Codes 1-translatés d'un code de Reed et Muller généralisé

1-translated codes of a generalized Reed and Muller code

Pascale CHARPIN

Informatique Théorique, Institut de Programmation et LITP
Université Paris-VI, 4, place Jussieu, 75005 PARIS

Enseignante en Informatique à l'Institut de Programmation (Université Paris-VI) et chercheur au Laboratoire d'Informatique Théorique et Programmation. Réalise actuellement une thèse de Doctorat d'État sur l'interprétation algébrique des codes de longueur p^m dans une algèbre modulaire.

RÉSUMÉ

Un translaté d'un code de Reed et Muller généralisé (GRM-code) qui est compris entre deux GRM-codes successifs est dit 1-translaté. Les GRM-codes sont ici considérés comme les puissances du radical d'une algèbre modulaire A. La stabilité des codes 1-translatés sous certains automorphismes de l'algèbre A spécifie les propriétés algébriques de ces codes.

MOTS CLÉS

Codes de Reed et Muller, code translaté, code cyclique, code autodual, code idéal.

SUMMARY

A coset of a generalized Reed and Muller code (GRM-*code*) *which is between two successive* GRM-*codes is called* 1-*translated. The* GRM-*codes are here characterized as the powers of an* A-*modular-algebra radical. The steadiness of the* 1-*translated codes over some* A *algebra automorphisms points their algebraic properties.*

KEY WORDS

Reed and Muller codes, translated code, cyclic code, self-dual code, ideal code.

TABLE DES MATIÈRES

Introduction

Une étude détaillée des codes de Reed et Muller binaires (RM-codes) se trouve dans l'ouvrage de F. J. MacWilliams et N. J. A. Sloane ([15], chap. 13 à 15). Les codes de Reed et Muller généralisés (GRM-codes) sont décrits par T. Kasami, S. Lin et W. W. Peterson [14] et par P. Delsarte [10, 11]. *Il s'agit de codes linéaires de longueur* p^m (p est un nombre premier) *définis sur un corps* K *de caractéristique* p ($K=F_q$, $q=p^m$). De tels codes sont habituellement considérés comme des K-espaces vectoriels: en fait, ils sont aussi sous-ensembles d'une algèbre modulaire de p-groupe abélien élémentaire G ($G\simeq(F_{p^m}, +)$) que nous notons A :

$$(1) \qquad A=\{x=\sum_{g\in G} x_g X^g \,|\, x_g\in K\}.$$

Les GRM-codes sont une suite décroissante d'idéaux de l'algèbre A et ceci à partir du seul idéal maximal de A jusqu'au seul idéal minimal de A; ils sont aussi des codes cycliques étendus et dans ce contexte, on peut considérer que les codes de Reed-Solomon étendus sont un cas particulier de GRM-codes [6, 10]. L'intérêt que suscitent les GRM-codes tient à ces propriétés à la fois algébriques et arithmétiques, qui sont impliquées dans l'étude ou la construction de nombreux autres codes. Par ailleurs, des problèmes importants, telle la distribution des poids des GRM-codes, ne sont pas résolus.

Nous notons P *le radical de l'algèbre* A (seul idéal maximal de A [2]) qui est aussi l'ensemble des éléments nilpotents; en effet un élément de A est soit nilpotent soit inversible car :

$$(2) \qquad (\sum_{g\in G} x_g X^g)^p=\sum_{g\in G} x_g^p X^{pg}=(\sum_{g\in G} x_g)^p.$$

Soit P^j la puissance j-ième du radical P, c'est-à-dire l'idéal engendré par l'ensemble :

$$(3) \qquad \left\{\prod_{k=1}^{j} x_k \,|\, x_k\in P\right\}.$$

La description des codes P^j est due d'abord à A. Poli [16, 17] et poursuivie dans [6, 7, 8].

Rappelons certaines propriétés de ces idéaux :

$$(4) \qquad \begin{aligned} &- \{P^j \,|\, j\geqq 1\} \text{ est une suite décroissante;}\\ &P^{M+1}=\{0\} \quad \text{où} \quad M=m(p-1);\\ &- (P^j)^{\perp}=\operatorname{Ann} P^j;\\ &- \operatorname{Ann} P^j=P^{M-j+1} \end{aligned}$$

(où $M+1$ est l'index de nilpotence de P).

Les puissances du radical de A *sont les GRM-codes* [7]. Nous dirons que P^j *est le GRM-code de degré* j (ceci correspond à l'appellation « GRM-code d'ordre $M-j$ »).

L'importance des translatés des RM-codes apparaît clairement dans [15]; citons, à titre d'exemple, la construction des codes de Kerdock et de Preparata et le calcul du polynôme des poids du RM-code d'ordre 2. Dans ces deux cas, les translatés utilisés sont du type :

$$(5) \qquad x+P^j, \qquad x=0 \qquad \text{ou} \qquad x\in P^{j-1}\setminus P^j.$$

Nous appelons *code* 1-*translaté* un code qui est une réunion de translatés du type (5). Nous étudions (§ 1) le comportement d'un code 1-translaté sous deux transformations isométriques de l'algèbre; avec les résultats obtenus (th. 1) nous montrons (§ 2) qu'un code 1-translaté linéaire est un idéal de l'algèbre A. La classe de codes ainsi obtenue a des propriétés similaires à celles des GRM-codes (il s'agit des propriétés données par (4)).

Nous précisons ceci au paragraphe 3; nous voulons mettre en évidence qu'il s'agit là d'une sorte de généralisation des GRM-codes: avec une base de l'algèbre (considérée comme K-espace vectoriel) nous construisons un ensemble d'idéaux vérifiant (4) de telle façon que chaque dimension est atteinte. Pour illustrer ce propos nous étudions d'abord les codes 1-translatés autoduaux; nous exhibons un code autodual $(2^m, 2^{m-1}, 2^{m/2})$ ceci lorsque m est pair. Nous considérons ensuite les codes 1-translatés qui sont l'extension d'un code cyclique (§ 4); là aussi le caractère cyclique s'exprime d'un GRM-code à son suivant et le passage à l'annulateur se fait de la même façon que pour un GRM-code.

