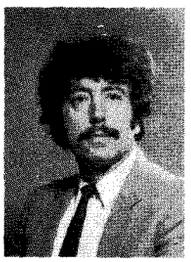
Codes autoduaux 2 k circulants de caractéristique impaire

Self dual 2 k circulant codes



Alain POLI

Laboratoire AAECC, Université P.-Sabatier, 31000 TOULOUSE

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

C. RIGONI

Laboratoire AAECC, Université P.-Sabatier, 31000 TOULOUSE

Étudiant 3e cycle, boursier DGRST, à l'Université P.-Sabatier de Toulouse. Diplôme : DEA Informatique. Membre du AAECC, laboratoire LSI, domaine : les codes correcteurs polynômiaux et leurs applications.

RÉSUMÉ

Nous caractérisons une famille de codes qui généralise la famille des codes doublement circulants étudiés en particulier par MacWilliams, Karlin, Beenker, Ventou, Rigoni (ref. [1 à 4]).

MOTS CLÉS

Codes autoduaux, codes 2*k* circulants, décomposition d'algèbres, construction de codes, dénombrement de codes

SUMMARY

We characterize a family of codes which generalize the family of doubly circulant codes studied in particular by MacWilliams, Karlin, Beenker, Ventou, Rigoni (ref. [1 to 4]).

KEY WORDS

Self dual codes, 2k circulant codes, decomposition of algebras, construction of codes, enumeration of codes.

TABLE DES MATIÈRES

Introduction

La découverte d'une matrice génératrice double circulante du code de Golay binaire étendu est à l'origine de l'étude des codes doubles circulants.

Karlin, MacWilliams et Beenker principalement développent des études sur de tels codes [2, 3, 4].

Dans un papier très récent (réf. [1]), Ventou et Rigoni caractérisent de manière constructive tous les codes doubles circulants qui sont autoduaux.

Une généralisation des codes doubles circulants est constituée, d'une certaine manière, par les codes quasi cycliques dont une matrice génératrice est obtenue par concaténation de matrices circulantes. En particulier P. Piret donne des résultats intéressants dans [7].

Les codes k circulants (en abrégé CkC) que nous étudions dans ce papier généralisent les deux familles de codes dont nous venons de parler.

L'étude que nous présentons dans ce papier fournit une méthode de construction de tous les CkC autoduaux sur $\mathbb{F}_q$ ($q=p^r$, p premier impair). De plus nous établissons les conditions nécessaires et suffisantes d'existence de ces codes, et lorsque celles-ci sont vérifiées nous indiquons le nombre de codes.

Pour cela nous rappelons, dans une première partie, une description des résultats qui nous sont utiles, concernant l'algèbre A :

$$A=\mathbb{F}_q[X_1, \ldots, X_k]/(X_1^{n_1}-1, \ldots, X_k^{n_k}-1).$$

Nous montrons ensuite dans la partie II comment transformer le problème matriciel de la recherche de CkC autoduaux en la résolution d'une équation dans $\mathbb{F}_q$, et d'une équation dans A.

Nous présentons enfin dans une dernière partie une méthode de construction des CkC autoduaux. Nous en déduisons les conditions nécessaires et suffisantes d'existence des CkC autoduaux, et lorsque ces conditions sont vérifiées nous précisons le nombre de ces codes.

1re partie. Cadre algébrique

Donnons tout d'abord les notations que nous utilisons par la suite.

Nous désignons par m_i la multiplicité des racines de $X_i^{n_i}-1$, et nous supposons $m_i \leqq m_j (1 \leqq i \leqq j \leqq k)$.

Nous posons $m=m_k$ et $n=n_1 \times \ldots \times n_k$.

La polynôme $p_i(X_i)$, de degré d_i, désignera un facteur irréductible de $X_i^{n_i}-1$. Nous noterons α_i une racine de $p_i(X_i)$. On désigne par $\omega_i, \ldots, \alpha_{i-1}, X_i)$ un facteur irréductible de $p_i(X_1)$ dans $\mathbb{F}_q(\alpha_1, \ldots, \alpha_{i-1})[X_1]$. Nous notons pour simplifier ω_i le polynôme $\omega_i(X_1, \ldots, X_i)$.

Enfin $\{(\alpha_1, \ldots, \alpha_k)\}$ désigne la classe de transitivité de $(\alpha_1, \ldots, \alpha_k)$ sous l'exponentiation par q.

