Discrete Mathematics 80 (1990) 229–247
North-Holland

CODES CYCLIQUES ÉTENDUS AFFINES-INVARIANTS ET ANTICHAINES D'UN ENSEMBLE PARTIELLEMENT ORDONNE

Pascale CHARPIN

Institut de Programmation et LITP, Univ. Paris VI, 4 Place Jussieu, 75252 Paris Cedex 05, France*

Received 5 January 1988

Nous montrons que l'ensemble des codes cycliques étendus primitifs, d'une longueur donnée, invariants sous le groupe affine (codes affines-invariants), peut être identifié à l'ensemble des antichaînes d'un certain produit de chaînes. Nous proposons ainsi une classification de ce corpus de codes dont l'intérêt principal est qu'une antichaîne donnée permet d'obtenir de nombreuses propriétés sur le code qu'elle définit. Notamment nous obtenons ainsi une description de chaque code affine-invariant considéré comme un idéal d'une algèbre modulaire. Nous montrons aussi qu'un résultat récent sur les ensembles partiellement ordonnés, du à Griggs [12], s'applique immédiatement dans ce contexte.

We show that the set of primitive extended cyclic codes, with a given length, which are invariant under the affine group (affine-invariant codes) can be identified with the set of antichains in a product of chains. We then propose a classification of affine-invariant codes the main interest of which is that a given antichain permits to obtain many properties of the defined code. Particularly we give a description of each affine-invariant code considered as ideal in a modular algebra. In the same time, we show that a recent result over posets, due to Griggs [12], is here immediately applicable.

1. Introduction

Les codes étudiés ici sont des codes cycliques primitifs, étendus dans une algèbre modulaire de p-groupe abélien élémentaire. Aussi leur définition fait-elle intervenir deux algèbres de polynômes: l'algèbre des codes cycliques, que nous notons $\boldsymbol{R}$, et l'algèbre modulaire dans laquelle les codes de $\boldsymbol{R}$ sont étendus, que nous notons $\boldsymbol{A}$. Nous supposons connues les propriétés de base des codes linéaires, en particulier des codes cycliques, dévellopées dans plusieurs ouvrages classiques [16, 20]. D'autre part les codes de $\boldsymbol{A}$ ont maintenant fait l'objet d'un certain nombre de publications, suite à l'article de Berman, qui identifie les codes de Reed et Muller binaires avec les puissances du radical de A [4, 5, 17]. Nous supposons donc acquises certaines définitions ou propriétés pour lesquelles nous donnerons des références dans le texte.

Quand nous parlons de distance, il s'agit toujours de la distance de Hamming. Tous les codes sont ici des codes linéaires; nous adoptons donc la terminologie

* Laboratoire d'Informatique Théorique et Programmation.

des espaces vectoriels finis; notamment, un mot de code est un vecteur identifié à l'ensemble de ses composantes.

Soit p un nombre premier; les codes cycliques de longueur $p^m - 1$, définis sur un corps de caractéristique p, dont l'extension est un code invariant sous le groupe affine, ont été caractérisés par Kasami, Lin et Peterson; ces auteurs mettent en évidence, dans [13], une propriété de type combinatoire de l'ensemble des zéros des codes cycliques ainsi définis. Nous notons $\boldsymbol{K}(p, m)$ ce corpus de codes. Tout code de $\boldsymbol{K}(p, m)$ a pour extension un idéal de l'algèbre modulaire $\boldsymbol{A}$ dans laquelle s'effectue l'extension. Ce sont ces idéaux particuliers que nous appelons *codes affines-invariants*. Nous rappelons leur définition dans le paragraphe 2; les codes de Bose–Chaudhuri–Hocquenguem primitifs étendus (codes BCH), les codes de Reed et Muller Généralisés (codes GRM) et les codes de Reed–Solomon étendus (codes RS) sont des codes affines-invariants. Nous proposons une nouvelle formulation du Théorème de Kasami et al. (Théorème 1), utilisant le fait que l'intervalle $S = [0, n]$ peut être muni d'une relation d'ordre partiel, notée $\ll$. Soit $S_{\ll}$ l'ensemble partiellement ordonné ainsi obtenu. Dans la terminologie usuelle, l'ensemble $S_{\ll}$ est un *produit de chaînes de taille p* [12]. Nous montrons, dans le paragraphe 3, que l'ensemble des codes affines-invariants de longueur p^m s'identifie à l'ensemble des antichaînes du produit de chaînes $S_{\ll}$. De plus, une antichaîne donnée fournit d'autres éléments de définition du code, ainsi son corps de base, son dual on sa borne-BCH. Dans les paragraphes 4 et 5, nous étudions les codes affines-invariants dans l'ensemble des idéaux de l'algèbre modulaire $\boldsymbol{A}$. Nous prouvons que, là aussi, l'étude des antichaînes de $S_{\ll}$ fournit des outils de définition ou de description. Ainsi le cardinal d'une antichaîne donnée F est une paramètre descriptif du code U qu'elle définit, appelé *taille* de U. La taille d'un idéal de $\boldsymbol{A}$ est le cardinal de ses systèmes minimaux de générateurs. Le Théorème 3 montre comment, connaissant F, on peut construire effectivement un système minimal de générateurs de U. Ceci permet de caractériser, par une propriété des antichaînes, les idéaux affines-invariants dits *à type de profondeur constante* (Théorème 4). Nous montrons comment calculer explicitement la taille des codes RS et la taille des codes GRM p-aires. Un résultat récent de J.R. Griggs sur les ensembles partiellement ordonnés permet d'affirmer que, pour une longueur de code donnée, ce sont certains codes GRM p-aires qui ont la plus grande taille.

2. Définition des codes affines-invariants

Dans la suite de l'article, K et G désignent deux corps de caractéristique p : G est le corps de Galois $GF(p^m)$ et K est un sous-corps de G. Chaque choix de K, en tant que sous-corps de G, permet de définir l'algèbre quotient $\boldsymbol{R} = K[Z]/(Z^n - 1)$, où $n = p^m - 1$, et l'algèbre modulaire $\boldsymbol{A} = K[G]$. L'algèbre $\boldsymbol{A}$ est

l'ensemble des polynômes formels

$$x = \sum_{g \in G} x_g X^g, \qquad x_g \in K, \tag{1}$$

muni des opérations usuelles d'addition et de multiplication des polynômes:

$$a \sum_{g \in G} x_g X^g + b \sum_{g \in G} y_g X^g = \sum_{g \in G} (a x_g + b y_g) X^g$$

$$a X^g b X^h = ab X^{g+h}$$

avec $a \in K$, $b \in K$, $x \in \boldsymbol{A}$, $y \in \boldsymbol{A}$, $g \in G$, $h \in G$. Nous appelons *code de* $\boldsymbol{A}$ un K-sous-espace vectoriel de $\boldsymbol{A}$.

Un *code cyclique de longueur n sur K* est un idéal principal de l'algèbre $\boldsymbol{R}$. Nous dirons que c'est un *code de* $\boldsymbol{R}$; un tel code, soit C, est défini par son polynôme générateur

$$g(Z) = \prod_{k \in T} (Z - \alpha^k), \qquad T \subset [0, n[. \tag{2}$$

où α est une racine primitive du corps G.

