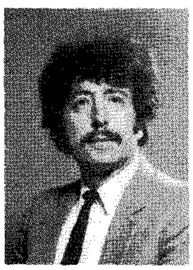
Codes autoduaux principaux nilpotents dans l'algèbre

$A=F_{2^r}[X_1, \dots, X_n]/(X_1^{2^{l_1}}-1, \dots, X_n^{2^{l_n}}-1)$

Principal nilpotent self dual codes in

$A=F_{2^r}[X_1, \dots, X_n]/(X_1^{2^{l_1}}-1, \dots, X_n^{2^{l_n}}-1)$



Alain POLI

Laboratoire AAECC, Université P.-Sabatier, 31000 TOULOUSE

Professeur à l'IUT Informatique de l'Université P.-Sabatier de Toulouse. Diplômes : thèse de 3^e cycle et thèse d'état. Directeur du AAECC, laboratoire LSI, domaine : les codes correcteurs polynômiaux et leurs applications.

J. A. THIONG LY

Laboratoire AAECC, Université P.-Sabatier, 31000 TOULOUSE

Maître-assistant à l'Université de Toulouse-Mirail. Diplôme : thèse de 3^3 cycle. Membre du AAECC, laboratoire LSI, domaine : les codes correcteurs polynômiaux et leurs applications.

RÉSUMÉ

On démontre que les codes autoduaux principaux nilpotents étudiés dans [2], sont isomorphes à des codes à une seule variable. Nous donnons également une formule pour les dénombrer.

MOTS CLÉS

Codes autoduaux, codes principaux à *n* variables.

SUMMARY

We prove that the autodual principal nilpotent codes studied in [2] *are isomorphic to one variable codes. The number of these codes is also given.*

KEY WORDS

Self dual codes, principal n variable codes.

TABLE DES MATIÈRES

Introduction

On considère l'algèbre de groupe non semi simple sur $\mathbb{F}_q (q=2^r)$ d'un groupe abélien, de représentation polynomiale :

$$A=\mathbb{F}_q[X_1, \ldots, X_n]/(t_1^2(X_1), \ldots, t_n^2(X_n))$$
$$(t_i(X_i)=X_i^{l_i}-1,\ l_i \text{ impair},\ 1 \leqq i \leqq n).$$

Dans un précédent article, exposé au colloque international à Toulouse de juin 1983, [2], nous avons donné une caractérisation des codes (c'est-à-dire des idéaux) de A qui sont autoduaux, principaux et nilpotents, et nous avons montré que tous ces codes sont isomorphes.

Dans le présent article, nous démontrons que tous ces codes sont isomorphes à des codes à une seule variable, et nous donnons leur dénombrement.

Partie I. Cadre algébrique

Dans cette première partie, nous rappelons seulement les principales propriétés démontrées dans [3] qui concernent l'algèbre A.

Pour une étude générale des codes polynomiaux à n variables, *voir* [1].

Soient :

– $\Pi P_i(X_i)$ la décomposition de $t_i(X_i)$ en facteurs irréductibles sur $\mathbb{F}_q$;

– H_i les racines de $t_i(X_i)$ dans un corps de décomposition on définit la relation d'équivalence R sur l'ensemble $H_1 \times \ldots \times H_n$;

$$(\mu_1, \ldots, \mu_n) R (\mu_1', \ldots, \mu_n') \Leftrightarrow \mu_1'=\mu_1^{q^s}, \ldots, \mu_n'=\mu_n^{q^s}$$

pour un certain entier s.

On désignera par $C(\mu_1, \ldots, \mu_n)$ la classe d'équivalence de $(\mu_1, \ldots, \mu_n)$, et N le nombre de classes d'équivalence. L'automorphisme involutif τ défini de la manière suivante, joue un rôle fondamental dans l'étude de l'algèbre A : pour tout $a(X_1, \ldots, X_n)$ de A :

$$\tau(a(X_1, \ldots, X_n))=a(X_1^{-1}, \ldots, X_n^{-1}).$$

Propriété 1 : (*a*) *L'algèbre* A *est somme directe de* N *algèbres locales* A_k :

$$A-A_1 \oplus \ldots \oplus A_N,$$

où :

$$A_{ai}=\tau(A_{ai-1}) \qquad (1 \leqq i \leqq t),$$
$$A_j=\tau(A_j) \qquad (2t+1 \leqq j \leqq N).$$

(*b*) *L'ensemble des composantes* A_k, *l'ensemble des classes* $C(\mu_1, \ldots, \mu_n)$ *et l'ensemble des idempotents primitifs de* A, *sont en bijection.*

Preuve dans [1] et [6].