1. Définitions et propriétés générales

Pour représenter les éléments de l'algèbre, nous utilisons des bases du K-espace A qui contiennent une base de chaque P^j.

Ces bases sont obtenues par automorphisme de l'algèbre A, à partir de celles-ci :

$$(6)\quad B(e)=\left\{\prod_{k=1}^{m}(X^{e_k}-1)^{i_k}\,\middle|\,(i_1,\ldots,i_m)\in[0,p-1]^m\right\},$$

$$(7)\quad B_j(e)=\left\{\prod_{k=1}^{m}(X^{e_k}-1)^{i_k}\in B(e)\,\middle|\,\sum_{k=1}^{m}i_k\geqq j\right\}.$$

On désigne par e une base $\{e_1\ldots e_m\}$ du F_p-espace vectoriel G; $B(e)$ *est une base de* A et pour chaque j, $j\in[1, M]$, $B_j(e)$ *est une base de* P^j considéré comme K-sous-espace de A. Ainsi un élément x, s'il est dans $P^{j-1}\setminus P^j$, s'écrit x_1+x_2 où $x_2\in P^j$ et x_1 est une combinaison K-linéaire d'éléments de $B_{j-1}(e)\setminus B_j(e)$.

Cette représentation est particulièrement intéressante lorsque nous étudions un translaté de P^j dans P^{j-1}.

Définition 1: Soit $j\in[1, M]$. Un code C de A est dit *code 1-translaté du GRM-code de degré j* s'il est de la forme:

$$(8)\quad C=\bigcup_{x\in L}(x+P^j)\qquad \text{où}\quad L\subset(P^{j-1}\setminus P^j)\cup\{0\}.$$

Par convention, un code 1-translaté n'est pas un des GRM-codes et $P^0=A$.

Remarques: 1° Un code C, défini par (8), est contenu dans P^{j-1} mais ne contient pas forcément P^j. Si C est linéaire alors il contient P^j.

2° Sous son aspect le plus simple, le code C est un translaté particulier du code P^j:

$$(9)\qquad C=x+P^j\qquad \text{où}\quad x\in P^{j-1}\setminus P^j.$$

Exemples: C'est essentiellement dans le cas binaire ($K=F_2$) que l'on trouve des exemples d'utilisation ou d'existence.

1° L'étude des codes 1-translatés du type (9) du RM-code de degré $m-1$ (ou d'ordre 1) aboutit au calcul du polynôme énumérateur de poids du RM-code de degré $m-2$ ([15], chap. 15).

2° Les codes de Preparata sont des codes 1-translatés du RM-code de degré 3 [4, 12, 15].

3° B. K. Dass et S. K. Mutto présentent dans [9] « une généralisation binaire des RM-code », utilisant la base sur F_2 qui décrit usuellement ces codes (*cf.* [18] ou [15]). Dans les paragraphes 3 et 4 nous donnons une description plus générale ($K=F_{p^r}$) et l'utilisation de la structure algébrique permet de répondre aux questions posées sur la dualité des codes obtenus.

Une isométrie est une bijection K-linéaire de A dans A qui conserve la distance de Hamming. Nous nous intéressons maintenant aux isométries de A qui nous permettent, dans les paragraphes suivants, de doter un code 1-translaté linéaire d'une autre structure algébrique et d'un dual.

Définition 2: Soit $h\in G$. Nous appelons *h-translation* l'isométrie de A:

$$(10)\qquad \sigma_h:\ \sum_{g\in G}x_gX^g\rightsquigarrow\sum_{g\in G}x_gX^{g+h}.$$

Remarques: Pour justifier la définition, il est clair que σ_h est K-linéaire; d'autre part σ_h conserve les poids de Hamming:

$$w(x)=w(\sigma_h(x))=|\{g\in G\,|\,x_g\neq 0\}|.$$

Un sous-espace de A est un idéal de l'algèbre A si et seulement si il est invariant sous chaque *h*-translation; en effet la multiplication dans A s'écrit:

$$xy=\sum_{g\in G}x_gX^g\sum_{h\in G}y_hX^h=\sum_{h\in G}y_h\sum_{g\in G}x_gX^{g+h}.$$

Soit $j\in[1, M]$ et T un code 1-translaté défini par (9). Nous étudions l'action de σ_h sur T:

$$\sigma_h(T)=\sigma_h(x+P^j)=\sigma_h(x)+P^j$$

(P^j étant un idéal de A est invariant sous σ_h):

$$\sigma_h(x)=X^hx=(X^h-1)x+x,$$

où $x\in P^{j-1}\setminus P^j$ et $(X^h-1)\in P$.

Donc: $x(X^h-1)\in P^j$ [*cf.* (3)].

Finalement: $\sigma_h(T)=x+P^j$. On peut énoncer:

Lemme 1: *Soit* T, *un translaté du GRM-code de degré j tel que:*

$$T=x+P^j\qquad avec\quad x\in P^{j-1}\setminus P^j,$$

alors T *est invariant sous chaque h-translation de* A.

Définition 3: 1° Soit $x\in A$ avec $x=\sum_{g\in G}x_gX^g$.

L'opposé de x, noté $\tilde{x}$, est l'élément de A:

$$(11)\qquad \tilde{x}=\sum_{g\in G}x_{-g}X^g.$$

2° Soit I un sous-ensemble de A.