On peut dire aussi que la donnée de l'ensemble T définit le code C. Nous dirons que *T est l'ensemble de définition du code C*, et nous supposons désormais que $0 \notin T$. Avec cette hypothèse, on peut étendre le code C en un code linéaire C_e de longueur p^m, en ajoutant à chaque mot de C un symbole dit "de parité":

$$c \in C, \qquad c = (c_0, \ldots, c_{n-1}) \to c' \in C_e, \qquad c' = \left(-\sum_{i=0}^{n-1} c_i, c_0, \ldots, c_{n-1} \right) \tag{3}$$

Dans l'extension définie par (3), on indice chaque symbole c_i du mot étendu par l'elément α^i du corps G; le symbole de parité est étiqueté par l'élément 0. On obtient ainsi la transformation polynômiale

$$\sum_{i=0}^{n-1} c_i Z^i \in C \to \left(-\sum_{i=0}^{n-1} c_i \right) X^0 + \sum_{i=0}^{n-1} c_i X^{\alpha^i} \in C_e, \tag{4}$$

et donc la définition du code C_e:

$$C_e = \{ x \in \boldsymbol{A} \mid \phi_s(x) = 0, \forall s \in T_e \}. \tag{5}$$

où $\phi_s(x) = \sum_{g \in G} x_g g^s$ et $T_e = T \cup \{0\}$. Nous dirons que l'ensemble $T_e = T \cup \{0\}$ est *l'ensemble de définition* du code C_e.

Remarque. Si $s \neq 0$ alors $\phi_s(x) = \sum_{g \in G^*} x_g g^s$. D'autre part, $\phi_0(x) = \sum_{g \in G} x_g$.

Le groupe des *permutations affines* de G est l'ensemble des applications:

$$p_{u,v} : g \to ug + v, \qquad u \in G, \qquad v \in G, \qquad u \neq 0.$$

Définition 1. Un code de A, soit U, est *affine-invariant* si et seulement s'il est invariant sous le groupe des permutations affines de G, c'est-à-dire s'il vérifie:

$$\sum_{g\in G} x_g X^g \in U \to \sum_{g\in G} x_g X^{p_{u,v}(g)} \in U \qquad u \in G, \qquad v \in G, \qquad u \neq 0. \tag{6}$$

Proposition 1. *Une code de $\boldsymbol{A}$ affine-invariant est un code cyclique primitif étendu dans $\boldsymbol{A}$ qui est un idéal de $\boldsymbol{A}$.*

Preuve. Soit U un code de $\boldsymbol{A}$ soit x un élément de U. Nous notons $p_{u,v}(x)$ l'image de x par $p_{u,v}$, telle qu'elle est décrite par (6). Nous avons:

$$p_{u,v}(x) = \sum_{g\in G} x_g X^{ug+v} = X^v \sum_{g\in G} x_g X^{ug}.$$

On en déduit que U est un idéal de $\boldsymbol{A}$ si et seulement s'il est invariant par les applications $p_{1,v}$, $v \in G$; d'autre part U est un code cyclique étendu si et seulement s'il est invariant par les applications $p_{u,0}$. □

A l'ensemble $\boldsymbol{K}(p, m)$ correspond bijectivement l'ensemble des codes affine-invariants, c'est-à-dire, d'après la Proposition 1, *l'ensemble des codes cycliques étendus qui sont des idéaux d'une algèbre modulaire de type $K[G]$ où K est un sous-corps de G.* Mais ceci est l'aspect algèbrique de la définition; la définition "arithmétique" des codes affine-invariants fait intervenir les ensembles de définition des codes, et eux seuls (cf. (5)), c'est-à-dire les sous-ensembles de l'intervalle S. Le Théorème de Kasami et al. permet de déterminer si un sous-ensemble de S est l'ensemble de définition d'un code affine-invariant. Sa démonstration – et notamment l'utilisation du Théorème de Lucas – fait clairement intervenir un ordre partiel sur les éléments de S. La Définition 2 précise ci-après la structure de l'ensemble S; la terminologie est empruntée à Griggs [12]. Le Théorème 1 est une nouvelle formulation du Théorème de Kasami et al.; nous ne donnons pas ici sa démonstration que le lecteur pourra consulter dans [5] ou [13].

Définition 2. $S = [0, n]$ où $n = p^m - 1$. Chaque élément s de S est identifié à sa représentation dans la base p:

$$s = (s_0 \cdots s_{m-1}) \quad \text{où} \quad s = \sum_{i=0}^{m-1} s_i p^i, \qquad s_i \in [0, p-1].$$

On désigne par $S_{\ll}$ l'ensemble S muni de la relation d'ordre partiel ci-dessous définie:

$$s \ll t \quad \leftrightarrow \quad s_i \leqslant t_i \qquad i \in [0, m-1].$$

Le *rang* de s est la quantité $\sum_{i=0}^{m-1} s_i$. L'ensemble $S_{\ll}$ est un *produit de chaînes de taille p.* Lorsque $s \ll t$ nous dirons que *s est un descendant de t* ou que *t est un*

majorant de s pour la relation $\ll$. Les éléments s et t sont dits *irrelatés* lorsque s n'est pas un descendant de t et que t n'est pas un descendant de s. Une *antichaîne* de $S_{\ll}$ est un ensemble d'éléments de S irrelatés.

On note Δ l'application qui, à toute partie I de S, fait correspondre l'ensemble des descendants des éléments de I dans S:

$$\Delta : I \subset [0, n] \to \Delta(I) = \bigcup_{t \in I} \{s \in S \mid s \ll t\} = \bigcup_{t \in I} \Delta(t) \tag{7}$$

où $\Delta(\{t\})$ est noté $\Delta(t)$.

Théorème 1. *Soit U un code cyclique étendu qui est un code d'une algèbre de type A; soit I l'ensemble de définition de U. Alors U est affine-invariant si et seulement si I est un point fixe de l'application* Δ (*i.e.* $\Delta(I) = I$).

Exemple 1. On montre facilement que les codes BCH et les codes GRM sont affines-invariants [13]. A titre d'exemple nous donnons ci-aprés l'ensemble de définition I du code BCH binaire, de longueur 16 et de distance construite 5; I est l'ensemble des classes cyclotomiques de 2 modulo 15 qui ont un représentant dans $[0, 5[: I = \{0, 1, 2, 4, 8, 3, 6, 9, 12\}$, c'est-à-dire

$$I = \left\{ \begin{matrix} (0\ 0\ 0\ 0), & (1\ 0\ 0\ 0), & (0\ 1\ 0\ 0), & (0\ 0\ 1\ 0), & (0\ 0\ 0\ 1) \\ (1\ 1\ 0\ 0), & (0\ 1\ 1\ 0), & (1\ 0\ 0\ 1), & (0\ 0\ 1\ 1) & \end{matrix} \right\}.$$

Il est clair tout élément de I a ses descendants dans I : I est un point fixe de Δ.