Désignons par τ l'automorphisme involutif de A défini par :

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

Illustrons les notations par l'exemple suivant :

Choisissons :

$$A=\mathbb{F}_2[X_1, X_2, X_3]/(X_1^3-1, X_2^{10}-1, X_3^{24}-1).$$

Nous avons donc :

$$n=720, \quad m_1=1, \quad m_2=2, \quad m_3=m=8.$$

La factorisation des polynômes $X_i^{n_i}-1$ est :

$$X_1^3-1=(X_1+1)(1+X_1+X_1^2),$$
$$(X_2^5-1)^2=(X_2-1)^2(1+X_2+X_2^2+X_2^3+X_2^4)^2,$$
$$(X_3^3-1)^8=(X_3-1)^8(1+X_3+X_3^2)^8.$$

Choisissons les facteurs de $x_i^{n_i}-1$ suivant :

$$P_1(X_1)=1+X_1+X_1^2,$$
$$P_2(X_2)=1+X_2+X_2^2+X_2^3+X_2^4,$$
$$P_3(X_3)=1+X_3+X_3^2.$$

On a :

$$d_1=2, \quad d_2=4, \quad d_3=2,$$
$$\omega_2(\alpha_1, X_2)=1+\alpha_1 X_2+X_2^2,$$
$$\omega_3(\alpha_1, \alpha_2, X_3)=1+\alpha_1+X_3.$$

La classe de transitivité sous l'exponentiation par 2 de $(\alpha_1, \alpha_2, \alpha_3)$ est :

$$\{(\alpha_1 \alpha_2, \alpha_3)\}=\{(\alpha_1, \alpha_2, \alpha_3), (\alpha_1^2, \alpha_2^2, \alpha_3^2), (\alpha_1, \alpha_2^4, \alpha_3), (\alpha_1^2, \alpha_2^8, \alpha_3^2)\}.$$

Donnons maintenant quelques propriétés de A. Ces résultats sont des développements classiques des travaux du AAECC. C'est pourquoi ils ne sont pas démontrés ici. Nous renvoyons le lecteur à des références bibliographiques [5], [6] et [8].

Proposition 1 :

— A se décompose en une somme directe d'idéaux principaux : $A = A_1 \oplus \ldots \oplus A_N$, *et l'on a*

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

— Il existe une bijection entre l'ensemble des idéaux A_i *et l'ensemble des classes* $\{(\alpha_1, \ldots, \alpha_k)\}$. *Si* A_i *correspond à* $\{(\alpha_1, \ldots, \alpha_k)\}$ *alors* $\tau(A_i)$ *correspond à* $\{(\alpha_1^{-1}, \ldots, \alpha_k^{-1})\}$.

— Si A_i *correspond à* $\{\alpha_1, \ldots, \alpha_k)\}$, *alors il existe un isomorphisme* φ_i *entre* A_i *et l'algèbre* B_i :

$$B_i = \frac{\mathbb{F}_q[X_1, \ldots, X_k, Z_1, \ldots, Z_k]}{(p_1, \omega_2, -, \omega_k, Z_1^{m_1}, \ldots, Z_k^{m_k})}.$$

Ces trois points sont démontrés par A. Poli (réf. [5, 6]).

L'idempotent de A_i sera noté e_i. On conviendra que A_N correspond à $\{(1, 1, \ldots, 1)\}$.

2e partie. Les codes autoduaux $2k$ circulants

Donnons dans un premier temps deux définitions relatives aux C*k*C.

Définition 1 : Une matrice *k* circulante sur $\mathbb{F}_q$ est une matrice carrée Q du type suivant :

$$Q = \begin{pmatrix} Q_0 & Q_1 & \ldots & Q_{n_k-1} \\ Q_{n_k-1} & Q_0 & \ldots & Q_{n_k-2} \\ \vdots & \vdots & & \vdots \\ Q_1 & Q_2 & & Q_0 \end{pmatrix},$$

où chaque Q_i est une matrice $(k-1)$ circulante si $(k-1)$ est non nul, et où Q_i est un élément de $\mathbb{F}_q$ sinon.

Définition 2 : Un code est dit *k* circulant pur si il admet une matrice génératrice de la forme : (I Q).

Un code est dit *k* circulant bordé si il admet une matrice génératrice de la forme :

$$\begin{pmatrix} a & 0 \ldots 0 & a & 1-1 \\ b & & d & \\ \vdots & I & \vdots & Q \\ b & & d & \end{pmatrix},$$

où *a*, *b*, *c* et *d* sont des éléments de $\mathbb{F}_q$.

Indiquons maintenant le lien qui existe entre l'algèbre des matrices *k* circulantes et A.

