Codage & cryptage

Dany-Jack Mercier, Robert Rolland

Polynômes homogènes à plusieurs variables sur un corps fini $\mathbb{F}_q$ qui s'annulent sur l'espace projectif $\mathbb{P}^m(\mathbb{F}_q)$

Dany-Jack Mercier & Robert Rolland

Résumé

Nous étudions dans l'anneau $\mathbb{F}_q[X_0, X_1, \cdots, X_m]$ des polynômes à $m+1$ variables et à coefficients dans le corps fini à q éléments, l'idéal homogène $\mathcal{J}$ engendré par les polynômes homogènes qui s'annulent sur tout l'espace. Cet idéal s'introduit naturellement lors de l'étude des codes de Reed-Muller projectifs ([7], [8]). Nous donnons une résolution libre du quotient $\mathbb{F}_q[X_0, \cdots, X_m]/\mathcal{J}$ en utilisant le complexe de Eagon et Northcott [4] qui généralise le complexe de Koszul [5]. Ceci permet en particulier de calculer directement les dimensions des composantes homogènes de l'idéal.

Mots clés : corps fini, polynôme homogène, résolution libre, complexe de Koszul.

1 Introduction - Notations.

Soit p un nombre premier, $q = p^s$ et $\mathbb{F}_q$ le corps fini à q éléments. Soit m un entier ≥ 1. Nous notons $\mathcal{P}(q, m+1)$ l'espace $\mathbb{F}_q[X_0, X_1, .., X_m]$ des polynômes à $m+1$ variables et à coefficients dans $\mathbb{F}_q$. Notons aussi $\mathcal{H}(q, m+1, d)$ le sous espace de $\mathcal{P}(q, m+1)$ constitué des polynômes homogènes de degré d.

La décomposition :

$$\mathcal{P}(q, m+1) = \bigoplus_{d \geq 0} \mathcal{H}(q, m+1, d)$$

fournit à $\mathcal{P}(q, m+1)$ une structure d'algèbre graduée.

Soit $\mathcal{A}$ l'idéal de l'anneau $\mathcal{P}(q, m+1)$ constitué des polynômes qui s'annulent sur tout l'espace $\mathbb{F}_q^{m+1}$.

Il est bien connu que (cf. [6] théorème 1) :

Lemme 1 *L'idéal $\mathcal{A}$ est engendré par les polynômes $X_i^q - X_i$ où $0 \leq i \leq m$.*

[0] [ccod0010] Journal of Pure and Applied Algebra 124, pp. 227-240, 1998.

D.-J. Mercier, Equipe Applications de l'Algèbre et de l'Arithmétique de l' Université des Antilles et de la Guyane, I.U.F.M., Morne Ferret, BP399, F97159 Pointe-à-Pitre CEDEX

R. Rolland, C.N.R.S. Laboratoire de Mathématiques Discrètes, Luminy Case 930, F13288 Marseille, mél: rolland@lmd.univ-mrs.fr CEDEX 9

et aussi que (cf. [6] lemme 1 ou [3] lemme 1.3) :

Lemme 2 *Si f est un polynôme réduit (i.e. les degrés partiels de f sont tous $\leq q-1$) alors f s'annule sur tout $\mathbb{F}_q^{m+1}$ si et seulement si $f=0$.*

Que dire du problème analogue concernant les polynômes homogènes? Plus précisément soit $\mathcal{J}_d$ le sous espace constitué des polynômes $f \in \mathcal{H}(q, m+1, d)$ tels que $f(x)=0$ pour tout x dans $\mathbb{F}_q^{m+1}$. Notons $\mathcal{J}$ l'idéal homogène :

$$\mathcal{J} = \bigoplus_{d\geq 0} \mathcal{J}_d.$$

Peut-on donner une description simple de cet idéal ?

Remarque — Pour chaque d nous avons $\mathcal{J}_d \subset \mathcal{A}$ et donc $\mathcal{J} \subset \mathcal{A}$.

2 Générateurs de l'ideal $\mathcal{J}$.

Appelons $\mathcal{I}$ l'idéal homogène de $\mathcal{P}(q, m+1)$ engendré par les polynômes $X_i X_j^q - X_i^q X_j$ où $0 \leq i < j \leq m$. Ainsi :

$$\mathcal{I} = \bigoplus_{d\geq 0} \mathcal{I}_d$$

où $\mathcal{I}_d$ est l'espace des polynômes f tels que :

$$f(X_0, X_1, \cdots, X_m) = \sum_{0\leq i<j\leq m} (X_i^q X_j - X_i X_j^q) Q_{i,j}(X_0, X_1, \cdots, X_m)$$

avec :

$$Q_{i,j} \in \mathcal{H}(q, m+1, d-q-1) \ si \ d \geq q+1$$

et :

$$Q_{i,j} = 0 \ si \ d \leq q.$$

Dans [2] le lemme 7.2.4 page 38 énonce l'égalité des idéaux $\mathcal{J}$ et $\mathcal{I}$. Nous donnons ici notre propre démonstration de ce résultat.

