

CAHIERS DU BURO

PASCALE CHARPIN

Étude sur la valuation des H -codes binaires

Cahiers du Bureau universitaire de recherche opérationnelle.

Série Recherche, tome 41 (1983), p. 3-54

http://www.numdam.org/item?id=BURO_1983__41__3_0

© Institut Henri Poincaré — Institut de statistique de l'université de Paris, 1983, tous droits réservés.

L'accès aux archives de la revue « Cahiers du Bureau universitaire de recherche opérationnelle. Série Recherche » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

ÉTUDE SUR LA VALUATION DES H-CODES BINAIRES

Pascale CHARPIN

Résumé

Ce travail fait suite à l'article de P. CAMION [5] sur les codes idéaux principaux de l'algèbre H_2G où G est un 2-groupe abélien élémentaire. Notre principal résultat est que cette classe de codes ne satisfait pas à la borne de GIBERT-VARSĦAMOV ; nous énumérons les codes extrémaux et caractérisons leurs générateurs.

Abstract

This paper follows up P. CAMION's contribution [5] on the self-dual codes which are principal ideals of the algebra H_2G , where G is a 2-elementary abelian group. Our main result is that this class does not meet the GIBERT-VARSĦAMOV bound ; we enumerate the extremal codes and characterize their generators.

ÉTUDE SUR LA VALUATION DES H-CODES BINAIRES

Pascale CHARPIN*

1. INTRODUCTION

Les H-codes binaires ont été introduits par P. CAMION dans [5]. Il s'agit d'une classe de codes autoduaux à poids multiples de 2 ou 4 qui sont des idéaux principaux d'une algèbre modulaire A de 2-groupe abélien. Ultérieurement A. POLI et M. VENTOU montrent que tout idéal principal autodual de A est un H-code. L'étude sur une extension de F_2 est poursuivie par P. CAMION, G. PASQUIER et J. WOLFMANN [14]. Elle fournit une nouvelle méthode de construction de codes autoduaux binaires ; ceci permet une autre définition du code de GOLAY (24,12,8) [17] et la mise en évidence d'un code autodual (64,32,12) à poids multiples de 4 [6] (seul code de ce type connu à présent).

Un des objectifs de ces travaux est de déterminer une classe de codes autoduaux binaires à poids multiples de 2 ou de 4 ayant des valuations intéressantes. Ce contexte est défini dans l'ouvrage de F.J. MAC WILLIAMS et N.J.A. SLOANE [13, ch.19].

Dans [5], P. CAMION montre qu'un nombre important de H-codes de longueur 32 sont extrémaux et pose le problème de la valuation des H-codes de longueur supérieure.

Nous donnons (§2) les propriétés et définitions nécessaires à la compréhension du texte. La caractérisation des générateurs de H-codes (§3) est largement utilisée ensuite. Nous démontrons (§4)

* Institut de programmation. Université P. et M. Curie.

que la classe des H-codes est asymptotiquement mauvaise et qu'un H-code de longueur supérieure à 32 ne peut être extrémal. Nous dénombrons les H-codes extrémaux de longueur 32 et nous montrons que leur existence est liée à celle des ensembles à différences sur F_{16} (§6). Nous exposons quelques résultats pratiques sur la valuation des H-codes (§5 et §7).

2. TERMINOLOGIE, NOTATIONS, RAPPELS

Lorsque nous parlons de codes, il s'agit toujours de codes linéaires, ici sous-espaces d'un espace vectoriel fini sur F_2 . Un code autodual est un code identique à son complémentaire orthogonal. La distance utilisée est toujours celle de Hamming qui induit la distance minimale ou valuation du code. Un code autodual à poids multiples de 2 ou de 4 a une valuation inférieure à une valeur fonction de sa longueur (cf. [13], p. 629) ; si cette valeur est atteinte le code est dit extrémal. Le comportement asymptotique d'une classe de codes est l'évolution du rapport valuation sur longueur lorsque la longueur tend vers l'infini [13].

L'exposé fait suite à l'article de P. CAMION [5] dont nous avons conservé les principales notations :

- G est le groupe additif $(F_2, +)$; la structure de F_2 -espace vectoriel de G est en général utilisée.

- Nous notons A ou F_2G l'algèbre modulaire de 2-groupe abélien G . A est l'ensemble des polynômes :

$$A = \{ \sum_{g \in G} x_g x^g \mid x_g \in F_2 \}$$

A est munie en tant qu'algèbre des opérations usuelles de multiplication et addition de polynômes.

$$(h \in G, g \in G : x^g x^h = x^{g+h})$$

- H désigne un hyperplan de G que nous identifions à $(F_{2^{m-1}}, +)$ ce qui justifie la notation $F_2 H$.

- Le support d'un mot de A est l'ensemble,

$$x \in A, x = \sum_{g \in G} x_g x^g \quad s(x) = \{g \mid x_g \neq 0\} \quad (1)$$

- Le poids d'un mot de A est le cardinal de son support :

$$\omega(x) = |s(x)|. \quad (2)$$

Rappelons [4] que le radical d'un anneau est l'intersection de tous ses idéaux maximaux. Le produit IJ de deux idéaux I et J d'un même anneau est l'idéal engendré par l'ensemble :

$$\{ij \mid i \in I, j \in J\}.$$

L'annulateur d'un idéal I de A est l'ensemble : [4]

$$\text{Ann } I = \{x \in A \mid y \in I \Rightarrow xy = 0\}. \quad (3)$$

Dans A , l'annulateur d'un idéal est égal au complémentaire orthogonal de cet idéal [12].

Soit x un élément de A , nous notons (x) l'idéal principal engendré par x dans A .

2.1 Propriétés de l'algèbre A [12]

Un élément x de A est soit nilpotent soit une unité de A ; en effet :

$$x^2 = \left(\sum_{g \in G} x_g x^g \right)^2 = \sum_{g \in G} x_g^2 x^{2g} = \left(\sum_{g \in G} x_g \right) x^0$$

(A est de caractéristique 2).

On en déduit les propriétés :

Propriété 1 : L'algèbre A possède un seul idéal maximal P qui est son radical et l'ensemble de ses éléments nilpotents :

$$P = \{x \in A \mid x^2 = 0\} \quad (4)$$

Remarque : $x^2 = 0 \Leftrightarrow \sum_{g \in G} x_g = 0$

$\Leftrightarrow x$ est de poids pair .

Propriété 2 : Un idéal principal de A est contenu dans son annulateur.

Soit $\{e_1, \dots, e_k\}$ un ensemble de k vecteurs libres du F_2 -espace vectoriel G et soit x l'élément de A dont le support est le sous-espace V de G engendré par cet ensemble. Alors :

$$x = \sum_{g \in V} x^g = \prod_{i=1}^k (X^{e_i} - 1) . \quad (5)$$

Les éléments de A du type de x jouent un rôle important dans la définition des puissances P^j du radical de A :

Proposition 1 : Soit $e = \{e_1, \dots, e_m\}$ une base de G . Alors l'ensemble ,

$$B(e) = \left\{ \prod_{k=1}^m (X^{e_k} - 1)^{i_k} \mid i_k = 0 \text{ ou } 1 \right\} \quad (6)$$

est une base de A. Pour chaque j ($j \in \{1, m\}$) l'ensemble,

$$B^j(e) = \{ \prod_{k=1}^m (x^{e_k} - 1)^{i_k} \mid i_k = 0 \text{ ou } 1, \sum_{k=1}^m i_k \geq j \} \quad (7)$$

est une base de P^j .

Cette proposition permet de montrer [12] :

- $P^{m+1} = \{0\}$
- P^m est le seul idéal minimal de A . Il est de dimension 1 et engendré par le vecteur : $\prod_{i=1}^m (x^{e_i} - 1)$.
- $\text{Ann } P^j = P^{m-j+1}$.

' Nous dirons que $P^j \setminus P^{j+1}$ est l'ensemble des éléments de profondeur j de A .

Définition 1 : Soit V une variété linéaire du F_2 -espace G .

Soit $y \in A$, $y = \sum_{g \in G} y_g x^g$.

La restriction de y à V est l'élément $y' = \sum_{g \in V} y_g x^g$.

y est une unité sur V si y' est une unité de A .

y est nilpotent sur V si y' est un élément de P .

Proposition 2 : L'ensemble $P^j \setminus P^{j+1}$ est l'ensemble des éléments y de A vérifiant :

(1) Pour tout sous espace V de dimension $m-j+1$ de G , y est nilpotent (de poids pair) sur V et ses translatés.

(2) Il existe un sous-espace W de G de dimension $m-j$ tel que y est une unité (de poids impair) sur W et ses translatés.

Cette proposition est obtenue à l'aide du Lemme suivant que nous utiliserons ultérieurement :

Lemme 1 : Soit V un sous-espace de G et $x = \sum_{g \in V} x^g$.

Soit $V' = V + h$ un translaté de V .

Soit $y \in A$ et y' la restriction de y à V .

Alors,

y est une unité sur V' si et seulement si : le produit xy' est non nul et dans ce cas : $xy' = x^h x$.

Rappelons enfin que les puissances du radical de A sont les codes de Reed et Muller ([2] et [12]). Donc, P^{m-1} est l'ensemble des éléments de A du type (5) où V a pour dimension $m-1$ ou m (cf. dans [13] : le code de Reed et Muller d'ordre 1). On en déduit :

Propriété 3 : Soit $x \in P^j \setminus P^{j+1}$ où $j < m$. Alors l'idéal principal (x) de A contient un élément dont le support est un hyperplan de G .

2.2 Les H-codes

Définition 2 : [5]

Soit $x \in P$; $x = \sum_{g \in G} x_g x^g$.

S'il existe un hyperplan h du F_2 -espace vectoriel G tel que $\sum_{g \in h} x_g = 1$, on dit alors que l'idéal principal de A engendré par

x est un H-code de A .

