Europ. J. Combinatorics (1989) **10**, 1–12

Definition et Caracterisation d'une Dimension Minimale pour les Codes Principaux Nilpotents d'une Algebre Modulaire de p-Groupe Abelien Elementaire

PASCALE CHARPIN

L'ensemble des idéaux de l'algèbre est partitionné en sous-ensembles, déterminés à partir de la situation d'un idéal dans la suite décroissante d'idéaux que forment les codes de Reed et Muller Généralisés (GRM-codes). Dans chaque sous-ensemble, la dimension des idéaux est bornée inférieurement. Nous caractérisons les idéaux de dimension minimale; nous en déduisons une nouvelle représentation des éléments du GRM-code d'ordre 1.

The set of the ideals belonging to the algebra is divided into subsets; they are determined by the place of an ideal in the decreasing series of ideals composed by the Generalized Reed and Muller codes (GRM-codes). A lower bound is obtained for the dimension of the ideals in each subset. We characterize the minimal dimension ideals and such investigation permits us to represent elements of the first order GRM-code.

1. INTRODUCTION

Soit p un nombre premier; nous notons K le corps de Galois F_{p^r} et G le groupe additif $\{\mathrm{F}_{p^m}, +\}$. Nous désignons par $\mathbf{A}$ l'algèbre modulaire de p-groupe abélien élémentaire G, que nous représentons comme suit:

$$\mathbf{A} = \left\{ \sum_{g \in G} x_g X^g | x_g \in K \right\}. \tag{1}$$

Un élément de $\mathbf{A}$ est un polynôme et les opérations dans $\mathbf{A}$ sont celles usuelles d'addition et de multiplication de polynômes; le polynôme nul est élément neutre pour l'addition et le polynôme X^0, noté aussi 1, est élément neutre pour la multiplication.

Nous appelons *code de* $\mathbf{A}$ un idéal non trivial de $\mathbf{A}$. Soit P le *radical* de l'algèbre $\mathbf{A}$ et soit $P^j, j \in [1, M]$, la suite décroissante des puissances du radical de $\mathbf{A}$ où $M + 1$ est l'*indice de nilpotence* de P [3].

Pour chaque élément de $\mathbf{A}$ et pour chaque idéal non trivial de $\mathbf{A}$, il existe un indice j tel que P^j est la plus grande puissance de P qui le contienne. Nous pouvons ainsi réaliser une partition de l'ensemble des codes de $\mathbf{A}$: chaque code de $\mathbf{A}$ a pour paramètre sa *situation* dans la suite décroissante des P^j. Ce paramètre a été appelé *profondeur* par A. Poli [14]:

DÉFINITION 1. $j \in [1, M]$:
(1) L'ensemble $P^j \backslash P^{j+1}$ est l'ensemble des *éléments de* $\mathbf{A}$ *de profondeur* j.
(2) Un idéal I de $\mathbf{A}$ est de profondeur j si et seulement si:

$$I \subset P^j \quad \text{et} \quad I \not\subset P^{j+1}.$$

Les puissances du radical de $\mathbf{A}$ sont une classe de codes de Reed et Muller Généralisés (GRM-codes). Nous avons donné dans [6] une démonstration de cette propriété. Aussi parlerons-nous indifféremment du code P^j et du GRM-code d'ordre $M - j$. Les GRM-codes sont des codes 'de référence' en ce sens qu'ils interviennent dans l'étude de nombreux autres codes; nous voulons ici renforcer cette affirmation en montrant que le paramètre 'profondeur' nous renseigne sur la structure du code considéré. Le contexte de notre article

0195-6698/89/010001 + 12 $02.00/0

est la recherche des dimensions des idéaux principaux de **A**. Nous avons montré dans [7] que l'on peut déterminer une dimension minimale pour les idéaux d'une même profondeur; nous avons pu ainsi prouver que certains codes de Reed–Solomon étendus sont des idéaux principaux de **A** du fait qu'ils sont de dimension minimale. Nous voulons maintenant répondre à la question suivante: Quels sont les idéaux de dimension minimale et peut-on caractériser un de leurs générateurs?

Dans le Paragraphe 2 nous rappelons les résultats utiles pour la suite du texte. Ils ont été établis et développés dans [6], dans le cadre d'une étude globale sur les codes de l'algèbre **A**. Le lecteur pourra, s'il désire d'autres éléments, se reporter à [6], [7] et [8] et aux travaux de A. Poli [13].

Dans le Paragraphe 3 nous étudions un ensemble d'idéaux principaux qui ont une dimension minimale. Ceux-ci sont obtenus à partir d'ensembles de profondeur 1 que nous avons appelés *systèmes libres de* **A** *modulo* P^2. Nous montrons comment caractériser un système libre modulo P^2; les produits des éléments d'un tel système engendrent des idéaux principaux de dimension minimale dont nous étudions les propriétés.

Pour chaque profondeur donnée, les idéaux principaux définis ci-dessus sont isomorphes. Il est alors assez naturel de formuler la conjecture suivante:

CONJECTURE. A un isomorphisme près il n'existe qu'un seul idéal principal de profondeur donnée dont la dimension est minimale.