Par la suite l_N désignera l'idempotent primitif en bijection avec la classe $C(1, 1, \ldots, 1)$.

Pour nos constructions, nous nous placerons dans une algèbre B_k plus simple, grâce à la propriété suivante :

Propriété 2 : (*a*) *Chaque* $\mathbb{F}_q$*-algèbre* A_k *est isomorphe en tant qu'anneau à une* $\mathbb{F}_{q'}$*-algèbre* B_k *de la forme :*

$$B_k=\mathbb{F}_{q'}[Z_1, \ldots, Z_n]/(Z_1^2, \ldots, Z_n^2),$$

où :

$$\mathbb{F}_{q'}=\mathbb{F}_q(\mu_1, \ldots, \mu_n) \qquad (F_{q'} \textit{ dépend de } B_k).$$

(*b*) *L'isomorphisme* $\varphi_k : B_k \to A_k = A\, l_k$ *est défini par les substitutions :*

$$\mu_i \to X_i^2 l_k$$
$$Z_j \to P_j l_k$$

(P_j *est le polynôme minimum de* μ_j *sur* $\mathbb{F}_q$, $1 \leqq j \leqq n$).

(*c*) *Pour tout* k *tel que* $2t+1 \leqq k \leqq N-1$, *le corps* $F_{q'}$ *est une extension de degré pair de* $\mathbb{F}_q$.

Pour $k=N$, *on a* $F_{q'}=F_q$.

Preuve de (*a*) et de (*b*) dans [3].

Preuve de (*c*) dans [5].

Par la suite, N_k désignera l'idéal maximal de B_k :

$$N_k=(Z_1, \ldots, Z_n);$$

on posera :

$$M_k=\varphi_k(N_k).$$

Rappelons que tout élément de N_k est de carré nul. Pour tout k tel que $2t+1 \leqq k \leqq N$, désignons par $\hat{\tau}$ l'automorphisme de B_k conjugué par φ_k de l'automorphisme τ. On obtient directement la propriété suivante :

Propriété 3 : $\hat{\tau}$ *est un automorphisme involutif de* B_k *défini par l'ensemble des substitutions :*

$$\mu_i \to \mu_i^{-1}$$
$$Z_j \to \alpha_j Z_j \qquad (\alpha_j \in F_{q'},\ 1 \leqq j \leqq n).$$

Partie II. Dénombrement des codes étudiés

Dans cette seconde partie, après avoir rappelé (*cf.* [2]) la construction des codes autoduaux principaux de A, nous démontrons que ces codes sont isomorphes à des codes à une variable, puis nous donnons leur dénombrement.

Soit $g=g_1+\ldots+g_N$ un élément de A.

Proposition 1 : *L'idéal* (g) *est un code autodual nilpotent de* A *si et seulement si :*

$1°$ g_k *appartient à :* $M_k \setminus M_k^2 \quad (1 \leq k \leq N)$;

$$2° \quad \begin{cases} g_{2t}=\tau(g_{2k-1}) & (1 \leq k \leq t), \\ g_k\,\tau(g_k)=0 & (2t+1 \leq k \leq N). \end{cases}$$

Preuve dans [2].

Remarque : En pratique, la recherche des éléments g_k vérifiant les conditions 1° et 2° de la proposition 1, s'effectue non directement dans A_k mais dans B_k, en utilisant les isomorphismes φ_k et $\hat{\tau}$. Par la suite, Lorsqu'on sera dans B_k, *on se référera encore à ces conditions* 1° *et* 2° de la proposition 1.

Soit Π l'ensemble des diviseurs premiers de $t_1(X_1)$. Pour tout π appartenant à Π, notons Q_π le reste de la division de $t_1(X_1)/\pi$ par π.

Désignons par Q_π^{-1} l'inverse de Q_π dans A.

Théorème 1 : *Tous les codes autoduaux principaux nilpotents de* A *sont isomorphes au code à une variable engendré par :*

$$\sum_\pi \frac{t_1^2(X_1)}{\pi} Q_\pi^{-2},$$

où π *parcourt l'ensemble* Π.

Démonstration : Soit (g) un code autodual nilpotent de A. Pour chaque algèbre $A_k = A\,l_k$, en bijection avec la classe C $(\mu_1, \ldots, \mu_n)$, désignons par Π_k le polynôme minimum de la première composante μ_1 $(1 \leq l \leq N)$.

