Minimal polynomial of Cayley graph adjacency matrix for Boolean functions

Michel Mitton
SGDN/DCSSI/SDS/Crypto Lab

51 boulevard de la Tour-Maubourg
75700 Paris-07 SP, France
e-mail: michel.mitton@sgdn.pm.gouv.fr

April 23, 2007

Abstract

The subject of this paper is the algebraic study of the adjacency matrix of the Cayley graph of a Boolean function. From the characteristic polynomial of this adjacency matrix we deduce its minimal polynomial.

Keywords

Boolean functions, Walsh and Fourier transforms, Cayley graph, adjacency matrix, homomorphisms of algebras, characteristic and minimal polynomials.

1 Introduction

In a previous paper [1], we have obtained the polynomial expression of

$$P(X) = \prod_{a \in \mathbf{F}_2^n} (X - W_f(a))$$

and as a corollary, the evaluation of $\prod_{a \in \mathbf{F}_2^n} W_f(a)$ where f is an arbitrary Boolean function of n variables and W_f the Walsh spectrum of f.

The proofs of these results are based on the use of the adjacency matrix $M_f = (f(i \oplus j)_{i \in [0,2^n-1], j \in [0,2^n-1]})$ of the Cayley graph of f (see [2], [3]) associated with the Cayley set $f^{-1}(1)$.

If we consider M_f as an element of $M_{2^n}(\mathbf{R})$, the $\mathbf{R}-$ algebra of the $2^n \times 2^n$ matrix in real coefficients for matrix addition, multiplication, and product by a real, we can consider the homomorphism of $\mathbf{R}-$ algebras

$$\Psi_f : \mathbf{R}[X] \to M_{2^n}(\mathbf{R})$$

$$Q(X) \longmapsto \Psi_f(Q(X)) = Q(M_f). \tag{1}$$

We have seen in [1] that, if we denote $P(X) = \det_{\mathbf{R}}(M_f - XI_{2^n})$ the characteristic polynomial of M_f, we have $P(X) = \prod\limits_{a\in\mathbf{F}_2^n} (X - W_f(a))$.

Our aim in the sequel is to compute the minimal polynomial of Ψ_f and to obtain some properties of this polynomial.

2 Basic definitions and notation

In this paper, the finite field $(\mathbf{Z}/2\mathbf{Z}, \oplus, .)$ with its additive and multiplicative laws will be denoted by $\mathbf{F}_2$ and the $\mathbf{F}_2$-algebra of Boolean functions of n variables $\mathcal{F}(\mathbf{F}_2^n, \mathbf{F}_2)$ will be denoted by $\mathcal{F}$.

$(\mathbf{R}, +_{\mathbf{R}}, \cdot_{\mathbf{R}})$ denotes the field of the real numbers.

For $f \in \mathcal{F}$ and $a \in \mathbf{F}_2$, recall that $f^{-1}(a) = \{u \in \mathbf{F}_2^n | f(u) = a\}$.

$W_f(a)$ is the Walsh spectrum of $f \in \mathcal{F}$ to a point $a = (a_0, ..., a_{n-1}) \in \mathbf{F}_2^n$ defined by

$$W_f(a) = \sum_{x\in\mathbf{F}_2^n} f(x)(-1)^{<a,x>}. \tag{2}$$

In this formula, the sum on the right is calculated in $\mathbf{Z}$, and $< a, x >= a_0x_0 \oplus ... \oplus a_{n-1}x_{n-1}$ represents the scalar product on $\mathbf{F}_2^n$.

Sometimes, we will identify $\mathbf{F}_2^n$ with $[0, 2^n - 1]$, or with the subset $\{0, 1\}^n$ of $\mathbf{R}^n$. In this last case $< a, x >_{\mathbf{R}}= a_0x_0 +_{\mathbf{R}} ... +_{\mathbf{R}} a_{n-1}x_{n-1}$ denotes the scalar product on $\mathbf{R}^n$.

Remark that, for each $x, y \in \mathbf{Z}$,$(-1)^{x+_{\mathbf{R}}y} = (-1)^{x\oplus \mathbf{y}}$.

We denote δ_a^b the Kronecker's symbol. With the following notation

$W_f^*(a) = 2^{n-1}\delta_a^0 - W_f(a)$, we have the relation $2W_f^*(a) = \hat{f}(a)$ between Walsh and Fourier transforms, with

$\hat{f}(a) = \sum\limits_{x\in\mathbf{F}_2^n} (-1)^{f(x)+_{\mathbf{R}}<a,x>} = \sum\limits_{x\in\mathbf{F}_2^n} (-1)^{f(x)\oplus<a,x>}$.