L'opposé de I, *noté* $\tilde{I}$, est le sous-ensemble de A:

$$(12)\qquad \tilde{I}=\{\tilde{x}\,|\,x\in I\}.$$

Soit l'application $\gamma: x\rightsquigarrow\tilde{x}$. Il s'agit là d'une isométrie de A; mais γ est aussi un automorphisme de l'algèbre A car:

$$\tilde{x}=\sum_{g\in G}x_{-g}X^g=\sum_{h\in G}x_hX^{-h}=\sum_{g\in G}x_gX^{\Gamma(g)},$$

où Γ appartient au groupe linéaire $GL(F_p, m)$.

Or on peut identifier le groupe $GL(F_p, m)$ avec l'ensemble des automorphismes isométriques de A [6, 16]. D'où :

Proposition 1 : *L'application* $\gamma : x \rightsquigarrow \tilde{x}$ *est un automorphisme isométrique de l'algèbre* A.

Soit I un idéal de A et soit $I^\perp$ son complémentaire orthogonal lorsque I est pris comme K-espace vectoriel. Nous notons Ann I *l'idéal annulateur de* I :

$$\text{Ann I} = \{ x \in A \mid y \in I, xy = 0 \}. \tag{13}$$

C'est l'application γ qui lie annulateur et complémentaire orthogonal d'un idéal de A :

Proposition 2 : *Soit* I *un idéal de l'algèbre* A, *alors :*

$$\text{Ann I} = (\tilde{I}^\perp) = (\tilde{I})^\perp.$$

C'est dire qu'il existe un automorphisme isométrique de A (*l'application* γ *définie par la proposition* 1) *qui transforme* $I^\perp$ *en* Ann I.

Preuve : Il faut montrer :

$$x \in \text{Ann I} \Leftrightarrow \tilde{x} \in I^\perp. \tag{I}$$

Soit $x \in \text{Ann I}$ et $y \in I$. Le point xy est nul, c'est-à-dire :

$$xy = \sum_{h \in G} \sum_{g \in G} x_g y_h X^{g+h} = \sum_{u \in G} \Big(\sum_{g \in G} x_g y_{u-g} \Big) X^u = 0.$$

On en déduit les équivalences :

$$\forall y, \quad xy = 0 \Leftrightarrow \forall y, \ \forall u, \quad \sum_{g \in G} x_g y_{u-g} = 0,$$

$$\Leftrightarrow \forall y, \ \forall u, \quad \sum_{h \in G} x_{-h} y_{u+h} = 0,$$

$$\Leftrightarrow \forall y, \ \forall u, \quad \langle \tilde{x}, X^u y \rangle = 0.$$

Ceci prouve (I) car si xy est nul alors en particulier le produit scalaire $\langle \tilde{x}, y \rangle$ est nul; inversement si $y \in I$, chaque élément $X^u y$ est dans I car I est un idéal; dès que $\tilde{x} \in I^\perp$, la condition ci-dessus à droite est vérifiée.

Enfin l'égalité $(\tilde{I}^\perp) = (\tilde{I})^\perp$ se déduit de l'écriture du produit scalaire :

$$\langle x, \tilde{y} \rangle = \sum_{g \in G} x_g y_{-g} = \sum_{h \in G} x_{-h} y_h,$$

d'où il vient,

$$x \in (\tilde{I})^\perp \Leftrightarrow \tilde{x} \in I^\perp \Leftrightarrow x \in (\tilde{I}^\perp).$$

Remarques : 1° Lorsqu'il s'agit de corps de caractéristique 2, un élément de l'algèbre est confondu avec son opposé car : $g \in F_{2^m} \Rightarrow g = -g$; dans ce cas on peut parler indifféremment, pour un idéal I, de son annulateur ou de son complémentaire orthogonal.

2° Plus généralement un idéal de A, invariant sous l'application $\gamma : x \to \tilde{x}$, est tel que son annulateur est égal à son complémentaire orthogonal. C'est le cas pour les GRM-codes, comme nous l'avons rappelé dans le paragraphe 1.

3° Soit a un élément de la base $B(e)$ donnée par (6). Étudions l'action de γ sur a :

$$\tilde{a} = \widetilde{\prod_{k=1}^{m} (X^{e_k} - 1)^{i_k}} = \prod_{k=1}^{m} (X^{-e_k} - 1)^{i_k},$$

$$\tilde{a} = \prod_{k=1}^{m} [-X^{-e_k} (X^{e_k} - 1)]^{i_k}.$$

Nous obtenons, avec :

$$i = \sum_{k=1}^{m} i_k \quad \text{et} \quad g = -\sum_{k=1}^{m} i_k e_k,$$

$$\tilde{a} = (-1)^i X^g a = (-1)^i [a + (x^g - 1) a]. \tag{14}$$

On en déduit :

$$\tilde{a} = (-1)^i a + a' \quad \text{où} \quad a' \in P^{i+1}. \tag{15}$$

Considérons maintenant un code T, 1-translaté du GRM-code P^j et donné par (9). Le code T peut s'écrire $x + P^j$ où x est une combinaison K-linéaire d'éléments de $B_{j-1}(e) \setminus B_j(e)$. Pour calculer $\tilde{T}$ nous utilisons (14) et (15) :

$$\gamma(T) = \gamma(x) + P^j = \tilde{x} P^j \quad [\text{car } \gamma(P^j) = P^j]$$
$$= (-1)^{j-1} x + x' + P^j,$$

où $x' \in P^j$ d'après (15).

