# Factorisation des polynomes de Fq[X]

Paul Camion

IRIA
CENTRE DE ROCQUENCOURT

Rapports de Recherche

Coll dif

N° 93

# FACTORISATION DES POLYNOMES DE $\mathbb{F}_q[X]$

Paul CAMION

Septembre 1981

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP 105
78153 Le Chesnay Cedex
France
Tel 954 90 20

# FACTORISATION DES POLYNOMES DE $\mathbb{F}_q[X]$

*Paul CAMION*
CNRS-INRIA

Résumé :

Après un rappel des propriétés utiles de l'algèbre $\mathbb{F}_q[X]/(f(X))$, nous proposons un algorithme de factorisation exploitant à la fois une technique d'exponentiation introduite en [4] et [5] et celle obtenue par R.J. Mc Eliece [9]. Ceci pour éviter le long temps de calcul qu'exigeait la première étape du premier algorithme de E.R. Berlekamp [3].

Abstract :

Some properties of the Algebra $\mathbb{F}_q[X]/(f(X))$ usefull for the following, are first recalled. Then we suggest a factoring algorithm exploiting simultaneously an exponentiation technique introduced in [4] and [5] and the one published by R.J. Mc Eliece [9]. This is to avoid the long calculation required in the first step of the first algorithm of E.R. Berlekamp [3].

# FACTORISATION DES POLYNOMES DE $\mathbb{F}_q[X]$

## 1 - INTRODUCTION

Dans P. Camion [4] et [5], nous traitons du problème général de la construction des idempotents primitifs de tout idéal de $A = \mathbb{F}_q[X_1,\ldots,X_r]/(t_1(X_1),\ldots,t_r(X_r))$ dans le cas où les $t_i(X_i)$, $i = 1,\ldots,r$ ont des racines simples. Nous ne traiterons ici que le cas où $r = 1$, ce qui conduit à la factorisation de tout $f(X)$ de $\mathbb{F}_q[X]$ quel que soit $\mathbb{F}_q$, q pair ou impair.

Notons que notre algorithme permet la factorisation dans le cas où q est un nombre premier très grand, opération qui permet la factorisation des polynômes à coefficients entiers, mais aussi lorsque q est une puissance de deux. Dans ce dernier cas, il peut être utile d'obtenir les facteurs linéaires de $f(X)$ dans $L[X]$ où L est le corps de décomposition de $f(X)$. Cela signifie que l'on obtient alors les racines de $f(X)$. Lorsque $f(X)$ est le polynôme localisateur d'erreurs du mot reçu d'un code B-C-H, nous effectuons de cette manière une étape décisive du décodage de ce mot et ceci par un algorithme dont l'utilisation pourrait être très performante.

## 2 - L'ALGEBRE A = K[X]/(f(X))

### 2.1 - Le polynôme f(X)

Soit K un corps de caractéristique p et f(X) un polynôme de K[X]. Si nous n'étions pas assurés que le polynôme f(X) n'a que des racines simples, nous calculerions d'abord le p.g.c.d. de f(X) et de f'(X). Nous procéderions alors à la factorisation de f(X)/(f(X), f'(X)) qui lui n'aura que des racines simples. Ses facteurs irréductibles sont ceux de f(X) et leurs multiplicités dans f(X) seront aisément déterminées. (Le cas où f'(X) = 0 peut être écarté car alors $f(X) = g^p(X) = g(X^p)$ et g(X) se calcule alors sans difficulté [8].) Dans la suite, f(X) n'a que des racines simples, sauf mention expresse ; soient $\xi_1,\ldots,\xi_n$ ces racines.

### 2.2 - La transformation de Lagrange de A

Le cas où A est une algèbre à plusieurs indéterminées est traité en [14], [4] et [5].

A tout polynôme g représentant une classe de l'algèbre A, quotient de K[X] par l'idéal principal (f(X)), faisons correspondre l'élément $\hat{g} = (g(\xi_1),\ldots,g(\xi_n))$ de $L^n$, où L est le corps de décomposition de f(X). Si $\bar{g} \in A$ est la classe de polynômes qui contient g(X), tout polynôme h(X) de $\bar{g}$ s'écrit :

$$h(X) = g(X) + q(X)f(X) \tag{1}$$

et l'on voit que $\hat{h} = \hat{g}$.

$g(\xi_i)$ est nommé coefficient de Lagrange de g.

La transformation définie par $g \to \hat{g}$ est donc bien une application de A dans $L^n$.

Si nous considérons l'ensemble

$$\hat{A} = \{\hat{g}/g \in A\} \tag{2}$$

muni de l'addition et de la multiplication composante à composante (produit

de Hadamard), nous observons que $\hat{A}$ est une K-sous-algèbre de la K-algèbre produit $L^n$ et que l'application définie par $g \to \hat{g}$ de A sur $\hat{A}$ est un morphisme de K-algèbres. La transformation que nous venons de définir est connue sous le nom de la transformation de Lagrange de A [14].

## 2.3 - La transformation inverse

Si l'on nous donne $(\hat{g}_1,\ldots,\hat{g}_n) = (g(\xi_1),\ldots,g(\xi_n))$, nous pouvons reconstituer le polynôme g(X), unique représentant de degré inférieur à n de la classe $\bar{g}$ de A au moyen de l'interpolation de Lagrange :

$$(3) \qquad g(X) = \sum_{1\le j\le n} \frac{\prod_{i\neq j} (X - \xi_i)}{\prod_{i\neq j} (\xi_j - \xi_i)}\, g(\xi_j).$$

Notons toutefois immédiatement que nous n'aurons jamais à effectuer cette transformation inverse dans les algorithmes que nous allons proposer. Observons néanmoins que g(X) de degré inférieur à n est déterminé de façon unique par ses n valeurs prises en les racines $\xi_1,\ldots,\xi_n$ distinctes de f(X). Donc la transformation de Lagrange est un isomorphisme de A sur $\hat{A}$.

## 2.4 - Rappels sur l'algèbre A

### 2.4.1 - Résultats généraux

Ici le polynôme f(X) définissant A est quelconque.