Dans le Paragraphe 4 nous prouvons que la conjecture est vraie dans deux cas particuliers: lorsque la profondeur j est un multiple de $p-1$, d'une part, et lorsqu'elle est supérieure à $(m-1)(p-1)$, d'autre part. En particulier, lorsque la caractéristique des corps est 2, nous caractérisons complètement l'ensemble des idéaux principaux de dimension minimale; pour une caractéristique $p > 2$, nous proposons une caractérisation partielle induite par les propriétés développées précédemment. A titre d'application, nous décrivons le GRM-code d'ordre 1.

En conclusion nous présentons plusieurs conjectures ainsi que les perspectives de notre travail.

2. PRÉLIMINAIRES

L'élévation à la puissance p-ième, dans l'algèbre **A**, est un endomorphisme du groupe additif de **A**. Nous avons donc:

$$x^p = \left(\sum_{g\in G} x_g X^g\right)^p = \sum_{g\in G} x_g^p X^0 = \left(\sum_{g\in G} x_g\right)^p X^0.$$

Ainsi un élément de **A** est soit nilpotent, si $x^p = 0$, soit inversible et dans ce cas on dit qu'il est une *unité de* **A**. L'ensemble des éléments nilpotents de **A** est le seul idéal maximal de **A** et est donc égal au radical de **A** [3]. Nous notons P le radical de **A**:

$$P = \left\{x \in \mathbf{A} \mid \sum_{g\in G} x_g = 0\right\}. \tag{2}$$

La puissance j-ième de P, notée P^j, est le K-sous-espace de **A** engendré par l'ensemble:

$$\left\{\prod_{k=1}^{j} a_k \mid a_k \in P\right\}.$$

Etant donné un idéal I de **A**, nous notons $\mathrm{Ann}(I)$ l'idéal annulateur de I. Rappelons que:

$$\mathrm{Ann}(I) = \{x \in \mathbf{A} \mid xy = 0, y \in I\}. \tag{3}$$

La proposition suivante contient les premières propriétés des codes P^j; elle peut se démontrer en utilisant une base du K-espace **A**, particuliérement pratique lorsque l'on s'intéresse à la profondeur des éléments; cette base est définie ci-après par la Proposition 2.

PROPOSITION 1. *Soit* $M = m(p-1)$; *nous notons* **1** *le polynôme de* **A** *dont tous les coefficients sont égaux à* 1. *La suite des puissances* P^j *du radical de* **A** *est une suite décroissante d'idéaux qui vérifie les propriétés suivantes*:
(1) $P^{M+1} = \{0\}$;
(2) $\mathrm{Ann}(P^j) = P^{M-j+1}$;
(3) $P^M = \{a\mathbf{1} | a \in K\}$.

PROPOSITION 2. *Soit* $e = \{e_1, \ldots, e_m\}$, *une base du* F_p*-espace vectoriel* G. *Alors l'ensemble*

$$B(e) = \left\{ \prod_{k=1}^{m} (X^{e_k} - 1)^{i_k} | i_k \in [0, p-1] \right\} \tag{4}$$

est une base du K*-espace vectoriel* **A**. *De plus, pour chaque* j *de* $[1, M]$, *le sous-ensemble de* $B(e)$

$$B(j, e) = \left\{ \prod_{k=1}^{m} (X^{e_k} - 1)^{i_k} \in B(e) | \sum_{k=1}^{m} i_k \geqslant j \right\} \tag{5}$$

est une base de P^j.

On peut aussi définir P^j par un système de générateurs ayant la même profondeur; ces générateurs sont, en outre, des mots de plus petit poids de P^j et chacun est élément d'une base de type $B(e)$:

PROPOSITION 3. *Soit* $j \in [1, M]$ *et soient* s *et* t *le quotient et le reste de la division de* j *par* $p-1$. *Alors le code* P^j *est l'idéal de* **A** *engendré par l'ensemble*

$$Ge(j) = \left\{ (X^{g_1} - 1)^t \prod_{k=2}^{s+1} (X^{g_k} - 1)^{p-1} \,\middle|\, \begin{array}{l} \{g_1, \ldots, g_{s+1}\} \\ \text{est une base de } G \end{array} \right\}. \tag{6}$$

où, par convention, le produit ci-dessus, pour k *variant de* 2 *à* $s+1$, *est égal à* 1 *lorsque* $s = 0$.

Soit x un élément de **A** de profondeur j; x étant exprimé avec une base du type $B(e)$, il est clair que l'on peut déterminer un élément y de $Ge(M-j)$ tel que le produit xy soit égal au vecteur **1**, à un scalaire prés:

$$\exists y, \quad y \in Ge(M-j); \qquad yx \in P^M \backslash \{0\}. \tag{7}$$

Nous notons (x) l'idéal principal engendré par x. Le résultat formulé en (7) est utilisé pour exhiber un système libre de l'idéal (x), système du type Vx où V est un sous-ensemble d'une base du type $B(e)$. Le théorème suivant s'en déduit immédiatement:

THÉORÈME 1. *Soient* $j \in [1, M]$ *et* x *un élément de profondeur* j. *On considère la division entière* $j = s(p-1) + t$. *Alors*:
(1) $\dim(x) \geqslant (p-t)p^{m-s-1}$;
(2) $x \in Ge(j) \rightarrow \dim(x) = (p-t)p^{m-s-1}$.