Théorème 1 *Pour tout degré $d \geq 0$ nous avons :*

$$\mathcal{J}_d = \mathcal{I}_d.$$

En particulier si $d \leq q$ alors $\mathcal{J}_d = \{0\}$.

Preuve — Chaque élément du corps $\mathbb{F}_q$ vérifie $x^q = x$. Il en découle que $\mathcal{I}_d \subset \mathcal{J}_d$. Il reste à prouver que $\mathcal{J}_d \subset \mathcal{I}_d$. Examinons trois cas.

- Cas $0 \leq d \leq q-1$. Un polynôme de $\mathcal{J}_d$ est alors un polynôme réduit s'annulant sur $\mathbb{F}_q^{m+1}$. D'après le lemme 1.1, il est nul. Donc $\mathcal{J}_d = \{0\}$.
- Cas $d = q$.
- Cas $d \geq q+1$.

Nous renvoyons la démonstration des deux derniers cas après les deux lemmes clés suivants. ■

Le lemme suivant est une amélioration du lemme 1.1.

Lemme 3 *Si f est dans $\mathcal{A}$, nous avons :*

$$f(X_0, X_1, \cdots, X_m) = \sum_{i=0}^{m} Q_i(X_0, X_1, \cdots, X_m)(X_i^q - X_i)$$

où Q_i est un polynôme tel que $deg(Q_i) \leq deg(f) - q$.

Preuve — Soit $f \in \mathcal{P}(q, m+1)$. Chaque monôme de f :

$$aX_0^{\alpha_0} \cdots X_m^{\alpha_m}$$

tel que $\alpha_0 \geq q$ peut être écrit :

$$\begin{aligned} aX_0^{\alpha_0} \cdots X_m^{\alpha_m} &= a(X_0^{\alpha_0} - X_0^{\alpha_0-q+1})X_1^{\alpha_1} \cdots X_m^{\alpha_m} + aX_0^{\alpha_0-q+1}X_1^{\alpha_1} \cdots X_m^{\alpha_m} \\ &= aX_0^{\alpha_0-q}X_1^{\alpha_1} \cdots X_m^{\alpha_m}(X_0^q - X_0) + aX_0^{\alpha_0-q+1}X_1^{\alpha_1} \cdots X_m^{\alpha_m}. \end{aligned}$$

Remarquons que :

$$deg(aX_0^{\alpha_0-q}X_1^{\alpha_1} \cdots X_m^{\alpha_m)} \leq deg(f) - q.$$

Maintenant si $\alpha_0 - q + 1 \geq q$ nous itérons le procédé sur le terme :

$$aX_0^{\alpha_0-q+1}X_1^{\alpha_1} \cdots X_m^{\alpha_m}$$

avec la même variable X_0, et ceci jusqu' à obtenir un exposant de X_0 strictement inférieur à q. De telle sorte que :

$$aX_0^{\alpha_0} \cdots X_m^{\alpha_m} = q_0(X_0, X_1, \cdots, X_m)(X_0^q - X_0) + aX_0^{\beta_0}X_1^{\alpha_1} \cdots X_m^{\alpha_m}$$

avec $\deg(q_0) \leq \deg(f) - q$. Nous recommençons alors avec la variable X_1, en partant du terme :

$$aX_0^{\beta_0}X_1^{\alpha_1} \cdots X_m^{\alpha_m}.$$

Après traitement de toutes les variables nous obtenons en conclusion :

$$aX_0^{\alpha_0}\cdots X_m^{\alpha_m} = \sum_{i=0}^{m} q_i(X_0, X_1, \cdots, X_m)(X_i^q - X_i) + aX_0^{\beta_0}X_1^{\beta_1}\cdots X_m^{\beta_m}$$

où $\deg(q_i) \leq \deg(f) - q$ and $\beta_i \leq q-1$. Par linéarité f peut être écrit :

$$f(X_0, X_1, \cdots, X_m) = \sum_{i=0}^{m} Q_i(X_0, X_1, \cdots, X_m)(X_i^q - X_i) + f^*(X_0, X_1, \cdots, X_m)$$

où $\deg(Q_i) \leq \deg(f) - q$ et où f^* est un polynôme réduit. Si f s'annule sur tout l'espace, il est clair que f^* en fait de même, et d'après le lemme 1.2 $f^* = 0$. ■

Lemme 4 *Supposons $d \geq q+1$. Soit f un élément de $\mathcal{J}_d$ tel que X_m soit en facteur dans f. Alors f est dans $\mathcal{I}_d$.*

Preuve — Calculons dans le corps des fractions de $\mathbb{F}_q(X_0, X_1, .., X_m)$.