Propriétés :

1) Le sous-ensemble de A, $\{X^g x \mid g \in H\}$, est une base du H-code (x) [5] .

Ceci prouve que la dimension de (x) est égale à 2^{m-1} . Or (x) contient son annulateur. Donc le code (x) est autodual.

2) Matrice génératrice d'un H-code [5] .

Soit $x \in A$ et soit I un sous-ensemble de G tel que l'ensemble $\{X^g x \mid g \in I\}$ est une base de l'idéal (x) . Nous désignons par M_x la matrice génératrice du code (x) : chaque ligne de la matrice M_x est un vecteur $X^g x$, $g \in I$, exprimé par ses coordonnées dans la base canonique de A . Lorsque (x) est un H-code, il existe un générateur y de (x) qui s'écrit :

$$y = 1 + X^h x', h \notin H, x' \text{ est une unité de } F_2 H . \quad (8)$$

En conséquence, la matrice génératrice d'un H-code (x) est :

$$M_x = \left(\begin{array}{ccc|ccc} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & \ddots & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{array} \quad M_{x'} \right) \quad (9)$$

où $M_{x'}$ est la matrice génératrice de x' dans $F_2 H$ ($M_{x'}$ est de rang égal à 2^{m-1} puisque x' est une unité de $F_2 H$).

Définir la matrice génératrice d'un H-code de longueur 2^m , c'est se donner une unité de $F_2 H$ avec $H \simeq (F_{2^{m-1}}, +)$.

Soit un H-code (x) , où x est donné par (8) et M_x par (9) . Nous noterons comme suit un mot de (x) :

$$y \in (x) \Leftrightarrow y = (u, u x'), u \in F_2 H \quad (10)$$

Le poids d'un mot de (x) est :

$$\omega(y) = \omega(u, u x') = \omega(u) + \omega(ux') \quad (11)$$

Le code (x) vérifie la propriété suivante :

$$(u, u x') \in (x) \Leftrightarrow (u x', u) \in (x) \quad (12)$$

car
$$y = (u, u x') \Leftrightarrow x' y = (u x', u)$$

3) Soit (x) un H-code de $F_2 G$; (x) est un code à poids multiples de 4 si et seulement si le poids de x est un multiple de 4 [5].

4) L'ensemble des H-codes de l'algèbre $F_2 G$ est l'ensemble des idéaux principaux de $F_2 G$ engendrés par un élément de profondeur 1 ([5] et [12, Ch. III]) qui est lui-même l'ensemble des idéaux principaux autoduals de $F_2 G$ [15] .

$$(x) \text{ est un H-code} \Leftrightarrow x \in P \setminus P^2 \Leftrightarrow \dim(x) = 2^{m-1} \quad (13)$$

3. AUTRES DEFINITIONS POUR LE GENERATEUR D'UN H-CODE

Soit $e = \{e_1, \dots, e_m\}$ une base de G et soit H l'hyperplan de G engendré par l'ensemble $\{e_1, \dots, e_{m-1}\}$.

Soit (x) un H-code de $F_2 G$. L'expression de x suivant la base $B(e)$, donnée par (6), est :

$$x = \sum_{i=1}^m a_i (X^{e_i} - 1) + y, y \in P^2, a_i \in F_2 \text{ et } \underline{a_m \neq 0} \quad (14)$$

En effet, x est une unité sur H et sur le complémentaire de H , ceci par définition. On obtient, en appliquant le Lemme 1 :

$$(X^{e_1} - 1) \dots (X^{e_{m-1}} - 1) x = \prod_{i=1}^m (X^{e_i} - 1) .$$

Ceci signifie que si l'on exprime x avec la base $B(e)$, le coefficient de $(X^{e_m} - 1)$ dans cette expression est non nul.

Proposition 2

Soit (x) un H-code de $F_2 \in G$. Alors :

(I) il existe $g, g \in G \setminus H$, et un générateur y de (x) qui a la forme suivante :

$$y = (X^g - 1) + x' , \underline{x' \in P \setminus P^2} \text{ et } s(x') \subset H \quad (15)$$

(II) il existe $g, g \in G \setminus H$, et un générateur y de (x) qui a la forme suivante :

$$y = (X^g - 1) + x' , \underline{x' \in P^2} \text{ et } s(x') \subset H \quad (16)$$

(La notation $s(x') \subset H$ signifie que le support de x' est dans H et en ce sens x' est un élément de l'algèbre $F_2 F_{2^{m-1}}$ notée aussi $F_2 H$).

Preuve

Soit (x) un H-code de $F_2 \in G$ et soit $e = \{e_1, \dots, e_m\}$, une base de G telle que l'ensemble $\{e_1, \dots, e_{m-1}\}$ est une base de H . L'élément x est exprimé par (14) dans la base $B(e)$. On peut donc écrire :

$$x = (X^{e_m} - 1) z + a , z \in A \setminus P , a \in P \quad (I)$$

où z et a sont sans facteurs $(X^{e_m} - 1)$ ($s(z) \subset H$ et $s(a) \subset H$).

Le produit $z \cdot x$ est aussi un générateur y de $\langle x \rangle$:

$$y = (X^{e_m} - 1) + x' , \quad x' \in P \text{ et } s(x') \subset H \quad (II)$$

Remarquons que : $x' \in P \setminus P^2 \Leftrightarrow a \in P \setminus P^2$.

Deux cas sont à envisager pour y :

1°) $x' \in P^2$ ((16) est alors vérifiée) .

Soit $g \in G^*$ tel que : $g = e_m + \sum_{i=1}^{m-1} a_i e_i$ et $g \neq e_m$, $a_i \in F_2$

(donc $g \notin H$). Nous avons alors ,

$$\begin{aligned} (X^{e_m} - 1) &= (X^g - 1) + 1 \left[\prod_{i=1}^{m-1} ((X^{a_i e_i} - 1) + 1) \right] - 1 \\ &= (X^g - 1) + \sum_{i=1}^{m-1} a_i (X^{e_i} - 1) + b \quad \text{où } b \in P^2 . \end{aligned} \quad (III)$$

Alors, d'après (II), y s'écrit :

$$y = (X^g - 1) + \sum_{i=1}^{m-1} a_i (X^{e_i} - 1) + b' \quad \text{où } b' \in P^2$$

et les a_i sont non tous nuls, car $g \neq e_m$.

$$\text{Donc : } y = (X^g - 1) y' + y'' , \quad y' \in A \setminus P , \quad y'' \in P \setminus P^2$$

où y' et y'' sont sans facteurs $(X^g - 1)$.

On obtient un autre générateur de $\langle x \rangle$:

$$y'y = (X^g - 1) + y'y'' , \quad y'y'' \in P \setminus P^2 \text{ et } s(y'y'') \subset H .$$

La formule (15) est vérifiée.

2°) $x' \in P \setminus P^2$ ((15) est alors vérifiée).

Ceci signifie que : $x' = \sum_{i=1}^{m-1} a_i (X^{e_i} - 1) + x''$ où $x'' \in P^2$ et

au moins un élément a_i , $a_i \in F_2$, est non nul. Alors :

$$y = (X^{e_m} - 1) + \sum_{i=1}^{m-1} a_i (X^{e_i} - 1) + x'', \quad x'' \in P^2.$$

Soit $g \in G^* \setminus \{e_m\}$ tel que $g = e_m + \sum_{i=1}^{m-1} a_i e_i$. D'après (III):

$$(X^{e_m} - 1) = (X^g - 1) + \sum_{i=1}^{m-1} a_i (X^{e_i} - 1) + b, \quad b \in P^2$$

D'où : $y = (X^g - 1) + b + x''$, $b + x'' \in P^2$.

Donc : $y = (X^g - 1) t + t'$ où $t \in A \setminus P$, $t' \in P^2$, t et t' sont sans facteurs $(X^g - 1)$. Le produit $y t$ est un générateur de (x) qui vérifie (16).

Corollaire 1.

$G = F_{2^m}$; H est un hyperplan de G ; H' est un hyperplan de H .

S'il existe un H' -code (x) qui est un code $(2^{m-1}, 2^{m-2}, d)$, alors on peut construire un H -code (y) qui est un code $(2^m, 2^{m-1}, d)$.

Preuve

Soit (x) un H' -code de l'algèbre $F_2 H$ qui a pour valuation d . Si l'on se place dans $F_2 G$, le support de x est dans un hyperplan H de G . Soit $g \in G^* \setminus H$ et $y = (X^g + 1) + x$.

L'élément y est de profondeur 1 ; (y) est un H -code de valuation supérieure ou égale à d .

On peut choisir $x : x = 1 + X^e x', e \in H^* \setminus H', s(x') \subset H' .$
 Soit $u \in F_2 H'$ avec $\omega(u x) = d$. Alors :

$$u y = u X^g + u + u + X^e x' u = u X^g + X^e x' u$$

$$\omega(u y) = \omega(u) + \omega(x' u) = \omega(u x) = d .$$

La valuation de (y) est donc égale à d .

Corollaire 2

Si tous les H' -codes de longueur 2^{m-1} ont une valuation inférieure ou égale à d , alors tous les H -codes de longueur 2^m ont une valuation inférieure ou égale à $2d$.

Preuve

Soit (x) un H -code de $F_2 G$ avec, d'après (15),

$$x = (1 + X^g) + x', g \in G \setminus H, x' \in F_2 H, x' \in P \setminus P^2 .$$

Si le code (x') , considéré comme un H' -code de longueur 2^{m-1} , a une valuation inférieure ou égale à d , alors il existe $u \in F_2 H$ tel que :

$$u x' = 0 \text{ (c'est-à-dire } u \in (x')) \text{ et } \omega(u) \leq d .$$

Alors

$$u x = u(1 + X^g) \text{ et donc } \omega(u x) = 2 \omega(u) .$$

Ainsi la valuation de (x) est au plus égale à $2d$.