*THEOREME 0 : Il existe une bijection isotone de l'ensemble des idéaux de* A *ordonné par l'inclusion sur l'ensemble des idéaux de* K[X] *contenant* f(X).

Cette bijection est définie par $I \to \bigcup_{\bar{g} \in I} \bar{g}$ où l'on note I un idéal de A et $\bar{g}$ l'ensemble des polynômes formant une classe de K[X] modulo son idéal (f(X)). La vérification de l'assertion du théorème 0 est alors immédiate.

*COROLLAIRE 1 : Il existe une bijection isotone de l'ensemble des idéaux de* A *ordonné par l'inclusion sur l'ensemble des diviseurs de* f(X) *ordonné par la relation de divisibilité.*

En effet, tout idéal de K[X] est principal, puisque K[X] est un anneau Euclidien, et dans K[X], pour deux idéaux $I_1$ et $I_2$, on a $I_1 \supset I_2$ si et seulement si le générateur de $I_1$ divise le générateur de $I_2$. En particulier, l'ensemble des générateurs des idéaux de K[X] qui contiennent (f(X)) est formé de l'ensemble des diviseurs de f(X).

Dans la suite, nous désignerons indifféremment un élément de A par $\bar{g}$ qui est une classe de polynômes ou par g ou g(X) qui est l'unique polynôme de degré inférieur à n de cette classe.

*COROLLAIRE 2 : Soit* $g_1(X)g_2(X) = f(X)$ *où* $g_i(X)$ *est de degré* $d_i$, $i = 1,2$. *Alors l'idéal* $(\bar{g}_1)$ *de* A *a pour dimension* $d_2$.

En effet, les polynômes $g_1(X)$, $Xg_1(X),\ldots,X^{d_2-1}g_1(X)$ sous-tendent sur K un sous-space vectoriel de dimension $d_2$. Or tout représentant de plus petit degré d'une classe de $(\bar{g}_1)$ appartient à cet espace vectoriel puisqu'il a $g_1(X)$ en facteur.

□

Notons $r_1(X),\ldots,r_k(X)$ les facteurs irréductibles de f(X). Lorsque f(X) n'a que des racines simples, on a $f(X) = r_1(X)\ldots r_k(X)$. Notons également $m_i(X) = f(X)/r_i(X)$, $i = 1,\ldots,k$.

Observons que tout idéal minimal de A est de la forme $(m_i)$ et qu'un idéal minimal est engendré par chacun de ses éléments non nuls.

Rappelons le

*LEMME : La somme de deux idéaux minimaux de* A, *considérés comme* K-*sous-espaces vectoriels de* A *est directe.*

Soient $I_1$ et $I_2$ deux idéaux minimaux, donc simples, de A. Si $x \in I_1 \cap I_2$, on a nécessairement $x = 0$ ou bien $(x) = I_1$ et $(x) = I_2$. Donc $I_1 \neq I_2$ entraine $x = 0$.

*COROLLAIRE 3 : Lorsque* $f(X)$ *n'a que des racines simples,* A *est la somme directe de ses idéaux minimaux.*

Considérons la somme directe dans A

$$(4) \qquad \bigoplus_{1 \leq i \leq k} (m_i(X))$$

des idéaux minimaux de A. Puisque la dimension de $(m_i(X))$ sur K est le degré de $r_i(X)$ et que, par hypothèse, la somme des degrés de $r_i(X)$ est le degré n de $f(X)$, donc la dimension de A, la somme (4) est bien l'algèbre A tout entière.

## 2.5 - Les idempotents de A et l'espace de Berlekamp

### 2.5.1 - Propriétés des idempotents de A

En vertu du corollaire 3, l'unité de A peut s'écrire de façon unique.

$$(5) \qquad 1 = e_1 + \ldots + e_k$$

où $e_i \in (m_i(X))$, $i = 1, \ldots, k$.

Chaque $e_i$ est non nul, car

$$A = \left(\sum_i e_i\right) A \subset \sum_i e_i A \subset \sum_{e_i \neq 0} (m_i).$$

Puisque pour $j \neq s$, $e_j e_s \in I_j \cap I_s = \{0\}$ où l'on note $I_i = (m_i(X))$, $i = 1,\ldots,k$, on a $e_j e_s = 0$. Les idempotents $e_j$ et $e_s$ sont dits orthogonaux.

Le carré de 1 s'exprime, par (5), $1 = e_1^2 + \ldots + e_k^2$, de sorte que en vertu de la propriété d'une somme directe,

$$e_i^2 = e_i, \quad i = 1,\ldots,k. \tag{6}$$

Les $e_i$ sont nommés idempotents primitifs de l'algèbre A. Plus généralement, un idempotent est un élément $x \in A$, $x \neq 0$ et $x^2 = x$. Nous avons la

*PROPRIETE 1* : *Dans l'hypothèse du corollaire 3, chaque idéal minimal de* A *contient un et un seul idempotent.*

Par (5), chaque idéal minimal $I_i$ contient un idempotent $e_i$. Soit e un idempotent quelconque de $I_i$. Puisque $I_i$ est engendré par l'un quelconque de ses éléments, on a donc

$$e_i\, a = e, \tag{7}$$

pour un $a \in A$. Elevant au carré les deux membres de (7),

$$e_i\, a^2 = e, \tag{8}$$

d'où $e_i\, a(a-1) = 0$.

Si $(a-1) \neq 0$, il existe $b \in A$ tel que $(a-1)b = e_i$, donc $0 = e_i\, a(a-1)b = e_i\, a = e$, contrairement à l'hypothèse.

Par conséquent $e = e_i$.

*PROPRIETE 2 : Dans l'hypothèse du corollaire 3, à tout idéal* I *de* A *correspond un idempotent unique* $u \in I$ *tel que* $(u) = I$ ; u *est la somme des idempotents primitifs contenus dans* I.

Notons d'abord que tout élément de tout idéal minimal $I_i$ est de la forme $e_i\, a$ et que si $e_i\, a \neq 0$, $(e_i\, a) = I_i$.

Soit E l'ensemble des indices i, $i = 1,\ldots,k$ tels que $e_i \in I$. Montrons que $u = \sum_{i\in E} e_i$ est le seul idempotent de I qui engendre I.