3. Codes affines-invariants et antichaînes de $S_{\ll}$

Le Théorème 1 prouve que l'ensemble des codes affines-invariants de longueur p^m est en bijection avec l'ensemble des points fixes de Δ. Nous allons voir maintenant que chaque point fixe de Δ est défini par une antichaîne de $S_{\ll}$.

Définition 3. Soit I un sous-ensemble de S. Nous appelons *frontière de I*, et nous notons $F(I)$, *l'ensemble des éléments minimaux du complémentaire de I dans S.* En d'autres termes, la frontière de I est l'ensemble suivant:

$$F(I) = \{s \in S \mid s \notin I \text{ et } \Delta(s) - \{s\} \subset I\}. \tag{8}$$

Proposition 2. *La frontière d'un sous-ensemble I de S est une antichaîne de* $S_{\ll}$.

Preuve. Si deux éléments de $S_{\ll}$ sont des éléments minimaux d'un même sous-ensemble de S alors ils sont irrelatés. □

A chaque sous-ensemble I de S, correspond une antichaîne de $S_{\ll}$: sa frontière $F(I)$. Cependant plusieurs sous-ensembles de S peuvent avoir la même frontière.

Nous allons voir maintenant qu'à une antichaîne correspond un et un seul point fixe de Δ (i.e. un et un seul code affine-invariant).

Proposition 3. *Soit $f \in S$; on note $N(f)$ l'ensemble des non-majorants de f dans S:*

$$N(f) = \{s \in S - \{f\} \mid s \ll f \text{ ou } s \text{ et } f \text{ sont irrelatés}\}. \tag{9}$$

Soit F une antichaîne du produit de chaînes $S_{\ll}$. Alors l'ensemble

$$I = \bigcap_{f \in F} N(f) \tag{10}$$

est un point fixe de Δ et I est le seul point fixe de Δ de frontière F.

Preuve. Soient $s \in I$ et $t \in \Delta(s)$. Supposons que $t \notin I$, c'est-à-dire qu'il existe $f \in F$ tel que t soit un majorant de f; on a alors $f \ll t \ll s$ ce qui est contradictoire avec $s \in I$. Donc $\Delta(s) \subset I : I$ est un point fixe de Δ.

Soit I' le complémentaire de I dans S; I' est l'ensemble des majorants des éléments de F:

$$I' = \bigcup_{f \in F} \{s \in S \mid f \ll s\} \tag{11}$$

Par définition de I', un élément minimal de I' est un élément de F; d'autre part, un élément f de F est irrelaté avec tous les autres éléments de F, car F est une antichaîne; donc il ne peut être que minimal dans I'. L'antichaîne F est donc l'ensemble des éléments minimaux de I', c'est-à-dire, par définition, la frontière de I.

Enfin supposons qu'il existe un autre point fixe de Δ, soit J, dont la frontière est aussi F. Alors $J \subset I$ car J ne peux contenir un élément de I'. D'autre part supposons qu'il existe $s \in I \backslash J$. Cela signifie que la frontière de J contient un descendant de s. C'est impossible car $s \in I$. Donc $J = I$. □

Théorème 2. *$S = [0, n]$ et Δ est définie par (7). Il existe une bijection entre l'ensemble des points fixes de Δ et l'ensemble des antichaînes du produit de chaînes $S_{\ll}$. En d'autres termes, chaque code affine-invariant de longueur p^m est déterminé d'une manière unique par une antichaîne de $S_{\ll}$, cette antichaîne étant la frontière du code concerné.*

Preuve. Le Théorème 1 prouve qu'il existe une bijection entre les codes de $\boldsymbol{K}(p, m)$ et les points fixes de Δ. La Proposition 3 prouve qu'il existe une bijection entre les points fixes de Δ et les antichaines de $S_{\ll}$: d'une part, chaque point fixe posséde une frontière qui est une antichâine et d'autre part chaque antichaîne définit un et un seul point fixe dont elle est la frontière (cf. (8) et (10)). □

Nous appelons *frontière d'un code affine-invariant*, ou du code cyclique correspondant dans $\boldsymbol{K}(p, m)$, l'antichaîne qui définit ce code. Le calcul de la frontière nécessite en général l'emploi d'un calculateur. On peut dans certains cas obtenir une formule explicite: nous étudions plus loin le cas des codes RS et des codes GRM p-aires. Dans l'Exemple 1, la frontière du code BCH étudié est l'ensemble $\{5, 10\}$.

Nous avons montré qu'il suffit de connaitre la frontière d'un code affine-invariant pour connaitre le code lui-même. C'est donc une simplification, une façon plus économique de voir l'ensemble $\boldsymbol{K}(p, m)$, que nous proposons. Dans la suite de cet article, nous voulons prouver qu'en outre, la frontière fournit de nombreux renseignements sur le code qu'elle définit. Ainsi les résultats présentés dans les propositions suivantes montrent que la donnée d'une antichaîne détermine un code avec son corps de base, son dual et sa borne-BCH.

Soit $C \in \boldsymbol{K}(p, m)$; soit L un sous-corps de G. Nous dirons que *C est un code sur L* si les coefficients du polynôme générateur de C sont dans L. Toutefois, si C est un code sur L, on peut considérer l'extension de C dans toute algèbre $K[G]$ où K est un sur-corps de L. Soit q l'ordre de L; C est un code sur L si et seulement si son ensemble de définition est une réunion de classe cyclotomiques de q modulo n. La proposition suivante montre que cette propriété est une propriété de la frontière de C.

Proposition 4. *Soit $q = p^s$ où s divise m. Soit F une antichaîne de $S_{\ll}$. Alors F définit un code affine-invariant sur $GF(q)$ si et seulement si F est une réunion de classes cyclotomiques de q modulo n.*

Preuve. Soit I le point fixe de Δ défini par F. L'ensemble I est défini par (10) et l'ensemble I' par (11). Nous devons montrer que I est invariant par la transformation $\sigma : i \to qi$ si et seulement si F l'est. Or par définition de $\ll$,

$$f \ll s \quad \leftrightarrow \quad qf \ll qs \tag{12}$$

où qf et qs sont calculés modulo n.

Supposons que I est stable par σ; alors I' l'est aussi. Si f est un élément minimal de I', il est clair que qf l'est aussi et donc F est stable par σ.

Inversement, si F est une réunion de classes cyclotomiques, on applique (12): l'ensemble des majorants de qf est l'ensemble des qs où s est un majorant de f. □

Proposition 5. *Soit une antichaîne F et soit C_e le code affine-invariant défini par F. Soit d le plus petit élément de F. Alors la borne-BCH du code C_e est égale à d; la distance minimale de C_e est au moins égale à $d + 1$.*

Preuve. Par borne-BCH du code C_e, nous entendons borne-BCH du code cyclique C dont C_e est l'extension. Si d est la borne-BCH de C, alors la distance

minimale de C est au moins égale à d. Si le code C_e est affine-invariant, sa distance minimale est au moins égale à $d+1$ [16]. Pour montrer que d est la borne-BCH de C_e, il suffit de montrer que l'intervalle $[0, d[$ est contenu dans l'ensemble de définition I du code C_e.