Corollaire 3

S'il existe un élément y de profondeur supérieure ou égale à 2 dans l'algèbre $F_2 F_{2^m-1}$, tel que :

$$v \in (y) \Rightarrow \omega(v) \geq d \quad (I)$$

$$\text{et, } v \in \text{Ann}(y) \Rightarrow \omega(v) \geq \frac{d}{2} \quad (II)$$

alors il existe un H-code de longueur 2^m et de valuation d .

Preuve

Soit (x) un H-code de $F_2 F_{2^m}$ avec, d'après (16),

$$x = (X^g - 1) + y, \quad g \in G \setminus H, \quad y \in P^2 \cap F_2 H.$$

Supposons que y vérifie les hypothèses du Corollaire.

Soit $u \in F_2 H$.

- Si $u y = 0$, alors $\omega(u x) = 2 \omega(u)$. D'après (II), $\omega(u x) \geq d$ et si $\omega(u) = \frac{d}{2}$, alors $\omega(u x) = d$.

- Si $u y \neq 0$, alors $\omega(u x) = \omega(X^g u) + \omega(u + u y)$.

D'où, $\omega(u x) \geq \omega(X^g u) + \omega(u y) - \omega(u)$. Or, d'après (I), $\omega(u y) \geq d$.

Donc $\omega(u x) \geq d$.

4. H-CODES EXTREMAUX

$G \cong (F_{2^m}, +)$. La longueur des codes considérés est 2^m .

Théorème 1

Soit (x) un H-code de $F_2 G$. Alors, pour chaque entier i tel que $m - i \geq 2^{i-1}$, il existe un élément y de (x) dont le support est un sous-espace de dimension $m - i$ de G .

Preuve

La démonstration se fait par récurrence sur la valeur de i ;

. $i = 0$. Chaque m vérifie $m \geq 1$ et chaque H-code de longueur 2^m contient y tel que $s(y) = G$ (Cf. § 2.1).

. $i = 1$. Soit (x) , un H-code de longueur 2^m , avec $m \geq 2$.

Alors il existe $y \in F_2 G$ tel que :

$y \cdot x = 0$ et $s(y)$ est un hyperplan de G .

(x est profondeur 1 ; on applique la propriété 3).

. Nous supposons que la Proposition est vraie jusqu'à $i - 1$, c'est-à-dire ,

$\forall k, k \in [1, i - 1], i > 1 :$

$m \geq k + 2^{k-1} \Rightarrow$ Chaque H-code de longueur 2^m contient un mot y dont le support est un sous-espace de dimension $m - k$ de G .

Nous allons démontrer qu'elle est vraie pour la valeur i .
Soit donc $m = i + 2^{i-1}$ et soit (x) un H-code de longueur 2^m ; (x) est un code de $F_2 G$. D'après l'hypothèse de récurrence, il existe y dans (x) tel que $s(y)$ est un sous-espace de dimension $m - (i - 1)$ de G .

Soit $V = s(y)$, $t = m - i + 1$ et $\{e_1, \dots, e_t\}$ une base de V complétée en une base $\{e_1, \dots, e_m\}$ de G . Alors $y = \prod_{j=1}^t (X^{e_j} - 1)$ et $y x = C$.

On peut appliquer le Lemme 1 : x est nilpotent sur V et sur chaque translatée de V . Ceci s'exprime :

$$z = \prod_{j=t+1}^m (X^{e_j} - 1)$$

$$x = \sum_{g \in s(z)} X^g x(g), \quad x(g) \in P, \quad x(g) \in F_2 V \quad (I)$$

($X^g x(g)$ est la restriction de x à la variété linéaire $g + V$ (définition 1)).

Chaque $x(g)$, $g \in s(z)$, qui est tel que $x(g) \in P \setminus P^2$, engendre un K -code de $F_2 V$. D'après (16), $x(g)$ s'écrit à une unité de $F_2 V$ près :

$$x(g) = (1 + X^h) + x', \quad h \in V \setminus W, \quad x' \in P^2. \quad (II)$$

Soit Q le sous-espace de G engendré par l'ensemble des éléments h exhibés par (II) (à chaque $x(g)$, $g \in s(z)$ et $x(g) \in P \setminus P^2$, correspond un élément h).

Nous avons : $|s(z)| = 2^{m-t} = 2^{i-1}$ (car $t = m - i + 1$).
Donc : $\dim Q \leq 2^{i-1}$.

Soit V' un hyperplan de V contenant Q . (V' existe bien car, $\dim V = t = m - i + 1 = (i + 2^{i-1}) - i + 1 = 2^{i-1} + 1$).

Soit $a \in F_2 G$ tel que $s(a) = V'$. Etudions les produits $a x(g)$, $g \in s(z)$:

. Si $x(g) \in P^2$, alors $a x(g)$ est de profondeur au moins $t + 1$ dans $F_2 V$; or l'index de nilpotence du radical de $F_2 V$ est justement égal à $t + 1$. Donc, dans ce cas, $a x(g) = 0$.

. Si $x(g) \in P \setminus P^2$, $x(g)$ est donné par (II). On obtient :

$$a x(g) = a(1 + X^h) + a x'.$$

Or $h \in Q$, $Q \subset s(a)$ et $s(a) = V'$; donc $a(1 + X^h) = 0$. Puisque $x' \in P^2$, nous sommes dans le cas précédent : $a x(g) = 0$.

Finalement, x étant donné par (I), nous avons :

$$a x = \sum_{g \in s(z)} X^g a x(g) = 0.$$

Donc $a \in (x)$ et $s(a)$ un sous-espace de dimension $m - i$ de G ($\dim V' = \dim V - 1 = m - i$).

Notre hypothèse était : $m = i + 2^{i-1}$. Il reste à montrer que si m est strictement supérieur à $i + 2^{i-1}$, (x) contient un mot dont le support est un sous-espace de G de dimension $m - i$.

Nous avons montré que chaque H -code de longueur 2^m avec $m = i + 2^{i-1}$ vérifie cette propriété. Soit alors un G -code de longueur 2^{m+1} . D'après (15), un générateur de ce code est :

$$x = (X^g - 1) + x', \quad g \in F_{2^{m+1}}^* \setminus G, \quad x' \in P \setminus P^2, \quad x' \in F_2 G.$$

Alors, il existe a , $a \in (x')$ et $s(a)$ est un sous-espace de dimension $m - i$ de G .

D'où $a x = a(X^g - 1)$. Donc $s(a x)$ est un sous-espace de dimension $(m+1) - i$ de $F_{2^{m+1}}$. Le code (x) , dont la longueur est 2^{m+1} ,

vérifie encore la propriété. La Proposition est ainsi démontrée.

Corollaire 4

$N = 2^m$ avec $m > 1$.

On désigne par d la valuation d'un H-code de longueur N .
Soit $i = \max\{k \in \mathbb{N} \mid m \geq k + 2^{k-1}\}$. Alors, la valeur d est inférieure ou égale à 2^{m-i} et le rapport $\frac{d}{N}$ tend vers zéro lorsque m tend vers l'infini.

Preuve

Les notations et hypothèses sont celles de l'énoncé. Soit (x) un H-code de longueur N et de valuation d .

D'après la Proposition 6.2, (x) contient un mot de poids 2^{m-i} .
Donc $d \leq 2^{m-i}$. On en déduit : $\frac{d}{N} \leq 2^{-i}$. Lorsque m tend vers l'in-

fini, i tend vers l'infini et donc le rapport $\frac{d}{N}$ tend vers zéro.

Remarque : Le corollaire 4 prouve que la classe des H-codes n'est pas une classe de bons codes autoduaux car elle ne satisfait pas à la borne de GIBERT-VARSAMOV [24, p. 557]. Pour qu'elle y satisfasse il faut que pour chaque m , $m > 1$, il existe un H-code qui est un code $(2^m, 2^{m-1}, d)$ tel que :

$$K\left(\frac{d}{2^m}\right) \leq \frac{1}{2} \text{ où } K(x) = 1 + x \log_2(x) + (1-x) + (1-x) \log_2(1-x) \quad (I)$$

Or, $K\left(\frac{1}{8}\right) = 0,4564$ et $K\left(\frac{1}{16}\right) = 0,7520$.

Pour tout m , $m \geq 12$, (I) n'est pas vérifiée.

Théorème 2

Un H-code extrémal est l'un des codes suivants :

- un code (4, 2, 2) à poids multiples de 2
- un code (8, 4, 4) à poids multiples de 4
- un code (16, 8, 4) à poids multiples de 4
- un code (32, 16, 8) à poids multiples de 4 .

Preuve

1°) Un code autodual défini sur F_2 , de longueur 2^m et à poids multiples de 2, a une valuation d inférieure ou égale à λ ,
 $\lambda = 2^{m-2} + 2$. Lorsque $d = \lambda$, le code en question est dit EXTREMAL [24, p. 629]. Soit (x) un H-code de longueur 2^m à poids multiples de 2. D'après le théorème 1, $m \geq 4 \Rightarrow (x)$ contient un mot de poids 2^{m-2} . Donc, dès que m est supérieur ou égal à 4, (x) ne peut être extrémal. Lorsque $m = 3$, si (x) est un code (8,4,4) il est à poids multiples de 4, ceci de par la forme de sa matrice génératrice (cf. (9)).

2°) Un code autodual sur F_2 , à poids multiples de 4 et de longueur 2^m , est extrémal lorsque sa valuation est égale à λ avec

$$\lambda = 4 \left[\frac{2^{m-2}}{3} \right] + 4 \quad \left(\left[\frac{2^{m-3}}{3} \right] \text{ signifie que l'on prend la partie en-} \right.$$

tière de la valeur entre crochets).

