations has been performed. It has been shown that, for all the representations, the eigenvalues are either zero or roots of unity. For a given vectorial Boolean function with the same number of inputs and outputs, a link has been made between the eigenvalues of its matrix representations and the structure of the graph assigned to this function. The distinction between zero and nonzero eigenvalues plays an important role for that purpose. Finally, the eigenspace associated to the eigenvalues of the matrix representations has been studied. For nonzero eigenvalues, the corresponding eigenvectors can be determined from the cycles of the graph. On the other hand, the eigenvector corresponding to the zero and unique eigenvalue can be determined by the junctions of the graph.
We think that this work can be helpful, not only to people working in the realm of Boolean function in general, but also to people interested in application of Boolean functions to cryptography.

Acknowledgment
This work was partially supported by Research Grants ANR-13-INSE-0005-01 from the Agence Nationale de la Recherche. We also thank Eric Garrido for providing the idea of introducing the polynomial matrices.

References

1. C. Carlet. Boolean functions for cryptography and error-correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge Press, 2010.
2. Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, pages 549–562, 1989.
3. Dorothy Bollman, Omar Colón-Reyes, Victor A. Ocasio, and Edusmildo Orozco. A control theory for boolean monomial dynamical systems. *Discrete Event Dynamic Systems*, 20(1):19–35, 2010.
4. J. Daemen, R. Govaerts, and J. Vandewalle. Correlation matrices. In *Fast Software Encryption : Second International Workshop, LNCS 1008*, pages 275–285. Springer-Verlag, 1994.
5. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes*. Number pties. 1 à 2 in North-Holland mathematical library. North-Holland Publishing Company, 1977.
6. C. Carlet and P. Guillot. A new representation of boolean functions. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Computer Science*, pages 731–731. Springer Berlin / Heidelberg, 1999. 10.1007/3-540-46796-3_10.
7. C. Carlet. Vectorial boolean functions for cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge Press, 2010.
8. C. Godsil and G. Royle. *Algebraic Graph Theory*. Springer, 2001.
9. François Robert and J. Jon Rokne. *Discrete iterations : a metric study*. Springer series in computational mathematics. Springer-Verlag, Berlin, New York, Tokyo, 1986.
10. J. Parriaux, P. Guillot, and G. Millérioux. Towards a spectral approach for the design of self-synchronizing stream ciphers. *Cryptography and Communications*, 3:259–274, 2011. 10.1007/s12095-011-0046-2.
11. P. Guillot. *Fonctions courbes binaires et transformation de Möbius*. PhD thesis, 1999.