Finalement :

Lemme 2 : *Soit* T, *un translaté du GRM code de degré* j *tel que :*

$$T = x + P^j \quad \textit{avec} \quad x \in P^{j-1} \setminus P^j,$$

alors :

$$\tilde{T} = (-1)^{j-1} T. \tag{16}$$

Remarque : Lorsque p vaut 2 ou lorsque j est impair nous avons d'après le lemme 2 : $T = \tilde{T}$. Dans tous les cas, on a l'équivalence :

$$\forall y, \quad y \in T, \ \langle x, y \rangle = 0 \Leftrightarrow \forall y, \quad y \in T, \ xy = 0.$$

Les résultats énoncés dans les lemmes 1 et 2 portent sur des translatés particuliers d'un GRM-code. Un code 1-translaté est par définition une réunion de tels codes; soit C un code 1-translaté du GRM-code P^j; nous avons :

$$C = \bigcup_{x \in L} (x + P^j), \ x = 0 \quad \text{ou} \quad x \in P^{j-1} \setminus P^j,$$

d'où :

$$\tilde{C} = \widetilde{\bigcup_{x \in L} (x + P^j)} = \bigcup_{x \in L} [(-1)^{j-1} (x + P^j)] = (-1)^{j-1} C,$$

$$\sigma_h(C) = \bigcup_{x \in L} \sigma_h(x + P^j) = \bigcup_{x \in L} (x + P^j)$$

(en appliquant successivement les lemmes 1 et 2).

Théorème 1 : *Soit* $j \in [1, M]$. *Soit* C *un code* 1-*translaté du GRM-code de degré* j. *Alors :*

(I) *Toute h-translation laisse* C *invariant :*

$$h \in G, \qquad \sigma_h(C) = C.$$

(II) *L'opposé de* C *est* C *ou* $-C$ *selon que* j *est impair ou non :*

$$\tilde{C} = (-1)^{j-1} C.$$

2. Idéaux 1-translatés d'un GRM-code

Soit $j \in [1, M]$ et soit I un code 1-translaté de P^j qui est linéaire. Le code I est donc compris entre deux GRM-codes consécutifs; en effet :

$$x + P^j \subset I \quad \Rightarrow \quad (x - x) + P^j \subset I.$$

Donc :

$$I \text{ linéaire} \quad \Rightarrow \quad P^j \subset I \subset P^{j-1}.$$

Nous avons remarqué, après la définition 2, que I est un idéal de A si et seulement si il est invariant par toute h-translation.

D'après le théorème 1, *le code* I *est donc un idéal de l'algèbre* A.

Toujours d'après le théorème 1 et du fait que I est linéaire, nous avons : $\tilde{I} = I$. Ceci entraîne (prop. 2) : $\mathrm{Ann}\, I = I^{\perp}$.

Enfin le code $I^{\perp}$ possède les mêmes caractéristiques que I :

$$P^j \subset I \subset P^{j-1}$$

$$\Rightarrow \quad \mathrm{Ann}\, P^{j-1} \subset \mathrm{Ann}\, I \subset \mathrm{Ann}\, P^j$$

$$\Rightarrow \quad P^{M-j+2} \subset \mathrm{Ann}\, I \subset P^{M-j+1}$$

(*voir* les propriétés de P^j, § 1).

Théorème 2 : *Soit* I *un code* 1-*translaté du GRM-code de degré* j. Si I est un code linéaire *alors* I *a les propriétés suivantes :*

(I) $P^j \subset I \subset P^{j-1}$.

(II) *Le code* I *est un idéal de l'algèbre* A.

(III) $\mathrm{Ann}\, I = I^{\perp}$.

(IIII) *Le code* $\mathrm{Ann}\, I$ (*ou* $I^{\perp}$) *est un code* 1-*translaté du GRM-code de degré* $M - j + 2$.

Un code 1-translaté linéaire est appelé *idéal* 1-*translaté.*

Le théorème 2 généralise certaines propriétés des GRM-codes; il met en évidence que pour toute dimension λ ($1 \leqq \lambda \leqq p^m$) on peut déterminer un idéal de A ayant les propriétés du théorème, les GRM-codes en étant alors un cas particulier.

Dans les paragraphes 4 et 5 nous montrons qu'un idéal 1-translaté (donc, par convention, différent d'un GRM-code) peut être autodual et peut être l'extension d'un code cyclique.

3. Idéaux 1-translatés autoduaux

Nous présentons d'abord une construction générale d'idéaux 1-translatés qui nous permettra d'exhiber des codes autoduaux. Nous utilisons maintenant « une extension » des bases définies par (6) et (7), ceci en utilisant les automorphismes de l'algèbre A [16] : aux éléments simples du type $X^{e_i} - 1$ on substitue m éléments de $P \setminus P^2$ tels que la correspondance est bijective. La preuve détaillée de la proposition suivante est dans [6] :

proposition 3 :

$$a = \{a_1, \ldots, a_m\} \qquad \text{où} \quad a_i \in P \setminus P^2,$$

$$B(a) = \left\{ \prod_{k=1}^{m} a_k^{i_k} \,\middle|\, i_k \in [0, p-1] \right\}, \tag{17}$$

$$B_j(a) = \left\{ \prod_{k=1}^{m} x_k^{i_k} \in B(a) \,\middle|\, \sum_{k=1}^{m} i_k \geqq j \right\}, \tag{18}$$

alors l'ensemble $B(a)$ *est une base du* K-*espace vectoriel* A *et chaque ensemble* $B_j(a)$ *est une base du sous-espace* P^j *si et seulement si le produit* $\prod_{i=1}^{m} a_i^{p-1}$ *est non nul.*

Soit $j \in [1, M]$.

Soit $s \in [1, \dim P^{j-1} - \dim P^j[$.

Chaque choix de s éléments dans $B_{j-1}(a) \setminus B_j(a)$ détermine un code 1-translaté que nous notons $I_{j,s}$. Il s'agit d'un sous-espace engendré par une base du type suivant :

$$E = B_j(a) \cup B_s \qquad \text{où} \quad B_s \subset B_{j-1}(a) \setminus B_j(a). \tag{19}$$

Le code $I_{j,s}$ est par définition linéaire. Il est donc un idéal (th. 2). *Nous notons* $J(a)$ *l'ensemble des idéaux de* A *du type* $I_{j,s}$, le m-uple a vérifiant l'hypothèse du théorème 2.