Each $f \in \mathcal{F}$ verifies the important Parseval's relation

$$\sum_{a\in\mathbf{F}_2^n} \left(W_f^*(a)\right)^2 = 2^{2(n-1)}. \tag{3}$$

If R is a ring, for each $r \in R$ we denote $(r) = rR$ the principal ideal generated by r, and $R[X]$ is the ring of polynomials in the indeterminate X over R.

For $P(X), Q(X) \in R[X]$, we denote $P(X)|Q(X)$ when $P(X)$ divides $Q(X)$.

$\deg P(X)$, $\gcd(P(X), Q(X))$ and $\mathrm{lcm}(P(X), Q(X))$ denotes, in $R[X]$, respectively the degree of $P(X)$, the greatest common divisor and the least common multiple of $P(X)$ and $Q(X)$.

In [2][3], the Walsh-Fourier analysis is viewed as an eigenvalue problem of adjacency matrix of Cayley graph.

For $f \in \mathcal{F}$, we consider $f^{-1}(1)$ and the following graph G_f where the vertex set is $\mathbf{F}_2^n$, and the edge set is defined by

$$\{(a, b) \in \mathbf{F}_2^n \times \mathbf{F}_2^n | a \oplus b \in f^{-1}(1)\}.$$

This definition implies that $G_f = G(\mathbf{F}_2^n, f^{-1}(1))$ is the Cayley graph of $\mathbf{F}_2^n$ with respect to the Cayley set $f^{-1}(1)$, and the symmetric matrix $M_f = (m_{i,j})_{i,j \in [0,2^n-1] \times [0,2^n-1]}$ with $m_{i,j} = f(i \oplus j)$ is the adjacency matrix of G_f, where we identify $[0, 2^n - 1]$ with $\mathbf{F}_2^n$.

For a detailed study on this topic, see [2], [3] and [4].

For each $a \in \mathbf{F}_2^n$ we denote $\chi_a =^t ((-1)^{<a,0>}, (-1)^{<a,1>}, ..., (-1)^{<a,2^n-1>}) \in \mathbf{R}^{2^n}$. It can be shown that $M_f \chi_a = W_f(a)\chi_a$.

3 The minimal polynomial of Ψ_f

Let us consider Ψ_f and its kernel $\Psi_f^{-1}(0) \subset \mathbf{R}[X]$. We know that $\mathbf{R}[X]$ is a principal ring.

As $\Psi_f^{-1}(0)$ is an ideal of $\mathbf{R}[X]$, there exists only one monic polynomial $I(X)$ such that $\Psi_f^{-1}(0)$ is a principal ideal generated by $I(X)$: $\Psi_f^{-1}(0) = (I(X))$.

$I(X)$ is called the minimal polynomial associated with Ψ_f and, from the Hamilton-Cayley's theorem applied to the characteristic polynomial $P(X) = \det_{\mathbf{R}}(M_f - XI_{2^n})$, we obtain $\Psi_f(P(X)) = P(M_f) = O_{2^n}$, so $P(X) \in \Psi_f^{-1}(0)$ and finally $I(X) | \prod_{a \in \mathbf{F}_2^n} (X - W_f(a))$.

We deduce from this that there exists a subset $E \subset \mathbf{F}_2^n$ such that $I(X) = \prod_{a \in E} (X - W_f(a))$.

Our aim is now to determine explicitely E.

First, we have the following lemma:

Lemma 1 *Let R be a field. For each $r \in R$ and each $Q(X) \in R[X]$ where $\deg Q(X) > 0$, we have $X - r | Q(X)$ or $\gcd(X - r, Q(X)) = 1$.*

Proof. As $\deg(X - r) > 0$ and R a field, the property of the Euclidean division implies the existence of two polynomials $S(X)$ and $T(X)$ in $R[X]$ such that $Q(X) = (X - r)S(X) + T(X)$ where $0 \leq \deg T(X) < \deg(X - r) = 1$.

We deduce from this that $T(X) \in R$ so we have the two following cases:

– $T(X) = 0$ and then $X - r | Q(X)$.

– $T(X) \neq 0$ and, bccause R is a field, $T(X)$ is invertible in R. So we can write $Q(X)T(X)^{-1} - (X - r)S(X)T(X)^{-1} = 1$ which implies, from Bezout's theorem, $\gcd(X - r, Q(X)) = 1$. ■

This lemma is useful to prove the following second lemma:

Lemma 2 *For each $a \in \mathbf{F}_2^n$, $(X - W_f(a))|I(X)$.*

Proof. We have seen that $I(X)|P(X)$, so $I(X) \neq 0$.

