

Sur une classe de polynômes scindés de l'algèbre $F_{2^m}[Z]$

D. Augot^{*} P. Charpin[†] N. Sendrier[‡]

Résumé

Nous montrons que la classe des polynômes de $F_{2^m}[Z]$, qui sont les polynômes localisateurs des mots de plus petit poids du code BCH primitif binaire de longueur $2^m - 1$ et distance minimale $2^{m-2} - 1$, est en bijection avec l'ensemble des F_2 -sous-espaces de dimension $m - 2$ de F_{2^m} .

ON A CLASS OF $F_{2^m}[Z]$ POLYNOMIALS WHICH SPLIT IN F_{2^m}

ABSTRACT

We prove that the class of polynomials of $F_{2^m}[Z]$, which are the locator polynomials of the minimum weight codewords of the binary primitive BCH-code of length $2^m - 1$ and minimal distance $2^{m-2} - 1$, is in a one-to-one correspondance with the set of the $m - 2$ dimensional F_2 -subspaces of F_{2^m} .

^{*}Université Paris 6, UFR d'Informatique, LITP, 2 pl. Jussieu, 75251 Paris CEDEX 05

[†]INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex

[‡]INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex

1 Introduction

Nous notons $B(m, \delta)$ le code de Bose-Chaudhury-Hocquenghem (code BCH) binaire de longueur $n = 2^m - 1$ et distance construite δ ; le symbole α désigne une racine primitive du corps F_{2^m} . Nous considérons ici des codes BCH *au sens strict* (the narrow-sense BCH-codes [3,ch.9]): le code $B(m, \delta)$ est l'idéal de l'algèbre quotient $F_2[X]/(X^n - 1)$, composé des polynômes qui s'annulent sur l'ensemble

$$\{\alpha^j, j \in [1, \delta - 1]\} ;$$

son polynôme générateur est donc le *ppcm* des polynômes minimaux des α^j , $j \in [1, \delta - 1]$. Les mots de $B(m, \delta)$ ont un poids supérieur ou égal à δ . En général, on ne sait pas décrire l'ensemble des mots de $B(m, \delta)$ de poids δ .

Chaque mot de code $x \in B(m, \delta)$, de poids ω , peut être identifié à un sous-ensemble de $F_{2^m}^*$, soit $L_x = \{X_1, \dots, X_\omega\}$, et donc à un polynôme de $F_{2^m}[Z]$:

$$\sigma_x(Z) = \prod_{i=1}^{\omega} (1 - X_i Z) .$$

L_x est l'ensemble des *localisateurs* de x et $\sigma_x(Z)$ est le *polynôme localisateur* du mot de code x .

Inversement, on sait caractériser les polynômes localisateurs des mots de $B(m, \delta)$:

Proposition 1 [3,p. 260] *Soit un polynôme $Q(Z) = \sum_{i=0}^{\omega} q_i Z^i$ de $F_{2^m}[Z]$, $\omega \geq \delta$. Alors $Q(Z)$ est le polynôme localisateur d'un mot de code de $B(m, \delta)$ si et seulement si les conditions (i) et (ii) sont vérifiées:*

- (i) $i \in [1, \delta - 1]$ et i impair $\Rightarrow q_i = 0$.
- (ii) $Q(Z)$ est scindé¹ dans $F_{2^m}^*$ et ses racines sont distinctes.

Le résultat présenté ici met en évidence une propriété des polynômes scindés de degré $2^{m-2} - 1$ de l'algèbre $F_{2^m}[Z]$; on en déduit l'ensemble des mots de poids minimum des codes $B(m, \delta)$ pour $\delta = 2^{m-2} - 1$.

¹i.e. chacun de ses facteurs est de degré 1

2 Une propriété des polynômes scindés de $F_{2^m}[Z]$

On désigne par J le sous-ensemble de $[1, n]$:

$$J = \{ 2^{m-2} - 2^j \mid j \in [0, m-2] \} .$$

Théorème 1 *Soit le polynôme de degré $\delta = 2^{m-2} - 1$:*

$$Q(Z) = \sum_{i=0}^{\delta} q_i Z^i , \quad q_i \in F_{2^m} .$$

Si $Q(Z)$ vérifie (i) et (ii), alors il vérifie:

$$i \notin J \Rightarrow q_i = 0 . \quad (1)$$

Preuve: Nous supposons que $q_0 = 1$. Soit $\mathbf{Y} = \{Y_1, \dots, Y_\delta\}$ l'ensemble des racines de $Q(Z)$; soit $X_i = Y_i^{-1}$. Du fait que $Q(Z)$ vérifie (i) et (ii), on sait que le cardinal de $\mathbf{Y}$ est exactement égal à δ . Nous définissons les *fonctions-puissances* des X_i :

$$A_k = \sum_{i=1}^{\delta} X_i^k , \quad k \in [1, n].$$

Alors les q_i et les A_k vérifient les *Identités de NEWTON* sur $F_{2^m}[2, p.245]$:

$$r \leq \delta , \quad I_r : A_r + \sum_{i=1}^{r-1} A_{r-i} q_i + r q_r = 0 , \quad (2)$$

$$r > \delta , \quad I_r : A_r + \sum_{i=1}^{\delta} A_{r-i} q_i = 0 . \quad (3)$$