Soit $g \in I$, $g \neq 0$. On a $g = \sum_{1\leq i\leq k} a_i\, e_i$, où $a_i \in A$, $i = 1,\ldots,k$ et $a_j \neq 0$ pour un j au moins. Alors $e_j\, g = a_j\, e_j \in I$, donc $e_j \in I$. Donc E est non vide, et l'on voit que tout élément g de I s'exprime sous la forme $\sum_{i\in E} a_i\, e_i$. Donc

$$(9) \qquad \bigoplus_{i\in E} (e_i) \supset I \supset \bigoplus_{i\in E} (e_i) \; ;$$

$$I = \bigoplus_{i\in E} (e_i).$$

D'autre part, il est clair que u est un idempotent ; $u \in I$ et puisque $ue_j = e_j$, $\forall j \in E$ : $(u) \supset \bigoplus_{j\in E} (e_j) = I$.

En d'autres termes, u engendre I.

Soit v un idempotent quelconque de I qui engendre I. Nécessairement, v s'écrit $\sum_{i\in E} a_i\, e_i$ et chaque coefficient $a_i$, $i \in E$ est non nul. En effet, si $a_j = 0$ pour $j \in E$, on aurait, puisque $e_j \in I$, $e_j = vg$ ; $e_j = (ve_j)g = 0g = 0$.

D'autre part, par hypothèse, $v = \sum_{i\in E} a_i^2\, e_i$ et puisque I est la somme directe des $I_i$, $i \in E$, on a $a_i^2\, e_i = a_i\, e_i$, $i = 1,\ldots,k$. Par le même raisonnement que celui de la preuve de la propriété 1, on en déduit que $a_i = 1$, $\forall i \in E$, donc $u = v$.

□

2.5.2 - L'espace de Berlekamp

Revenons à la transformation de Lagrange de A. Nommons support s(g) d'un élément g de A l'ensemble

(10) $$\{i/g(\xi_i) \neq 0,\ i = 1,\ldots,n\}$$

En particulier, on voit que le seul élément $g \in A$ dont le support est vide est 0 alors que le support de l'unité de A est l'ensemble $[n]$ tout entier. En effet, plus généralement, tous les coefficients de Lagrange d'une constante $\alpha \in K \subset A$ sont égaux à cette constante. Remarquons aussi que si u est un idempotent de A, on doit avoir pour chaque coefficient de Lagrange $\hat{u}_i$ : $\hat{u}_i^2 = \hat{u}_i$ ; $\hat{u}_i(\hat{u}_i - 1) = 0$ et puisque $\hat{u}_i \in L$, cette équation a deux racines : 1 et 0.

Si deux éléments g et h de A sont orthogonaux, donc si gh = 0, c'est que $s(gh) = \emptyset$. Mais, de toute évidence, $s(gh) = s(g) \cap s(h)$. On voit donc que deux éléments sont orthogonaux si leurs supports sont disjoints. Examinons la relation (5) à la lumière de ceci. On constate que

$$s(e_j) \cap s(e_s) = \emptyset,\ 1 \leq j < s \leq k,$$

(11) $$\bigcup_{1 \leq i \leq k} s(e_i) = [n],$$

$$\forall i \in s(e_j) : e_j(\xi_i) = 1,$$

$$\forall i \notin s(e_j) : e_j(\xi_i) = 0,$$

$$\dim_K (e_i) = \text{Card } s(e_i),\ i = 1,\ldots,k.$$

Seule la dernière relation écrite demande une explication. Puisque l'idéal minimal $I_j$ est engendré aussi bien par $m_j$ que par $e_j$, il existe deux éléments a et b de A tels que $am_j = e_j$ et $be_j = m_j$.

On en déduit que $s(e_j) \subset s(m_j)$, $s(m_j) \subset s(e_j)$ : $s(e_j) = s(m_j)$. D'autre part, $m_j(X) = f(X)/r_j(X)$, où $r_j(X)$ est le $j^{ième}$ facteur irréductible de $f(X)$. Par conséquent, $m_j(X)$ ne s'annule pas aux racines de $r_j(X)$ et le cardinal de son support est donc égal au degré de $r_j(X)$ qui est précisément la dimension sur K de $(m_j(X)) = I_j = (e_j)$. □

Ceci nous conduit également à constater que l'ensemble $\{\xi_i / i \in s(e_j)\}$ est une classe d'éléments conjugués de L sur K, puisque ce sont les racines du polynôme irréductible $r_j(X)$.

Donnons ici un énoncé où intervient la notion de support.

PROPRIETE 3 : *Soit* u *l'idempotent générateur d'un idéal* I *de* A. *Alors, tout générateur* g *de* A *a pour support* $s(u)$ *et* $\dim_K(I) = \text{Card } s(u)$.

Soit g un générateur de I et $g = \sum_{j \in E} a_j e_j$ où $a_j \neq 0 \quad \forall j \in E$. Le support de tout élément h de I est contenu dans celui de g, puisque $h = ag$, $a \in A$. Nous avons vu que $e_j \in I, \forall j \in E$. On a alors $s(g) \supset \bigcup_{j \in E} s(e_j) = s(u)$. Mais aussi, par (11), $\forall i \notin s(u)$, $e_j(\xi_i) = 0$, $\forall j \in E$, et par suite $g(\xi_i) = 0$. Donc $s(g) = s(u)$. □

*Il y a donc bijection de l'ensemble des idéaux de* A *sur l'ensemble des supports d'éléments de* A. *Cette bijection est antitone pour la relation d'inclusion.*

Nommons cosupport le complémentaire du support. Il découle de la propriété 2 que si $f(X) = f_1(X)\, f_2(X)$, alors $\text{cos}(f_1) = s(f_2)$, $\text{cos}(f_2) = s(f_1)$. Plus généralement si pgcd $(f(X), g(X)) = h(X)$, $\text{cos}(g) = \text{cos}(h) = s(f(X)/h(X))$.

Soit $K = \mathbb{F}_q$. Par définition, l'espace de Berlekamp est la K-sous-algèbre de A formée des éléments g tels que $g^q = g$, que nous noterons B. Le lecteur vérifiera sans peine que B est une K-algèbre, c'est-à-dire que B est stable dans la multiplication, l'addition et la multiplication par tout élément de K. On a le

*THEOREME 1* : *B est le sous-espace sur* K *de* A *sous-tendu par les idempotents primitifs de* A.