$$\begin{aligned} f(X_0, X_1, \cdots, X_m) &= X_m^d f(\frac{X_0}{X_m}, \cdots, \frac{X_{m-1}}{X_m}, 1) \\ &= X_m^d f(Y_0, Y_1, \cdots, Y_{m-1}, 1). \end{aligned}$$

Comme X_m apparaît dans chaque monôme de f, le polynôme à m variables $f(Y_0, Y_1, \cdots, Y_{m-1}, 1)$ est de degré $\leq d-1$. De plus, puisque $f(X_0, X_1, \cdots, X_m)$ s'annule pour tout $x \in \mathbb{F}_q^{m+1}$, le polynôme $f(Y_0, Y_1, \cdots, Y_{m-1}, 1)$ s'annule pour tout $y \in \mathbb{F}_q^m$. D'après le lemme 2.1 :

$$f(Y_0, Y_1, \cdots, Y_{m-1}, 1) = \sum_{i=0}^{m-1} Q_i(Y_0, Y_1, \cdots, Y_{m-1})(Y_i^q - Y_i)$$

où :

$$d_i = deg(Q_i) \leq deg(f(Y_0, Y_1, \cdots, Y_{m-1}, 1)) - q \leq d - 1 - q$$

si bien que :

$$f(X_0, X_1, \cdots, X_m) = X_m^d \sum_{i=0}^{m-1} Q_i(\frac{X_0}{X_m}, \cdots, \frac{X_{m-1}}{X_m}) \left((\frac{X_i}{X_m})^q - \frac{X_i}{X_m} \right)$$

$$= \sum_{i=0}^{m-1} Q_i(\frac{X_0}{X_m}, \cdots, \frac{X_{m-1}}{X_m})(X_i^q X_m^{d-q} - X_i X_m^{d-1}).$$

Mais pour chaque i :

$$Q_i(\frac{X_0}{X_m}, \cdots, \frac{X_{m-1}}{X_m}) = \frac{1}{X_m^{d_i}} L_i(X_0, X_1, \cdots, X_m)$$

où $L_i(X_0, X_1, \cdots, X_m)$ est un polynôme homogène de degré d_i. Donc :

$$f(X_0, X_1, \cdots, X_m) = \sum_{i=0}^{m-1} \frac{1}{X_m^{d_i}} L_i(X_0, X_1, \cdots, X_m) X_m^{d-1-q}(X_i^q X_m - X_i X_m^q)$$

$$= \sum_{i=0}^{m-1} X_m^{d-1-q-d_i} L_i(X_0, X_1, \cdots, X_m)(X_i^q X_m - X_i X_m^q).$$

Mais $d - 1 - q - d_i \geq 0$, donc $f \in \mathcal{I}_d$. ■

Remarque — En fait cette dernière expression obtenue pour f est plus précise que la conclusion du lemme 2.2.

Fin de la démonstration du théorème 2.1: Examinons d'abord le cas $d = q$. Si f est dans $\mathcal{J}_d$, f est aussi dans $\mathcal{A}$. Par le lemme 2.1 nous savons que :

$$f(X_0, X_1, \cdots, X_m) = \sum_{i=0}^{m} A_i(X_i^q - X_i).$$

où les A_i sont des polynômes constants. Il est facile de voir maintenant qu'une telle somme n'est homogène que si les A_i sont nuls. Donc $f = 0$ et $\mathcal{J}_d = \{0\}$.

Traitons maintenant le cas $d \geq q + 1$.
La démonstration est faite par récurrence sur m.

- Si $m = 1$, $f(X_0, X_1)$ est un polynôme homogène à 2 variables et de degré d :

  $$f(X_0, X_1) = a_d X_0^d + \sum_{i=0}^{d-1} a_i X_0^i X_1^{d-i}.$$

  Comme f s'annule sur tout l'espace, $f(1, 0) = 0$ et donc $a_d = 0$.

  Par suite $f(X_0, X_1)$ satisfait aux hypothèses du lemme 2.2. On en déduit le résultat pour $m = 1$.

- Si $m > 1$, supposons le résultat vrai pour tout $1 \leq k < m$. Soit $f(X_0, X_1, \cdots, X_m)$ un polynôme de $\mathcal{J}_d$. Nous pouvons écrire :

  $$f(X_0, X_1, \cdots, X_m) = g(X_0, X_1, \cdots, X_m) + h(X_0, X_1, \cdots, X_{m-1})$$

où :

$$g(X_0, X_1, \cdots, X_m) = \sum_{\substack{\alpha_0+\cdots+\alpha_m=d \\ \alpha_m \neq 0}} a_{\alpha_0 \cdots \alpha_m} X_0^{\alpha_0} \cdots X_m^{\alpha_m}$$

et :

$$h(X_0, X_1, \cdots, X_{m-1}) = \sum_{\alpha_0+\cdots+\alpha_{m-1}=d} a_{\alpha_0 \cdots \alpha_{m-1} 0} X_0^{\alpha_0} \cdots X_{m-1}^{\alpha_{m-1}}.$$