Étant donné un élément x de $B(a)$, il existe un unique élément $\bar{x}$ de $B(a)$ tel que :

$$x\bar{x} = \prod_{i=1}^{m} a_i^{p-1}.$$

La formulation de $\bar{x}$ est :

$$x = \prod_{k=1}^{m} a_k^{i_k} \quad \Leftrightarrow \quad \bar{x} = \prod_{k=1}^{m} a_k^{p-1-i_k}. \tag{20}$$

Proposition 4: *Soit* $I_{j,s} \in J(a)$. *La base qui définit* $I_{j,s}$ *est donnée par* (19); *alors, l'annulateur de* $I_{j,s}$ *est caractérisé par:*

1° $\text{Ann } I_{j,s} \in J(a)$.

2° $\text{Ann } I_{j,s}$ *est du type* $I_{k,t}$ *où :*

$$k = M - j + 2,$$
$$t + s = \dim P^{M-j+1} - \dim P^{M-j+2}.$$

3° *La base qui définit* $I_{k,t}$ *est :*

$$E' = B_{k-1}(a) \setminus \{\bar{x} \mid x \in B_s\}.$$

Preuve: Soit $X = \text{Ann } I_{j,s}$. D'après le théorème 2, nous avons:

$$P^{M-j+2} \subset X \subset P^{M-j+1}.$$

D'autre part:

$$\dim I_{j,s} + \dim X = p^m.$$

Donc:

$$\begin{aligned}\dim X &= p^m - \dim I_{j,s} \\ &= p^m - (\dim P^j + s) \\ &= (p^m - \dim P^j) - s \\ &= \dim P^{M-j+1} - s.\end{aligned}$$

Soit t l'entier positif tel que la dimension de X est la dimension de P^{M-j+2} augmentée de t. Alors:

$$t + \dim P^{M-j+2} = \dim P^{M-j+1} - s.$$

Pour achever la démonstration, il reste à déterminer t vecteurs de l'ensemble $B_{k-1}(a) \setminus B_k(a)$ qui annulent X ($k = M - j + 2$).

Soit $x \in B_s$; x s'écrit:

$$x = \prod_{n=1}^{m} a_n^{i_n} \qquad \text{avec} \qquad \sum_{n-1}^{m} i_n = j - 1.$$

Soit $y \in B_{k-1}(a)$; de même nous avons:

$$y = \prod_{n=1}^{m} a_n^{l_n}$$

avec:

$$\sum_{n=1}^{m} l_n = k - 1 = M - j + 1.$$

Si l'on multiplie deux éléments tels que x et y, le degré du produit est M. Ou bien xy est nul ou bien ce produit est égal à $\prod_{i=1}^{m} a_i^{p-1}$. D'après la définition de $\bar{x}$, on a l'équivalence [*cf.* (20)]:

$$xy = 0 \quad \Leftrightarrow \quad \bar{x} \neq y.$$

Ceci implique 3° et montre donc que X est un élément de $J(a)$ du type $I_{k,t}$.

3.1. Les conditions d'autodualité

Un code linéaire est dit «autodual» s'il est égal à son complémentaire orthogonal. Un code C de A, autodual, vérifie:

$$\dim A = p^m = \dim C + \dim C^{\perp} = 2 \dim C.$$

Donc, si p est impair A ne possède pas de codes autoduaux. Nous supposons désormais que $p = 2$ ($M = m$, $K = F_{2^r}$, $G = F_{2^m}$).

Soit I un idéal 1-translaté de P^j; nous avons, d'après le théorème 2:

$$P^j \subset I \subset P^{j-1} \qquad \text{et} \qquad P^{m-j+2} \subset \text{Ann } I \subset P^{m-j+1}.$$

Soit s tel que : $\dim I = \dim P^j + s$.

Si I est autodual, les deux formules d'inclusion doivent être confondues.

Nous obtenons des conditions nécessaires d'autodualité:

(I) $P^j = P^{m-j+2} \Leftrightarrow j = m - j + 2$

$$\Leftrightarrow \quad j = \frac{m}{2} + 1,$$

(II) $\text{Ann } P^j = P^{j-1}$

$$\Leftrightarrow \quad \dim P^j + \dim P^{j-1} = 2^m$$
$$\Rightarrow \quad 2 \dim P^j + (\dim P^{j-1} - \dim P^j) = 2^m$$
$$\Rightarrow \quad s = \frac{1}{2}(\dim P^{j-1} - \dim P^j)$$
$$\Rightarrow \quad s = \frac{1}{2}\binom{m}{j-1}.$$

La formule (II) peut se déduire des formules (17) et (18) qui définissent une base pour chaque GRM-code:

$$\begin{aligned}\dim P^{j-1} - \dim P^j &= |B_{j-1}(e) \setminus B_j(e)| \\ &= \left|\left\{ \prod_{i=1}^{m} a_i^{k_i} \,\middle|\, k_i = 0 \text{ ou } 1 \right.\right. \\ &\qquad \left.\left. \text{et } \sum_{i=1}^{T} k_i = j - 1 \right\}\right|.\end{aligned}$$

Théorème 3: *Les codes considérés sont binaires et de longueur* 2^m. *Soit* I *un idéal* 1-*translaté du GRM-code de degré* j.

Alors si I *est autodual, les conditions suivantes sont vérifiées:*

1° m *est pair et* $j = (m/2) + 1$.

2° $\dim I = \dim P^j + \binom{m-1}{(m/2)-1}$.