Soit $s \in [0, d[$; s ne peut pas majorer un élément f de F car sinon on aurait $f \leqslant s < d$ ce qui contredirait le fait que d est le plus petit élément de F. D'aprés (10), on en déduit que $s \in I$. □

Proposition 6. *Soit F une antichaîne de $S_{\ll}$; soient U le code affine-invariant défini par F et soit I l'ensemble de définition de U. Alors l'antichaîne $n-F$ définit le dual $\hat{U}$ de U; en effet l'ensemble $n-F$ est l'ensemble des éléments maximaux de l'ensemble de définition $\hat{I}$ de $\hat{U}$:*

$$\hat{I} = \bigcup_{f \in F} \{s \in S \mid s \ll n-f\}. \tag{13}$$

Preuve. Il est clair que $n-F$ est une antichaîne puisque F est une antichaîne. Un code et son dual ont le même groupe d'automorphismes; donc $\hat{U}$ est un code affine-invariant, et on peut parler de son ensemble de définition. On sait que l'ensemble de définition de $\hat{U}$ est:

$$\hat{I} = \{s \in S \mid n-s \notin I\}. \tag{14}$$

D'après (10) et (11), on obtient (13) car

$$s \in \hat{I} \leftrightarrow n-s \notin I \leftrightarrow \exists f; n-s \gg f \leftrightarrow \exists f; s \ll n-f.$$

Donc, tout élément de $n-F$ est élément maximal de $\hat{I}$. D'autre part, tout élément maximal de $\hat{I}$ est dans $n-F$ car sinon il serait majoré par un élément de $n-F$. □

Corollaire 1. *Les notations sont celles de la Proposition 6. Soit $F(\hat{I})$ la frontière de l'ensemble $\hat{I}$. Alors*

$$F(\hat{I}) = \{n-s \mid s \text{ est un élément maximal de } I\}.$$

Preuve. C'est clair si l'on applique les résultats précédents au dual de $\hat{U}$ qui est justement le code U. □

Remarque. La formule (14) est un résultat classique. On peut la prouver directement dans l'algèbre $\boldsymbol{A}$ [10]. En effet, *tout code de $\boldsymbol{A}$ affine-invariant est le dual de son annulateur.* On montre que $\hat{U}$, défini par (14), est tel que l'idéal produit $U\hat{U}$ est réduit à $\{0\}$.

Exemple 2. $p=3$, $n=3^3-1$, $S=[0, 26]$. Soit l'antichaîne F qui est une classe cyclotomique de 3 modulo 26:

$$F = \{4, 10, 12\} = \{(1\ 1\ 0)(1\ 0\ 1)(0\ 1\ 1)\}.$$

Elle définit le code affine-invariant U, code de $K[G]$ où $K = GF(3)$ et $G = GF(3^3)$, d'ensemble de définition I; I est l'ensemble des éléments de S qui ne majorent pas 4, 10 ou 12:

$$I = \{(0\ 0\ 0)(1\ 0\ 0)(2\ 0\ 0)(0\ 1\ 0)(0\ 2\ 0)(0\ 0\ 1)(0\ 0\ 2)\}$$
$$= \{0, 1, 2, 3, 6, 9, 18\}$$

Le code U est le code BCH étendu de longueur 27 *et de distance construite* 4 *sur* $GF(3)$.

Le dual de U est entièrement défini par l'antichaîne

$$\hat{M} = \{n - f \mid f \in F\} = \{22, 16, 14\} = \{(1\ 1\ 2)(1\ 2\ 1)(2\ 1\ 1)\}.$$

Son ensemble de définition est

$$\hat{I} = \{s \in S \mid s \ll 22 \text{ ou } s \ll 16 \text{ ou } s \ll 14\}$$
$$= \{0, 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 22\}$$

$\hat{M}$ est l'ensemble des éléments maximaux de $\hat{I}$. On peut obtenir la frontière de $\hat{I}$, soit $F(\hat{I})$, avec l'ensemble M des éléments maximaux de I:

$$M = \{(2\ 0\ 0)(0\ 2\ 0)(0\ 0\ 2)\} = \{2, 6, 18\}$$

d'où

$$F(\hat{I}) = \{n - k \mid k \in M\} = \{24, 20, 8\}.$$

4. Idéaux affines-invariants

Nous considérons maintenant les codes affines-invariants comme des idéaux particuliers d'une algèbre de type $\boldsymbol{A}$. Notre but est de montrer que, dans ce contexte aussi, la donnée de la frontière est fondamentale: elle induit une description du code qu'elle définit et donc certaines propriétés structurelles.

Tout idéal U de $\boldsymbol{A}$ est une somme d'idéaux principaux de $\boldsymbol{A}$. Or, de tout système de générateurs de U, on peut extraire un système minimal dont le cardinal est une constante, un paramètre de l'idéal U:

Définition 4. Soit U un idéal de $\boldsymbol{A}$ et soit $x = \{x_1, \ldots, x_k\}$ un sous-ensemble de U. On dit que x est *un système de générateurs de l'idéal* U lorsque

$$U = x_1\boldsymbol{A} + \cdots + x_k\boldsymbol{A}. \tag{15}$$

Dans ce cas, x est *un système minimal de générateurs de* U, (un *SMG* de U), si tout système de générateurs de U a un cardinal supérieur ou égal à k. Nous dirons alors que k est la *taille* de l'idéal U.

L'algèbre $\boldsymbol{A}$ n'étant pas semi-simple, posséde un radical non réduit à $\{0\}$. *Soit P le radical de $\boldsymbol{A}$*; P est le seul idéal maximal de $\boldsymbol{A}$ et est aussi l'ensemble des éléments nilpotents de $\boldsymbol{A}$:

$$P = \left\{ x \in A \;\middle|\; \sum_{g \in G} x_g = 0 \right\}. \tag{16}$$

On peut dire aussi que P est le code de $\boldsymbol{A}$ affine-invariant dont l'ensemble de définition est réduit à $\{0\}$.

La Proposition 7 montre que le radical de $\boldsymbol{A}$ intervient de façon décisive dès que l'on veut exhiber un *SMG* d'un idéal U. Le lecteur trouvera une preuve de cette propriété dans [15]; l'idéal produit PU est l'idéal engendré par les éléments xy où $x \in P$ et $y \in U$.

Proposition 7. *Soit U un idéal de $\boldsymbol{A}$. Etant donné $y \in U$, on note $\bar{y}$ l'image de y dans l'espace-vectoriel quotient U/PU. Alors les assertions suivantes sont équivalentes*:

(i) $x = \{x_1, \ldots, x_k\}$ *est un SMG de U.*

(ii) $\bar{x} = \{\bar{x}_1, \ldots, \bar{x}_k\}$ *est une base de U/PU.*

On suppose que le code U est affine-invariant. Soit F l'antichaîne qui définit le code U (i.e. sa frontière). Nous allons voir maintenant que la seule donnée de F permet de construire un *SMG* de U. En effet, la proposition suivante montre qu'avec F on peut définir le code PU et ainsi utiliser la Proposition 7; le Théorème 3 montre que l'on peut effectivement définir un *SMG* de U, sur la donnée de F et du corps de base du code U – c'est-à-dire de l'algèbre $\boldsymbol{A}$ dans laquelle on se place.