Puisque $e_j^2 = e_j$, on a aussi $e_j^q = e_j$, $j = 1,\ldots,k$, donc $e_j \in B$, $j = 1,\ldots,k$. Soit alors $g = \sum_{1\le j\le k} l_j e_j$, où $l_j \in K$, $j = 1,\ldots,k$. On a

$$g^q = \sum_{1\le j\le k} l_j^q e_j^q = \sum_{1\le j\le k} l_j e_j = g, \tag{12}$$

d'où $g \in B$. Il reste donc à vérifier que tout $g \in B$ s'exprime sous la forme $\sum_{1\le j\le k} l_j e_j$ avec $l_j \in K$, $j = 1,\ldots,k$.

Or $g^q(\xi_i) = g(\xi_i)$ pour $i = 1,\ldots,n$ montre que $g_i \in K$, $i = 1,\ldots,n$. Par conséquent, les $g_i$ sont égaux pour $i \in s(e_j)$, $j = 1,\ldots,k$, les $\xi_i$ étant conjugués pour $i \in s(e_j)$. Si nous notons $l_j$ la valeur commune des $g_i$ pour $i \in s(e_j)$, nous constatons par $(11)_3$ et $(11)_4$ que $\sum_{1\le j\le k} l_j e_j$ a les mêmes coefficients de Lagrange que g et est donc égal à g. □

*COROLLAIRE 1* : *La dimension de l'espace de Berlekamp est égale au nombre de facteurs irréductibles de* f(X).

*COROLLAIRE 2* : *B est formé des éléments de* A *dont tous les coefficients de Lagrange sont dans* K.

*COROLLAIRE 3* : *Soit* $g \in B/\{0\}$. *La dimension sur* K *de* gB *est égale au nombre d'idempotents primitifs de* A *contenus dans* gB *qui est aussi le nombre d'idempotents primitifs de* A *dont le support est contenu dans* s(g).

PREUVE :

Par le théorème 1, $g = \sum_{j\in E} s_j\, e_j$ où $s_j \in K^*$, $\forall j \in E$ et $E \subset [1,k]$. Il est clair que $\forall j \in E$, $e_j \in gB$, puisque $e_j = s_j^{-1}\, e_j\, g$. D'autre par, par la propriété d'orthogonalité des idempotents primitifs, on voit que tout $gh \in gB$ s'écrit sous la forme $\sum_{j\in E} t_j\, e_j$. Donc pour un idempotent primitif $e_i \in gB$, on a $i \in E$. On peut donc écrire

$$gB = \bigoplus_{j\in E} K\, e_j \tag{13}$$

Ceci démontre la première assertion. La deuxième découle de ce que $g = \sum_{e_j\in gB} s_j\, e_j$ avec $s_j \in K^*$, $\forall e_j \in gB$ et des relations $(11)_3$ et $(11)_4$. □

## 3 - LES ALGORITHMES

### 3.1 - Rappel sur le premier algorithme de Berlekamp [3]

#### 3.1.1 - Construction d'une base de l'espace de Berlekamp

Le fait surprenant de l'algorithme de Berlekamp est qu'il est possible de construire une base du K-espace B sur la seule donnée de f(X), dans le cas où K est un corps fini $\mathbb{F}_q$. Il n'est même pas nécessaire de déterminer le corps de décomposition L de f(X).

Soit en effet $g \in B$. Alors $g(X) = \sum_{i<n} a_i X^i$ et

$$g^q(X) = g(X^q) \equiv g(X) \bmod f(X). \tag{13}$$

Soit alors $h_i(X)$ le reste de la division de $X^{iq}$ par f(X), i=0,...,n-1. On pourra alors écrire au lieu de (13)

$$\sum_{0 \le i < n} a_i (h_i(X) - X^i) = 0. \tag{14}$$

Donc une base de l'espace vectoriel des $g \in B$ s'obtient en triangularisant la matrice M des coefficients des polynômes $h_i(X) - X^i$, i=0,...,n-1.

Observons que $h_0(X) = X^0 = 1$ et que par conséquent la matrice n×n de rang égal à n-Dim B a au moins une ligne nulle. Mais nous savions que Dim B ≥ 1 puisque Dim B = 1 ssi f(X) est irréductible. Cette constatation nous permet déjà dans une première étape de vérifier si f(X) est irréductible

#### 3.1.2 - L'algorithme de factorisation

Observons que tout élément de K considéré comme un polynôme réduit à un terme constant est dans B, en vertu du corollaire 2 du théorème 1. En effet les coefficients de Lagrange d'un polynôme de A réduit à $s \in K$ sont tous égaux à s. Réciproquement, un polynôme de B dont tous les coefficients de Lagrange sont égaux est réduit à un terme constant puisque la transformation de Lagrange est injective.

Soit alors $g(X) \in B$, non réduit à une constante.

Parmi les coefficients de Lagrange de g figureront donc deux valeurs distinctes $s_1$ et $s_2$. Par conséquent $g(X)-s_1$ a un coefficient de Lagrange, soit $g(\xi_{i_1})-s_1$, égal à 0 et un autre, soit $g(\xi_{i_2})-s_1$, égal à $s_2-s_1 \neq 0$. Cela signifie que $g(X)-s_1$ partage avec $f(X)$ la racine $\xi_{i_1}$ mais pas $\xi_{i_2}$.

Donc pgcd $(g(X)-s_1, f(X))$ est un facteur non trivial de $f(X)$.

Dans le premier algorithme de Berlekamp, cet auteur propose de calculer de pgcd $(g(X)-s, f(X))$, pour $g(X)$ fixe de B non réduit à un terme constant, en faisant parcourir à s le corps $K=\mathbb{F}_q$.

### 3.1.3 - Efficacité de l'algorithme et améliorations proposées

#### 3.1.3.1. - Introduction

Reprenons l'analyse de l'algorithme de Berlekamp faite par Robert Moenck [15]. Cet auteur se limite au cas où $K=\mathbb{F}_p$ est un corps premier. Le nombre d'étapes de l'algorithme est une fonction de p et du degré n de $f(X)$. On suppose que toute opération dans K à l'exception du calcul d'un inverse exige $O(1)$ pas.