Soit (x) un H-code de longueur 2^m à poids multiples de 4 .
D'après le Théorème 1, $m \geq 7 \Rightarrow (x)$ contient un mot de poids 2^{m-3} .
Donc : $m \geq 7 \Rightarrow (x)$ ne peut être extrémal.

Il est clair que l'on construit facilement un H-code qui est un code (8, 4, 4) ou bien un code (16, 8, 4).

Pour démontrer la Proposition il reste à prouver que (x) ne peut être un code (64, 32, 12) :

Lemme 2

Soit (x) un H-code de longueur 64 . Alors, (x) contient un mot dont le support est un sous-espace de dimension 3 de F_{64} .

Preuve

$$G = F_{64} \quad ; \quad V = F_{32} \quad .$$

Soient $x_1 \in F_2 V$ et $x_2 \in F_2 V$ où x_1 et x_2 sont nilpotents. Si x_1 et x_2 sont de profondeur 1, ils s'écrivent respectivement à une unité de $F_2 V$ près :

$$x_1 = (X^g - 1) + x' \quad , \quad x' \in P^2 \quad , \quad g \in V^*$$

$$x_2 = (X^h - 1) + x'' \quad , \quad x'' \in P^2 \quad , \quad h \in V^*$$

(cf. (16)).

$$\text{Soient } v = (X^g - 1)(X^h - 1)x_1 \quad \text{et} \quad w = (X^g - 1)(X^h - 1)x_2 \quad .$$

Alors $v \in P^4$ et $w \in P^4$; P^4 est, dans $F_2 V$, le code de Reed et Muller d'ordre 1 : chaque mot de P^4 a pour support une variété linéaire de dimension 4 ou 5, ou bien le mot est nul (cf. §2.1).

Il est donc clair qu'il existe u avec $u \in V$ et $\{g, h, u\}$ est un système libre de V , tel que : $(X^u - 1) v = (X^u - 1) w = 0$.

Finalement :

$$\exists y \quad ; \quad y = (X^g - 1)(X^h - 1)(X^u - 1), \quad y x_1 = 0 \quad \text{et} \quad y x_2 = 0 \quad (I)$$

Lorsque $h = g$, on peut prendre pour h un autre élément de V^* et la démonstration de (I) est alors inchangée.

Si x_1 (ou x_2) est de profondeur 2, on choisit de même g ,
 $g \in V^*$ et $g \neq h$ (ou h , $h \in V$ et $h \neq g$).

Soit (x) un H -code de $F_2 G$ (H est un hyperplan de G) ;
 $x \in P \setminus P^2$; il existe donc $z \in F_2 G$ tel que $s(z)$ est un hyperplan
 H' de G et $z \in (x)$. (Propriété 3).

D'après le Lemme 1, x est nilpotent sur H' et sur le complément-
 taire de H' c'est-à-dire :

$$x = x_1 + X_g x_2, \quad g \in G^* \setminus H', \quad x_1 \in F_2 H', \quad x_2 \in F_2 H'$$

et x_1 et x_2 sont nilpotents .

On identifie H' et V et on applique (I) ;

$$\exists y, \dot{y} \in F_2 H' \text{ et } \omega(y) = 8 \text{ tel que :}$$

$$y x = y x_1 + X^g y x_2 = 0 .$$

Donc, (x) contient un mot de poids 8 dont le support est un sous-
 espace de dimension 3 de G . Le Théorème 2 est ainsi démontré.

CONCLUSION

Le corollaire 4 fournit une borne supérieure pour la valuation
 d'un H -code de longueur 2^m . Si d désigne cette borne supérieure,
 elle est pour de petites longueurs :

$m = 4$	$d = 2^{m-2} = 4$
$m = 5$	$d = 2^{m-2} = 8$
$m = 6$	$d = 2^{m-3} = 16$
$m = 7$	$d = 2^{m-3} = 16$
$m = 8$	$d = 2^{m-3} = 32$.

Il existe une proportion importante de H-codes de longueur 32 qui sont des codes (32, 16, 8).

Nous avons exhibé, en utilisant un ordinateur, des H-codes qui sont des codes (128, 64, 16). Nous prouvons (§8 de ce chapitre) que l'on peut construire une classe de H-codes qui ont une valuation qui croît avec leur longueur. Ces résultats peuvent être améliorés. Nous conjecturons que :

1°) La borne supérieure fournie par le corollaire 4 n'est plus atteinte dès que $m \geq 8$.

2°) Lorsque m est impair, il existe un H-code de valuation égale à 2^k avec $k = \frac{m+1}{2}$.

5. POIDS DES GENERATEURS D'UN H-CODE

$G = F_{2^m}$; H est un hyperplan de G que l'on identifie, si c'est nécessaire, à $(F_{2^{m-1}}, +)$. Dans ce paragraphe nous utilisons la notation suivante :

$$\begin{aligned} C_y &= (x) \\ C_y \text{ est un H-code} &\Leftrightarrow \begin{aligned} x &= 1 + X^g y \\ g &\in G \setminus H, y \text{ est une unité de } F_2 H \end{aligned} \end{aligned} \quad (17)$$

(cf. (8) et (9)).

Lemme 3

Le code C_y est défini par (17). Soit $u \in F_2 H$, u de poids impair.

Alors :

$$\omega(u x) \geq \omega(u) + \frac{\omega(y)}{\omega(u)} \quad (18)$$

Preuve

Soit u , une unité de $F_2 H$; alors $u^2 = 1$ et :

$$\begin{aligned} u x &= (u, u y) \Rightarrow \omega(u x) = \omega(u) + \omega(u y) \\ \omega(y) &= \omega(u^2 y) \Rightarrow \omega(y) \leq \omega(u y) \omega(u) \end{aligned}$$

Donc :

$$\omega(u x) - \omega(u) \geq \frac{\omega(y)}{\omega(u)} .$$

Proposition 3

Soit un H -code C_y .

Soit d une valeur entière paire donnée et telle que :

$$\lambda \in \mathbb{N}, \lambda \text{ impair}, 1 \leq \lambda < \frac{d}{2} \Rightarrow \omega(y) \geq \lambda(d - \lambda) \quad (19)$$

Alors, chaque générateur du code C_y a un poids supérieur ou égal à d .

Preuve

Un générateur du code C_y est un mot $(u, u y)$ où u est une unité de $F_2 H$ (u est de poids impair). Pour vérifier que chaque mot de ce type a un poids supérieur ou égal à d il suffit d'étudier les mots $(u, u y)$ tels que $\omega(u) < \frac{d}{2}$ (cf. (9), (12) et [5]).

Supposons que C_y est tel que y vérifie (19) pour une valeur d donnée. Soit u une unité de $F_2 H$.

Alors, d'après (18), $\omega(u, u y) \geq \omega(u) + \frac{\omega(y)}{\omega(u)}$. Donc :

$$\begin{aligned}
 1 \leq \omega(u) < \frac{d}{2} &\Rightarrow \omega(y) \geq \omega(u) (d - \omega(u)) \quad (\text{d'après (19)}) \\
 &\Rightarrow \omega(u, uy) \geq \omega(u) + d - \omega(u) \\
 &\Rightarrow \omega(u, uy) \geq d .
 \end{aligned}$$

Corollaire 5

Soit un H-code C_y de longueur 2^m et soit d une valeur entière paire tels que :

$$d = 4k + 2, \quad d^2 \leq 4(2^{m-1} + 3)$$

$$\omega(y) \geq \frac{d^2}{4} - 4 \quad (20)$$

Alors, si C_y est un code à poids multiples de 2 (respectivement à poids multiples de 4), chaque générateur de C_y a un poids supérieur ou égal à d (respectivement à $d + 2$).

Preuve

Soit un H-code C_y et soit d tels que les hypothèses du corollaire 5 sont vérifiées. Montrons que dans ce cas y et d vérifient (19) :

L'application $f : \lambda \rightarrow \lambda(d - \lambda)$ est croissante dans l'intervalle $[0, \frac{d}{2}]$. La plus grande valeur impaire de l'intervalle $[1, \frac{d}{2}]$ est $\frac{d}{2} - 2$; or $f(\frac{d}{2} - 2) = \frac{d^2}{4} - 4$.

$$\text{Donc, d'après (20) : } \omega(y) \geq \sup_{\lambda \in [1, \frac{d}{2} - 2]} f(\lambda) .$$

Nous appliquons alors la Proposition 3. Chaque générateur du code C_y a un poids supérieur ou égal à d .

Si C_y est un code à poids multiples de 4, chaque générateur de C_y a donc un poids supérieur ou égal à $d + 2$.

Remarquons que la condition $d^2 \leq 4(2^{m-1} + 3)$ est une condition sans laquelle (20) ne peut être vérifié. En effet, si C_y est de longueur 2^m , le poids de y est strictement inférieur à 2^{m-1} . Nous obtenons donc :

$$\frac{d^2}{4} - 4 \leq 2^{m-1} - 1 \Rightarrow d^2 \leq 4(2^m + 3).$$

Utilisation pratique du corollaire 5

Remarquons d'abord qu'un code C_y de longueur 2^m peut être tel que ses générateurs ont un poids élevé alors que sa valuation est peu élevée. Ainsi par exemple, si $\omega(y) = 2^{m-1} - 1$ avec $m > 2$, le code C_y a pour valuation 4 alors que chacun de ses générateurs a un poids supérieur à la valeur $2 \cdot 2^{\frac{m-1}{2}}$. D'autre part la condition (20) est une condition suffisante mais non nécessaire.