On sait [3] que l_k est de la forme :

$$l_k = \frac{t_1^2}{\pi_k^2}\theta_k^2, \tag{1}$$

pour un certain polynôme $\theta_k(X_1, \ldots, X_n)$ tel que :

$$\text{(2)} \quad \begin{cases} \left(\dfrac{t_1}{\pi_k}\theta_k\right)(\mu_1, \mu_2, \ldots, \mu_n)=1, \\ \left(\dfrac{t_1}{\pi_k}\theta_k\right)(\mu_1, \mu_2', \ldots, \mu_n')=0 \\ \text{pour} \quad \mu_i' \neq \mu_i \quad (2 \leq i \leq n). \end{cases}$$

Dans [2], nous avons démontré que les codes autoduaux principaux nilpotents sont isomorphes au code engendré par :

$$P = P_1\,l_1 + \ldots + P_N\,l_N. \tag{3}$$

Considérons la décomposition suivante de A :

$$A \simeq \prod_{\pi \in \Pi} \mathbb{F}_q[X_1, \ldots, X_n]/(\pi^2, t_2^2, \ldots, t_n^2).$$

Supposons $\mathbb{F}_q[X_1, \ldots, X_n]/(\pi^2, t_2^2, \ldots, t_n^2)$ égale à une somme de n_π algèbres locales.

Nous pouvons alors écrire (3) de la manière suivante :

$$P = \sum_{\pi \in \Pi} \pi(l_1 + \ldots + l_{n_\pi}).$$

D'après (1), on a :

$$e_1 + \ldots + l_{n_\pi} = Q_\pi^{-2}\frac{t_1^2}{\pi^2}(Q_\pi\theta_1 + \ldots + Q_\pi\theta_{n_\pi})^2.$$

Mais, par définition de Q_π, et d'après (2), on vérifie que $Q_\pi\theta_k$ est l'un des n_π idempotents primitifs de l'algèbre :

$$\mathscr{F}_q[X_1, \ldots, X_n]/(\pi, t_2, \ldots, t_n).$$

On a donc :

$$Q_\pi\theta_1 + \ldots + Q_\pi\theta_{n_\pi} \equiv 1 \bmod (\pi, t_2, \ldots, t_n).$$

Ceci implique :

$$l_1 + \ldots + l_{n_\pi} \equiv Q_\pi^{-2}\frac{t_1^2}{\pi^2} \bmod (t_1^2, t_2^2, \ldots, t_n^2).$$

D'où :

$$P = \sum_\pi \frac{t_1^2(X_1)}{\pi} Q_\pi^{-2}.$$

CQFD

Cherchons maintenant le dénombrement.

D'après la proposition 1, le problème est de dénombrer les éléments x de B_k $(2t+1 \leq k \leq N)$ appartenant à $N_k \setminus N_k^2$ et vérifiant :

$$x\,\hat{\tau}(x)=0. \tag{4}$$

Ordonnons la base des monômes $Z_1^{i_1} \ldots Z_n^{i_n}$ de B_k suivant l'ordre lexicographique sur les n-uples $(i_1, \ldots, i_n)$.

Posons

$i = i_1 + i_2\,2 + \ldots + i_n 2^{n-1}$ et $j = j_1 + \ldots + j_n 2^{n-1}$.

Si on a :

$$(i_1, \ldots, i_n) \leq (j_1, \ldots, j_n),$$

on écrira encore :

$$i \leq j.$$

Tout élément x appartenant à $N_k \setminus N_k^2$ s'écrit :

$$x = \sum_{1 \leq i} x_i Z_1^{i_1} \ldots Z_n^{i_n} \qquad (x_i \in \mathbb{F}_{q'}),$$

où un au moins des coefficients x_i $(1 \leq i \leq n)$ non nul.

On dira que $\sum_{i=1}^{n} x_i Z_i$ est le terme linéaire de x. On a, d'après la propriété 3 :

$$\hat{\tau}(x)=\sum_{1 \leqq i} \hat{\tau}(x_i)\,\alpha_1^{i_1} \ldots \alpha_n^{i_n} Z_1^{i_1} \ldots Z_n^{i_n},$$

avec :

$$\alpha_1^{i_1} \ldots \alpha_n^{i_n}\,\hat{\tau}(\alpha_1^{i_1} \ldots \alpha_n^{i_n})=1.$$

Nous poserons pour tout i : $x_i'=\hat{\tau}(x_i)\,\alpha_1^{i_1} \ldots \alpha_n^{i_n}$. L'équation (4) s'écrit :

$$x\,\hat{\tau}(x)=\sum_k \Bigg(\sum_{\substack{i+j=k \\ i<k}} x_i x_j'\Bigg) Z_1^{k_1} \ldots Z_n^{k_n}=0.$$

Ceci implique, pour tout k :

$$(5) \qquad F_k=\sum_{i<k} x_{k-i}'=0.$$

Définition : Nous dirons qu'une équation F_k (resp. une inconnue x_i) est de poids $\omega(k)$ lorsque le n-uple binaire $k=(k_1, \ldots, k_n)$ possède $\omega(k)$ composantes non nulles (resp. de poids $\omega(i)$).