Propriété 2 : L'algèbre des matrices *k* circulantes Q est isomorphe à l'algèbre A. L'isomorphisme est défini de la façon suivante : à Q nous faisons correspondre le polynôme $Q(X_1, \ldots, X_k)$ dont les coefficients sont ceux de la première ligne de Q dans la base canonique de A où les monômes sont classés par rapport à l'ordre lexicographique.

La proposition suivante permet d'énoncer le problème de la recherche de C*k*C autoduaux en termes de polynômes.

Proposition 2 : *Un C*k*C est autodual si et seulement s'il possède une matrice génératrice vérifiant la (les) condition(s) suivante(s) :*

(a) Code pur : -1 *doit être résidu quadratique dans* $\mathbb{F}_q$, *et on doit avoir :* $Q\tau(Q) = -1$ *dans* A.

(b) Code bordé :

$$(1) \qquad a^2 + c^2 = -n,$$

$$(2) \quad Q\tau(Q) = \begin{cases} -1 \text{ si } -1 \text{ est rendu quadratique dans } \mathbb{F}_q, \\ -1 + e_N \text{ sinon.} \end{cases}$$

Cette proposition est prouvée par *k* égal à 1 dans [1], et se démontre directement pour *k* quelconque en généralisant ce dernier résultat.

L'équation (1) est résolue dans [1].

3e partie. Résolution

Nous résolvons dans cette partie l'équation (2) en utilisant la décomposition de A indiquée dans la partie I

Posons : $Q = q_1 + \ldots + q_N$ avec $q_i \in A_i (1 \leqq i \leqq N)$.

Résoudre l'équation (2) revient à caractériser les éléments $q_1, \ldots, q_N$.

Lemme 1 : *Les sommes partielles* $q_{2i-1} + q_{2i}$ $(1 \leqq i \leqq M)$ *sont de la forme:* $s_{2i-1} - \tau(s_{2i-1}^{-1})$, *où* S_{2i-1} *est un inversible quelconque de* A_{2i-1}.

La preuve de ce lemme est directe.

Déterminons maintenant $q_j (2M < j \leqq N)$, ce qui est un problème plus délicat.

Pour des commodités de notation, nous appelons :

— B l'algèbre isomorphe à A_j (*cf.* proposition 1) :

$$B = \frac{\mathbb{F}_q[X_1, \ldots, X_k, Z_k]}{(p_1, \omega_2, \ldots, \omega_k, Z_1^{m_1}, \ldots, Z_k^{m_k})}.$$

— K le corps résiduel de B :

$$K = \mathbb{F}_q[X_1, \ldots, X_k]/(p_1, \omega_2, \ldots, \ldots, \omega_k).$$

— δ la dimension de K. D'après [8] :

$$\delta = \text{ppcm}(d_1, \ldots, d_k).$$

— τ' l'automorphisme conjugué de la restriction de τ à A_j, dans B.

En utilisant l'isomorphisme φ_i défini dans la partie I, nous ramenons la détermination des q_j à la détermination des éléments *r* de B tels que :

$$r\tau'(r) = -1 \quad \text{dans B.}$$

Posons :

$$r = x(1+u) \qquad \text{avec} \quad \begin{cases} x \in K, \\ u \text{ nilpotent de B.} \end{cases}$$

L'équation précédente se transforme en les deux équations :

$$\begin{cases} x\tau'(x) = -1 \quad \text{dans K.} \\ (1+u)\tau'(1+u) = 1 \quad \text{dans B.} \end{cases}$$

Donnons un lemme qui nous permettra de caractériser les éléments x.

Lemme 2 : *Lorsque* K *est une extention stricte de* $\mathbb{F}_q$, *il est de dimension* δ *paire* ($\delta = 2t$) *et on a :*

$$\tau'(x) = x^{q^t} \qquad (\forall x \in K).$$

De plus l'ensemble des points fixes de τ' *est un espace vectoriel de dimension t.*

On caractérise maintenant les éléments x.

Lemme 3 : *Les solutions de l'équation :* $x\tau'(x) = -1$ *dans* K *sont :*

- *les* $q^t + 1$ *racines du polynôme* $Y^{q^t+1} + 1$ *si* $\delta = 2t$.
- $\pm\sqrt{-1}$ *si* $\delta = 1$.

Cherchons maintenant les éléments $1+u$ de B tels que :

$$(1+u)\tau'(1+u) = 1.$$

Soit N l'ensemble des nilpotents de B.

Considérons :

$$I = \{1+u / u \in N\}.$$

φ et ψ deux applications de B dans B définies par :

$$\varphi : x \to x\tau'(x),$$
$$\psi : x \to x + \tau'(x).$$

Nous présentons maintenant un lemme qui permet de caractériser les éléments $1+u$.