Si l'on recherche un code C_y qui est un code $(2^m, 2^{m-1}, d')$ le tableau ci-après montre comment l'on peut utiliser le Corollaire 5 de façon à ne pas avoir à vérifier le poids des générateurs du code C_y . Les notations sont celles du corollaire : pour une valeur d donnée, si d et y vérifient (20), la vérification de $d' = d$ (ou $d' = d + 2$) se fait sans étudier les mots (u, uy) où u est une unité de F_2^H .

Notation

' C_y à p m 2' signifie ' C_y est à poids multiples de 2'.

d'	d		$\omega(y) \geq$		m $\geq$	
	$\hat{a} \cdot p \cdot m \cdot 2$	$\hat{a} \cdot p \cdot m \cdot 4$	$\hat{a} \cdot p \cdot m \cdot 2$	$\hat{a} \cdot p = 4$	$\hat{a} \cdot p \cdot m \cdot 2$	$\hat{a} \cdot p \cdot m \cdot 4$
8	10	6	21	7	6	4
10	10		21		6	
12	14	10	45	23	7	6
16	18	14	77	47	8	7
20	22	18	117	79	8	8
24	26	22	165	119	9	8
28	30	26	221	167	9	9
32	34	30	285	223	10	9

A titre d'exemple, le corollaire suivant montre que le corollaire 5 simplifie la recherche d'un H-code de valuation supérieure à 12.

Corollaire 6

Soit un H-code C_y de longueur 2^m avec $m \geq 7$ et tel que :

$$u \in F_2^H, u = (x^g - 1)(x^h - 1), h \neq g \neq 0 \Rightarrow (u, y) > 4 \quad (I)$$

Alors :

(I) Si C_y est à poids multiples de 2 et si $\omega(y) \geq 45$, C_y a une

valuation supérieure ou égale à 12 .

(||) Si C_y est à poids multiples de 4 et si $\omega(y) \geq 23$, C_y a une valuation supérieure ou égale à 12 .

Preuve

$$G = F_{2^m} .$$

Soit un H-code C_y défini par :

$$C_y = (x), x = 1 + X^v y, v \in G^* \setminus H ;$$

C_y est de longueur 2^m avec $m \geq 7$ et y vérifie (I) .

Rappelons [5] que pour vérifier que C_y a bien une valuation supérieure ou égale à 12 il suffit d'étudier le poids des mots $u x$ tels que :

$$u \in F_2 H, \quad 0 \in s(u) \quad \text{et} \quad \omega(u) < 6 .$$

Si y vérifie de plus les hypothèses données dans (i) et (||), le tableau précédent montre que chaque mot $u x$ tel que $\omega(u)$ est impair, a un poids supérieur ou égal à 12. Il reste donc à montrer (II) et (III).

$$u \in F_2 H, \quad u = X^g - 1, \quad g \in H^* \Rightarrow \omega(u x) \geq 12 \quad (II)$$

$$u \in F_2 H, \quad \omega(u) = 4 \quad \text{et} \quad u \in P \setminus P^2 \Rightarrow \omega(u x) \geq 12 \quad (III)$$

Supposons que C_y ne vérifie pas (II), c'est-à-dire [5] :

$$\exists u, u = (Y^1 - 1), \quad g \in H^* ; \quad \omega(u y) = 2 \text{ ou } 6$$

$$\begin{aligned}
 \cdot \quad \underline{\omega(u \cdot y) = 2} &\Rightarrow u \cdot y = X^h u, \quad h \in H; \\
 &\Rightarrow X^a u \cdot y = X^{h+a} u, \quad a \in H \setminus \{0, g\} \\
 &\Rightarrow (1 - X^a) u \cdot y = X^h (1 - X^a) u \\
 &\Rightarrow \omega((1 - X^a)(1 - X^g) y) = 4 \quad \text{avec } a \neq g \neq 0.
 \end{aligned}$$

Ceci contredit (I).

$$\begin{aligned}
 \cdot \quad \underline{\omega(u \cdot y) = 6} &\Rightarrow u \cdot y = X^{h_1} u + X^{h_2} u + X^{h_3} u \\
 &\text{où l'ensemble } \{h_i + \{0, g\}, i = 1, 2, 3\} \text{ est composé} \\
 &\text{de trois translatés du sous-espace } \{0, g\} \text{ de } G.
 \end{aligned}$$

Soit $h = h_1 + h_2$; h est non nul et h est différent de g .

Alors :

$$X^h y u = X^{h_2} u + X^{h_1} u + X^{h_3+h} u$$

$$\text{Donc} \quad (1 - X^h) y u = X^{h_3} (1 - X^h) u$$

D'où : $\omega((1 - X^h)(1 - X^g)y) = 4$ ce qui contredit (I)

Donc, si C_y vérifie (I), C_y vérifie (II).

b) Supposons que C_y ne vérifie pas (III), c'est-à-dire :

$$\exists u, u \in F_2 H, u \in P \setminus P^2 \quad \text{et} \quad \omega(u) = 4; \omega(u \cdot y) = 4.$$

Dans ce cas (u) est un H' -code (H' étant un hyperplan de H) et donc $u \cdot y = X^a u$, $a \in H \setminus \{5\}$ ($u \cdot y$ est un générateur du code (u) ; (u) est un H' -code tel que $\omega(u) = 4$).

Il est clair (cf. (9)) que (u) contient un mot t dont le support est un sous-espace de dimension 2 de H :

$$\exists z, z \in F_2 H \quad \text{et} \quad z \cdot u = t$$

D'où :

$$z u y = X^a z u = X^a t \text{ avec } t = (X^g - 1)(X^h - 1), h \neq y \neq 0 \text{ et } \omega(t y) = 4$$

Ceci contredit (I). Donc si C_y vérifie (I), C_y vérifie (III).

6. ENUMERATION DES H-CODES QUI SONT DES CODES (32, 16, 8) A POIDS MULTIPLES DE 4

Notations

$G = F_{32}$; H est un hyperplan de G . La donnée d'un H-code C_y (cf. (17)) est la donnée d'une unité y de $F_2 H$ (H étant alors identifié à $(F_{16}, +)$). Le code C_y est à poids multiples de 4 si et seulement si la quantité $\omega(y) + 1$ est divisible par 4 . Soit :

$$Y = \{y \in F_2 H \mid 4 \text{ divise } \omega(y) + 1\}$$

$$\text{Alors} \quad |Y| = \frac{2^{16}}{4} = 16\,384 \quad (21)$$

Si $y \in Y$, alors $\omega(y) = 3, 7, 11$ ou 15 . Il est clair qu'un code C_y tel que $\omega(y) = 3$ ou 15 , a pour valuation 4 . Ainsi, si C_y est extrémal (C_y est un code (32, 16, 8)) le poids de y est égal à 7 ou 11.

Chaque code C_y permet de définir 16 codes :

$$C_z, z = X^g y, g \in H$$

de même valuation que C_y . On réalise ainsi une partition de Y .

Pour étudier les H-codes extrémaux de $F_2 G$ nous étudions les codes C_y tels que Y appartient à l'un des deux ensembles Y_7 et Y_{11} définis comme suit : $i = 7$ ou 11 ;

$$\omega(y) = i \quad \text{et} \quad 0 \in s(y)$$

$$y \in Y_i \Leftrightarrow y \text{ est l'unique représentant dans } Y_i \text{ (22)} \\ \text{de l'ensemble } \{X^g y, g \in H\}$$

(Y_i contient 1 et un seul représentant de chaque classe définie ci-dessus et ceci dans un sous-ensemble de Y composé des unités de poids i dont le support contient 0). Calculons le cardinal de chaque Y_i :

$$|Y_7| = \frac{1}{16} \times \binom{16}{17} = 715 \quad (23)$$

$$|Y_{11}| = \frac{1}{16} \binom{16}{11} = 273 \quad (24)$$

Les deux propriétés suivantes sont démontrées dans [5] .

Propriété 4.

Soit $y \in Y$ avec $\omega(y) = 7$ ou 11 .

Alors C_y est un code $(32, 16, 8)$ si et seulement si

$$u \in F_2 H, 0 \in s(u) \quad \text{et} \quad \omega(u) = 2 \Rightarrow \omega(uy) > 2 \quad (25)$$

Propriété 5

Soit $y \in Y$ avec $\omega(y) = 7$ ou 11 .

Alors C_y est un code $(32, 16, 4)$ si et seulement si, il existe $u = X^g y + 1$ avec $g \in H^*$, tel que y est de poids impair sur un seul translaté de $s(u)$ dans H .

Lemme 4

Soit $u \in F_2 H$ tel que $0 \in s(u)$ et $\omega(u) = 2$. Alors :

(I) Il existe 35 éléments y tels que : $y \in Y_7$ et $\omega(uy) = 2$

(II) Il existe 21 éléments y tels que : $y \in Y_{11}$ et $\omega(u y) = 2$.

Preuve

Soit $u = 1 + X^g$ avec $g \in H^*$; les translatés de $s(u)$ dans H , forment une partition de H en huit sous-ensembles de deux éléments, soit :

$$\{0, g\}, \{g_1, g_1 + g\}, \dots, \{g_7, g_7 + g\}.$$

Soit $y \in Y_7$ tel que $\omega(u y) = 2$ (C_y est donc un code $(32, 16, 4)$). Alors, d'après la propriété 5, y est tel que $s(y)$ est composé de trois translatés de $s(u)$ plus un élément d'un quatrième translaté de $s(u)$. Il existe $16 \cdot \binom{7}{3}$ unités de $F_2 H$ de ce type : Y_7 en contient donc : $\binom{7}{3} = 35$.

De même, si $y \in Y_{11}$ et $\omega(u y) = 2$, le support de y est composé de cinq translatés de $s(u)$ plus un élément d'un sixième translaté de $s(u)$. Il existe $16 \cdot \binom{7}{5}$ unités de $F_2 H$ de ce type ; Y_{11} en contient donc : $\binom{7}{5} = 21$.