Nous savons que :

$$f(x_0, x_1, \cdots, x_{m-1}, 0) = h(x_0, x_1, \cdots, x_{m-1}) = 0$$

pour tout $(x_0, x_1, \cdots, x_{m-1}) \in \mathbb{F}_q^m$. Par hypothèse de récurrence :

$$h(X_0, \cdots, X_{m-1}) = \sum_{0 \leq i < j \leq m-1} q_{i,j}(X_0, \cdots, X_{m-1})(X_i^q X_j - X_i X_j^q).$$

Comme f et h s'annulent sur tout l'espace, g en fait de même. Si bien que g satisfait aux hypothèses du lemme 2.2. Donc :

$$g(X_0, X_1, \cdots, X_m) = \sum_{i=0}^{m-1} l_i(X_0, X_1, \cdots, X_m)(X_i^q X_m - X_i X_m^q).$$

Les expressions obtenues pour g and h permettent de conclure. ■

Comme conséquence directe du théorème 2.1 nous avons évidemment

Corollaire 1 *L'idéal homogène $\mathcal{J}$ est engendré par les polynômes :*

$$X_i^q X_j - X_i X_j^q.$$

3 Résolution libre de $\mathcal{P}(q, m+1)/\mathcal{I}$.

Soit A la matrice à coefficients dans l'anneau $\mathcal{P}(q, m+1)$ suivante :

$$A = \begin{pmatrix} X_0 & X_1 & \cdots & X_m \\ X_0^q & X_1^q & \cdots & X_m^q \end{pmatrix}.$$

Il est clair que l'idéal $\mathcal{I}$ est l'idéal engendré par les determinants d'ordre 2 extraits de la matrice A.

Calculons tout d'abord la **hauteur** $ht(\mathcal{I})$ de l'idéal $\mathcal{I}$, dont nous aurons besoin par la suite.

Lemme 5 *La hauteur $ht(\mathcal{I})$ de l'idéal $\mathcal{I}$ est m.*

Preuve — Notons $\overline{\mathbb{F}}_q$ la clôture algébrique de $\mathbb{F}_q$. Si on note $V(\mathcal{I})$ la variété algébrique projective de l'espace projectif $\mathbb{F}_q^m(\overline{\mathbb{F}}_q)$ de dimension m sur $\overline{\mathbb{F}}_q$ donnée par l'idéal $\mathcal{I}$, on a :

$$V(\mathcal{I}) = \mathbb{F}_q^m(\mathbb{F}_q).$$

Ainsi cette variété est formée d'un nombre fini de points et on obtient les idéaux premiers minimaux de $\mathcal{I}$ en prenant les idéaux $\mathcal{A}_P = I(\{P\})$ associés aux point $P \in \mathbb{P}^m(\mathbb{F}_q)$. Chacun de ces idéaux a pour hauteur m (pour le voir on peut par exemple se placer dans l'espace affine de dimension $m+1$ et travailler avec la variété conique associée à $V(\mathcal{I})$; dans ce cadre les idéaux $I(\{P\})$ définissent des variétés de dimension 1). Or on sait ([1], page 13, exemple 1.2.2) que $ht(\mathcal{I}) = min(ht(\mathcal{A}_P))$, on en déduit le résultat. ■

Remarque — On rappelle que la **profondeur** d'un idéal A d'un anneau R, notée $gr(A)$ est la longueur p maximale d'une suite $a_1, a_2, \cdots a_p$ d'éléments de A telle que pour tout $1 \leq i \leq p$, a_i ne soit pas un diviseur de zéro dans $R/(a_1, \cdots, a_{i-1})R$.

On sait que dans l'anneau de Cohen-Macaulay $\mathcal{P}(q, m+1)$, la profondeur de tout idéal propre est égale à sa hauteur. Par suite :

$$gr(\mathcal{I}) = m.$$

Suivons alors la démarche de [4] pour déterminer une résolution libre de $\mathcal{I}$.

Soient $Y_0, Y_1, \cdots, Y_m$ des indéterminées et $\mathcal{K}$ la $\mathcal{P}(q, m+1)$-algèbre extérieure construite sur ces indéterminées. L'algèbre $\mathcal{K}$ est graduée :

$$\mathcal{K} = \bigoplus_{d \geq 0} \mathcal{K}_d$$

où $\mathcal{K}_d$ a pour base les produits :

$$Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_d}$$

avec $0 \leq i_1 < i_2 < \cdots < i_d \leq m$.