REMARQUES. Le Théorème 1 nous permet d'affirmer, pour certains idéaux, qu'ils sont principaux. En effet un idéal de dimension minimale est un idéal principal; nous prouvons ainsi dans [8] que pour chaque valeur de j (i.e. pour chaque profondeur) il existe un code de Reed–Solomon étendu qui est un idéal principal de **A**.

D'autre part, nous venons de définir un corpus d'idéaux principaux de dimension minimale; nous allons nous intéresser à son image par un automorphisme de l'algèbre **A**. La proposition suivante rappelle qu'un automorphisme de **A** peut se définir par sa valeur en m éléments du type $(X^{e_i} - 1)$.

PROPOSITION 4. *La donnée d'un automorphisme ϕ de l'algèbre* **A** *est la donnée d'un ensemble de substitutions*:

$$\phi = \{\phi_1, \ldots, \phi_m\}, \qquad \phi_k \in P \qquad et \qquad \prod_{k=1}^{m} \phi_k^{p-1} \neq 0 \tag{8}$$

où $\phi_k = \phi((X^{e_k} - 1))$ et $\{e_1, \ldots, e_m\}$ est une base du K-espace G.

3. IDÉAUX PRINCIPAUX OBTENUS PAR SUBSTITUTION D'ELÉMENTS DE $B(e)$

D'après la Proposition 4, déterminer les images isomorphes des idéaux principaux engendrés par les éléments des ensembles $Ge(j)$, revient à caractériser des ensembles de profondeur 1 vérifiant (8). C'est ce que nous faisons maintenant.

DÉFINITION 2. Soit $k \in [1, m]$. Un ensemble $\{x_1, \ldots, x_m\}$ de k éléments de profondeur 1 est un *système libre de* **A** *modulo* P^2 si et seulement si toute combinaison K-linéaire, non nulle, des vecteurs x_i est un élément de profondeur 1.

On peut caractériser un système libre modulo P^2 en étudiant la profondeur des produits des éléments du système entre eux:

PROPOSITION 5. *Soit $x = \{x_1, \ldots, x_k\}$ un ensemble de k éléments de P, avec $k \in [1, m]$. Alors x est un système libre de* **A** *modulo P^2 si et seulement si la profondeur du produit $\Pi_{i=1}^{k} x_i^{p-1}$ est égale à $k(p-1)$.*

PREUVE. Chaque vecteur x_i, $i \in [1, k]$, écrit dans la base $B(e)$ donnée par (1), peut s'exprimer comme suit:

$$x_i = y_i + z_i \quad \text{où} \quad z_i \in P^2, \qquad y_i = \sum_{l=1}^{m} x_{i,l}(X^{e_l} - 1), \qquad x_{i,l} \in K.$$

Soit $b = \Pi_{i=1}^{k} x_i^{p-1}$. Alors $b = \Pi_{i=1}^{k} (y_i + z_i)^{p-1}$ où z_i est de profondeur supérieure ou égale à 2. Donc b est de profondeur $k(p-1)$ si et seulement si le produit c, $c = \Pi_{i=1}^{k} y_i^{p-1}$, est non nul.

Supposons d'abord que x n'est pas un système libre de **A** modulo P^2. Par définition, cela signifie que l'ensemble $\{y_1, \ldots, y_k\}$ n'est pas un système libre. Donc, par exemple:

$$y_1 = \sum_{i=2}^{k} a_i y_i, \qquad a_i \in K.$$

D'où

$$c = \left(\sum_{i=2}^{k} a_i y_i\right)^{p-1} \times \prod_{i=2}^{k} y_i^{p-1}.$$

Si l'on développe le produit c, chaque terme obtenu comporte au moins un facteur y_i^p qui l'annule car y_i est nilpotent. Donc $c = 0$ et la profondeur de b n'est pas égale à $k(p-1)$.

Supposons, inversement, que x est un système libre modulo P^2. Alors la matrice $k \times m$ dont les k lignes sont les vecteurs

$$\{x_{i,1}, \ldots, x_{i,m}\}, \qquad i \in [1, k]$$

est de rang k. On peut alors supposer, sans perdre en généralité, que ses k premières colonnes forment une matrice $k \times k$ inversible. C'est dire que le système

$$y_i = \sum_{l=1}^{m} x_{i,l}(X^{e_l} - 1), \qquad i \in [1, k]$$

est équivalent à un système du type suivant:

$$y_i' = (X^{e_i} - 1) + \sum_{l=k+1}^{m} x_{i,l}'(X^{e_l} - 1), \qquad i \in [1, k]$$

où $x_{i,l}' \in K$; y_i' est une combinaison K-linéaire des vecteurs $(y_1, \ldots, y_k\}$. Soit $c' = \Pi_{i=1}^{k} y_i'^{p-1}$. Si l'on développe c' en fonction des y_i, on trouve $c' = ac$ avec $a \in K$. Si l'on développe c' en fonction des $(X^{e_l} - 1)$, $l \in [1, m]$, c' s'exprime dans la base $B(e)$, l'élément $\Pi_{i=1}^{k} (X^{e_i} - 1)^{p-1}$ étant affecté du coefficient 1. Donc c' est non nul et donc il en est de même pour c du fait que $c' = ac$. On en conclut que b est de profondeur $k(p - 1)$. □