Le calcul de l'inverse se ramène à $O(\log p)$ multiplications dans K [16]. Dès lors, multiplier deux polynômes, l'un de degré n, l'autre de degré m se fait en $O(nm)$ opérations dans K. La division du premier par le second, que celui-ci soit unitaire ou non, se fait aussi en $O(nm)$ opérations. Par conséquent, multiplier deux polynômes de degré n-1 et calculer le reste modulo $f(X)$ demande $O(n^2)$ opérations dans K. Le calcul de $X^p$ mod $f(X)$ demande $O(n^2 \log p)$ opérations tandis que les n-2 lignes restantes de la matrice des coefficients des $h_i(X)$, $i=0,\ldots,n-1$, peuvent être obtenues en $O(n^3)$ opérations. Le calcul d'une base N de l'espace B requiert ensuite, par un algorithme classique de triangularisation, $O(n^3+n \log p)$ opérations.

Collins [17] montre que le pgcd $(g(X)-s, f(X))$ se calcule en $O(n^2+n \log p)$ opérations. Si $f(X)$ a k facteurs irréductibles, on voit que cette dernière étape conduit à $O(kp(n^2+n \log p)$ opérations dans K. Ce qui vient d'être dit reste valable lorsque K n'est pas un corps premier. Toutefois il conviendrait dans ce cas de distinguer l'addition et la multiplication dans K, l'une étant beaucoup plus coûteuse que l'autre.

Notons qu'en utilisant une table de logarithmes de Zech, c'est l'addition qui est la plus coûteuse, la multiplication se réduisant alors à une addition modulo q-1. Les corps finis de caractéristique 2 retiennent particulièrement notre attention puisque la recherche des racines du polynôme localisateur d'erreurs dans le décodage d'un B.C.H. consiste à trouver les facteurs linéaires d'un polynôme $f(X)\in \mathbb{F}_{2^m}[X]$. Les algorithmes que nous proposons en [4] et [5] et pour lesquels nous développons ici avec plus de précision le mode d'application, avec un regard attentif sur l'économie dans le processus des opérations, sont adaptés au cas de $f(X)\in\mathbb{F}_{2^m}[X]$.

Les algorithmes que nous développons dans les articles cités permet la construction des idempotents primitifs d'un idéal (h) de $A = \mathbb{F}_q[X_1,\ldots,X_r]/(t_1(X_1),\ldots,t_r(X_r))$ dans le cas où les $t_i(X_i)$, i=1,...,r, ont des racines simples. Comme dans le cas présent, on y montre que l'espace B de Berlekamp, qui est la sous-algèbre sur $\mathbb{F}_q$ de A engendrée par ses idempotents, peut être construite. Nous ne revenons pas sur ce problème qui généralise celui-ci lorsque r>1. L'essentiel pour le cas particulier de la factorisation est d'observer que la construction des idempotents primitifs de $A=\mathbb{F}_q[X]/(f(X))$ résout le problème de la construction des facteurs irréductibles de f(X). En effet si $1 = e_1 +\ldots+ e_h$ est la décomposition de l'unité de A en idempotents primitifs, on a $r_i(X)=f(X)/\text{pgcd}\,(e_i(X),f(X))$, i=1,...,h où $f(X)=r_1(X)\ldots r_h(X)$ est la factorisation complète de f(X).

Cet algorithme permet de remplacer le facteur p de $O(kp(n^2+n\log p))$ par un facteur log p.

D. Lazard attire notre attention alors sur le coût élevé de la construction de l'espace de Berlekamp, qui comporte un facteur en $n^3$. Nous allons éviter la construction complète d'une base de l'espace de Berlekamp en exploitant une idée de Mac Eliece [9].

3.1.3.2 - Etude préalable à l'application de la technique de Mac Eliece

Soit, comme au §2, A=K[X]/(f(X)) et L le corps de décomposition de f(X). Pour $K=\mathbb{F}_q$, on a $L=\mathbb{F}_{q^{n'}}$. Définissons sur A un opérateur T,K-linéaire :

(15) $$\forall h\in A,\ Th=h+h^q+\ldots+h^{q^{n'-1}}.$$

Dès lors, le $i^{\text{ème}}$ coefficient de Lagrange $(\hat{Th})_i$ de Th vaut $T_{L/K}(\hat{h}_i) \in K$.

*PROPRIETE 4 : L'espace de Berlekamp* B *est l'image par* T *de* A.

Puisque

$$A = \bigoplus_{1 \le i \le k} (e_i), \tag{16}$$

On a

$$TA = \bigoplus_{1 \le i \le k} T(e_i) = \bigoplus_{1 \le i \le k} Ke_i = B, \tag{17}$$

puisque $T_{L/K}$ est surjective et que $(e_i)$ comporte un élément g pour lequel $g(\xi_j)$, $j \in s(e_i)$ prend une valeur arbitrairement fixée dans L. □

Notons immédiatement que dans une première étape du processus de factorisation de f(X), après s'être ramené au cas où f(X) a des racines simples, on peut se ramener à celui où tous les facteurs irréductibles de f(X) ont le même degré [8]. Ceci s'obtient en calculant $(X^{q^i}-1, f(X))$ pour les valeurs entière croissantes de i jusqu'à obtention d'un pgcd $\neq 1$. On obtient ainsi un facteur de f(X) avec la propriété indiquée, l'autre facteur de f(X), s'il est différent de 1 sera traité de la même façon. Le résultat est alors que le degré n' de L sur K est n/k.

