Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 971–974
COMPTES RENDUS MATHEMATIQUE

Algèbre/Informatique théorique

Caractérisation des codes auto-duaux binaires de type II à partir du code de Hamming étendu [8, 4, 4]

Ayoub Otmani

Laboratoire d'arithmétique, de calcul formel et d'optimisation (LACO), Université de Limoges, 123, avenue Albert Thomas, 87060 Limoges cedex, France

Reçu le 6 janvier 2003 ; accepté après révision le 6 mai 2003

Présenté par Gilles Kahn

Résumé

Nous montrons que tout code binaire de type II peut être construit sous forme de code Cortex dont le code de base est le code de Hamming étendu de paramètres [8, 4, 4]. ***Pour citer cet article : A. Otmani, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Abstract

Characterization of binary type II codes from the [8, 4, 4] **extended Hamming code.** We show that any binary type II code can be built as a Cortex code where the basis code is the [8, 4, 4] extended Hamming code. ***To cite this article: A. Otmani, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

1. Introduction

Les codes Cortex introduits dans [2] fournissent un moyen simple de construire des codes auto-duaux binaires lorsque le code de base l'est [2,1]. Ils offrent de plus une méthode efficace pour construire des codes extrémaux lorsque le code de Hamming étendu $\mathbb{H}_8$ de longueur 8 est le code de base. Cette construction permet en effet d'obtenir des codes auto-duaux binaires extrémaux de type II pour des longueurs inférieures ou égales à 64, ainsi qu'un nouveau code extrémal de paramètres [88, 44, 16] (cf. [1]).

Dans cette note, nous étendons ces résultats en prouvant que tout code de type II peut être obtenu sous forme de code Cortex à partir du code $\mathbb{H}_8$.

2. Construction cortex

2.1. Définitions

Un *code* $\mathcal{C}$ de longueur $n \geqslant 1$ sur le corps à deux éléments $\mathbb{F}_2$ est un sous-ensemble de $\mathbb{F}_2^n$. Les éléments de $\mathcal{C}$ sont alors appelés *mot de code*. Le *poids de Hamming* de $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ est le nombre de x_i non-nul. Un

Adresse e-mail : otmani@unilim.fr (A. Otmani).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(03)00232-2

code $\mathcal{C}$ est dit *linéaire* s'il est un sous-espace vectoriel de $\mathbb{F}_2^n$. Dans ce cas, une *matrice génératrice* de $\mathcal{C}$ est une matrice dont les lignes forment une base de $\mathcal{C}$. Ainsi, une matrice génératrice G d'un code linéaire de dimension k et de longueur n est de taille $k \times n$. La matrice G est dite sous forme *systématique* si la sous-matrice de taille $k \times k$ obtenue en prenant les premières colonnes de G est égale à la matrice identité I_k. Le *rendement* d'un code (linéaire) de dimension k et de longueur n est $\frac{k}{n}$. Nous renvoyons à [3] pour une présentation classique de la théorie des codes.

Pour tout entier $n \geqslant 1$, l'espace $\mathbb{F}_2^n$ est muni d'une forme bilinéaire symétrique non-dégénérée définie pour tout x et y de $\mathbb{F}_2^n$ par :

$$x \cdot y = \sum_{i=1}^{n} x_i y_i .$$

Deux vecteurs x et y sont dits *orthogonaux* si $x \cdot y = 0$. Le *dual* d'un code est l'ensemble des vecteurs z de $\mathbb{F}_2^n$ tels que z est orthogonal à chaque mot de code. Un code est dit *auto-dual* si et seulement s'il est égal à son dual. Par conséquent, un code auto-dual est de rendement $\frac{1}{2}$. D'autre part, le poids de Hamming de tout mot d'un code auto-dual est pair.

Un code auto-dual binaire est dit de *type II* si *tous* ses mots sont de poids divisible par 4, sinon il est dit de *type I* [3]. Ces deux cas représentent les deux seules éventualités d'après le théorème de Gleason–Pierce [4].

Deux codes qui diffèrent d'une permutation des symboles sont dits *équivalents*. Il est d'usage de confondre la classe des codes équivalents avec un représentant de cette classe.

On note $\mathbb{H}_8$ le code de Hamming étendu défini par la matrice G_8 :

$$G_8 = (I_4 \mid H_4) \stackrel{\text{def}}{=} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

Pour tout $k \geqslant 1$, on note $\mathcal{O}_k$ l'ensemble des matrices orthogonales de taille $k \times k$, et $\mathcal{O}_k^+$ l'ensemble des matrices $R \in \mathcal{O}_k$ telles que chaque ligne de R est de poids de Hamming congru à 1 (mod 4).