Proposition 8. *Soient U un code de $\boldsymbol{A}$ affine-invariant, I son ensemble de définition et F sa frontière. Alors l'idéal produit PU est un code de $\boldsymbol{A}$ affine-invariant et son ensemble de définition est*:

$$\bar{I} = I \cup F. \tag{17}$$

Preuve. L'idéal PU est un code affine-invariant si et seulement s'il est invariant par les applications $p_{u,0}$ definies par (6). Or les $p_{u,0}$ sont clairement des automorphismes de $\boldsymbol{A}$ et les codes P et U sont eux-même invariants par les $p_{u,0}$. Alors, pour tout $x \in P$ et $y \in U$:

$$p_{u,0}(xy) = p_{u,0}(x)p_{u,0}(y) \text{ d'où } p_{u,0}(xy) \in PU.$$

L'idéal PU, puisqu'il est engendré par les $p_{u,0}(xy)$, est donc affine-invariant et on peut parler de son ensemble de définition. Soit J cet ensemble; nous allons montrer que $J = \bar{I}$, $\bar{I}$ étant donné par (17).

Le code P est l'idéal de $\boldsymbol{A}$ engendré par les éléments du type $X^g - 1$. Donc J est l'ensemble des éléments s de S tels que:

$$\phi_s((X^g - 1)y) = 0, \qquad g \in G, \qquad y \in U. \tag{18}$$

Alors:

$$\phi_s((X^g - 1)y) = \phi_s(X^g y) - \phi_s(y) = \sum_{\substack{i \ll s \\ i \in S}} \binom{s}{i} g^{s-i} \phi_i(y) - \phi_s(y)$$

$$= \sum_{\substack{i \ll s \\ i \neq s}} \binom{s}{i} g^{s-i} \phi_i(y)$$

car

$$\phi_s(X^g y) = \sum_{h \in G} y_h (h+g)^s = \sum_{i=0}^{s} \binom{s}{i} g^{s-i} \phi_i(y)$$

où, d'aprés le Théorème de Lucas, $\binom{s}{i} \equiv 0 \pmod{p} \leftrightarrow i \ll s$ [1].

Si l'on fixe y dans U, l'expression ci-dessus est nulle pour tout g si et seulement si les $\phi_i(y)$ sont nuls. Donc (18) équivaut à:

$$\phi_i(y) = 0, \qquad i \ll s, \qquad i \neq s, \qquad y \in U,$$

ce qui est vérifié si et seulement si s appartient à I ou s appartient à la frontière de I. On en déduit que $J = \bar{I}$. □

Théorème 3. *Soit C_e un code de $\boldsymbol{A}$ affine-invariant, C_e étant l'extension d'un code C de $\boldsymbol{K}(p, m)$. Soit τ le cardinal de la frontière de C_e. On définit un ensemble y de τ mots de C, $y = \{y_0, \ldots, y_{\tau-1}\}$, de la façon suivante:*

y_0 est le polynome générateur du code cyclique C.

$$y_i = Z^i y_0, \qquad i > 0. \tag{19}$$

Soit $y_e = \{y'_0, \ldots, y'_{\tau-1}\}$ l'extension de y dans $\boldsymbol{A}$ (i.e. l'ensemble des mots y_i étendus). Alors la taille de l'idéal C_e est égale à τ et l'ensemble y_e est un SMG du code C_e.

Preuve. Les y_i sont K-linéairement indépendants dans l'algèbre $\boldsymbol{R}$ en tant qu'éléments d'une base de C, la base usuelle des codes cycliques. Les y'_i eux-mêmes sont donc $\boldsymbol{K}$-linéairement indépendants dans $\boldsymbol{A}$.

Soit t le degré du polynôme y_0; soient z une combinaison K-linéaire des y_i et z_e l'extension de z. Par définition de l'extension

$$z = \sum_{i=0}^{\tau-1} \lambda_i y_i \leftrightarrow z_e = \sum_{i=0}^{\tau-1} \lambda_i y'_i.$$

Alors, d'après (19):

$$z = y_0 \sum_{i=0}^{\tau-1} \lambda_i Z^i \text{ et donc } \deg z \leqslant t + (\tau - 1).$$

Soit V le code de $\boldsymbol{K}$ dont l'extension est le code PC_e et soit $v(Z)$ le polynôme générateur de V. On déduit de la Proposition 8 que:

$$\deg v = \deg y_0 + \tau = t + \tau.$$

Donc le polynôme z, qui a un degré inférieur à celui de v, ne peut être un élément de V et, de ce fait, z_e ne peut être un élément du code PC_e. Nous avons ainsi montré que toute combinaison K-linéaire et non identiquement nulle des y_i' est dans l'ensemble $C_e \backslash PC_e$. C'est dire que les classes des y_i', modulo PC_e, constituent un système libre du K-espace vectoriel quotient C_e/PC_e; il s'agit même d'une base de cet espace, car, d'après la Proposition 8: $\dim C_e = \dim PC_e + \tau$. On applique alors la Proposition 7: y_e est un *SMG* de l'idéal C_e. □

Remarque. En fait, y_i' est l'image de y_0' par l'automorphisme $p_{\alpha^i,0}$ (α étant une racine primitive du corps G). On obtient ainsi une formulation précise dans $\boldsymbol{A}$: *Soit x l'extension du polynôme générateur du code C. Alors l'ensemble*

$$\{x, p_{\alpha,0}(x), \ldots, p_{\alpha^{\tau-1},0}(x)\} \tag{20}$$

est un SMG du code C_e.

Exemple 3. $K = G = GF(2^8)$. Le code C est le code de Reed–Solomon (255, 223, 33); le code C_e est donc un code (256, 223, 34) d'ensemble de définition $T_e = [0, 33[$. Nous montrons plus loin comment calculer la frontière d'un code RS étendu (cf. Théorème 5 et Exemple 4); ici nous avons:

$$F(T_e) = \{33 = 2^5 + 1, 2^5 + 2, 2^5 + 2^2, 2^5 + 2^3, 2^5 + 2^4, 2^6, 2^7\}.$$

La taille de C_e est égale à $7 - C_e = \boldsymbol{A}y_0' + \cdots + \boldsymbol{A}y_7'$ – et l'on construit les y_i' avec le polynôme générateur de C: $y_0 = \prod_{k \in [1,33[} (Z - \alpha^k)$.

Soient, $y_0 = \sum_{j=0}^{32} a_j Z^j$ et $a = -\sum_{j=0}^{32} a_j$. Alors:

$$y_i = \sum_{j=0}^{32} a_j Z^{i+j} \quad \text{et} \quad y_i' = aX^0 + \sum_{j=0}^{32} a_j X^{\alpha^{i+j}}.$$

Un idéal de $\boldsymbol{A}$ qui n'a qu'un seul générateur est un idéal principal. D'où:

Corollaire 2. *Un code de* $\boldsymbol{A}$ *affine-invariant est un idéal principal si et seulement si sa taille est égale à* 1.