Observons ensuite, et nous allons préciser ceci, que l'ensemble N d'éléments de B dont nous devrons disposer pour obtenir une factorisation complète de f(X), soit par l'algorithme de Berlekamp lorsque q est petit, soit par l'algorithme d'exponentiation que nous allons rappeler lorsque q est grand, ne doit pas être nécessairement une base de B. Nous dirons que $N \subset B$ sépare les idempotents primitifs de A lorsque pour une suite d'entiers $i_1, \ldots, i_k$ telle que $i_j \in s(e_j)$, $j=1,\ldots,k$,

$$\forall j,j',\ 1 \le j < j' < k,\ \exists h \in N :\ \hat{h}_{i_j} \neq \hat{h}_{i_{j'}}. \tag{18}$$

Nous avons alors la

*PROPRIETE 5 : Le nombre minimum d'éléments d'une partie* N *de* B *qui sépare les idempotents primitifs de* A *n'est pas plus petit que* $\log_q k$, *où* k *est le nombre de facteurs irréductibles de* f(X).

Soient $h_1,\ldots,h_t$ les éléments de N et soit E l'ensemble des supports des idempotents primitifs de A. L'élément $h_\ell$ de N définit une partition $P_\ell$ de E par le fait que $s(e_j)$ et $s(e_{j'})$ sont dans une même classe de $P_\ell$ lorsque $h_\ell(\xi_i) = h_\ell(\xi_{i'})$ pour $i\in s(e_j)$ et $i'\in s(e_{j'})$. Puisque $h_\ell(\xi_i)\in \mathbb{F}_q$, i=1,...,n, on voit que la partition $P_\ell$ comporte au plus q classes, $\ell$=1,...,t. L'intersection $P_\ell \wedge P_{\ell'}$ de deux partitions est la partition où chaque classe est interjection d'une classe de $P_\ell$ et d'une classe de $P_{\ell'}$. Il est clair que N sépare les idempotents primitifs ssi $P_1 \wedge\ldots\wedge P_t$ est la partition la plus fine de E. Désignons par $\alpha_\ell$ le nombre rationnel $\mathrm{Card}(P_1 \wedge\ldots\wedge P_{\ell+1})/\mathrm{Card}(P_1 \wedge\ldots\wedge P_\ell)$. On voit que $\alpha_\ell\leq q$, $\ell$=1,...t puisque chaque classe de $P_1 \wedge\ldots\wedge P_\ell$ peut être subdivisée en au plus q classes par $P_{\ell+1}$. On a donc

$$\alpha_1\ldots\alpha_t = \mathrm{Card}\ E=k,$$

(19)

$$t\geq \log_q \alpha_1+\ldots+\log_q \alpha_t = \log_q k. \qquad \square$$

*THEOREME 2 : Le plus petit nombre d'éléments d'une partie* N *de* B *qui sépare les idempotents primitifs de* A *est égal à* $\lceil \log_q k \rceil$.

La démonstration se fait par récurrence sur k.

En vertu de la propriété 5, il suffit de vérifier qu'une telle partie N de B avec $\mathrm{Card}\ N=\lceil \log_q k \rceil$ existe.

Soit $k=\beta_0+\beta_1 q +\ldots+ \beta_{t-1}q^{t-1}$ l'écriture en base q de k. Donc $t=\lceil \log_q k \rceil$. On peut définir une partition $P_1$ de E comportant $\beta_{t-1}$ classes de $q^{t-1}$ éléments et une classe de $\beta_0+\beta_1 q +\ldots+ \beta_{t-2}\, q^{t-2}$ éléments. Soit $E_2$ l'ensemble des éléments de cette classe et $E_1$ la réunion des autres classes. Notons $P_1'$ la restriction de $P_1$ à $E_1$. Clairement, il existe une suite $P_1',P_2',\ldots,P_t'$ de partitions

de $E_1$ telles que $P'_1 \wedge P'_2 \wedge \ldots \wedge P'_t$ soit la partition la plus fine de $E_1$. Par l'hypothèse de récurrence chaque partition $P'_\ell$ de cette suite se prolonge en une partition $P_\ell$ telle que $P_1 \wedge P_2 \wedge \ldots \wedge P_t$ soit la partition la plus fine de E. Il reste à montrer qu'à chaque partition $P_\ell$ de E correspond un élément $h_\ell$ de B tel que $h_\ell(\xi_i) \neq h_\ell(\xi_{i'})$ lorsque les supports $s(e_j)$ et $s(e_{j'})$ contenant respectivement i et i' sont dans des classes distinctes de $P_\ell$. Il suffit de prendre $h_\ell = \sum_{c \in P_\ell} a_c \sum_{s(e_j) \in c} e_j$ avec $a_c, a_{c'} \in \mathbb{F}_q$, $a_c \neq a_{c'}$ pour $c \neq c'$.

C'est possible puisque $P_\ell$ comporte au plus q classes, $\ell = 1, \ldots, t$.

3.1.3.3 - Application de la technique de Mac Eliece

Rappelons d'abord que toute base N de B a k éléments et sépare les idempotents primitifs de A. Ceci fut essentiellement observé par Berlekamp. Dans l'application que nous proposons ici, un ensemble N qui sépare les idempotents primitifs de A ne sera pas construit d'emblée, mais au fur et à mesure de l'exécution de l'algorithme. Notons que $\{X^i\}_{0 \leq i < n}$ engendre A et donc, par la propriété 4, $\{TX^i\}_{0 \leq i < n}$ contient une base de B, donc une partie N séparant les idempotents de A. Notre algorithme consiste à "fractionner" progressivement l'unité de A en somme d'idempotents et si un des termes de la somme, soit $u_i$ est primitif, nous pouvons le constater en calculant le pgcd$(u_i, f(X))$ dont le degré doit alors être égal à n-n', où, rappelons le, n est le degré de f(X) et n' le degré de chaque facteur irréductible de f(X). Soit alors $N_\ell = \{TX^i\}_{1 \leq i \leq \ell}$.