Lemme 1 : *Dans une extension $\mathbb{F}_{q'}$ de $\mathbb{F}_q$ de degré pair ($q'=q^{2k}$) l'équation :*

$$y+a\,\hat{\tau}(y)=b \qquad \textit{avec} \quad a\,\hat{\tau}(a)=1$$

admet q^k solutions si et seulement si $b=a\,\hat{\tau}(b)$.

Preuve : dans [ ].

Lemme 2 : *Pour tout* K, *on a :*

$$\sum_{k<K} x_{K-k} E_k=0.$$

Preuve : Notons d'abord l'équivalence suivante :

$$i \leqq k \quad \Leftrightarrow \quad K-k \leqq K-i.$$

Considérons un terme $x_i x_{k-i}'$ ($i<k$) de l'équation E_k. Alors le terme $x_{K-k}(x_i x_{k-i}')$ de $x_{K-k} E_k$ s'annule avec le terme :

$$x_i(x_{K-k} x_{K-i-}'(K-k))\,\text{de}\, x_i E_{K-i}.$$

On montre ainsi que dans $\sum_{k<K} x_{K-k} E_k$, tous les termes s'annulent deux à deux.

Supposons $x_1 \neq 0$ (on effectuera un raisonnement analogue en supposant $x_1=0, \ldots, x_{i-1}=0$, $x_i \neq 0$, $2 \leqq i \leqq n$).

Lemme 3 : *Parmi les C_n^j équations de poids j, il y a C_{n-1}^j équations redondantes.*

Preuve : Le nombre d'équations non redondantes est C_{n-1}^{j-1} (considérer la répartition des inconnues de poids $j-1$ distinctes de x_1).

Montrons que les C_{n-1}^j équations restantes sont redondantes. Le nombre de n-uplets $K=(K_1, \ldots, K_n)$ de poids $j+1$ de la forme $(1, K_2, \ldots, K_n)$ est justement C_{n-1}^j.

Le lemme 2 permet de conclure.

Désignons dans ce qui suit par :

– $F_{q^{r_k}}$ le corps de base de B_k ($1 \leqq k \leqq t$);

– $F_{q^{2t_k}}$ le corps de base de B_k ($2t+1 \leqq k \leqq N-1$);

– $F_{q^{r_0}}$ le corps de base de B_N ($r_0=1$).

Proposition 2 : *Le nombre d'éléments x de B_k vérifiant les conditions analogues aux conditions* 1 *et* 2 *de la proposition* 1, *est :*

(*a*) *Lorsque k vérifie $2t+1 \leqq k \leqq N-1$:*

$$\mathcal{N}_k=(q^{t_k}+1)(q^{nt_k}-1)\,q^{t_k(2^n+2^{n-1}-n)}.$$

(*b*) *Lorsque k vérifie $1 \leqq k \leqq t$:*

$$\mathcal{N}_k=(q^{r_k n}-1)\,q^{r_k(2^n-n-1)}.$$

Lorsque $k=N$:

$$\mathcal{N}_N=(q^n-1)\,q^{2^n-n-1}.$$

Démonstration : (*a*) Considérons les équations de poids j ($3 \leqq j \leqq n$).

Le nombre total d'inconnues de poids $j-1$ dans l'ensemble des C_n^j équations de poids j est C_n^{j-T}.

Il y a donc : C_{n-1}^{j-1} inconnues principales et C_{n-1}^{j-2} inconnues secondaires ou libres.

On peut supposer par récurrence déterminées les inconnues de poids inférieur ou égal à $j-2$.

Nous avons alors (lemme 1) :

$q^{t_k C_{n-1}^{j-1}}$ valeurs possibles pour les inconnues principales et $q^{2t_k C_{n-1}^{j-2}}$ valeurs possibles pour les inconnues libres.

On a donc $q^{t_k[C_{n-1}^{j-1}+2C_{n-1}^{j-2}]}$ solutions pour l'ensemble des équations de poids j ($3 \leqq j \leqq n$).