Lemme 5

Soit $y \in Y_7$.

(I) Si $s(y)$ est contenu dans un hyperplan de H , alors il existe 7 éléments u tels que :

$$u \in F_2 H, 0 \in s(u), \omega(u) = \omega(u y) = 2.$$

(II) Si $s(y)$ n'est contenu dans aucun hyperplan de H et si C_y a pour valuation 4, alors il existe un seul élément u tel que

$$u \in F_2 H, 0 \in s(u), \omega(u) = \omega(u y) = 2.$$

Preuve

(I) Soit V un hyperplan de H et soit $\bar{V}$ le complémentaire de V dans H . Soit $y \in Y_7$ tel que $s(y) \subset V$. Chaque $u, u = 1 + X^g$ avec

$g \in V^*$, est tel que : un translaté de $s(u)$ dans H est soit dans V soit dans $\bar{V}$. Un tel u vérifie $\omega(u) = \omega(u y) = 2$ car y est de poids impair sur un seul translaté de $s(u)$ ($\omega(y) = 7$, $|V| = 8$ et $s(y) \subset V$).

Par contre si $u = 1 + X^g$ avec $g \in \bar{V}$, il est clair que y est de poids impair sur plus d'un translaté de $s(u)$. Puisque $|V^*| = 7$, ceci démontre (I).

(II) Nous supposons maintenant que : $y \in Y_7$, C_y n'est pas extrémal et $s(y)$ est de rang 4 dans H . Alors, d'après la propriété 5, il existe u , $u = X^g + 1$ avec $g \in H^*$, tel que y est de poids impair sur un seul translaté de $s(u)$. Supposons qu'il existe v , $v = X^h + 1$ avec $h \in H^* \setminus \{g\}$, tel que y vérifie cette même propriété pour v . On peut supposer, sans perdre en généralité que $s(y)$ a la forme suivante :

$$s(y) = \{0, g_1, g_1 + g, g_2, g_2 + g, g_3, g_3 + g\}, \quad g_i \neq g.$$

L'existence de v suppose que l'ensemble $s(y) \cap s(X^h y)$ comporte 6 éléments, c'est-à-dire au moins deux translatés de $\{0, g\}$. Supposons par exemple que $g_2 = g_1 + h$. Alors :

$$\{g_1, g_1 + g, g_2, g_2 + g\} \subset s(y) \cap s(X^h y).$$

On a dans ce cas : $g_3 = h$ ou $g_3 + g = h$ ou $g_3 + h = g_3 + g$.

Or ceci est impossible car $h \neq g$ et $s(y)$ est de rang 4 : on ne peut avoir une relation du type $g_1 + g_2 + g_3 = 0$ ou $g_1 + g_2 + g_3 + g = 0$.

Donc la seule solution est $v = u$; u est l'unique élément de $F_2 H$ vérifiant :

$$u = X^g + 1, \quad g \in H^* \quad \text{et} \quad \omega(uy) = 2.$$

Lemme 6

Soit $y \in Y_{11}$ tel que C_y a pour valuation 4. Alors, il existe trois éléments u du type suivant :

$$u = X^g + 1, \quad g \in H^* \quad \text{et} \quad \omega(uy) = 2.$$

Preuve

$y \in Y_{11}$ et C_y n'est pas extrémal. D'après la propriété 4, il existe $u = X^g + 1$ avec $g \in H^*$ et $\omega(uy) = 2$.

D'après la propriété 5 et puisque y est un représentant de l'ensemble $\{X^h y \mid h \in H\}$, on peut représenter $s(y)$ comme suit :

$$s(y) = \{0, g_1, g_1 + g, \dots, g_5, g_5 + g\}, \quad g_i \neq g$$

avec $H = s(y) \cup \{g, g_6, g_6 + g, g_7, g_7 + g\}$.

Soit alors $h \in H \setminus \{g\}$. Trois cas sont à envisager :

1°) $h = g_6 + g_7$. Dans ce cas, $s(X^h y) \subset s(y) \cup \{g\}$. ($X^h y$ a pour

poids 11 et son support est contenu dans la réunion de 6 translatés de u). Donc, $(1 + X^h)y$ est de poids 2. On a ainsi exhibé v , $v = 1 + X^h$, tel que $\omega(vy) = 2$. (h est différent de 0 et de g puisque $g_6 \neq g_7 + g$ et $g_6 \neq g_7$).

2°) $h = g_6 + g_7 + g$. On a, de même qu'au 1°),

$s(X^h y) \subset s(y) \cup \{g\}$. Donc, on exhibe $w = 1 + X^h$ avec $\omega(wy) = 2$; w diffère de u et de v car $g_6 + g_7 + g \notin \{0, g, g_6 + g\}$.

3°) $h = g_6 + g_7 \notin \{0, g\}$. On obtient :

$$h + \{g_6, g_6 + g, g_7, g_7 + g\} \subset s(y) \cup \{g\}.$$

D'où, le poids de $(1 + x^h) y$ est supérieur à 2 .

On a finalement trois éléments u ne vérifiant pas (25).

Théorème 3

Parmi les 16 384 matrices génératrices de H-codes de longueur 32 et à poids multiples de 4, 7 168 sont des matrices génératrices de codes autoduaux extrémaux, soit une proportion de 43,75 % .

Parmi 4 368 H-codes C_y tels que $\omega(y) = 11$, 2 688 (soit 61,54 %) sont extrémaux.

Parmi 11 480 H-codes C_y tels que $\omega(y) = 7$, 4 480 (39,60 %) sont extrémaux.

Preuve

Soit $Y_i' = \{y \in Y_i \mid C_y \text{ est extrémal}\}$, $i \in \{7, 11\}$.
(y_i est défini par (22)).

Nous allons calculer le cardinal de Y_7' et le cardinal de Y_{11}' .

Soit $U = \{u \in F_2^H \mid 0 \in s(u) \text{ et } \omega(u) = 2\}$.

Le code C_y , $y \in Y_7 \cup Y_{11}$, est extrémal si et seulement si pour chaque u , $u \in U$, $\omega(uy)$ est strictement supérieur à 2 .

1°) Cardinal de Y_7' :

Pour chaque hyperplan H' de H il n'existe qu'un seul y de Y_7 tel que $s(y) \subset H'$ car :

$$y' \in Y_7 \text{ et } s(y') \subset H' \Rightarrow y' = x^g y, \quad g \in H' .$$

Il existe dans H , 15 hyperplans distincts. Donc pour 15 éléments de Y_7 , il existe 7 éléments u de U tels que $\omega(uy) = 2$ (Lemme 5, (I)). Nous avons vu, dans la démonstration du Lemme 5, que :

$$\begin{aligned} H' = \text{hyperplan de } H, s(y) \subset H' & \Rightarrow s(u) \subset H' \\ u \in U \text{ et } \omega(uy) = 2 & \end{aligned}$$

Soit $h \in H^*$; on peut construire t hyperplans de H contenant h et $t = \frac{14 \times 12}{6 \times 4} = 7$.

On peut conclure : pour chaque $u, u \in U$, il existe 7 éléments de $y, y \in Y_7$, tels que $s(y)$ est contenu dans un hyperplan de H et $\omega(uy) = 2$. D'après le Lemme 4 il reste alors 28 éléments y de Y_7 tels que $\omega(uy) = 2$. D'après le Lemme 5 (II), un tel y vérifie $\omega(uy) = 2$ pour ce seul u de U .

Donc, sur les 715 éléments de Y_7 (cf. (23)) :

- 15 ont leur support dans un hyperplan de H ;
- $|U| \times 28 = 15 \times 28 = 420$ vérifient les hypothèses du Lemme 5, (II).

Il reste 280 éléments de y de Y_7 , tels que C_y est un code extrémal. Donc : $|Y'_7| = 280$;

$$|\{C_y \mid \omega(y) = 7\}| = 16 \times |Y'_7| = 11\,440$$

$$|\{C_y \mid \omega(y) = 7, C_y \text{ est extrémal}\}| = 16 \times |Y'_7| = 4\,480 .$$

On obtient un pourcentage de 39,16 % de H -codes C_y tels que $\omega(y) = 7$ et C_y est extrémal.

2°) Cardinal de Y'_{11}

Le lemme 6 prouve que pour chaque y de Y_{11} , soit C_y est extrémal, soit il existe exactement trois éléments u , $u \in U$ et $\omega(u, y) = 2$.

Or chaque u de U vérifie $\omega(u, y) = 2$ pour 21 éléments y de Y_{11} (Lemme 4 (II)). Donc :

$$|Y'_{11}| = |Y_{11}| - \frac{|U| \times 21}{3}$$

$$|Y'_{11}| = 273 - \frac{15 \times 21}{3} = 168$$

$$|\{C_y \mid \omega(y) = 11\}| = 4 \cdot 168$$

$$|\{C_y \mid \omega(y) = 11, C_y \text{ est extrémal}\}| = 2 \cdot 168.$$

Ainsi, 61,54 % de H-codes C_y avec $\omega(y) = 11$, sont extrémaux.

3°) CONCLUSION

On a déterminé en tout 7 168 codes extrémaux sur les 16 384 H-codes de longueur 32 et à poids multiples de 4, soit une proportion de 43,75 %.

Nous allons maintenant définir un générateur d'un H-code extrémal. Rappelons la définition d'un ensemble à différences dans un groupe abélien d'ordre 2^k [7].

Définition 3

Soit G un groupe abélien fini. Un sous-ensemble D de G est un ENSEMBLE à DIFFERENCES s'il vérifie pour tout h de G^* :

$$|D \cap D + h| = \lambda.$$

Théorème de H.B. MANN

Soit G un groupe abélien d'ordre 2^k et soit D un ensemble à différences de G . Alors, si $D \neq \{0\} \cup G'$, où G' est un sous-groupe de G , la seule possibilité est :

$$k = 2t, |D| = 2^{t-1} (2^t + \epsilon), \lambda = 2^{t-1} (2^{t-1} + \epsilon)$$

où $\epsilon = \pm 1$ et $\lambda = |D \cap D + h|$, $h \in G^*$.