Nous venons de voir que l'opération à effectuer est d'obtenir u=u'+u" où u' et u" sont des idempotents orthogonaux, pour un idempotent u de A dont on a vérifié qu'il n'est pas primitif. On effectue les produits $u.TX^i$, i=1,... jusqu'à obtenir un élément h∈B non multiple scalaire de u. Cela signifie comme cela fut montré en 3.1.3 que h à deux coefficients de Lagrange distints $s_1$ et $s_2$ dans le support de u. Cela se produit nécessairement pour $\ell$ assez grand puisque $N_{n-1}$ sépare les idempotents primitifs de A. Observons que si q est très grand vis-à-vis de k, la probabilité que $N_1$ sépare les éléments primitifs de A est voisine de 1. D'autre part, ayant calculé les termes de $TX^{i_1}$ et de $TX^{i_2}$ on peut calculer $TX^{i_1+i_2}$ en effectuant n' produits seulement, au lieu d'une moyenne de $1{,}5(n'-1)\log_2 q$ par calcul direct. Pour tout i>1, on peut donc obtenir $TX^i$ de cette manière. On applique alors :

*pour q petit, la technique du premier algorithme de Berlekamp*

Soit $g_0(X) = \text{pgcd}(u(X),f(X))$ et $g(X)=f(X)/g_0(X)$. Notre problème est donc de fractionner l'idempotent u en deux idempotents orthogonaux u' et u", u=u'+u". Il est clair que les supports de g et u sont complémentaires dans [1,n]. Soit h le premier élément rencontré dans $N_\ell$ tel que uh ne soit pas un multiple scalaire de u. Dès lors uh a deux coefficients de Lagrange distincts $s_1$ et $s_2$ dans s(u). On calcule le pgcd(uh(X)-s,g(X)) pour les valeurs successives s de $\mathbb{F}_q$. Si $s\neq(\hat{uh})_i, \forall i\in s(u)$, ce pgcd est 1, puisque dans ce cas s(uh-s)=s(u). Au contraire si $s=(\hat{uh})_i$ pour $i\in s(u)$, uh(X)-s a un zéro en commun avec g(X) et le pgcd est un polynôme k(X), facteur non réduit à une constante de g(X). Alors $k^{q-1}$ qui a tous ses coefficients de Lagrange égaux à 0 ou 1 est un idempotent et $s(1-k^{q-1}) \subset s(u)$. On a donc u=u'+u" pour $u'=1-k^{q-1}$.

*pour q grand, la technique introduite en* [4] *et* [5].

1er cas, q impair

Soit encore h le premier élément rencontré dans $N_\ell$ tel que uh ne soit pas un multiple scalaire de u. Notons k=uh. Alors k a deux coefficients de Lagrange distincts $s_1$ et $s_2$ dans s(u) et la probabilité pour que $s_1$ et $s_2$ ne soit pas simultanément carrés ou non carrés dans $\mathbb{F}_q$ est $> \frac{1}{2}$. (On peut avoir $s_1=0$ ou $s_2=0$.) Si tel est le cas, $k^t$, pour t=(q-1)/2 a deux coefficients de Lagrange distincts de l'ensemble {1,-1,0} dans s(u). Ceci se produit ssi $k^t \neq \pm u$. Notons $w=k^t$. Si $w\neq \pm u$, alors l'un au moins de w'=w(w+1)/2 ou w"=w(w-1)/2 est non nul et différent de u. Soit $w'\neq 0$. Dès lors w' est un idempotent à support proprement inclus dans s(u) et u=u'+u" avec u'=w' et u"=u-w'. D'autre part, pour tout couple d'éléments distincts $s_1,s_2\in \mathbb{F}_q^*$, tous deux carrés ou tous deux non carrés, et pour tout choix de $s\in\mathbb{F}_q^*$, la probabilité que $s_1+s$ et $s_2+s$ ne soient pas tous deux carrés ou tous deux non carrés est $>1/2$. Donc, si $k^t=\pm u$, à chaque tirage d'un $s\in \mathbb{F}_q^*$ il y a une probabilité $>1/2$ que $(k-s)^t\neq\pm u$. Le nombre moyen d'essais nécessaires pour obtenir le fractionnement de u en u'+u" est donc plus petit que 2.

Dans un article à paraître dans les "Annals of Discrete Mathematics" numéro spécial des actes du "Colloque Combinatoire 81", nous montrons que à chaque $\mathbb{F}_q$ correspond un algorithme déterministe se substituant à la dernière phase décrite ci-dessus.

Nommons factorisante une partie $P=\{s_{i_1},\ldots,s_{i_d}\} \subset \mathbb{F}_q^*$ telle que pour tout polynôme $f(X)$, pour tout $h$ non réduit à une constante de l'espace de Berlekamp et pour tout idempotent $u$ tel que $uh$ n'est pas multiple scalaire de $u$, il existe $s \in P$ tel que $(uh-s)^t \neq \pm u$. Le résultat est plus précisemment celui-ci :

*THEOREME 3 : Quel que soit le corps fini $\mathbb{F}_q$ avec $q$ impair, il existe une partie $P \subset \mathbb{F}_q^*$ factorisante telle que*

$$\text{Card } P < 2 \log_2 q,$$

*de plus, toute partie P factorisante vérifie*

$$\log_2 q < \text{Card } P.$$

2ème cas, q pair

Lorsque $q$ est impair, $\mathbb{F}_q^*$ contient le sous-groupe $\{1,-1\}$, propriété qui a permis d'obtenir le fractionnement de l'idempotent $u$ au moyen d'une exponentiation donnant la racine carrée d'un idempotent ayant donc ses coefficients de Lagrange dans $\{1,-1,0\}$.

Dans le cas où $q$ est impair, nous exploitons en [5] le fait que si $\mathbb{F}_q$ est une extention de degré pair de $\mathbb{F}_2$, ce corps contient le sous-corps $\{0,1,\gamma,\gamma^2\} = \mathbb{F}_4$. Donc $\mathbb{F}_q^*$ contient un sous-groupe d'ordre 3. Plus précisement, soit $K = \mathbb{F}_q$ et $K' = \mathbb{F}_q(\gamma)$. Eventuellement $K'$ est une extension de degré 2 de $\mathbb{F}_q$, sinon $K'=K$.

L'algorithme est analogue à celui traité dans le premier cas, toutefois, on fera ici $t=(q-1)/3$ ou $(q^2-1)/3$, selon le cas, et le tirage des éléments $s$ se fera dans $K'$.