Nous allons maintenant étudier un ensemble d'idéaux de $\boldsymbol{A}$ dont la structure est une généralisation de la structure d'idéal principal. Pour cela, nous devons rappeler certaines propriétés des idéaux de $\boldsymbol{A}$; pour plus de détails, le lecteur peut consulter [5, Ch. 1 à 3]. Soit P^j la puissance j-ième du radical P de $\boldsymbol{A}$. L'index de nilpotence de P est égal à $m(p-1)$. La suite des P^j, $j \in [1, m(p-1)]$,

réalise une filtration de l'idéal P; chaque élément x et chaque idéal U de $\boldsymbol{A}$ est situé dans cette filtration par un paramètre appelé *profondeur*:

$$\text{prof}(x) = j \leftrightarrow x \in P^j \text{ et } x \notin P^{j+1}$$

$$\text{prof}(U) = j \leftrightarrow U \subset P^j \text{ et } U \not\subset P^{j+1}$$

La définition du paramètre "profondeur" induit une classification intéréssante des idéaux de $\boldsymbol{A}$ (cf. [5] et [17]). S'agissant des codes affines-invariants, cet intérêt est renforcé par le fait que les P^j sont eux-mêmes des codes affines-invariants importants: P^j est le code de Reed et Muller p-aire d'ordre $m-j$ [2], [6]. Sa frontière est facilement obtenue, étant donnée la forme de son ensemble de définition. Soit T_j cet ensemble; on le construit avec les différents rangs des éléments de S. Le *rang* de $s \in S$ (cf. Definition 2), est couramment appelé *p-poids de s* en Théorie des Codes et noté $\omega_p(s)$.

$$T_j = \{s \in S \mid \omega_p(s) < j\}. \tag{21}$$

Proposition 9. *Soient* $j \in [1, m(p-1)]$ *et soit l'antichaîne de* $S_{\ll}$:

$$F_j = \{s \in S \mid \omega_p(s) = j\}. \tag{22}$$

Alors F_j *est la frontière du code GRM p-aire d'ordre* $m-j$, *c'est-à-dire de l'idéal* P^j. *La taille de* P^j *est égale au nombre d'eléments de S ayant un p-poids égal à j.*

Preuve. Elle se déduit immédiatement de la définition de la frontière d'un code: un élément de F_j est un élément s tel que $\omega_p(s) \geqslant j$ et dont tous les descendants ont un p-poids strictement inférieur à j. □

Soit (x), l'idéal principal de $\boldsymbol{A}$ engendré par l'élément x. Un générateur de (x) est un élément λx où λ est une unité de $\boldsymbol{A}$ (i.e. $\lambda \notin P$). *Les générateurs de* (x) *sont les éléments de* (x) *qui ont la même profondeur que x.* Soit maintenant un idéal U quelconque de $\boldsymbol{A}$. On peut toujours construire un *SMG* de U dont les éléments ont tous la même profondeur, celle de U (cf. Théorème 3 pour les codes affines-invariants). Mais certains idéaux sont tels que tous leurs *SMG* ont cette propriété. Ces idéaux sont dits *à type de profondeur constante* (*idéaux tpc*) [15]. La structure d'idéal *tpc* est, comme le montre la Proposition 10, déterminée par une propriété de l'idéal PU; mais, dans le cas des codes affines-invariants, il s'agit d'une propriété de l'antichaîne définissant le code (cf. Théorème 4). En fait, c'est le cardinal seul de la frontière qui intervient dans le Théorème 3; mais la frontière nous renseigne aussi sur la situation du code dans la filtration P^j: elle permet d'abord de connaître la profondeur du code qu'elle définit:

Lemme 1. *Soit F une antichaîne de* $S_{\ll}$ *et soit U le code qu'elle définit. Alors*

$$\text{prof}(U) = \min\{\omega_p(s) \mid s \in F\}. \tag{23}$$

Preuve. Soit j la profondeur de U et soit I l'ensemble de définition de U. Par définition de la profondeur et T_j étant donné par (21), nous avons:

$$\text{prof}(U) = j \leftrightarrow T_j \subset I \text{ et } T^{j+1} \not\subset I.$$

Donc, si $\text{prof}(U) = j$, tout élément de F a un p-poids supèrieur ou égal à j, car $F \not\subset I$; d'autre part, il existe $s \notin I$ tel que $\omega_p(s) = j$. Or $s \in F$ car tous les descendants de s ont un poids strictement inférieur à j et sont donc dans I: (23) est vérifié. □

Proposition 10. *Soit U un idéal de $\boldsymbol{A}$ de profondeur j. Alors U est un idéal à type de profondeur constant si et seulement si*

$$PU = P^{j+1} \cap U. \tag{24}$$

Preuve. Soit $x = \{x_1, \ldots, x_k\}$ un *SMG* de U. Les x_i n'appartiennent pas à l'idéal PU, d'aprés la Proposition 7. Si (24) est vérifiée, les x_i ont donc la même profondeur. Inversement supposons que tout *SMG* x de U est composé d'éléments de même profondeur j. Alors toute base du K-espace U/PU est composée de classes d'éléments de $\boldsymbol{A}$ de profondeur j. Ceci implique que tout élément de l'ensemble $U \backslash PU$ est de profondeur j. □

Théorème 4. *Soit U un code affine-invariant, soit $j = \text{prof}(U)$ et soit F la frontière de U. Alors U est un idéal à type de profondeur constant (un idéal tpc) si et seulement si tous les éléments de F ont un p-poids égal à j.*

Preuve. Soit I l'ensemble de définition de U. Le code $U \cap P^{j+1}$ est affine-invariant puisque les codes U et P^{j+1} le sont aussi; son ensemble de définition est:

$$J = I \cup \{s \in S \backslash I \mid \omega_p(s) = j\}. \tag{25}$$

En effet, le polynôme générateur de l'intersection de deux codes cycliques est le plus petit commun multiple des polynômes générateurs des codes concernés. On en déduit que l'ensemble de définition du code $U \cap P^{j+1}$ est égale à $I \cup T_{j+1}$. Mais U est de profondeur j, d'où $T_j \subset I$. Donc, les seuls éléments rajoutés à I sont ceux dont le p-poids est égal à j.

Supposons d'abord que tous les éléments de F ont le même p-poids égal à j. Soit $s \in S$ tel que $\omega_p(s) = j$. Si $s \notin F$ alors s est irrelaté avec chacun des éléments de F, ayant le même poids qu'eux; donc $s \in I$. On en déduit l'égalité $\bar{I} = J$ où J est donné par (25) et $\bar{I}$ par (17). Donc les codes PU et $P^{j+1} \cap U$, ayant le même ensemble de définition, sont égaux. D'aprés la Proposition 10, U est *tpc*.