Théorème 4

$G = F_{32}$; H est un hyperplan de G . Un H -code (x) est un code $(32, 16, 8)$ à poids multiples de 4 si et seulement si, il existe un générateur y de (x) qui a la forme suivante :

$$y = 1 + \chi^g(1+z), g \in G \setminus H, s(z) \subset H, \omega(z+1) = 7 \text{ ou } 11$$

et $s(z)$ est un ensemble à différences de F_{16} .

Preuve

Les codes étudiés sont à poids multiples de 4.

1°) Soit (x) , un code de $F_2 G$, possédant un générateur y qui vérifie les hypothèses de la Proposition.

Soit $u = 1 + \chi^h$, $h \in H^*$. D'après le Théorème de H.B. MANN :

$$|s(z) \cap s(z) + h| = 2 \text{ ou } 6 \text{ et } |s(z)| = 6 \text{ ou } 10 \quad (t=2)$$

$$\text{Or, } \omega(uz) = 2 \omega(z) - 2 |s(z) \cap s(\chi^h z)|$$

$$= 12 - 4 \text{ (ou } 20 - 12, \text{ car } s(\chi^h z) = h + s(z))$$

$$= 8$$

Donc $\omega(uy) = \omega(u, u+uz)$ où $\omega(u+uz) = 6 \text{ ou } 10$.

D'après la propriété 4, (x) est un code extrémal.

2°) Inversement, supposons que (x) est un H -code qui est un code $(32, 16, 8)$. Alors, d'après (16), il existe un générateur y de (x) tel

que :

$$y = 1 + X^g (1+z), g \notin H, \underline{s(z) \subset H \text{ et } z \in P^2}.$$

Nous allons montrer que $s(z)$ est un ensemble à différences de F_{16} . Pour cela il suffit de montrer :

$$u = X^h + 1, h \in H^* \Rightarrow \omega(uz) = 8 \quad (I)$$

Soit u ci-dessus défini. Alors, $uz \in P^3$ avec $s(uz) \subset H$.
Donc uz est un élément du code de Reed et Muller d'ordre 1 et de longueur 16. Ainsi, $\omega(uz) = 0, 8$ ou 16 .

On ne peut avoir $uz = 0$ car (x) est extrémal. Supposons que $\omega(uz) = 16$.

On définit une base de H , soit $\{e_1, e_2, e_3, e_4\}$ où $e_1 = h$.

Alors, $uz = \prod_{i=1}^4 (X^{e_i} - 1)$; donc z s'exprime comme suit dans la base

$\{ \prod_{i=1}^4 (X^{e_i} - 1)^{j_i} \mid j_i \in [0, 1] \}$ de $F_2 H$:

$$z = (X^{e_1} - 1) z_1 + (X^{e_2} - 1)(X^{e_3} - 1)(X^{e_4} - 1)$$

où $z_1 \in P \setminus P^2$ et z_1 est sans facteur $(X^{e_1} - 1)$.

Soit V le sous-espace de H engendré par $\{e_2, e_3, e_4\}$;
(z_1) est un V' -code de $F_2 V$. D'après (16), on a à une unité de $F_2 V$ près :

$$z_1 = 1 + X^t + a, t \in V \setminus V' \text{ et } a \in P^2.$$

D'où : $(1 + X^t) z_1 \in P^3$. Ceci entraîne : $(1 + X^t) z \in P^4$, et donc

$$(1 + X^t) z = uz = \prod_{i=1}^4 (X^{e_i} - 1) \quad (\text{car } (x) \text{ est extrémal}).$$

On en déduit :

$$\begin{aligned} (1 + X^t + 1 + X^{e_1}) z &= 0 \\ (X^t + X^{e_1}) z &= 0 \end{aligned}$$

Donc $(X^t + X^{e_1})_y = (X^t + X^{e_1}, X^t + X^{e_1})$. Ceci contredit le fait que (x) est extrémal. La seule possibilité est $\omega(uz) = 8$, ce qui démontre (I).

Exemples

Soit $\{e_1, e_2, e_3, e_4, e_5\}$, une base de G ; H est engendré par $\{e_i \mid i=1, 4\}$. On peut formuler comme suit le générateur x d'un H -code (x) de valuation 8 et à poids multiples de 4 :

$$(\text{notation : } X^{e_i} = X_i)$$

- $x = 1 + X_5(1 + (X_1 + 1)(X_2 + 1) + (X_3 + 1)(X_4 + 1))$
où $\omega(x) = 8$
- $x = 1 + X_5(1 + (X_1 + 1)(X_2 + 1) + (X_3 + 1)(X_4 + 1) + X_4 \prod_{i=1}^3 (X_i + 1))$
où $\omega(x) = 12$.

Par contre, si

$$x = 1 + X_5(1 + (X_1 + 1)(X_2 + 1) + (X_3 + 1)(X_4 + 1) + \prod_{i=1}^3 (X_i + 1)),$$

(x) est un code $(32, 16, 6)$ à poids multiples de 2.

7. UNE CLASSE DE H-CODES DONT LA VALUATION CROIT AVEC LA LONGUEUR

$G = F_{2^m}$; H est un hyperplan de G engendré par une base

$\{e_1, \dots, e_{m-1}\}$; $e = \{e_1, \dots, e_m\}$ est une base de G .

Notations :

$X^{e_i} = X_i$; $B(e)$ est la base de $F_2[G]$ définie au §2-1.

Le but de ce paragraphe est de montrer le résultat suivant :

PROPOSITION 4

Soit $j \in \mathbb{N}$, $j \geq 3$.

Alors pour chaque m , $m \geq (j-1)^2 + 1$, il existe au moins un H -code qui est un code $(2^m, 2^{m-1}, 2^j)$.

Pour cela nous allons définir une classe de H -codes vérifiant la proposition 4.

DEFINITION

Soit $j \geq 3$ et $m = (j-1)^2 + 1$. Soit $\{I_i \mid i=1, \dots, j-1\}$ une partition de l'ensemble d'indices $\{1, 2, \dots, m-1\}$ en $j-1$ ensemble dis-joints de $j-1$ éléments chacun. On désigne alors par C_j un H -code de longueur 2^m du type suivant :

$$\begin{aligned} C_j &= (x_j) \\ x_j &= 1 + X_m y_j, \quad y_j \in F_2^H \\ y_j &= 1 + \left[\sum_{i=1}^{j-1} \prod_{k \in I_i} (X_k + 1) \right] + \alpha_j, \quad \alpha_j \in P^j \end{aligned} \quad (26)$$

(y_j est ici exprimé avec la base $B(e)$ de F_2^G , mais le support de y_j est dans H : y_j est sans facteur $(X_m - 1)$).

Valuation d'un code C_j

Nous devons étudier les mots : $u x_j$, $u \in F_2^H$ et $\omega(u) < 2^{j-1}$.

- $u \in P^S \setminus P^{S+1}$, $s \in [1, j-2]$. (si $s = j-1$, le poids de u est supérieur ou égal à 2^{j-1}).

Alors, si l'on exprime u dans la base $B(e)$:

$$u = \left[\sum_{\{i_1, \dots, i_s\}} u_{i_1 \dots i_s} (X_{i_1} + 1) \dots (X_{i_s} + 1) \right] + \alpha'$$

où $u' \in P^{S+1}$, $u_{i_1 \dots i_s} \in \{0,1\}$ et $\{i_1, \dots, i_s\} \subset \{1, 2, \dots, m-1\}$.

Par hypothèse ($u \in P^S \setminus P^{S+1}$) un terme $u_{i_1 \dots i_s}$ au moins est non nul.

Alors il existe k , $k \in [1, j-1]$, tel que :

$$T = u_{i_1 \dots i_s} \left(\prod_{t \in I_k} (X_t + 1) \right) \times (X_{i_1} + 1) \dots (X_{i_s} + 1) \neq 0$$

car $s < j-1$ et donc : $\exists k ; \{i_1 \dots i_s\} \cap I_k = \emptyset$.

Soit $z_j = y_j + 1$. Si l'on effectue le produit $u z_j$, le terme T ne peut apparaître qu'une fois puisque les I_k sont disjoints et chaque I_k contient plus de s éléments. Donc, le produit $u z_j$ exprimé dans la base $B(e)$ a au moins un terme non nul : $u z_j \neq 0$ et $u z_j \in P^{j-1+s}$.

Nous avons montré :

$$\begin{aligned} u \in P \setminus P^{j-1} &\Rightarrow u x_j = (u, u + u z_j), u z_j \in P^j \setminus \{0\} \\ &\Rightarrow \omega(u x_j) \geq \omega(u) + \omega(u z_j) - \omega(u) \\ &\Rightarrow \omega(u x_j) \geq 2^j \end{aligned}$$

- $u \in A \setminus P$ et $\omega(u) < 2^{j-1}$. Il faut d'abord remarquer que la démonstration précédente est valable quel que soit α_j .

Nous allons maintenant déterminer α_j de telle façon que C_j soit de valuation au moins égale à 2^j . Nous supposons $j > 3$ car lorsque $j = 3$ et $m = 5$ nous donnons à la fin du § 6 un exemple de H-code qui est un code (32, 16, 8) du type C_5 .

Nous utilisons la Proposition 3 :

Si $\omega(y_j) \geq \max\{\lambda(2^j - \lambda) \mid \lambda \in [1, 2^{j-1}]\}$, alors chaque générateur de C_j a un poids supérieur à 2^j .

Il suffit donc que : $\omega(y_j) \geq 2^{2(j-1)} - 1$, $j > 3$.