D'après (i) et (2), il est clair que: $A_r = 0$ pour $r < \delta$. On démontre par récurrence que $Q(Z)$ vérifie (1), le principe d'induction étant:

$$k \in [1, \delta - 1] , \quad H_k : k \notin J \Rightarrow A_{\delta+k} = 0 \text{ et } q_k = 0 .$$

Pour cela, on montre d'abord que l'identité $I_{\delta+k}$ se réduit à: $A_{\delta+k} + A_\delta q_k = 0$. On prouve ensuite H_k en étudiant:

- l'identité $I_{2\delta+3k}$ lorsque $k \leq 2^{m-3}$,
- l'identité $I_{2(\delta+k)}$ lorsque $k > 2^{m-3}$. $\square$

EXEMPLE: $m = 6$, $\delta = 15$, $Q(Z) = 1 + \sum_{i=1}^7 q_{2i}Z^{2i} + q_{15}Z^{15}$. Le Théorème montre que quelles que soient les valeurs données aux q_j dans F_{2^m} , $q_{15} \neq 0$, le polynôme $Q(Z)$, s'il est scindé, a la forme suivante:

$$Q(Z) = 1 + q_8Z^8 + q_{12}Z^{12} + q_{14}Z^{14} + q_{15}Z^{15}.$$

3 Mots de poids minimum des codes BCH de distance construite $2^k - 1$

Définition 1 [2,p.108] *Un 2-polynôme sur F_{2^m} est un polynôme de la forme:*

$$L(Z) = \sum_{i=0}^k l_i Z^{2^i}, \quad l_i \in F_{2^m}.$$

Soit $\mathcal{W}_\delta$, la classe des polynômes localisateurs des mots de $B(m, \delta)$ dont le poids est δ .

Lorsque $\delta = 2^k - 1$, $k \in [2, m-1]$, on connaît un sous-ensemble de $\mathcal{W}_\delta$; il est constitué des polynômes $\sigma(Z)$ construits ainsi:

- 1) Soit V un F_2 -sous-espace de dimension k de F_{2^m} et soit le polynôme $L(Z) = \prod_{v \in V} (Z - v)$. Alors $L(Z)$ est un 2-polynôme [2].
- 2) Il est clair que le polynôme

$$\sigma(Z) = Z^{2^k} L(Z^{-1}) = \sum_{i=0}^k \sigma_i Z^{2^k - 2^i},$$

vérifie les conditions (i) et (ii).

On peut donc identifier un sous-ensemble de $\mathcal{W}_\delta$ avec l'ensemble des sous-espaces V de F_{2^m} de dimension k . Le Théorème 1 prouve que, lorsque $k = m-2$, tout polynôme appartenant à $\mathcal{W}_\delta$ a la forme ci-dessus. Nous obtenons donc, dans ce cas, la description complète de l'ensemble $\mathcal{W}_\delta$:

Corollaire 1 *L'ensemble des mots de poids $2^{m-2} - 1$ du code $B(m, 2^{m-2} - 1)$ s'identifie avec l'ensemble des F_2 -sous-espaces de dimension $m-2$ de F_{2^m} .*

Le code engendré par l'ensemble des mots de poids $2^{m-2} - 1$ définis dans le Corollaire 1, est le code de Reed et Muller raccourci d'ordre 2. Lorsque $m > 5$, ce code est strictement contenu dans $B(m, 2^{m-2} - 1)$; son groupe d'automorphismes est le groupe linéaire $GL(m, 2)$ [3,p.398]. Donc le résultat présenté dans le Théorème 1 induit, de façon immédiate, deux propriétés du code $B(m, 2^{m-2} - 1)$:

Corollaire 2

1. *Lorsque $m > 5$, le code $B(m, 2^{m-2} - 1)$ n'est pas engendré par ses mots de plus petit poids.*
2. *Le groupe d'automorphismes du code $B(m, 2^{m-2} - 1)$ est contenu dans le groupe $GL(m, 2)$.*

References

- [1] T. KASAMI, S. LIN & W.W. PETERSON *New generalisation of the Reed-Muller codes*, IEEE Trans. Info Theory, vol. IT-14, p. 189-199 (1968).
- [2] R. LIDL & H. NIEDERREITER *Finite Fields*, Cambridge University Press.
- [3] F.J. MACWILLIAMS & N.J.A. SLOANE *The theory of Error Correcting Codes*, North-Holland 1986.