Nous pouvons alors associer à chacune des deux lignes de la matrice A une dérivation sur $\mathcal{K}$ en posant :

$$\Delta_1(Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_d}) = \sum_{j=1}^{d} (-1)^{j+1} X_{i_j} Y_{i_1} \wedge Y_{i_2} \wedge \cdots \widehat{Y}_{i_j} \cdots \wedge Y_{i_d}$$

et :

$$\Delta_2(Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_d}) = \sum_{j=1}^{d} (-1)^{j+1} X_{i_j}^q Y_{i_1} \wedge Y_{i_2} \wedge \cdots \widehat{Y}_{i_j} \cdots \wedge Y_{i_d}$$

où suivant la convention habituelle le chapeau sur une indéterminée signifie que celle-ci manque dans le produit.

Soit $\mathcal{P}(q, m+1)[Z_1, Z_2]$ l'anneau des polynômes en deux variables et à coefficients dans l'anneau $\mathcal{P}(q, m+1)$. Notons $\mathcal{D}_d$ le $\mathcal{P}(q, m+1)$-module constitué des éléments de $\mathcal{P}(q, m+1)[Z_1, Z_2]$ homogènes de degré d.

On définit alors pour tout $0 \leq j \leq m-1$ le produit tensoriel :

$$\mathcal{N}_{j+1} = \mathcal{K}_{j+2} \otimes \mathcal{D}_j$$

et on pose :

$$\mathcal{N}_0 = \mathcal{P}(q, m+1).$$

On dispose alors pour tout $1 \leq j \leq m$ de la dérivation d_j, homomorphisme de $\mathcal{N}_j$ dans $\mathcal{N}_{j-1}$, définie pour $j > 1$ par :

$$d_j(Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_{j+1}} \otimes Z_1^\alpha Z_2^{j-1-\alpha}) = \Delta_1(Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_{j+1}}) \otimes Z_1^{\alpha-1} Z_2^{j-1-\alpha} +$$

$$\Delta_2(Y_{i_1} \wedge Y_{i_2} \wedge \cdots \wedge Y_{i_{j+1}}) \otimes Z_1^\alpha Z_2^{j-2-\alpha}$$

et pour $j = 1$ par :

$$d_1(Y_{i_1} \wedge Y_{i_2} \otimes 1) = X_{i_1} X_{i_2}^q - X_{i_1}^q X_{i_2}.$$

Nous obtenons alors le théorème suivant :

Théorème 2 *La suite $(\mathcal{N}_j)_{0 \leq j \leq m}$ est une résolution libre de l'idéal $\mathcal{I}$ c'est-à-dire que la suite :*

$$0 \to \mathcal{N}_m \to \mathcal{N}_{m-1} \to \cdots \to \mathcal{N}_1 \to \mathcal{N}_0 \to \mathcal{P}(q, m+1)/\mathcal{I} \to 0$$

est exacte (s est la surjection canonique de $\mathcal{P}(q, m+1)$ sur $\mathcal{P}(q, m+1)/\mathcal{I}$).

Preuve — L'anneau $\mathcal{P}(q, m+1)$ est Noetherien, $\mathcal{I}$ en est un idéal propre défini par une matrice $2 \times (m+1)$ et la profondeur de $\mathcal{I}$ est $(m+1) - 2 + 1 = m$ (cf. la remarque du lemme 3.1). En vertu du théorème 2 de [4] on en déduit le résultat. ■

4 Relations entre les polynômes $X_iX_j^q - X_i^qX_j$.

Il s'agit de déterminer les familles de polynômes :

$$(Q_{i,j}(X_0, X_1, \cdots, X_m))_{0\leq i<j\leq m}$$

telles que :

$$\sum_{0\leq i<j\leq m} Q_{i,j}(X_0, X_1, \cdots, X_m)(X_iX_j^q - X_i^qX_j) = 0.$$

Une telle famille donne une **relation** entre les polynômes $X_iX_j^q - X_i^qX_j$. On notera $\mathcal{R}_1$ l'ensemble de ces familles de polynômes.

Théorème 3 *$\mathcal{R}_1$ est l'idéal de $\bigoplus_{0\leq i<j\leq m}\mathcal{P}(q, m+1)$ engendré par les éléments :*

$$e_{i_1,i_2,i_3} = (Q_{i,j}(X_0, X_1, \cdots, X_m))_{0\leq i<j\leq m}$$

où $0 \leq i_1 < i_2 < i_3 \leq m$ et où :

$$Q_{i_1,i_2}(X_0, X_1, \cdots, X_m) = X_{i_3} \quad Q_{i_1,i_3}(X_0, X_1, \cdots, X_m) = -X_{i_2}$$

$$Q_{i_2,i_3}(X_0, X_1, \cdots, X_m) = X_{i_1} \quad Q_{i,j}(X_0, X_1, \cdots, X_m) = 0 \text{ sinon}$$

et les éléments :

$$f_{i_1,i_2,i_3} = (Q_{i,j}(X_0, X_1, \cdots, X_m))_{0\leq i<j\leq m}$$

où $0 \leq i_1 < i_2 < i_3 \leq m$ et où :

$$Q_{i_1,i_2}(X_0, X_1, \cdots, X_m) = X_{i_3}^q \quad Q_{i_1,i_3}(X_0, X_1, \cdots, X_m) = -X_{i_2}^q$$

$$Q_{i_2,i_3}(X_0, X_1, \cdots, X_m) = X_{i_1}^q \quad Q_{i,j}(X_0, X_1, \cdots, X_m) = 0 \text{ sinon.}$$