On obtient ainsi une nouvelle caractérisation des automorphismes de **A**:

COROLLAIRE 1. *Soit ϕ un endomorphisme de* **A** *défini par l'ensemble des substitutions*:

$$(X^{e_k} - 1) \to \phi_k \in P.$$

Alors ϕ est un automorphisme de l'algèbre **A** *si et seulement si l'ensemble $\{\phi_1, \ldots, \phi_m\}$ est un système libre de* **A** *modulo P^2.*

PREUVE. La proposition 5 montre que ϕ est un système libre modulo P^2 si et seulement si le produit $\Pi_{i=1}^{m} \phi_k^{p-1}$ est non nul. D'aprés (8), il est équivalent de dire que ϕ est un automorphisme de **A**. □

On obtient ainsi une formulation plus générale des bases définies par (4) et (5):

THÉORÈME 2. *Soit $x = \{x_1, \ldots, x_m\}$ un système libre de* **A** *modulo P^2. Alors l'ensemble*

$$B(x) = \left\{ \prod_{k=1}^{m} x_k^{i_k} \mid i_k \in [0, p - 1] \right\} \tag{9}$$

est une base du K-espace vectoriel **A**. *De plus, pour chaque j de $[1, M]$, le sous-ensemble de $B(e)$*

$$B(j, x) = \left\{ \prod_{k=1}^{m} x_k^{i_k} \in B(e) \mid \sum_{k=1}^{m} i_k \geqslant j \right\} \tag{10}$$

est une base de P^j.

PREUVE. Ces bases se déduisent des bases définies par (4) et (5) par un automorphisme de l'algèbre **A**. □

Nous avons caractérisé les images isomorphes des éléments des ensembles $Ge(j)$; aussi pouvons-nous compléter le Théorème 1 par le corollaire suivant. La formule (11) définit complètement le gènérateur d'un idéal principal de dimension minimale caractérisé par le Théorème 1.

COROLLAIRE 2. *Soit $j \in [1, M]$ et la division entière $j = s(p - 1) + t$. Alors l'idéal principal engendré par*

$$x' = x_1^t x_2^{p-1} \cdots x_{s+1}^{p-1} \tag{11}$$

où $\{x_1, \ldots, x_{s+1}\}$ *est un système libre modulo* P^2, *a une dimension minimale* (*i.e. sa dimension est égale à* $(p-t)p^{m-s-1}$).

Nous allons maintenant étudier certaines propriétés particulières des idéaux principaux de **A** engendrés par un élément d'une base de type $B(x)$.

PROPOSITION 6. *Soit* $\{x_1, \ldots, x_m\}$ *un système libre de* **A** *modulo* P^2 *et soit* $y = \Pi_{k=1}^m x_k^{i_k}$, *avec* $i_k \in [0, p-1]$. *Alors*:

(i) $\dim(y) = \prod_{k=1}^{m} (p - i_k)$;

(ii) $\mathrm{Ann}(y) = \dot{+}_{k=1}^{m} (x_k^{p-i_k})$.

PREUVE. Soit

$$\mathbf{U} = \left\{ \prod_{k=1}^{m} x_k^{j_k} \mid j_k \in [0, p - i_k - 1] \right\}.$$

En tant que sous-ensemble de $B(x)$, l'ensemble $\mathbf{U}y$ est un système libre du K-espace (y); $\mathbf{U}y$ est une base de (y) car:

$$z \in B(x) \backslash \mathbf{U} \leftrightarrow zy = 0.$$

Cette égalité fournit une base de l'annulateur de y et démontre (ii). Le cardinal de l'ensemble $\mathbf{U}y$ est égal à $\Pi_{k=1}^m (p - i_k)$, ce qui démontre (i). □

REMARQUES. Si, dans la définition de y, un seul i_k est différent de 0 et de $p-1$, alors l'idéal (y) a une dimension minimale; sinon la dimension de (y) est strictement non minimale.

COROLLAIRE 3. *Soit* $y \in P \backslash P^2$. *Alors*:
(i) $\dim(y) = p^{m-1}(p-1)$;
(ii) $\forall s, s \in [1, p-1]$, $\mathrm{Ann}(y^s) = (y^{p-s})$.

PREUVE. Nous conservons les notations de la Proposition 6. Si y est de profondeur 1, alors $y = x_l$ et donc $i_k = 0$ pour $k \neq l$. On applique alors les résultats de la Proposition 6 à ce cas particulier. □

REMARQUES. Tous les idéaux principaux de profondeur 1 sont isomorphes et ont donc la même dimension; ceci permet de calculer le nombre d'idéaux de **A** de profondeur 1 (cf. Proposition 7, ci-après). Lorsque $p = 2$, on trouve ainsi des codes autoduaux; ces codes, appelés H-codes, ont d'abord été étudiés par P. Camion dans [4]. En petites longueurs, et sur F_2, ils sont de 'bons codes autoduaux' à poids multiples de 2 ou de 4.