Inversement, supposons que $\bar{I} = J$ c'est-à-dire que

$$I \cup F = I \cup \{s \in S \mid \omega_p(s) = j\}.$$

Si $s \in F$ alors $s \notin I$ et donc $\omega_p(s) = j$. □

d	Frontière	
1	1 2 4 8 16 32	*tpc*
3	3 5 6 9 10 12 17 18 20 24 33 34 36 40 48	*tpc*
5	5 9 10 17 18 20 34 36 40	*tpc*
7	7 9 14 18 21 28 35 36 42 49 56	
9	9 18 21 36 42	
11	11 13 19 21 22 25 26 37 38 41 42 44 50 52	*tpc*
13	13 19 21 26 38 41 42 52	*tpc*
15	15 21 27 30 39 42 45 51 54 57 60	
21	21 27 42 45 54	
23	23 27 29 43 45 46 53 54 58	*tpc*
27	27 45 54	*tpc*
31	31 47 55 59 61 62	*tpc*

Fig. 1. Frontières des codes BCH binaires de longueur 64 et de distance construite d. Ceux qui ont pour extension un idéal *tpc* sont signalés.

Dans le contexte de cet article, l'intérêt premier des idéaux *tpc* est que de nombreux codes affines-invariants sont *tpc*. Nous avons énuméré dans [9] les codes de Reed–Solomon *tpc*; nous avons aussi caractérisé les paramètres des codes affines-invariants principaux [8]; la Fig. 1 donne une exemple des résultats obtenus avec un calculateur: plusieurs codes BCH sont *tpc* dans chaque classe étudiée. Enfin, la Proposition 9 montre que les codes GRM p-aires sont *tpc*; les codes *tpc* sont définis par des antichaînes particulières dites *de rang constant.* Il est clair que l'antichaîne formée de tous les éléments de S ayant un même p-poids est maximale et donc:

Corollaire 3. *Les codes GRM p-aires sont définis par les antichaînes maximales de rang constant.*

5. La taille des codes affines-invariants: le théorème de Griggs

Nous avons montré qu'une antichaîne F a pour cardinal la taille de l'idéal qu'elle définit; on cherche donc très naturellement à classifier les codes affines-invariants suivant leur taille en utilisant certaines propriétés des antichaînes de $S_{\ll}$. Une illustration simple de cette démarche est obtenue lorsque l'on s'intéresse aux codes affines-invariants de l'algèbre $\boldsymbol{A} = K[G]$ où $K = GF(p)$ et $G = GF(p^m)$, m premier. L'ensemble de ces codes et l'ensemble des antichaînes de $S_{\ll}$, qui sont une réunion de classe cyclotomiques de p, sont en bijection. On en déduit donc, du fait que m est premier, que *chaque code de* $\boldsymbol{A}$ *affine-invariant a pour taille un multiple de m* (mis à part l'idéal $P^{m(p-1)}$, seul idéal minimal de $\boldsymbol{A}$, qui a une taille égale à 1).

Les résultats que nous donnons maintenant utilisent les calculs explicites des frontières des codes RS (Théorème 5) et des codes GRM p-aires pour ébaucher

une évaluation globale de la taille des codes affines-invariants. Nous faisons apparaître que les codes RS nécessitent peu de générateurs, alors que certains des codes GRM sur $GF(p)$ (i.e. certains codes P^j) ont les plus grands *SMG*. La démonstration s'appuie sur les travaux de Griggs, eux-mêmes fondés sur les travaux de Sperner et de De Bruijn [11, 12]; nous obtenons ainsi la valeur maximale que peut prendre le cardinal d'un *SMG* d'un code affine-invariant d'une longueur donnée.

Théorème 5. *$n = p^m - 1$ et $S = [0, n]$; soit $d \in S$, $d = (d_0, \ldots, d_{m-1})$. Soit*

$$\nu = \min\{k \in [0, m-1] \mid d_k \neq 0\}. \tag{26}$$

Soient aussi

$$d(k) = (d_k + 1)p^k + \sum_{i=k+1}^{m-1} d_i p^i, \qquad k \in [0, m-1[$$

$$d(m-1) = (d_{m-1} + 1)p^{m-1}. \tag{27}$$

Alors la frontière de l'intervalle $[0, d[$, c'est-à-dire de l'extension du code de Reed–Solomon de distance d et de longueur n, est:

$$F(d) = \{d\} \cup \{d(k) \mid k \in]\nu, m-1],\ d_k < p-1\}. \tag{28}$$

Preuve. D'abord les éléments de $F(d)$ sont supérieurs à d et croissants suivant la valeur de k car

$$d(k) - d = p^k - \sum_{l=0}^{k-1} p^l d_l \quad \text{et} \quad d(k+1) - d(k) = p^{k+1} - p^k.$$

Donc $F(d) \subset [d, n]$ et tout majorant d'un élément de $F(d)$ est dans $[d, n]$. Soient $d(k) \in F(d)$ et $d(j) \in F(d)$ avec $k < j$. Nous avons:

$$d = (0, \ldots, d_\nu, \ldots, d_k, \ldots, d_j, \ldots, d_{m-1})$$
$$d(k) = (0, \ldots, 0, \ldots, d_k + 1, \ldots, d_j, \ldots, d_{m-1})$$
$$d(j) = (0, \ldots, 0, \ldots, 0, \ldots, d_j + 1, \ldots, d_{m-1})$$

Clairement ces trois éléments sont deux à deux irrelatés, car, à l'indice ν, le coefficient de d est strictement supérieur aux autres, alors qu'à l'indice k, ou j, c'est le coefficient de $d(k)$, ou de $d(j)$, qui est strictement supérieur aux autres. On en déduit que $F(d)$ est une antichaîne.

Pour montrer que $F(d)$ est la frontière de $[0, d[$ il reste à prouver que tout élément de $[d, n]$ majore un élément de $F(d)$.

Soit $s > d$, $s = (s_0, \ldots, s_{m-1})$. Soit k le plus grand indice tel que $s_k > d_k$; l'indice k existe bien, car s est strictement supérieur à d et, pour cette même raison, tous les s_j suivants sont égaux aux d_j correspondants:

$$s = (s_0, \ldots, s_k, d_{k+1}, \ldots, d_{m-1}).$$

On en déduit immédiatement:

si $k \leqslant v$, alors s majore d

si $k > v$, alors s majore $d(k)$.

Donc s est un majorant d'un élément de $F(d)$ et, avec ce qui précède, nous avons prouvé que $[0, d[$ est l'ensemble des non majorants de $F(d)$. □

Ainsi l'écriture de d dans la base p nous fournit immédiatement la frontière de $[0, d[$ et, donc, le nombre de générateurs nécessaires pour le code RS de distance d; l'exemple suivant montre comment s'effectue le calcul. Le Théorème 5 prouve aussi que la taille d'un RS-code étendu est réduite:

Corollaire 4. *La taille d'un code de Reed–Solomon étendu de longueur p^m est inférieure ou égale à m.*