Lemme 4 :

$$I \cap \operatorname{Im}\psi = \varphi(I).$$

Démonstration : Nous ne démontrons que le seul point non trivial :

$$I \cap \operatorname{Im}\psi \subset \varphi(I).$$

Soit : $1+u \in I \cap \operatorname{Im}\psi$.

L'ordre multiplicatif de $1+u$ est de la forme q^s. On a donc :

$$1+u = (1+u)^{(q^s+1)/2}\,\tau'(1+u)^{(q^s+1)/2}.$$

Ce qui signifie que : $1+u \in \varphi(I)$.

Le lemme précédent nous conduit donc à dénombrer les éléments de $I \cap \operatorname{Im}\psi$.

Proposition 3 :

$$|I \cap \operatorname{Im}\psi| = q^{(m_1 \cdots m_k - 1)\delta/2}.$$

Démonstration : Dénombrons donc les éléments u de N fixés par τ'. Pour cela posons :

$$C_1 = K[Z_1]/(Z_1^{m_1})$$
$$C_l = C_{l-1}[Z_l]/(Z_l^{m_l}) \qquad (2 \leqq l \leqq k).$$

N_l l'ensemble des nilpotents de C_l ($1 \leqq l \leqq k$). Notons : ψ_l, la restriction de ψ à N_l; λ_l, la dimension de $\operatorname{Im}\psi_l$ sur $\mathbb{F}_q$.

Nous faisons un raisonnement par récurrence sur l. Supposons que :

$$\lambda_{l-1} = \frac{(m_1 \ldots m_{l-1} - 1)\delta}{2}$$

et démontrons que :

$$\lambda_l = \frac{(m_1 \ldots m_l - 1)\delta}{2}.$$

Considérons la famille F_l :

$$F_l = \{ f_i = (Z_l - \tau'(Z_l))^i / 0 \leqq i < m_l \},$$

F_l est une C_{l-1} base de C_l.

Soit un élément u, point fixe de τ' dans N_l. Alors nous pouvons écrire :

$$u = u_0 f_0 + u_1 f_1 + \ldots + u_{m_l-1} \cdot f_{m_l-1}$$

et

$$\tau'(u) = \tau'(u_0) f_0 - \tau'(u_1) f_1 + \ldots + \tau'(u_{m_l-1}) f_{m_l-1}.$$

Soit :

$$\begin{cases} u_{2i} = \tau'(u_{2i}) & \left(0 \leqq i \leqq \dfrac{m_l - 1}{2}\right), \\ u_{2i-1} = -\tau'(u_{2i-1}) & \left(1 \leqq i \leqq \dfrac{m_l - 1}{2}\right). \end{cases}$$

D'après l'hypothèse de récurrence il y a autant d'éléments de N_{l-1} invariants par τ' que d'éléments tels que : $u = -\tau'(u)$ car :

$$\lambda_{l-1} = \frac{\dim(N_{l-1})}{2} = \dim(\operatorname{Ker}\psi_{l-1}).$$

D'où :

$$\lambda_l = \begin{cases} \lambda_{l-1} + (\lambda_{l-1} + t)\dfrac{(m_l - 1)}{2} \\ \quad + (\lambda_{l-1} + t)\left(\dfrac{m_l - 1}{2}\right) & \text{si} \quad \delta = 2t, \\ \lambda_{l-1} + (\lambda_{l-1} + 1)\dfrac{(m_l - 1)}{2} \\ \quad + \lambda_{l-1}\dfrac{(m_l - 1)}{2} & \text{si} \quad \delta = 1. \end{cases}$$

Soit dans tous les cas :

$$\lambda_l = \frac{(m_1 \ldots m_l - 1)\,\delta}{2}.$$

La propriété est vraie pour l égal à 1. D'où :

$$\lambda_k = \frac{(m_1 \ldots m_k - 1)\,\delta}{2}$$

et

$$|\mathrm{I} \cap \mathrm{Im}\,\psi| = q^{(m_1 \cdots m_k - 1)\,\delta/2}.$$

Nous obtenons ainsi le corollaire suivant :

Corollaire : *Le nombre de choix possibles pour r est :*

$$c_0\, q^{(m_i \times \ldots \times m_k - 1)\,\delta/2}$$

avec :

$$c_0 = \begin{cases} q^t + 1 & si\ \ \delta = 2t, \\ 2 & si\ \ \delta = 1. \end{cases}$$

Démonstration : Il nous suffit de préciser le nombre d'éléments $(1+u)$ tels que :

$$(1+u)\,\tau'(1+u) = 1 \quad \text{dans B.}$$

D'après la proposition 3 nous avons :

$$|\varphi(\mathrm{I})| = q^{(m_1 \times \ldots \times m_k - 1)\,\delta/2}.$$

Le nombre de solutions $(1+u)$ est : $|\mathrm{I}|/|\varphi(\mathrm{I})|$ soit :

$$q^{(m_1 \times \ldots \times m_k - 1)\,\delta/2}.$$

Ces résultats permettent d'énoncer le théorème suivant.