Preuve — On peut clairement identifier le $\mathcal{P}(q, m+1)$-module $\mathcal{N}_1$ avec le module $\bigoplus_{0\leq i<j\leq m}\mathcal{P}(q, m+1)$ en identifiant $Y_i \wedge Y_j \otimes 1$ avec l'élément dont toutes les composantes sont nulles sauf celle d'indice (i, j) qui vaut 1.
En revenant à la définition de d_1, on voit que $\mathcal{R}_1 = Ker(d_1)$. Mais on sait que le noyau de d_1 est l'image de d_2. Il suffit alors de calculer l'image par d_2 de la base constituée des éléments $Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3} \otimes Z_1$ et des éléments $Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3} \otimes Z_2$ de $\mathcal{N}_2$ pour avoir un système de générateurs de l'idéal $\mathcal{R}_1$.

$$d_2(Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3} \otimes Z_1) = \Delta_1(Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3}) \otimes 1$$

$$= X_{i_1}Y_{i_2} \wedge Y_{i_3} \otimes 1 - X_{i_2}Y_{i_1} \wedge Y_{i_3} \otimes 1 + X_{i_3}Y_{i_1} \wedge Y_{i_2} \otimes 1$$

et :

$$d_2(Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3} \otimes Z_2) = \Delta_2(Y_{i_1} \wedge Y_{i_2} \wedge Y_{i_3}) \otimes 1$$
$$= X_{i_1}^q Y_{i_2} \wedge Y_{i_3} \otimes 1 - X_{i_2}^q Y_{i_1} \wedge Y_{i_3} \otimes 1 + X_{i_3}^q Y_{i_1} \wedge Y_{i_2} \otimes 1$$

ce qui démontre le résultat. ■

Remarque — Les vecteurs :

$$g_{i_1,i_2,i_3,i_4} = (0, \cdots, 0, X_{i_1}^q X_{i_2} - X_{i_1} X_{i_2}^q, 0, \cdots, 0, X_{i_3} X_{i_4}^q - X_{i_3}^q X_{i_4}, 0, \cdots, 0),$$

où les deux composantes non nulles $X_{i_1}^q X_{i_2} - X_{i_1} X_{i_2}^q$ et $X_{i_3} X_{i_4}^q - X_{i_3}^q X_{i_4}$ sont respectivement aux places d'indices (i_3, i_4) et (i_1, i_2), qui donnent clairement des relations, s'écrivent grâce aux générateurs indiqués sous la forme :

$$g_{1_1,i_2,i_3,i_4} = X_{i_4}^q e_{i_1,i_2,i_3} - X_{i_3}^q e_{i_1,i_2,i_4} + X_{i_2} f_{i_1,i_3,i_4} - X_{i_1} f_{i_2,i_3,i_4}.$$

5 Les dimensions.

5.1 Fonctions associées à des polynômes homogènes.

Suivons [7] pour associer à tout polynôme homogène une fonction définie sur l'espace projectif $\mathbb{P}^m(q)$.

Notons $\mathcal{F}(q, m)$ l'espace des fonctions definies sur $\mathbb{P}^m(q)$ à valeurs dans $\mathbb{F}_q$.

Si $x = (x_0 : x_1 : ... : x_m) \in \mathbb{F}_q^m(q)$, soit :

$$k(x) = \max\{j | x_j \neq 0\}.$$

Définissons l'application T_d de $\mathcal{H}(q, m+1, d)$ dans $\mathcal{F}(q, m)$ par :

$$T_d(f)(x_0 : \cdots : x_{k(x)} : 0 : \cdots : 0) = (\frac{1}{x_{k(x)}})^d f(x_0, \cdots, x_{k(x)}, 0, \cdots, 0).$$

T_d est une application linéaire et :

$$Ker(T_d) = \mathcal{J}_d.$$

Notons $C(q, m, d)$ le code de Reed Muller projectif d'ordre d sur $\mathbb{F}_q$, de longueur $q^m + q^{m-1} + \cdots + q + 1$ (cf. [7]) :

$$C(q, m, d) = T_d(\mathcal{H}(q, m+1, d))$$

si bien que :

$$dim(Ker(T_d)) = dim(\mathcal{H}(q, m+1, d)) - dim(C(q, m, d))$$

La dimension de l'espace $\mathcal{H}(q, m+1, d)$ est (cf. [7]) :

$$dim(\mathcal{H}(q, m+1, d)) = \left(\begin{array}{c} m+d \\ d \end{array} \right)$$

et la dimension de $C(q, m, d)$ est (cf. [8]) :

$$dim(C(q,m,d)) = \sum_{\substack{t=d \ mod \ q-1 \\ 0<t\leq d}} \left(\sum_{j=0}^{m+1} (-1)^j \left(\begin{array}{c} m+1 \\ j \end{array} \right) \left(\begin{array}{c} t-jq+m \\ t-jq \end{array} \right) \right)$$

où le coefficient binômial $\left(\begin{array}{c} t-jq+m \\ t-jq \end{array} \right)$ est zero si $t-jq<0$. En conclusion nous avons :