If $\deg I(X) = 0$, then $I(X) \in \mathbf{R} - \{0\}$ so $(I(X)) = \mathbf{R}[X]$ and $\Psi_f(Q(X)) = O_{2^n}$ for each $Q(X)$, which contradicts $\Psi_f(1) = I_{2^n}$. Consequently we have $\deg I(X) > 0$.

If we suppose now $(X - W_f(a)) \nmid I(X)$, the precedent lemma implies $\gcd(X - W_f(a), I(X)) = 1$ so there exists $A(X), B(X)$ in $\mathbf{R}[X]$ such that $A(X)(X - W_f(a)) + B(X)I(X) = 1$.

Using Ψ_f and $I(M_f) = O_{2^n}$, we obtain $A(M_f)(M_f - W_f(a)I_{2^n}) = I_{2^n}$ which implies $M_f - W_f(a)I_{2^n} \in GL_{2^n}(\mathbf{R})$.

On the other hand, we have seen in [1] that, for M_f, χ_a is an eigenvector associated to the eigenvalue $W_f(a)$, i.e. $(M_f - W_f(a)I_{2^n})\chi_a = 0$ with 0 the null vector in $\mathbf{R}^{2^n}$. This last property, together with $M_f - W_f(a)I_{2^n} \in GL_{2^n}(\mathbf{R})$, finally implies $\chi_a = 0$ and we obtain a contradiction which proves the initial property $(X - W_f(a))|I(X)$. ■

We can now state the following.

Theorem 3 *For each $f \in \mathcal{F}$, $I(X) = \prod\limits_{m \in W_f(\mathbf{F}_2^n)} (X - m)$.*

Proof. Let us consider the polynomial $J(X) = \prod\limits_{m \in W_f(\mathbf{F}_2^n)} (X - m)$.

If $m \in W_f(\mathbf{F}_2^n)$, there exists $a \in \mathbf{F}_2^n$ such that $m = W_f(a)$ and then, from lemma 2, we have $X - m|I(X)$. Then $I(X)$ is a common multiple of all the polynomials $X - m$ for each $m \in W_f(\mathbf{F}_2^n)$, so we obtain firstly $J(X) = \operatorname{lcm}\limits_{m \in W_f(\mathbf{F}_2^n)} (X - m)|I(X)$.

Now, consider $a \in \mathbf{F}_2^n$.

We have $\Psi_f(J(X))\chi_a = J(M_f)\chi_a = \left(\prod\limits_{m \in W_f(\mathbf{F}_2^n)} (M_f - mI_{2^n}) \right) \chi_a$

$= \left(\prod\limits_{m \in W_f(\mathbf{F}_2^n), m \neq W_f(a)} (M_f - mI_{2^n}) \right) ([M_f - W_f(a)I_{2^n}]\chi_a)$.

But $[M_f - W_f(a)I_{2^n}]\chi_a = M_f(\chi_a) - W_f(a)\chi_a = 0$ so we obtain

$\Psi_f(J(X))\chi_a = \left(\prod\limits_{m \in W_f(\mathbf{F}_2^n), m \neq W_f(a)} (M_f - mI_{2^n}) \right) (0) = 0.$

Furthermore, if we consider each vector χ_a as a vector in $\mathbf{R}^{2^n}$ it is easy to see that the 2^n vectors $(\chi_a)_{a \in \mathbf{F}_2^n}$ form an orthogonal basis of the $\mathbf{R}-$vector space $\mathbf{R}^{2^n}$ for the usual real scalar product $< .,. >_{\mathbf{R}}$.

As $\Psi_f(J(X))\chi_a = 0$ for each $a \in \mathbf{F}_2^n$, from the precedent property we deduce $\Psi_f(J(X))u = 0$ for each $u \in \mathbf{R}^{2^n}$, which finally gives us $\Psi_f(J(X)) = O_{2^n}$.

Then we have proved that $J(X) \in \Psi_f^{-1}(0) = (I(X))$, i.e. $I(X)|J(X)$.

As we have also proved $J(X)|I(X)$ and as $I(X)$ and $J(X)$ are monic polynomials, we obtain $I(X) = J(X)$. ■

From this theorem, we deduce the corollary below.

Corollary 4 *For each $f \in \mathcal{F}$, if $n \geq 3$ then $I(X) \neq P(X)$.*

Proof. Consider $f \in \mathcal{F}$. We have seen that $I(X) = \prod_{m \in W_f(\mathbf{F}_2^n)} (X - m)$. Furthermore we have

$\mathbf{F}_2^n = \mathring{\bigcup}_{m \in W_f(\mathbf{F}_2^n)} W_f^{-1}(m)$, so we can write

$$\prod_{a \in \mathbf{F}_2^n} (X - W_f(a)) = \prod_{m \in W_f(\mathbf{F}_2^n)} (X - m)^{\#W_f^{-1}(m)}$$

$= \left(\prod_{m \in W_f(\mathbf{F}_2^n)} (X - m) \right) \left(\prod_{m \in W_f(\mathbf{F}_2^n)} (X - m)^{\#W_f^{-1}(m)-1} \right)$ with $\#W_f^{-1}(m) \geq 1$ for each $m \in W_f(\mathbf{F}_2^n)$.