Nous avons montré dans [6] que la dimension d'un idéal principal de **A** est au plus égale à $p^{m-1}(p-1)$. A. Poli a montré ensuite que les idéaux principaux de profondeur 1, et eux seuls, atteignent cette borne [15]; si bien qu'en caractéristique 2, les seuls idéaux principaux autoduaux de **A** sont ceux de profondeur 1.

PROPOSITION 7. *L'algèbre* **A** *comporte*

$$q^{p^{m-1}-1} \frac{q^m - 1}{q - 1} \qquad (q = p^r)$$

idéaux principaux de profondeur 1.

PREUVE. Soit $y \in P\backslash P^2$. L'ensemble des générateurs de l'idéal (y) est l'ensemble des éléments de (y) de profondeur 1; le cardinal de cet ensemble est le même pour tout idéal de profondeur 1 (deux idéaux de profondeur 1 sont isomorphes). De plus, un élément de profondeur 1 appartient à un et un seul idéal principal dont il est générateur. Soient

$$\beta = |P\backslash P^2| \quad \text{et} \quad \gamma = |(y) \cap (P\backslash P^2)|;$$

alors:

$$|\{(x) | x \in P\backslash P^2\}| = \beta/\gamma.$$

Or dim P = dim $P^2 + m$, donc $\beta = (q^m - 1)q^{p^m - m - 1}$. Et $\gamma = (q-1)q^{p^{m-1}(p-1)-1}$ car l'ensemble $(y) \cap P^2$ est un hyperplan du K-espace (y) (cette propriété est demontrée dans [9]). □

Une autre conséquence de la Proposition 6 est qu'un idéal engendré par un élément de $B(x)$ est une intersection d'idéaux de même type:

COROLLAIRE 4. *Soit* $\{x_1, \ldots, x_m\}$, *un système libre de* **A** *modulo* P^2. *Alors*:

$$\left(\prod_{i=1}^{m} x_k^{i_k}\right) = \bigcap_{k=1}^{m} (x_k^{i_k}), \qquad (i_1, \ldots, i_m) \in [0, p-1]^m. \tag{12}$$

PREUVE. Rappelons d'abord l'égalité suivante, où I_i désigne un idéal de l'algèbre **A**:

$$\text{Ann}\left(\bigcap_{i=1}^{n} I_i\right) = \sum_{i=1}^{n} \text{Ann}\,(I_i). \tag{13}$$

Elle se déduit du fait que dans **A**, l'annulateur et l'orthogonal d'un idéal sont isomorphes [6]; or cette identité est bien connue lorsque les I_i sont n sous-espaces d'un même espace vectoriel et si l'on remplace Ann(I_i) par l'espace orthogonal de I_i.

Les notations étant celles de l'énoncé, soient

$$x = \prod_{k=1}^{m} x_k^{i_k} \quad \text{et} \quad I = \bigcap_{i=1}^{m} (x_k^{i_k}).$$

D'aprés la Proposition 6, $\text{Ann}(x) = +_{k=1}^{m} (x_k^{p-i_k})$. On déduit alors de (13) que les idéaux I et (x) ont le même annulateur; ils sont donc égaux. □

4. IDÉAUX DE A DE DIMENSION MINIMALE

Soit un idéal I de dimension minimale. Dans ce paragraphe nous voulons répondre à la question suivante: Connaissant la profondeur de I, peut-on exhiber un générateur de I? Nous allons montrer que l'utilisation des systèmes libres modulo P^2 apporte une réponse partielle à la question posée.

THÉORÈME 3. *Soient* $j \in [1, M]$ *et la division entière* $j = s(p-1) + t$. *Soit* x *un élément de* **A** *de profondeur* j. *Si l'idéal* (x) *a une dimension minimale, alors il existe un système libre de* **A** *modulo* P^2 *de cardinal* s, *soit* $\{a_1, \ldots, a_s\}$, *tel que*:

$$(x) \subset \left(\prod_{k=1}^{s} a_k^{p-1}\right). \tag{14}$$

PREUVE. D'aprés le Théorème 1, l'idéal (x) a une dimension minimale si dim $(x) = (p-t)p^{m-s-1}$. Dans cette démonstration, nous considérons la division entière $M - j = s'(p-1) + t'$ (avec cette notation: dim $(x) = p^{s'}(t'+1)$).

Lorsque $j = M$, (x) est l'idéal P^M; si $m = 1$, alors tous les idéaux de $\mathbf{A}$ sont principaux et ont un générateur du type $(X^e - 1)^t$, avec $e \in \mathbf{F}_p$. Dans ces deux cas, le théorème est clairement vérifié. Nous supposons désormais que $j \in [1, M[$ et $m > 1$.