Preuve: 1° se déduit de (I).

2° est calculé avec la valeur de s donnée par (II) et pour $j-1=m/2$:

$$\frac{1}{2}\binom{m}{m/2}=\frac{1}{2}\frac{m.(m-1)\ldots(m/2+1)}{1.2\ldots m/2}$$

$$=\frac{(m-1)\ldots(m/2+1)}{1.2\ldots(m/2-1)}$$

3.2. CONSTRUCTION DE CODES AUTODUAUX

Rappelons d'abord que lorsque m est impair, l'un des GRM-codes est autodual:

$$\text{Ann } P^{(m+1)/2}=P^{m-[(m+1)/2]+1}=P^{(m+1)/2}.$$

Ceci explique que dans ce cas un idéal 1-translaté ne peut être autodual.

Car cet idéal est contenu dans le GRM-code autodual ou bien le contient (il s'agit d'inclusions au sens strict); dans les deux cas la dimension de l'idéal ne peut être la moitié de la dimension de A.

Pour prouver l'existence de codes 1-translatés autoduaux nous allons construire des codes autoduaux éléments de $J(a)$. Soit donc un idéal 1-translaté de type $I_{j,s}$. Le code $I_{j,s}$ est engendré par la base $B_j(a)$ à laquelle on ajoute s vecteurs de $B_{j-1}(a)$ de plus petit degré. On désigne par B_s l'ensemble de ces s vecteurs. Alors:

Proposition 4: *m est pair,*

$$j=\frac{m}{2}+1 \qquad et \qquad s=\binom{m-1}{(m/2)-1}$$

Un élément de $J(a)$ de type $I_{j,s}$ est autodual si et seulement si:

$$(21) \qquad x\in B_s \Rightarrow \bar{x}\notin B_s.$$

Preuve: Les hypothèses impliquent la possibilité d'autodualité (th. 3).

Les valeurs de j et s données sont telles que la dimension de $I_{j,s}$ est la moitié de celle de A [*cf.* démonstration de (II)]. Il reste à exprimer que chaque vecteur de la base de $I_{j,s}$ est orthogonal aux autres.

Or par définition de $\bar{x}$ et d'après la proposition 4 la condition (21) exprime que les vecteurs de B_s s'annulent 2 à 2.

Exemple: Pour déterminer un élément de $J(a)$ autodual, le problème est le choix de B_s dès que j et s vérifient les hypothèses de la proposition 4.

Une possibilité est de prendre les éléments de $B_{j-1}(a)$ de degré $j-1$ ayant un même facteur:

$$(22) \qquad B_s=\left\{\prod_{k=1}^{m} a_k^{i_k} \;\middle|\; \begin{array}{c} i_1=1,\ i_k=0 \text{ ou } 1 \\ \sum_{k=1}^{m} i_k=\frac{m}{2} \end{array}\right\},$$

– par définition de $\bar{x}$ [*cf.* (20)] B_s vérifie (21);

– le cardinal de B_s est la moitié de $B_{j-1}(a)\setminus B_j(a)$ ce qui est conforme avec les hypothèses. Appelons X le code ainsi défini:

$$X=\bigcup_{x\in L}(x+P^{m/2+1}),$$

où L est le sous-espace engendré par l'ensemble B_s défini par (22).

En caractéristique 2, un GRM-code de degré j a une valuation égale à 2^j. Il est clair qu'un idéal 1-translaté de P^j a une valuation comprise entre 2^j et 2^{j-1}. La valuation de l'idéal X dépend de la distribution de poids de l'idéal principal engendré par a_1 (tous les éléments de B_s sont contenus dans cet idéal). Dans le cas où les a_i sont des éléments simples du type $(X^{ei}-1)$ [*cf.* les définitions données par (6) et (7)] la valuation de X est égale à la valuation de P^{j-1}, c'est-à-dire au poids des vecteurs de B_s, soit $2^{m/2}$.

Proposition 5: *Les codes considérés sont de longueur 2^m sur le corps F_{2^r}.*

Alors pour chaque valeur paire de m, on peut construire un code autodual $(2^m, 2^{m-1}, 2^{m/2})$ qui est un code 1-translaté du GRM-code de degré $(m/2)+1$.

Remarques: Dans le cas binaire, il s'agit d'un code autodual X compris entre le code de Reed et Muller d'ordre $m/2$ et le code de Reed et Muller d'ordre $(m/2)+1$.

4. Codes 1-translatés à caractère cyclique

Dans ce paragraphe, nous notons S l'intervalle $[0, n]$ avec $n=p^m-1$.

Étant donné un élément s de S, s peut être désigné par le m-uple $(s_1, \ldots, s_m)$, représentant de son écriture dans la base p:

$$(23) \qquad s=\sum_{i=0}^{m-1} s_i p^i, \qquad s_i\in[0, p-1].$$

Nous appelons *poids de s* la quantité:

$$(24) \qquad W(s)=\sum_{i=0}^{m-1} s_i.$$

Soit R l'algèbre de polynômes $K[X]/(X^n-1)$.

Un code cyclique de longueur n sur K est un idéal de l'algèbre R. Soit C un tel code; son polynôme générateur s'écrit:

$$(26) g(X)=\prod_{k\in L}(X-\alpha^k), \qquad L\subset S, \quad g(X)\in K[X],$$

où α est une racine primitive du corps G.

L'extension du code C *dans* A, soit $\hat{C}$, est obtenue en ajoutant un symbole supplémentaire à chaque mot de

C de telle façon que $\hat{C}$ soit linéaire [18]:

$$c \in C, \quad c=(c_1, \ldots, c_n) \Leftrightarrow c' \in \hat{C}, \quad c'=(c_0, c_1, \ldots, c_n), \quad c_0 = -\sum_{i=1}^{n} c_i.$$

Nous disons d'un code de A *qu'il est à caractère cyclique* s'il est l'extension d'un code cyclique. Sa définition dans A est :

$$\hat{C}=\{x \in A \mid \Phi_s(x)=0, s \in T\}, \tag{26}$$

où :
- $T=L \cup \{0\}$,
- $\Phi_s(x)=\sum_{g \in G} x_g g^s$.