Théorème 4 *La dimension de l'espace $\mathcal{J}_d$ est donnée par :*

$$dim(\mathcal{J}_d) = \left(\begin{array}{c} m+d \\ d \end{array} \right) - \sum_{\substack{t=d \ mod \ q-1 \\ 0<t\leq d}} \left(\sum_{j=0}^{m+1} (-1)^j \left(\begin{array}{c} m+1 \\ j \end{array} \right) \left(\begin{array}{c} t-jq+m \\ t-jq \end{array} \right) \right).$$

Remarque — L'application qui à d fait correspondre $dim(C(q, m, d)$ (dimension de la composante homogène de degré d du quotient $\mathcal{P}(q, m+1)/\mathcal{J}$) est la fonction de Hilbert de la variété $\mathbb{F}_q^m(q)$.

Remarque — Calculons la dimension de $\mathcal{J}_d$ dans quelques cas particuliers.

- si $d \leq q$ on sait d'après le théorème 2.1 que :

$$dim(\mathcal{J}_d) = 0$$

- Si $d = q+1$ on peut calculer la dimension en utilisant le théorème 5.1 (qui n'utilise pas le fait que $\mathcal{J} = \mathcal{I}$) ou en remarquant que les polynômes $X_i^q X_j - X_i X_j^q$ (avec $0 \leq i < j \leq m$) sont indépendants, si bien que :

$$dim(\mathcal{J}_d) = \frac{m(m+1)}{2}$$

- Si $d \geq m(q-1)+1$, on sait que (cf. [8]) $C(q, m, d)$ l'espace $\mathcal{F}(q, m)$ tout entier, dont la dimension est $p_m = q^m + q^{m-1} + \cdots + q + 1$. Donc :

$$dim(\mathcal{J}_d) = \left(\begin{array}{c} m+d \\ d \end{array} \right) - (q^m + q^{m-1} + \cdots + q + 1)$$

5.2 Calcul de la dimension utilisant la résolution libre.

Théorème 5 *La dimension de l'espace $\mathcal{I}_d$ (composante homogène de degré d de l'idéal homogène engendré par les polynômes $X_iX_j^q - X_i^qX_j$) est :*

$$dim(\mathcal{I}_d) = \sum_{j=2}^{m+1}(-1)^j \begin{pmatrix} m+1 \\ j \end{pmatrix} \sum_{\alpha=0}^{j-2} \begin{pmatrix} d+(\alpha+1)(q-1)-jq+m \\ d+(\alpha+1)(q-1)-jq \end{pmatrix}.$$

Preuve — Remarquons que nous pouvons écrire :

$$\mathcal{N}_{j-1} = \bigoplus_{\substack{0\le i_1<\cdots<i_j\le m \\ 0\le\alpha\le j-2}} \mathcal{P}(q, m+1)$$

en identifiant, par une démarche analogue à celle déjà faite au paragraphe 3, l'élément de base $Y_{i_1} \wedge \cdots \wedge Y_{i_j} \otimes Z_1^{\alpha} Z_2^{j-2-\alpha}$ de $\mathcal{N}_{j-1}$ avec l'élément de $\bigoplus_{\substack{0\le i_1<\cdots<i_j\le m \\ 0\le\alpha\le j-2}} \mathcal{P}(q, m+1)$ dont toutes les composantes sont nulles sauf celle d'indice $(i_1, i_2, \cdots, i_j, \alpha)$ qui vaut 1.
Posons :

$$(\mathcal{N}_0)_d = \mathcal{H}(q, m+1, d),$$

et pour $j \ge 2$:

$$(\mathcal{N}_{j-1})_d = \bigoplus_{\substack{0\le i_1<\cdots<i_j\le m \\ 0\le\alpha\le j-2}} \mathcal{H}(q, m+1, d-(q+1)-\alpha-q(j-2-\alpha)).$$