Le Théorème 1 est déduit du résultat suivant: quel que soit l'élément x de profondeur j, il existe une base $\{g_1, \ldots, g_m\}$ de G telle que l'ensemble $\mathbf{V}x$ où

$$\mathbf{V} = \left\{ \sum_{k=1}^{s'+1} (X^{g_k} - 1)^{i_k} | (i_1, \ldots, i_{s'+1}) \in [0, t'] \times [0, p-1]^{s'} \right\}$$

est un système libre du K-espace (x) [7]. Lorsque la dimension de (x) est minimale, l'ensemble $\mathbf{V}x$ est une base de (x). Nous avons donc

$$\forall k, \quad k \in [1, m], \quad (X^{g_k} - 1)x = V_k x$$

où V_k est une combinaison K-linéaire d'éléments de $\mathbf{V}$. Si l'on veut déterminer le nombre d'éléments du type $(X^{g_k} - 1)$ appartenant à $\mathbf{V}$, deux cas sont à étudier:
(1) si $t' = 0$, d'où $s = m - s'$, alors

$$k \notin [2, s' + 1] \to (X^{g_k} - 1) \notin \mathbf{V};$$

(2) si $t' \neq 0$, d'où $s = m - s' - 1$, alors

$$k \notin [1, s' + 1] \to (X^{g_k} - 1) \notin \mathbf{V}.$$

Donc, il existe s éléments $X^{g_k} - 1$ tels que

$$((X^{g_k} - 1) - V_k)x = 0 \quad \text{et} \quad (X^{g_k} - 1) \notin \mathbf{V}.$$

Nous obtenons ainsi s éléments de profondeur 1 qui annulent x; l'ensemble de ces éléments, que nous notons $\{a_1, \ldots, a_s\}$ est, par construction, un système libre de $\mathbf{A}$ modulo P^2.

Nous avons: $x \in \bigcap_{i=1}^{s} \mathrm{Ann}\,(a_i)$. Donc, d'aprés le Corollaire 3,

$$(x) \subset \bigcap_{i=1}^{s} (a_i^{p-1});$$

et d'aprés le Corollaire 4:

$$(x) \subset \left(\prod_{i=1}^{s} a_i^{p-1} \right). \qquad \square$$

COROLLAIRE 5. *Les hypothèses sont celles du Théorème* 3; *on suppose en outre que j divise* $p - 1$. *Alors il existe un système libre de* $\mathbf{A}$ *modulo* P^2 *de cardinal s, soit* $\{a_1, \ldots, a_s\}$, *tel que*:

$$(x) = \left(\prod_{k=1}^{s} a_k^{p-1} \right) = \bigcap_{k=1}^{s} (a_k^{p-1}). \tag{15}$$

PREUVE. Soit $a = \Pi_{k=1}^{s} a_k^{p-1}$; la profondeur de a est égale à $s(p-1)$ qui est ici la profondeur de x. D'aprés (14), nous avons $(x) \subset (a)$. Or un idéal principal de profondeur j ne contient qu'un seul idéal de profondeur j, lui-même. Donc $(x) = (a)$. La deuxième égalité dans (15) est immédiatement déduite de (12). $\square$

APPLICATION: LES IDÉAUX PRINCIPAUX DE PROFONDEUR $M - 1$. Soit $M = m(p-1)$; supposons d'abord que x est un élément de profondeur j, avec $j \in [(m-1)(p-1), m(p-1)]$, et tel que l'idéal (x) est de dimension minimale:

$$j = (m-1)(p-1) + t \quad \text{et} \quad \dim(x) = p - t.$$

Nous appliquons le Théorème 3: il existe un système libre de $\mathbf{A}$ modulo P^2, soit $a = \{a_1, \ldots, a_m\}$, tel que $(x) \subset (y)$, avec $y = \Pi_{k=1}^{m-1} a_k^{p-1}$. On en déduit: $x = zy$ avec $z \in P^t$.

On exprime alors x dans la base $B(a)$ définie par (9):

$$x = \left(\sum_{k=t}^{p-1} z_k a_m^k\right) y \qquad \text{où} \qquad z_k \in K, \quad z_t \neq 0$$

car tous les termes a_i^k tels que $i \neq m$ sont annulés par y. Donc:

$$x = \left(\sum_{k=t}^{p-1} z_k a_m^{k-t}\right) a_m^t y = c a_m^t y \qquad \text{où} \qquad c \in A \backslash P.$$

Nous avons ainsi démontré le corollaire suivant:

COROLLAIRE 6. *Soient* $j \in [(m-1)(p-1), m(p-1)]$ *et la division entière* $j = (m-1)(p-1) + t$; *soit* x *un élément de* **A** *de profondeur* j *et de dimension minimale. Alors il existe un système libre de* **A** *modulo* P^2, *soit* $a = \{a_1, \ldots, a_m\}$ *tel que*

$$(x) = \left(a_m^t \prod_{k=1}^{m-1} a_k^{p-1}\right). \tag{16}$$

Le Corollaire 6 permet une étude plus poussée des éléments de **A** de profondeur $M-1$, c'est-à-dire des mots du GRM-code d'ordre 1 ou encore des mots du code P^{M-1}. D'abord il est clair que tous les idéaux principaux de profondeur $M-1$ ont une dimension identique, égale à 2 (i.e. à dim $P^M + 1$). On peut donc, par le procédé utilisé pour la preuve de la proposition 7, obtenir le nombre d'idéaux principaux de **A** de profondeur $M-1$.