La quantité $\Phi_s(x)$ est calculée dans un sur-corps de K et de G; sa nullité exprime que α^s est racine du polynôme générateur du code cyclique primitif.

L'ensemble T, dit *ensemble de définition du code* $\hat{C}$, doit être maximal, c'est-à-dire:

$$\text{si } s \in T \Rightarrow \Phi_{s'}(\hat{C})=0 \text{ alors } s' \in T.$$

Chaque GRM-code est l'extension d'un code cyclique [5, 6]; son ensemble de définition est :

$$j \in [1, M], \quad T_j=\left\{ s \in S \mid \sum_{i=1}^{m} s_i < j \right\}. \tag{27}$$

Un code de A défini par (26) est un idéal de A si et seulement si il est invariant sous le groupe des permutations affines de G [13].

Lorsqu'il s'agit d'un code 1-translaté à caractère cyclique, le code vérifie toujours cette propriété: étant un sous-espace de A il est un idéal de A (th. 2):

Proposition 6: *Un code 1-translaté qui est l'extension d'un code cyclique est invariant sous le groupe des permutations affines de G: c'est un idéal de l'algèbre A.*

Soit donc I un idéal 1-translaté du GRM-code P^j *qui est à caractère cyclique. Soit T l'ensemble de définition de I, alors:*

$$P^j \subset I \subset P^{j-1} \Leftrightarrow T_{j-1} \subset T \subset T_j. \tag{28}$$

Nous obtenons (28) par application directe de la propriété suivante :

Propriété: Soient X et X′ deux codes de A à caractère cyclique ayant respectivement T et T′ pour ensemble de définition alors:

$$X \subset X' \Leftrightarrow T' \subset T.$$

Preuve: Par définition [*cf.* (26)]:

$$x \in X \Leftrightarrow \Phi_s(x)=0, \quad s \in T.$$

Si $x \in X$ implique $x \in X'$, en particulier la quantité $\Phi_s(x)$ est nulle pour tout s de T′. Il est équivalent de dire que T contient T′.

Proposition 7: *Un idéal 1-translaté du GRM-code* P^j, *à caractère cyclique, a pour ensemble de définition:*

$$T=T_{j-1} \cup L \tag{29}$$

où:

$$L \subset \{s \in S \mid W(s)=j-1\}.$$

Sa dimension est égale à $\dim P^{j-1} - |L|$.

Preuve: La définition de T est une conséquence immédiate de (27) et (28): T est obtenu en ajoutant à l'ensemble de définition de P^{j-1} quelques éléments de S de poids $j-1$.

La dimension d'un code de A à caractère cyclique est égale à $p^m - T$, si T est l'ensemble de définition du code [18]. Soit λ la quantité cherchée:

$$\lambda = p^m - |T_{j-1}| - |L|,$$
$$\lambda = \dim P^{j-1} - |L|.$$

Exemple: $m=6$, $K=F_2$; I est le code d'ensemble de définition T.

1° $\begin{cases} T=\{0, 1, 2, 2^2, \ldots, 3, 6, 12, 24, 48, 33\}, \\ P^3 \subset I \subset P^2. \end{cases}$

La valuation de I est 8 (T contient 6 valeurs consécutives, mais le code est à poids multiples de 2).

2° $\begin{matrix} T=T_{m-2} \cup \{15, 30, 60, 57, 51, 39, 14\}, \\ P^{m-1} \subset I \subset P^{m-2}. \end{matrix}$

Le code I est une réunion de translatés du RM-code d'ordre 1. Sa valuation est une des valeurs:

$$\left\{ 2^{m-1} - 2^{m-h-1} \text{ où } h \in \left[1, \frac{1}{2} m \right] \right\}$$

([15], chap. 15); elle est supérieure à 24.

Ici encore nous obtenons une généralisation de propriétés des GRM-codes. Ainsi, si nous nous intéressons à l'annulateur d'un idéal 1-translaté à caractère cyclique, nous savons (th. 2) qu'il s'agit encore d'un idéal 1-translaté de A et que annulateur et complémentaire orthogonal sont confondus. Nous pouvons encore démontrer la proposition suivante:

Proposition 8: *Soit I un idéal 1-translaté du GRM-code* P^j, *à caractère cyclique, dont l'ensemble de définition est donné par* (29). *Alors* Ann I *est un idéal 1-translaté du GRM-code* P^{M-j+2} *à caractère cyclique et son ensemble de définition est:*

$$T'=T_{M-j+1} \cup L', \tag{30}$$

où:

$$L'=\{u \in S \mid W(u)=M-j+1, (p^m-1)-u \notin L\}.$$

Preuve : Soit I′ l'ensemble défini par (30) :

$$\begin{aligned}\dim \mathrm{I}' &= \dim \mathrm{P}^{\mathrm{M}-j+1} - |\mathrm{L}'| \\ &= \dim \mathrm{P}^{\mathrm{M}-j+1} - (\dim \mathrm{P}^{\mathrm{M}-j+1} - \dim \mathrm{P}^{\mathrm{M}-j+2} - |\mathrm{L}|) \\ &= \dim \mathrm{P}^{\mathrm{M}-j+2} + |\mathrm{L}| \\ &= (p^m - \dim \mathrm{P}^{j-1}) + |\mathrm{L}| \\ &= p^m - (\dim \mathrm{P}^{j-1} - |\mathrm{L}|).\end{aligned}$$