Les coefficients de Lagrange de $(k-s)^t$ seront dans le sous-corps $\mathbb{F}_4$ de $K'$ et la probabilité que $(k-s)^t$ se ne soit pas un multiple dans $\mathbb{F}_4$ de $u$ est calculée en [5], elle est voisine de 2/3. Soit $w=(k-s)^t$. L'un des $w'_\alpha = (w+\alpha)u$,

où $\alpha$ parcourt $\mathbb{F}_4^*$ aura son support proprement inclus dans celui de u. On s'en assurera en vérifiant que pour l'un des $w'_\alpha$ on ait $(w'_\alpha)^3 \neq u$. Alors $u'=(w'_\alpha)^3$ et $u=u'+u''$, où $u''=u+u'$.

## 4 - L'ALGEBRE $A=\mathbb{F}_q[X_1,\ldots,X_r]/(t_1(X_1),\ldots,t_r(X_r))$ DANS LE CAS OU LES $t_i(X_i)$, $i=1,\ldots,r$ ONT DES RACINES SIMPLES

Ce cas est traité en [4] et [5]. Nous y observons que dans le cas où A est isomorphe à une algèbre de groupe abélien élémentaire semi-simple $\mathbb{F}_q G$, on connaît le corps de décomposition $\mathbb{F}_q m$ des polynômes $t_i(X_i)$, $v=1,\ldots,r$. Il est clair que la technique de Mac Eliece telle que nous l'avons appliquée ici est adaptable à ce cas.

## 5 - CONCLUSION

Il ressort d'une conversation avec D. Lazard sur l'efficacité de la méthode exposée en [4] et [5] que, la construction d'une base de l'espace B de Berlekamp étant coûteuse, il y aurait intérêt à se ramener classiquement comme cela fut rappelé au numéro 3, à factoriser des polynômes dont les facteurs irréductibles ont tous le même degré.

Soit $\mathbb{F}_q n'$ le corps de décomposition de f(X). D. Lazard propose d'exploiter la technique d'exponentiation rappelée en 3.1.3.3 pour q grand, en calculant $k^t$ pour k = u h mais en prélevant h dans A et non dans B et en faisant $t = (q^{n'}-1)/2$.

Soit $\alpha n^2 n' \log_2 q$ le coût d'une telle exponentiation. Si on néglige le coût des additions dans le produit de deux polynômes, on peut admettre que $\alpha$ vaut 3/2. Puisqu'il faut 2k exponentiations en moyenne pour obtenir les k idempotents primitifs, le coût total de ces exponentiations serait de $3n^3 \log_2 q$ puisque kn' = n.

Notons ici que pour n grand, k vaut approximativement $\frac{1}{n} n$ (Berlekamp [3], chapitre 3, exercice 3.6).

Dans la méthode que nous proposons, si q est grand devant n, nous avons vu que la probabilité est voisine de 1 d'obtenir une partie N de B, réduite à un seul élément, qui sépare les idempotents primitifs de A. Donc N s'obtiendrait en appliquant une seule fois l'opérateur de Mc Eliece, le coût de cette opération étant $1,5\ n'n^2 \log_2 q$, si là encore on néglige le coût des additions. Ensuite, pour t = (q-1)/2, le coût de chaque exponentiation est approximativement $1,5n^2 \log_2 q$, de sorte que le coût total de ces opérations d'exponentiation est ici $1,5n'n^2 \log_2 q + 3kn^2 \log_2 q$ qui est inférieur à $1,5n^3 \log_2 q$ pour n grand à comparer au précédent $3n^3 \log_2 q$.

Mais seule la mise en oeuvre permettra de constater la meilleure efficacité de telle ou telle méthode. Nous voulons seulement observer ici que la technique de Mc Eliece peut être exploitée avec des perspectives moins pessimistes que celles suggérées par son auteur.

# BIBLIOGRAPHIE

[1] E.R. BERLEKAMP,
"Factoring polynomials over finite fields",
Bell System Tech. J. 46 (1967) 1853-1859.

[2] E.R. BERLEKAMP,
"Factoring polynomials over large finite fields",
Math. Comp. 24 (1970) 713-735.

[3] E.R. BERLEKAMP,
"Algebraic Coding Theory",
Mac Graw-Hill (1968).

[4] P. CAMION,
"Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$",
C.R. Acad. Sc. Paris t. 291 (20 Octobre 1980).

[5] P. CAMION,
"Un algorithme de construction des idempotents primitifs d'idéaux d'algèbres sur $\mathbb{F}_q$",
Theory and Practice of Combinatorics, Annals of Discrete Mathematics (1981).

[6] P. CAMION,
"Un algorithme déterministe de factorisation des polynômes de $\mathbb{F}_q[X]$",
à paraître dans les actes du "Colloque Combinatoire 81"
Marseille-Luminy.

[7] P. CAMION
"Codes quadratiques abéliens et plans inversifs miquéliens",
C.R. Acad. Sc. Paris, t. 284 (6 Juin 1977).

[8] D.E. KNUTH,
The Art of Computer Programming, vol. 2
Seminumerical Algorithms. Reading, Mass. ; Addison-Wesley (1971).

[9] R.J. Mac ELIECE,
"Factorization of polynomials over finite fields",
Math. Comp. 23, 861-867.

[10] F.J. Mac WILLIAMS,
"The structure and properties of binary cyclic alphabets",
Bell System Tech. J. 44 (1965), 303-332.

[11] A. POLI,
"Codes dans certaines algèbres modulaires",
Thèse de Doctorat es Sciences, Toulouse (1978).

[12] A. POLI,
"Un groupe d'automorphismes d'algèbre de groupe abélien",
dans les actes du colloque Permutations, Gauthier-Villars, Paris (1972).

[13] M.O. RABIN,
"Probabilitic Algorithms in finite fields",
MIT/LCS/TR-213 (Jan. 1979).

[14] K.P. ZIMMERMAN and K.K. TZENG,
"Lagrange's interpolation formula and generelized Goppa Codes",
Preprint.

[15] R.T. MOENCK,
"On the Efficiency of Algorithms for Polynomial Factoring",
Math. Comp. 31, 235-250 (1977).

[16] G.E. COLLINS,
"Computing multiplicative inverses in GF(p)",
Math. Comp. 23, 197-200 (1969).

[17] G.E. COLLINS,
"Computing Time Analyses of some Arithmetic and Algebraic Algorithms",
Proc. IBM Summer Just. on Symbolic and Algebraic Computation (1968).