PROPOSITION 8. *L'algèbre* **A** *comporte* $(q^m - 1)/(q-1)$ *idéaux principaux de profondeur* $M-1$ ($q = p^r$, q *est l'ordre du corps de base* K).

Le corollaire suivant est une conséquence immédiate du Corollaire 6. Il exploite le fait que tout élément de profondeur $M-1$ a une dimension minimale et engendre donc un idéal du type (16).

COROLLAIRE 7. *Soit* y *un élément de* **A** *de profondeur* $M-1$. *Alors il existe un système libre de* **A** *modulo* P^2, *soit* $\{a_1, \ldots, a_m\}$ *tel que*

$$y = a_m^{p-2} \prod_{k=1}^{m-1} a_k^{p-1}. \tag{17}$$

Un élément de P^M est de la forme $c \prod_{k=1}^{m} a_k^{p-1}$, avec $c \in K$ et quel que soit le système libre modulo P^2 choisi. Donc nous venons de montrer que *tout mot du GRM-code d'ordre* 1 *est un élément d'une base de type* $B(M-1, a)$ *définie par le Théorème* 2.

Lorsque $K = \mathrm{F}_p$, on peut se rapprocher encore de la description des codes de Reed et Muller d'ordre 1. En effet, le nombre L de mots de plus petits poids du GRM-code d'ordre 1 est dans ce cas

$$L = |K^*| p \frac{p^m - 1}{p - 1} \tag{18}$$

(ce résultat est donné par P. Delsarte, J. M. Goethals et F. J. MacWilliams dans [10]). On en déduit que $L = \beta p(p-1)$ où β est le nombre d'idéaux de **A** de profondeur $M-1$, calculé par la Proposition 8. Or le code P^{M-1} a pour dimension $m+1$ et contient P^M, c'est-à-dire $p-1$ mots de poids p^m. On obtient donc:

PROPOSITION 9. *Lorsque* $K = F_p$, *le code* P^{M-1} *est un code à deux poids non nuls; il comporte*:

$p(p^m - 1)$ *mots de poids* $p^{m-1}(p-1)$ *et* $p-1$ *mots de poids* p^m.

Chaque idéal principal de profondeur $M-1$ comporte 1 mot de poids 0, $p-1$ mots de poids p^m et $p(p-1)$ mots de poids $p^{m-1}(p-1)$.

Nous avons montré dans [6] que les mots de plus petit poids de P^{M-1} sont les mots cy où c est une unité de **A** et où y est un élément du système de générateurs $Ge(M-1)$ défini par la Proposition 3. Donc *lorsque $K = F_p$, tout idéal principal de* **A** *de profondeur $M-1$ a pour générateur un élément x du type suivant*:

$$x = (X^{e_1} - 1)^{p-2} \prod_{k=2}^{m} (X^{e_k} - 1)^{p-1} \tag{19}$$

où $\{e_1, \ldots, e_m\}$ est une base du K-espace G.

Les mots des codes de Reed et Muller d'ordre 1 (i.e. les codes P^{M-1} avec $K = F_2$ et donc $M = m$) sont les mots de **A** ayant pour support une variété linéaire de G de dimension m ou $m-1$ (on trouve cette description dans [11], par exemple); cela signifie que les mots de P^{m-1}, lorsqu'il s'agit de codes binaires, s'écrivent

$$x = X^g \prod_{k=1}^{i} (X^{e_k} - 1) \qquad g \in G,\ i = m \quad \text{où} \quad i = m-1$$

où $\{e_1, \ldots, e_m\}$ est une base de G.

Le Corollaire 7 et les résultats donnés ensuite prouvent que ces propriétés des codes de Reed et Muller se généralisent lorsque le corps de base K est d'ordre strictement supérieur à 2: les mots du GRM-code d'ordre 1 sont de deux types (profondeur M ou $M-1$) obtenus à partir de produits d'éléments d'un système libre de **A** modulo P^2.

5. Conclusions

Nous avons montré que l'on peut déterminer, dans plusieurs situations, la forme d'un générateur d'un idéal principal de **A** de dimension minimale. Cette dimension minimale est définie dans le Théorème 1; la profondeur de l'idéal concerné doit toujours être connue; toutefois, nous conjecturons *qu'un idéal principal ayant la dimension minimale des idéaux de profondeur j, est lui-même de profondeur j.*

Etant donnée une profondeur j, les cas où l'on caractérise complétement un idéal de dimension minimale sont lorsque j est divisible par $p-1$ ou lorsque j est supérieur à $(p-1)(m-1)$ (cf. Corollaires 5 et 6). Il en résulte que, lorsque $p = 2$, on sait caractériser tout idéal de dimension minimale; le Corollaire 5 induit le résultat général:

Proposition 10. *$p = 2$ et $j \in [1, m]$. Soit x un élément de* **A** *de profondeur j. Si* $\dim(x) = 2^{m-j}$, *alors il existe un système libre de* **A** *modulo P^2, soit $\{a_1, \ldots, a_j\}$ tel que*

$$(x) = \left(\prod_{k=1}^{j} a_j\right).$$

Les résultats que nous donnons renforcent la conjecture énoncée dans l'introduction. En effet, dans tous les cas nous caractérisons des idéaux de dimension minimale appartenant au corpus défini par le Corollaire 2.