Théorème : *Il existe des C k C autoduaux de caractéristique impaire si et seulement si l'une des hypothèses suivantes est vérifiée :*

$(\mathrm{H}_1) - 1$ *est résidu quadratique dans* $\mathbb{F}_q$.

Alors il y a :

$$q^{(1/2)(n-(n/m_1 \times \ldots \times m_k))} \prod_{i=1}^{M} (q^{\delta 2i} - 1) \times \prod_{j=2M-1} c_j \quad \textit{codes purs.}$$

$$c_0\, q^{(1/2)(n-(n/m_1 \ldots m_k))} \prod_{i=1}^{M} (q^{\delta 2i} - 1) \times \prod_{j=2M-1}^{N} c_j \quad \textit{codes bordés.}$$

$(\mathrm{H}_2) - 1$ *n'est pas résidu quadratique dans* $\mathbb{F}_q$, *n est impair et non nul module p.*

Alors il y a :

$$c_0\, q^{(1/2)(n-(n/m_1 \times \ldots \times m_k))} \prod_{i=1}^{M} (q^{\delta 2i} - 1) \times \prod_{j=2M+1}^{N} c_j \quad \textit{codes bordés.}$$

Avec :

c_0 *est le nombre de couples* (a, c) *solutions de l'équation* (1) *et est égal à :*

$$c_0 = \begin{cases} 2(q-1) & si\ \ n \textit{ est nul modulo } p, \\ (q-3) & si\ -n \textit{ est un carré non nul modulo } p \\ (q-1) & \textit{sinon}, \end{cases}$$ ref. [1],

c_j *est :*

$$c_j = \begin{cases} 2 & si\ \ \delta_j = 1, \\ q^{t_j} + 1 & si\ \ \delta_j = 2\,t_j; \end{cases}$$

δ_j *est la dimension du corps résiduel de* B_j.

Nous indiquons que dans chaque cas le dénombrement dépend de l'algèbre A.

Conclusion

Nous avons apporté dans ce papier deux résultats qui à notre connaissance sont nouveaux.

Pour premier résultat nous avons généralisé l'étude des codes doubles circulants publiée par H. Ventou et C. Rigoni dans [1]. Pour second résultat nous avons précisé le nombre de C k C autoduaux définis sur des corps de caractéristique impaire.

De plus nous rappelons que la méthode que nous avons développée est une méthode constructive.

Nous n'avons pas traité dans ce papier le cas particulier où q est pair car les démonstrations sont totalement différentes. Nous publierons dans un prochain article les résultats dans ce cas.

BIBLIOGRAPHIE

[1] M. Ventou et C. Rigoni, Self Dual Doubly Circulant Codes, *Actes du Colloque de juin* 1983 *à Toulouse*, thème : « Algèbre et codes correcteurs : théorie et applications ».

[2] M. Karlin, New Binary Coding by Circulant, *IEEE trans. Info. theory*, 15, 1969, p. 81-92.

[3] G. F. H. Beenker, On Double Circulant Codes, TH report 80, WSK, 4 july 1980, Technological University Eindhoven.

[4] F. J. MacWilliams, Orthogonal Circulant Matrices, *Journal of comb. theory*, 10, 1971, p. 1-17.

[5] A. Poli, Codes dans certaines algèbres modulaires, *Thèse de doctorat d'état*, Université P.-Sabatier, 1978, Toulouse, France.

[6] A. Poli, Idéaux principaux nilpotents de dimension maximale dans l'algèbre $\mathbb{F}_q$G d'un groupe abelien fini G, *Communications in Algebra*, 12, (4), 1984, p. 391-401.

[7] P. Piret, Good linear codes of length 27 and 28, *IEEE trans on Info. theory*, IT-26, n° 2, mars 1980.

[8] C. Rigoni, Construction de codes à *n* variables, *Actes du Colloque de juin* 1983 *à Toulouse*, thème : « Algèbre et codes correcteurs : théorie et applications ».