Or $\omega(y_j + \alpha_j) = (j-1)(2^{j-1} - 1) + \epsilon$ ($\epsilon = 0$ ou 1 selon que j est pair ou

impair).

Si l'on prend par exemple $\alpha_j = \prod_{i=1}^{m-1} (X_i + 1)$, alors

$$\omega(y_j) = 2^{m-1} - (j-1)(2^{j-1} - 1) - \epsilon \quad \text{où } m-1 = (j-1)^2$$

$$\omega(y_j) = 2^{(j-3)(j-1)} 2^{2(j-1)} - (j-1)(2^{j-1} - 1) - \epsilon.$$

Il est clair que : $\omega(y) \geq 2^{2(j-1)} - 1$.

Dans ce cas, C_j est de valuation égale à 2^j :

Soit $u = (X_{k_1} + 1) \dots (X_{k_{j-1}} + 1)$ où $k_t \in I_t$; alors $u y_j = u$ et

$$\text{donc } \omega(u x_j) = 2 \omega(u) = 2^j.$$

Nous avons donc exhibé un H-code qui est un code $(2^m, 2^{m-1}, 2^j)$ avec $m-1 = (j-1)^2$. Ainsi, il existe pour chaque longueur 2^k , $k > m$, un H-code de valuation 2^j (Corollaire 1). Nous avons montré la Proposition 4.

Exemples

1) $j = 4, m = 10$

$$x = 1 + X_{10} (1 + (X_1 + 1)(X_2 + 1)(X_3 + 1) + (X_4 + 1)(X_5 + 1)(X_6 + 1) + (X_7 + 1)(X_8 + 1)(X_9 + 1) + \prod_{i=1}^9 (X_i + 1))$$

(x) est un code $(2^{10}, 2^9, 16)$ à poids multiples de 4 avec $\omega(x) = 492$.

2) $j = 5, m = 17$

$$x = 1 + X_{17} (1 + (X_1 + 1) \dots (X_4 + 1) + \dots + (X_{13} + 1) \dots (X_{16} + 1) + \prod_{i=1}^{16} (X_i + 1))$$

(x) est un code $(2^{17}, 2^9, 32)$ à poids multiples de 4.

Remarque

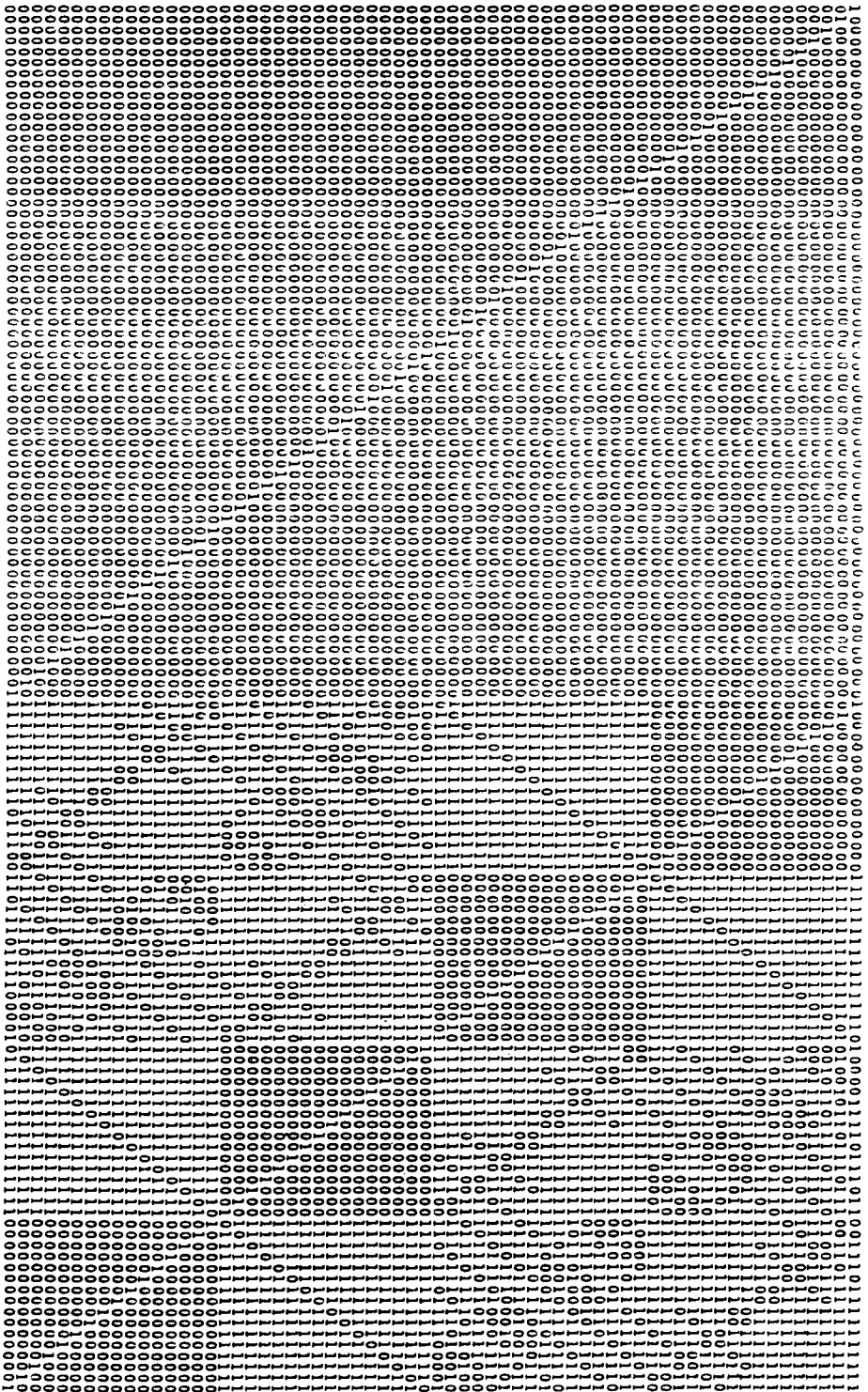
Nous donnons en annexe la matrice génératrice d'un H-code qui est un code $(128, 64, 16)$ à poids multiples de 4 . Les expériences que nous avons faites semblent prouver qu'il en existe un certain nombre de ce type. Nous pensons donc que les valuations obtenues ci-dessus peuvent être nettement améliorées.

A N N E X E

- 1) MATRICES GENERATRICES DE H-CODES QUI SONT DES CODES
(32, 16, 8)

- 2) MATRICE GENERATRICE D'UN H-CODE QUI EST UN CODE
(128, 64, 16).

[illegible]



BIBLIOGRAPHIE

- [1] E.R. BERLEKAMPF. Algebraic coding theory. Mc Graw Hill book Cie, New-York.
- [2] S.D. BERMAN. On the theory of group codes. Kibernetika. Vol. 1, n°1, pp. 31-39, (1967).
- [3] S.D. BERMAN. & I.I. GRUSHKO. Code parameters of principal ideals of group $(2, \dots, 2)$ over field of characteristic 2. Pr. Pe. Inform.. Vol. 14. n°4. pp. 3-12 (1978).
- [4] N. BOURBAKI. Livre II. Algèbre. Herman, Paris (1958).
- [5] P. CAMION. Etude de codes binaires abéliens modulaires autoduaux de petites longueurs. Revue du Cethedec, NS 79-2 (1979), pp. 3-24.
- [6] P. CAMION, G. PASQUIER & J. WOLFMAN. A class of self dual codes. I.E.E.E. Trans. Info. Theory. à paraître.
- [7] P. CAMION. Une généralisation dans les p-groupes abéliens élémentaires, $p > 2$, des théorèmes de H.B. MANN et J.F. DILLON sur les ensembles à différences des 2-groupes abéliens élémentaires. Combinatorics 79 (Proc. Colloq. Univ. Montreal, Que. 1979, Part. II). Ann. Discrete Math. 9 (1980), pp. 163-174.
- [8] P. CAMION. Differences sets in elementary abelian groups. Les Presses de l'Université de Montreal (1979).
- [9] P. CAMION. Codes abéliens autoduaux. Colloque du C.N.R.S., Cachan, 4-8 Juillet 1977.
- [10] P. CHARPIN. The extended of Reed Solomon codes considered as ideals of a modular algebra. Communicate at Marseille Luminy : 'Combinatoire 1981'. To appear in The Annals of Discrete Mathematics.
- [11] P. CHARPIN. Puissance du radical d'une algèbre modulaire et codes cycliques. Revue du Cethedec, 18ème année, 4ème trimestre 1981, NS 81-2, pp. 35-43.
- [12] P. CHARPIN. Codes idéaux de certaines algèbres modulaires. Thèse de 3ème cycle, Juin 1982, Université de Paris 7.
- [13] F.J. MAC WILLIAMS & N.J.A. SLOANE. The theory of error correcting codes. North-Holland (1977).
- [14] G. PASQUIER. Etude des codes sur une extension de F_2 et de leurs images binaires. Thèse de 3ème cycle. Université de Provence (1980).

- [15] A. POLI a M. VENTOU. Codes autoduaux principaux et groupes d'auto-morphismes de l'algèbre $F_{2^n}[X_1, \dots, X_n](X_1^2 - 1, \dots, X_n^2 - 1)$. Europ. Journal Combinatorics (1981).
- [16] A. POLI. Codes dans certaines algèbres modulaires. Thèse de Doctorat d'Etat, Université Paul Sabatier Toulouse (1978).
- [17] J. WOLFMANN. A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field. Discrete Math. 31 (1980), pp. 337-338.
- [18] J. WOLFMANN. Aspects geometriques et combinatoires de l'étude des codes correcteurs. Thèse de Doctorat d'Etat, Université de Paris VII. (1978).