Soit x un élément de profondeur j où $j \in [1, p-1]$ et tel que la dimension de l'idéal (x) est minimale (c'est-à-dire égale à $p^{m-1}(p-j)$). Alors l'annulateur de (x) a pour dimension:

$$\dim \mathrm{Ann}\,(x) = p^m - p^{m-1}(p-j) = p^{m-1}j.$$

L'idéal Ann (x) a une profondeur au plus égale à $p-j$; mais la valeur de sa dimension implique que sa profondeur est exacement $p-j$. ($p^{m-1}j$ est la dimension minimale des

idéaux de profondeur $p - j$); Ann (x) est donc un idéal principal. Dans ce cas particulier la question posée en détermine une autre: quels sont les idéaux de **A** qui ont pour annulateur un idéal principal?

Nous conjecturons que *les idéaux principaux de* **A** *qui ont pour annulateur un idéal principal sont déterminés par la Proposition* 6 c'est-à-dire qu'ils sont de la forme suivante:

$$(y^k), \qquad k \in [1, p-1], \qquad y \in P \backslash P^2.$$

Tous les idéaux principaux engendrés par un élément d'une base de type $B(e)$ (cf. Proposition 2), ont la *propriété de non-décroissance*; c'est-à-dire qu'un de leur générateur est un mot de plus petit poids du code principal considéré. Cette propriété est étudiée par S. D. Berman et I. I. Grusko dans le cas binaire [2]. On peut alors se poser le problème du poids des générateurs étudiés ici et se demander si la propriété de non-décroissance est encore vérifiée dans certains cas moins triviaux que celui des codes de Reed–Solomon; les codes de Reed–Solomon étendus qui sont des idéaux principaux ont en effet un générateur qui a le poids minimum [8].

Enfin, la description du GRM-code d'ordre 1 suggère que la distribution des poids du RM-code d'ordre 2 binaire peut se généraliser en caractéristique p quelconque, du moins partiellement.

Remerciements

Nous remercions l'un de nos rapporteurs pour ses remarques et ses suggestions qui nous ont permis d'améliorer la rédaction de notre texte.

Références

1. S. D. Berman, On the theory of group codes. *Kibernetica* **1** (1) (1967), 31–39.
2. S. D. Berman and I. I. Grushko, Code parameters of principal ideals of group $(2, \ldots, 2)$ over field of characteristic 2. *Pr. Pe. Inform.* **14** (4) (1978), 3–12.
3. N. Bourbaki, *Livre II—Algèbre*. Herman, Paris, 1958.
4. P. Camion, Etude de codes binaires abéliens modulaires autoduaux de petites longueurs. *Revue du CETHEDEC*, NS **79** (2) (1979), 3–24.
5. P. Camion, A proof of some properties of Reed–Muller codes by means of the normal basis. In: R. C. Bose and T. A. Dowling, eds, *Combinatorial Mathematics and its Applicants*. Univ. North Carolina Press, Chapel Hill, N.C., 1969.
6. P. Charpin, Codes idéaux de certaines algèbres modulaires. Thèse de 3ième cycle, Université de Paris VII, 1982.
7. P. Charpin, The extended Reed–Solomon codes considered as ideals of a modular algebra. *Ann. Discr. Math.* **17** (1983), 171–176.
8. P. Charpin, Les codes de Reed–Solomon en tant qu'idéaux d'une algèbre modulaire. *C. R. Acad. Sci. Paris* **294**, Série I (Mai 1982), 597–600.
9. P. Charpin, Codes cycliques étendus et idéaux principaux d'une algèbre modulaire. *C. R. Acad. Sci. Paris* **295**, Série I (Septembre 1982), 313–315.
10. P. Delsarte, J. M. Goethals, and F. J. MacWilliams, On generalized Reed–Muller codes and their relatives. *Inform. Control* **16** (1974), 403–442.
11. T. Kasami, S. Lin and W. W. Peterson, New generalisations of the Reed–Muller codes. *IEEE Trans. Inform. Theory* **II-14** (1968), 189–199.
12. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. North Holland, Amsterdam, 1977.
13. A. Poli, Codes dans certaines algèbres modulaires. Thèse de Doctorat d'Etat Univ. P. Sabatier, Toulouse, 1978.
14. A. Poli, Codes stables sous le groupe des automorphismes isométriques de $A = F_p[X_1, \ldots, X_n]/(X_1^p - 1, \ldots, X_n^p - 1)$. *C. R. Acad. Sci. Paris* **290** (1980).
15. A. Poli, Idéaux principaux nilpotents de dimension maximale dans l'algèbre $F_q[G]$ d'un groupe abélien fini *G. Commums. Algebra* **12**(4) (1984), 391–401.

16. J. H. Van Lint, *Coding Theory*. Springer Verlag, New York, 1971.
17. J. Wolfmann, A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field. *Discr. Math.* **31**(1980), 337–338.

Received 28 March 1983 and in revised form 1 June 1987

PASCALE CHARPIN
Institut de Programmation et Laboratoire d'Informatique Théorique et Programmation, 4 place Jussieu, 75252 Paris Cedex 05, France