Exemple 4. Nous reprenons le calcul de la frontière du code de Reed–Solomon (255, 223, 33) de l'Exemple 3 – on peut remarquer qu'il s'agit d'un code RS *tpc*. Nous avons:

$$d = 33 = (1\ 0\ 0\ 0\ 0\ 1\ 0\ 0).$$

Ici v est le premier indice, l'indice 0; comme c'est toujours le cas en caractéristique 2, le nombre d'éléments-frontière est égal au nombre de 0 à droite à partir de v augmenté de 1. On obtient les 7 éléments annoncés, c'est-à-dire en plus de d:

$$d(1) = (0\ 1\ 0\ 0\ 0\ 1\ 0\ 0) = 34$$

$$d(2) = (0\ 0\ 1\ 0\ 0\ 1\ 0\ 0) = 36$$

$$d(3) = (0\ 0\ 0\ 1\ 0\ 1\ 0\ 0) = 40$$

$$d(4) = (0\ 0\ 0\ 0\ 1\ 1\ 0\ 0) = 48$$

$$d(6) = (0\ 0\ 0\ 0\ 0\ 0\ 1\ 0) = 64$$

$$d(7) = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 1) = 128.$$

Théorème 6. *Soit U un code de $\mathbf{A}$ affine-invariant et soit $t(U)$ la taille de U. On désigne par μ le rang moyen (ou le p-poids moyen) dans S:*

$$\mu = \left\lceil \frac{m(p-1)}{2} \right\rceil.$$

On désigne par F_j, $j \in [1, m(p-1)]$, l'antichaîne maximale de rang constant j de $S_{\ll}$. Alors les deux propriétés suivantes sont vérifiées:

(i) $t(U) \leqslant |F_\mu|$.

(ii) *Si* $t(U) = |F_\mu|$ *alors le code* U *est un code GRM déterminé comme suit*:

$$m(p-1) \text{ est pair} \rightarrow U = P^\mu$$

$$m(p-1) \text{ est impair} \rightarrow U = P^\mu \text{ ou } U = P^{\mu+1}.$$

Preuve. Ce résultat est un Corollaire d'un Théorème de J.R. Griggs caractérisant les antichaînes d'un produit de chaînes quelconque dont le cardinal est le plus élevé.

(i) La taille de U est égale à la taille d'une antichaîne contenue dans S. D'après le Théorème de Griggs, elle est majorée par la taille de F_μ; si $m(p-1)$ est pair, F_μ est la seule antichaîne dans S dont la taille est maximale; lorsque $m(p-1)$ est impair, deux antichaînes ont la taille maximale: F_μ et $F_{\mu+1}$.

(ii) La taille de U est la taille de la frontière de U; d'après la Proposition 9, les antichaînes F_μ et $F_{\mu+1}$ sont justement les frontières respectives des codes P^μ et $P^{\mu+1}$; chaque antichaîne est la frontière d'un et un seul code affine-invariant; un code qui a la taille maximale est donc le code GRM défini par F_μ (si $m(p-1)$ est pair) ou par F_μ ou $F_{\mu+1}$ (si $m(p-1)$ est impair). □

La Fig. 2 donne la taille de S, $W(S) = |F_\mu|$, lorsque les codes considérés ont un longueur inférieure à 5000. Le calcul de $W(S)$ est un élément du calcul de la dimension des codes GRM, pour lequel on trouve un algorithme dans [5] ou [14]. Signalons toutefois un cas où le calcul est particulièrement simple: lorsque $m = 2$, $W(S)$ est égal au nombre de couples (i, j) tels que $i + j = p - 1$ c'est-à-dire à p.

Lorsque $p = 2$ et m est impair, le code $P^{\mu+1}$ est le code de Reed et Muller autodual de longueur 2^m.

p	m	N	$W(S)$	p	m	N	$W(S)$
2	2	4	2	3	6	729	141
2	3	8	3	3	7	2187	393
2	4	16	6	5	2	25	5
2	5	32	10	5	3	125	19
2	6	64	20	5	4	625	85
2	7	128	35	5	5	3125	381
2	8	256	70	7	2	49	7
2	9	512	126	7	3	343	37
2	10	1024	252	7	4	2401	231
2	11	2048	462	11	2	121	11
2	12	4096	924	11	3	1331	91
3	2	9	3	13	2	169	13
3	3	27	7	13	3	2197	127
3	4	81	19	17	2	289	17
3	5	243	51	17	3	4913	217

Fig. 2. La taille maximale, $W(S)$, des codes affines-invariants de longueur $N = p^m$ (pour $N < 5000$).

Les résultats donnés dans la Fig. 2 montrent que la taille $W(S)$ est en général bien plus élevée que m, c'est-à-dire que, si l'on interprète le Corollaire 4, la taille d'un code RS est très réduite par rapport à la taille maximale.

Remerciements

Je remercie P. Camion (CNRS, France) et J. Constantin (Université de Sherbrooke, Québec) dont les conseils et les suggestions ont amélioré ce travail.

Bibliographie

[1] E. Berlekamp, Algebraic Coding Theory (McGraw Hill, New York).
[2] S.D. Berman, On the theory of group codes, Kibernetica, 1, 1 (1967) 31–39.
[3] 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).
[4] P. Camion, Etude de codes binaires abéliens modulaires autoduaux de petites longueurs, Revue Cethedec, NS 79-2 (1979) 3–24.
[5] P. Charpin, Codes idéaux de certaines algèbres modulaires, Thèse de 3ième cycle (Université de Paris VII, 1982).
[6] P. Charpin, Puissance du radical d'une algèbre modulaire et codes cycliques, Revue du Cethedec, 18ième année, NS81-2, 35–43.
[7] P. Charpin, The extended Reed–Solomon codes considered as ideals of a modular algebra, Annals Discrete Mathemat. 17 (1983) 171–176.
[8] P. Charpin, Codes cycliques étendus et idéaux principaux d'une algèbre modulaire, C.R. Acad. Sci. Paris, t. 295, série I (Septembre 1982) 313–315.
[9] P. Charpin, A description of some extended cyclic codes with application to Reed–Solomon codes, Discrete Mathemat. 56 (1985) 117–124.
[10] P. Charpin, Codes cycliques étendus invariants sous le groupe affine, Thèse de Doctorat d'Etat (Publications du LITP, 1987).
[11] N. de Bruijn, C.A. van Ebbenhorst Tengbergen and D.R. Kruyswijk, On the set of divisors of a number, Nieuw Arch. Wisk., 23 (1952) 191–193.
[12] J.R. Griggs, Maximum antichains in the product of chains, Order 1 (1984) 21–28.
[13] T. Kasami, S. Lin and W.W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, Info. and Control 11 (1967) 475–496.
[14] T. Kasami, S. Lin and W.W. Peterson, New generalisations of the Reed–Muller codes, IEEE Trans. Info. Theory II-14 (1968) 189–199.
[15] F. Laubie, Codes idéaux de certaines algèbres modulaires et Ramification, Communications in Algebra 15(5) (1987) 1001–1006.
[16] F.J. Mac Williams and N.J.A. Sloane, The Theory of Error Correcting Codes (North Holland 1977).
[17] A. Poli, Codes dans certaines algèbres modulaires, Thèse de Doctorat d'Etat Univ. P. Sabatier (Toulouse 1978).
[18] 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 t. 290 (1980).
[19] A. Poli, Idéaux principaux nilpotents de dimension maximale dans l'algèbre $F_q[G]$ d'un groupe abélien fini G, Communications in Algebra 12(4) (1984) 391–401.
[20] J.H. van Lint, Coding Theory (Springer Verlag, New York 1971).