D'où :

$$\dim \mathrm{I}' + \dim \mathrm{I} = p^m.$$

Pour montrer que I′ est Ann I, il reste à prouver que le produit d'un élément x de I avec un élément y de I′ est nul. Pour cela nous utilisons la formule démontrée dans [6] :

$$\Phi_s(xy) = \sum_{t \in [0,\, s]} \binom{s}{t} \Phi_{s-t}(y)\, \Phi_t(x)$$

[$s \in \mathrm{S}$ et Φ_s est définie par (26)].
D'abord, le théorème de Lucas implique :

$$\binom{s}{t} \not\equiv 0 \pmod p \quad \Leftrightarrow \quad i \in [1, m], \qquad t_i \leqq s_i.$$

Soit $s \in \mathrm{S}$ et soit t tel que $\binom{s}{t}$ est non nul; alors trois cas sont possibles :

$$1^\circ \qquad \mathrm{W}(t) < j-1 \quad \Rightarrow \quad \Phi_t(x) = 0,$$

$$2^\circ \quad \mathrm{W}(t) > j-1 \quad \Rightarrow \quad \mathrm{W}(s-t) < \mathrm{M}-j+1 \quad \Rightarrow \quad \Phi_{s-t}(y) = 0,$$

$$3^\circ \quad \mathrm{W}(t) = j-1 \quad \Rightarrow \quad \mathrm{W}(s-t) \leqq \mathrm{M}-j+1 \quad \Rightarrow \quad \Phi_{s-t}(y) = 0$$

$$\text{ou } \mathrm{W}(s-t) = \mathrm{M}-j+1, \quad \mathrm{W}(t) = j-1 \text{ et}$$

$$\mathrm{W}(s-t) = \mathrm{M}-j+1 \quad \Rightarrow \quad t \in \mathrm{L} \quad \text{ou} \quad s-t \in \mathrm{L}' \quad \Rightarrow \quad \Phi_t(x) = 0 \quad \text{ou} \quad \Phi_{s-t}(y) = 0.$$

Donc :

$$\Phi_s(xy) = 0, \qquad s \in \mathrm{S}.$$

Ceci signifie que le produit xy est nul.

Conclusion

Nous avons prouvé que les codes 1-translatés, translatés particuliers d'un GRM-code, ont des propriétés algébriques intéressantes en ce sens qu'elles permettent une exploration utilisant les outils mis en place lors de l'étude systématique des idéaux de A.
A titre d'application nous caractérisons les codes cycliques étendus qui sont des codes 1-translatés; nous exhibons de nouveaux codes autoduaux.

Nous pensons que d'autres tentatives peuvent être faites pour mettre en évidence, avec le matériel décrit, de nouvelles propriétés pour certains codes 1-translatés.

BIBLIOGRAPHIE

[1] E. R. Berlekamp, *Algebraic coding theory*, McGraw Hill book Cie, New York.

[2] S. D. Bermann, On the theory of groups codes, *Kibernetika*, 1, n° 1, 1967, p. 31-39.

[3] N. Bourbaki, *Livre II, Algèbre*, Herman, Paris, 1953.

[4] P. Camion, *Codes de Preparata et codes de Kerdock. Théorie des codes*, D. Perrin, éd., ENSTA, 1979, p. 21-29.

[5] P. Camion, *A proof of some properties of Reed-Muller codes by means the normal basis*, in R. C. Bose et T. A. Dowling, éd., *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 3e cycle*, Université de Paris-VII, 1982.

[7] P. Charpin, Puissance du radical d'une algèbre modulaire et codes cycliques, *Revue du CETHEDEC*, 18e année, 4e trimestre 1981, MS 81-2, p. 35-43.

[8] P. Charpin, Codes cycliques étendus et idéaux principaux d'une algèbre modulaire, *C. R. Acad. Sc.*, 295, série I, 1982, p. 313-315.

[9] B. K. Dass et S. K. Mutto, A note on Reed-Muller codes, *Discrete Applied Mathematics*, 2, n° 4, 1980, p. 345-348.

[10] P. Delsarte, On cyclic codes that are invariant under the general linear group, *IEEE Trans. Info. Theory*, 16, 1970, p. 760-769.

[11] P. Delsarte, J. M. Goethals et F. J. MacWilliams, On generalized Reed-Muller codes and their relatives, *Info. and Control*, 16, 1974, p. 403-442.

[12] W. M. Kantor, On the inequivalence of generalized Preparata Codes, *IEEE Trans. Info. Theory*, IT-29, n° 3, May 1983.

[13] T. Kasami, S. Lin et W. W. Peterson, Some results of cyclic codes which are invariant under the affine group and their applications, *Info. and Control*, 11, 1967, p. 475-496.

[14] T. Kasami, S. Lin et W. W. Peterson, New generalisations of the Reed-Muller codes, *IEEE Trans. Info. Theory*, II-14, 1968, p. 189-199.

[15] F. J. MacWilliams et N. J. A. Sloane, *The theory of error correcting codes*, North Holland, 1977.

[16] A. Poli, Codes dans certaines algèbres modulaires, *Thèse de Doctorat d'État*, Univ. P.-Sabatier, Toulouse, 1978.

[17] A. Poli, Codes stables sous le groupe des automorphismes isométriques de

$$\mathrm{A} = \mathrm{F}_p[\mathrm{X}_1, \ldots, \mathrm{X}_m]/(\mathrm{X}_n^p - 1).$$

C.R. Acad. Sc., 290, série A, 1980, p.

[18] J. H. Van Lint, *Coding theory*, Springer-Verlag, New York, 1971.

[19] J. Wolfmann, Un problème d'extrémum dans les espaces vectoriels binaires, *Ann. Discrete Math.*, 9, 1980, p. 261-264.