Il est aisé de vérifier que la restriction de d_j à $(\mathcal{N}_j)_d$ a son image dans $(\mathcal{N}_{j-1})_d$ et que la suite :

$$0 \to (\mathcal{N}_m)_d \to (\mathcal{N}_{m-1})_d \to \cdots \to (\mathcal{N}_1)_d \to (\mathcal{N}_0)_d \to \mathcal{H}(q, m+1, d)/\mathcal{I}_d \to 0$$

est exacte. Donc :

$$dim(\mathcal{I}_d) = dim(Ker(s)) = dim(Im(d_1)).$$

En tenant compte du fait que :

$$dim(Im(d_k)) = dim\left((\mathcal{N}_k)_d\right) - dim(Ker(d_k))$$

et que :

$$dim(Ker(d_k)) = dim(Im(d_{k+1}))$$

on établit la formule :

$$dim(\mathcal{I}_d) = \sum_{j=2}^{m+1}(-1)^j dim\left((\mathcal{N}_{j-1})_d\right)$$

qui compte tenu de la définition de $(\mathcal{N}_{j-1})_d$ et de la formule :

$$dim(\mathcal{H}(q, m+1, k)) = \left(\begin{array}{c} m+k \\ k \end{array} \right)$$

donne le résultat attendu. ■

Remarque — Puisqu'on sait que l'idéal $\mathcal{I}$ coïncide avec l'idéal $\mathcal{J}$ on obtient l'égalité combinatoire :

$$\sum_{j=2}^{m+1} (-1)^j \left(\begin{array}{c} m+1 \\ j \end{array} \right) \sum_{\alpha=0}^{j-2} \left(\begin{array}{c} d+(\alpha+1)(q-1)-jq+m \\ d+(\alpha+1)(q-1)-jq \end{array} \right)$$

$$= \left(\begin{array}{c} m+d \\ d \end{array} \right) - \sum_{\substack{t=d \ mod \ q-1 \\ 0<t\leq d}} \left(\sum_{j=0}^{m+1} (-1)^j \left(\begin{array}{c} m+1 \\ j \end{array} \right) \left(\begin{array}{c} t-jq+m \\ t-jq \end{array} \right) \right)$$

En fait les deux formules donnant $dim(\mathcal{I}_d)$ et $dim(\mathcal{J}_d)$ ont été obtenues indépendamment du fait que $\mathcal{I} = \mathcal{J}$, si bien que si l'on démontre directement l'égalité combinatoire précédente, puiqu'on sait par ailleurs de façon simple que $\mathcal{I} \subset \mathcal{J}$, on obtient une autre démonstration du théorème 2.1.

Exemple — Donnons quelques valeurs numériques pour la dimension commune $dim(\mathcal{I}_d) = dim(\mathcal{J}_d)$

$q=3 \quad m=2 \quad d=\ 4 \quad dim=\ \ 3$
$q=3 \quad m=2 \quad d=\ 7 \quad dim=\ 23$
$q=3 \quad m=2 \quad d=\ 9 \quad dim=\ 42$
$q=3 \quad m=2 \quad d=10 \quad dim=\ 53$

$q=3 \quad m=5 \quad d=\ 4 \quad dim=\ 15$
$q=3 \quad m=5 \quad d=\ 7 \quad dim=\ 484$
$q=3 \quad m=5 \quad d=\ 9 \quad dim=1644$
$q=3 \quad m=5 \quad d=10 \quad dim=2640$

$q=4 \quad m=2 \quad d=\ 4 \quad dim=\ \ 0$
$q=4 \quad m=2 \quad d=\ 7 \quad dim=\ 15$
$q=4 \quad m=2 \quad d=\ 9 \quad dim=\ 34$
$q=4 \quad m=2 \quad d=10 \quad dim=\ 45$

$q=4 \quad m=5 \quad d=\ 4 \quad dim=\ \ 0$
$q=4 \quad m=5 \quad d=\ 7 \quad dim=\ 210$
$q=4 \quad m=5 \quad d=\ 9 \quad dim=1030$
$q=4 \quad m=5 \quad d=10 \quad dim=1875$

References

[1] Balcerzyk S. & Józefiak T., Commutative Rings, Ellis Horwood Series in Mathematics and its Applications, 1989.

[2] Bayer-Fluckiger E. & Serre J-P., Torsions quadratiques et bases normales autoduales, Amer. J. Math. 116, pp1-64, 1994.

[3] Delsarte P., Goethals J.M. & Mac Williams F.J., On Generalized Reed-Muller Codes and their Relatives, Inform. and Control 16, pp403-442, 1970.

[4] Eagon J.A. & Northcott D.G., Ideals defined by matrices and a certain complex associated with them, Proc. Roy. Soc. London Ser. A 269, pp188-204, 1962.

[5] Harris J., Algebraic Geometry. A First Course, Springer GTM 133, 1992.

[6] Joly J.R., Equations et variétés algébriques sur un corps fini, Enseignement Math. 19, pp1-117, 1973.

[7] Lachaud G., The parameters of Projective Reed-Muller Codes, Discrete Math. 81 pp217-221, 1990.

[8] Sørensen A.B., Projective Reed-Muller Codes, IEEE Trans. Inform. Theory 37, 1991.