Then we obtain $P(X) = I(X) \prod_{m \in W_f(\mathbf{F}_2^n)} (X - m)^{\#W_f^{-1}(m)-1}$ which implies the equivalence

$I(X) = P(X)$ if and only if $\prod_{m \in W_f(\mathbf{F}_2^n)} (X - m)^{\#W_f^{-1}(m)-1} = 1$, i.e.

$\#W_f^{-1}(m) - 1 = 0$ for each $m \in W_f(\mathbf{F}_2^n)$, so $W_f : \mathbf{F}_2^n \longrightarrow \mathbf{Z}$ is injective.

But we have proved ([1] lemma 3) that, when a scans $\mathbf{F}_2^n$, the relative integers $W_f(a)$ are all even or all odd.

On other hand the Parseval's relation (3) implies, for each $a \in \mathbf{F}_2^n$, $|W_f^*(a)| \leq 2^{n-1}$, i.e. $-2^{n-1} \leq W_f(a) \leq 2^{n-1}$ for each $a \in \mathbf{F}_2^n - \{0\}$.

Consequently, if $I(X) = P(X)$ we have a family of $2^n - 1$ distinct relative integers $(W_f(a))_{a \in \mathbf{F}_2^n - \{0\}}$ in $[-2^{n-1}, 2^{n-1}]$ which are all even or all odd.

So if $I(X) = P(X)$, when the spectrum of f is even (respectively odd) we have necessarily $2^n - 1 \leq \#\{k \in \mathbf{Z} \cap [-2^{n-1}, 2^{n-1}] | k \text{ even}\} = 2^{n-1} + 1$

(respectively $2^n - 1 \leq \#\{k \in \mathbf{Z} \cap [-2^{n-1}, 2^{n-1}] | k \text{ odd}\} = 2^{n-1}$), which implies $n \leq 2$ (respectively $n \leq 1$) and proves the corollary. ■

Associated with $W_f : \mathbf{F}_2^n \longrightarrow \mathbf{Z}$, we have $\mathbf{F}_2^n = \mathring{\bigcup}_{m \in W_f(\mathbf{F}_2^n)} W_f^{-1}(m)$ so we can consider the equivalence relation $\sim$ on $\mathbf{F}_2^n$ defined by $a \sim b$ if and only if $W_f(a) = W_f(b)$.

The quotient space $\mathbf{F}_2^n/_\sim$ of the equivalence classes $\bar{a}$ for $\sim$ is such that the function

$$\begin{aligned} \Gamma : \mathbf{F}_2^n/_\sim &\longrightarrow W_f(\mathbf{F}_2^n) \\ \bar{a} &\longmapsto \Gamma(\bar{a}) = W_f(a) \end{aligned}$$

is a bijection.

We deduce from this and Theorem 3 that

$$I(X) = \prod_{m \in W_f(\mathbf{F}_2^n)} (X - m) = \prod_{\bar{a} \in \mathbf{F}_2^n/_\sim} (X - \Gamma(\bar{a})) = \prod_{a \in \Delta(\mathbf{F}_2^n/_\sim)} (X - W_f(a))$$

with the injection $\Delta : \mathbf{F}_2^n/_\sim \longrightarrow \mathbf{F}_2^n$ such that $\Delta(\bar{a}) = a$.

Therefore, the answer to the question asked at the beginning of chapter 3 is $E = \Delta(\mathbf{F}_2^n/_\sim)$.

4 References

[1] M. Mitton, On the Walsh-Fourier analysis of Boolean functions, *Jour. of Discr. Math. Sciences & Crypto.,* Vol. 9 (3) (December 2006), pp. 429-439.

[2] A. Bernasconi, *Mathematical techniques for the analysis of Boolean functions,* Ph. D. Thesis TD-2/98, Università di Pisa-Udine, 1998,
`http://www.di.unipi.it/~annab/publications.html`

[3] A. Bernasconi and B. Codenotti, Spectral Analysis of Boolean Functions as Graph Eigenvalue Problem, *IEEE Transactions on Computers,* Vol. 48 (3) (1999), pp. 345-351.

[4] A. Bernasconi, B. Codenotti, and J. M. VanderKam, A Characterization of Bent Functions in terms of Strongly Regular Graphs, *IEEE Transactions on Computers,* Vol. 50 (9) (2001), pp. 984-985.