Remarque 1. Toutes les lignes d'une matrice de $\mathcal{O}_k$ sont de poids (de Hamming) congru à 1 (mod 2).

Enfin, pour tout entier $e \geqslant 1$ et toute matrice P, on note $P^{[e]}$ la matrice définie par blocs ayant e fois la matrice P sur sa diagonale et 0 partout ailleurs.

2.2. Description de la construction

Définition 2.1 [2,1]. Soit $(I_b|P)$ une matrice génératrice d'un code linéaire $\mathcal{B}$ de rendement $1/2$ et de dimension b. Soient e un entier non-nul et $\Pi_1, \ldots, \Pi_s$ des matrices de permutation de taille $k \times k$ avec $k = eb$ et $s \geqslant 1$.

Le *code Cortex défini à partir du code $\mathcal{B}$ suivant la suite de matrices de permutation $\Pi_1, \ldots, \Pi_s$* est le code linéaire généré par la matrice :

$$\left(I_k | P^{[e]} \Pi_1 P^{[e]} \cdots \Pi_s P^{[e]}\right).$$

Nous nous intéressons plus particulièrement à des codes Cortex dont le code de base est $\mathbb{H}_8$. Nous les appelons des codes $\mathbb{H}_8$-Cortex. La proposition suivante donne une propriété importante qu'ils vérifient.

Proposition 2.2 [1]. *Soient $k = 4e$ avec e un entier non nul et $\Pi_1, \ldots, \Pi_s$ une suite de matrices de permutation avec $s \geqslant 1$.*

Le code $\mathbb{H}_8$-Cortex défini suivant $\Pi_1, \ldots, \Pi_s$ est un code de type II (*resp. type I*) *si s est pair* (*resp. impair*).

3. Résultats

Proposition 3.1. *Soit e un entier non nul et posons $k = 4e$. Pour toute matrice $R \in \mathcal{O}_k^+$, il existe des matrices de permutation $\Pi_0, \ldots, \Pi_{2s}$ de taille $k \times k$ avec $s \leqslant e(e-1)$ telles que* :

$$R = \Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2s}.$$

Indications de preuve. Pour tout entier s, on note $\mathbf{1}_s$ (resp. $\mathbf{0}_s$) le vecteur de longueur s composé uniquement de 1 (resp. 0). Enfin, pour tous vecteurs binaires u et v, on note uv le vecteur obtenu par concaténation.

La proposition se démontre par récurrence sur e. Pour $e = 1$ il n'existe qu'une seule matrice R qui est la matrice identité I_4. On suppose ensuite que pour tout $M \in \mathcal{O}_{4(e-1)}^+$ avec $e \geqslant 2$, il existe une suite de permutations $\Pi_0, \ldots, \Pi_{2s}$ telles que :

$$M = \Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2s} \quad \text{avec } s \leqslant (e-1)(e-2).$$

Première étape. En multipliant par des matrices de permutation et la matrice $H_4^{[e]}$, il est possible de transformer les deux premières lignes de R en les vecteurs : $\mathbf{1}_\theta \mathbf{1}_{\theta_1} \mathbf{0}_{\theta_2} \mathbf{0}_\delta$ et $\mathbf{1}_\theta \mathbf{0}_{\theta_1} \mathbf{1}_{\theta_2} \mathbf{0}_\delta$ où θ, θ_1, θ_2 et δ sont des entiers. Comme ces lignes sont orthogonales entre elles, il existe donc un entier q tel que $\theta = 2q$. Il existe ainsi des entiers q_1 et q_2 tels que $\theta_1 = 2q_1 + 1$ et $\theta_2 = 2q_2 + 1$ pour lesquels on a :

$$\begin{cases} q + q_1 = 2\gamma_1, \\ q + q_2 = 2\gamma_2, \\ 2(q + q_1 + q_2 + 1) + \delta = 4e, \end{cases}$$

où γ_1 et γ_2 sont des entiers. On en déduit qu'il existe un entier δ' tel que $\delta = 2\delta'$, et que q, q_1 et q_2 ont la même parité. Deux cas peuvent par conséquent se présenter suivant la parité de δ'.

Or dans ces deux cas, il existe des permutations $\Pi_0, \ldots, \Pi_{2s}$ avec $s \leqslant e - 1$ telles que :

$$R\Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2s} = \left(\begin{array}{c|ccc} I_2 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{array}\right) \quad \text{où } Q_1\, Q_1^{\mathrm{T}} = I_{k-2},$$

où chaque ligne de Q_1 a un poids congru à 1 modulo 4.