Maintenant, les équations non redondantes de poids $j=2$ telles que $x_1=\ldots=x_{i-1}=0$ et $x_i \neq 0$ sont au nombre de C_{n-i}^1.

Toujours d'après le lemme 1, le nombre de solutions de l'ensemble de ces équations est $q^{t_k(n-i)}$.

Enfin, on a :

– $q^{2t_k}-1$ choix pour le premier coefficient non nul du terme linéaire de x, et

– q^{2t_k} choix pour le coefficient de $Z_1 Z_2 \ldots Z_n$.

Finalement, le nombre d'éléments x de B_k appartenant à $N_k \diagdown N_k^2$ et vérifiant $x\,\hat{\tau}(x)=0$ est :

$$\mathcal{N}_k=\sum_{i=1}^{n}(q^{2t_k}-1)\,q^{t_k(n-i)} \times \left[\prod_{j=3}^{n} q^{t_k[C_{n-1}^{j-1}+2C_{n-1}^{j-2}]}\right] q^{2t_k}.$$

Ce qui, en simplifiant, donne la formule (*a*) de la proposition.

(*b*) Lorsque $k=N$, nous avons $F_{q'}=F_q$ et quel que soit y appartenant à F_q, $\hat{\tau}(y)=y$.

L'équation $x\,\hat{\tau}(x)=0$ est alors vérifiée pour tout élément x dans $N_k \diagdown N_k^2$.

Lorsque k vérifie $1 \leqq k \leqq t$, on doit aussi considérer (proposition 1) tous les éléments de $N_k \setminus N_k^2$.
On déduit aisément les expressions de $\mathcal{N}_k$ au moyen des dimensions de N_k et de N_k^2.

CQFD

Par la suite, $\mathcal{N}_N$ sera noté $\mathcal{N}_0$.
Nous sommes maintenant en mesure de donner le nombre de codes étudiés.

Théorème 2 : *Le nombre de codes autoduaux nilpotents principaux de l'algèbre* A *est :*

$$\mathcal{N} = \prod_{k=0}^{t} q^{r_k (2^{n-1}-n)} (q^{nr_k} - 1)$$
$$\times \prod_{k=2t+1}^{N-1} q^{t_k (2^{n-1}-n)+1} (q^{t_k}+1)(q^{nt_k}-1).$$

Démonstration : Soit z un élément dans B_k appartenant à $N_k \setminus N_k^2$. On a :

$$\dim(z) = 2^{n-1}.$$

D'autre part, on sait que (*cf.* [4]) :

$$v_k = |(z) \cap N_k^2| = |(z) \cap (N_k \setminus N_k^2)|.$$

Pour déterminer le nombre d'idéaux (z) distincts dans chaque B_k, il suffit de diviser par V_k le nombre d'éléments z vérifiant les conditions analogues aux conditions 1° et 2° de la proposition 1.
La propriété 2 et la proposition 2 permettent de conclure.

Conclusion

Nous savons construire les codes autoduaux principaux nilpotents de A, et nous savons décrire leur groupe d'automorphismes [2].
Nous venons de montrer que tous ces codes sont isomorphes à des codes à une variable, et nous avons donné leur nombre.
Il reste à déterminer ceux de ces codes qui ne sont pas équivalents, au sens de la métrique de Hamming.

BIBLIOGRAPHIE

[1] A. Poli, Codes dans certaines algèbres modulaires, *Thèse de doctorat en sciences*, Université de Toulouse, 1978.

[2] A. Poli et J. A. Thiong-Ly, Automorphisms of principal nilpotent self dual codes in certain modular algebras, *Colloque international de Toulouse*, Algèbre et Codes, juin 1983 (soumis à publication).

[3] A. Poli, Important calculations in n-variable codes, *Colloque International de Toulouse*, Algèbre et Codes, juin 1983 (soumis à publication).

[4] A. Poli et M. Ventou, Codes autoduaux principaux et groupe d'automorphismes de l'algèbre $j = \mathbb{F}_q[K_1, \ldots, X_n]/(X_1^2-1, \ldots, X_1^2-1)$ $(q=2^1)$, *Eur. J. Comb.*, Acad. Press, 2, 1981, p. 179-183.

[5] A. Poli et C. Rigoni, Codes autoduaux $2k$-circulants, *Colloque : « Codes correcteurs »*, Cachan, mai 1984, *Actes* (à paraître).

[6] M. Ventou, Contribution à l'étude des codes correcteurs, *Thèse de spécialité*, Université P.-Sabatier, Toulouse, 1984.