Deuxième étape. On pose $R^{(1)} = R\Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2s}$. Étant données deux lignes différentes de $R^{(1)}$, il est toujours possible de trouver des entiers s, s_1, s_2 et α tels qu'à permutation près des colonnes, on ait :

$$00\,\mathbf{1}_{2s}\mathbf{1}_{2s_1+1}\mathbf{0}_{2s_2+1}\mathbf{0}_\alpha \quad \text{et} \quad 00\,\mathbf{1}_{2s}\mathbf{0}_{2s_1+1}\mathbf{1}_{2s_2+1}\mathbf{0}_\alpha$$

avec :

$$\begin{cases} s + s_1 = 2\gamma_1, \\ s + s_2 = 2\gamma_2, \\ 2(s + s_1 + s_2 + 2) + \alpha = 4e, \end{cases}$$

où γ_1 et γ_2 sont des entiers quelconques. Il existe donc un entier α' tel que $\alpha = 2\alpha'$. On en déduit que s, s_1, s_2 et α' ont la même parité, et que deux cas peuvent donc se présenter suivant la parité de α'.

Or dans les deux cas, nous pouvons toujours trouver $2r$ matrices de permutation $\Gamma_0, \ldots, \Gamma_{2r}$ avec $r \leqslant e - 1$ telles que :

$$R^{(1)}\Gamma_0 H_4^{[e]} \Gamma_1 \cdots H_4^{[e]} \Gamma_{2r} = \left(\begin{array}{c|ccc} I_4 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Z_1 & \\ 0 & & & \end{array}\right) \quad \text{où } Z_1 \in \mathcal{O}_{4(e-1)}^+.$$

En utilisant l'hypothèse de récurrence sur Z_1, on peut donc dire en conclusion qu'il existe $2d$ matrices de permutation $\Delta_0, \ldots, \Delta_{2d}$ avec $d \leqslant (e-1)(e-2) + 2(e-1)$ telles que :

$$R = \Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2d}. \qquad \square$$

Théorème 3.2. *Pour tout code $\mathcal{C}$ de type II de longueur $n = 8e$ où $e \geqslant 1$, il existe des matrices de permutation $\Pi_1, \ldots, \Pi_{2s}$ avec $s \leqslant e(e-1)$ telles que $\mathcal{C}$ soit un code $\mathbb{H}_8$-Cortex à équivalence près.*

Démonstration. Chaque mot d'un code de type II a un poids de Hamming congru à 0 modulo 4. Ainsi la partie redondante R de sa matrice génératrice (qui est sous forme systématique) a toutes ses lignes avec un poids congru à -1 modulo 4. Or, toutes les lignes de la matrice $RH_4^{[e]}$ sont de poids congru à 1 modulo 4. D'après la Proposition 3.1, il existe donc des permutations $\Pi_0, \ldots, \Pi_{2s}$ avec $s \leqslant e(e-1)$ telles que :

$$RH_4^{[e]} = \Pi_0 H_4^{[e]} \Pi_1 \cdots H_4^{[e]} \Pi_{2s}$$

c'est-à-dire

$$\Pi_0^{-1} R = H_4^{[e]} \Pi_1 \cdots \Pi_{2s} H_4^{[e]}.$$

Cette égalité prouve que $\mathcal{C}$ est un code $\mathbb{H}_8$-Cortex, car un code admettant une matrice génératrice dont la partie redondante est $\Pi_1^{-1} R$ est équivalent à $\mathcal{C}$. $\square$

Remarque 2. La preuve de la Proposition 3.1 permet d'en déduire un algorithme de décomposition effective de toute matrice de $\mathcal{O}^+ = \bigcup_{k \geqslant 1} \mathcal{O}_k^+$ en un produit de matrices de permutation et de $H_4^{[e]}$.

Références

[1] J.C. Carlach, A. Otmani, A systematic construction of self-dual codes, IEEE Trans. Inform. Theory, à paraître.
[2] J.C. Carlach, C. Vervoux, A new family of block turbo-codes, in: Proceedings of 13th Applicable Algebra in Engineering Communication and Computing (AAECC 13), Hawaii, USA, November 14–19, 1999, p. 15.
[3] F. MacWilliams, N. Sloane, The Theory of Error-Correcting Codes, 5th edition, North-Holland, Amsterdam, 1986.
[4] E.M. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.