On r-partitions designs in hamming spaces

Paul Camion, Bernard Courteau, Philippe Delsarte

INRIA
CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 626

ON *r*-PARTITIONS DESIGNS IN HAMMING SPACES

Paul CAMION
Bernard COURTEAU
Philippe DELSARTE

Février 1987

ON r-PARTITIONS DESIGNS IN HAMMING SPACES

SUR LES CONFIGURATIONS DE r-PARTITIONS DANS LES ESPACES DE HAMMING

Paul CAMION
INRIA
Domaine de Voluceau
78153 - Le Chesnay - France

Bernard COURTEAU *
Dept. de mathematiques et informatique
Universite' de Sherbrooke
Sherbrooke - Quebec -
Canada J1K 2R1

Philippe DELSARTE
Philips Research Laboratory
B-1170 Brussels
Belgium

ABSTRACT

We introduce the combinatorial matrix of a code, the notion of r-partition-design and using these notions we give a characterization of completely regular codes and a combinatorial interpretation to the fact that the distance matrix of a non-linear code contains the least possible number of distinct rows.

---

* This research was conducted when the second author was on a sabbatical leave at INRIA, Rocquencourt. It is supported in part by FCAR grants EQ 1886 and CRSNG grants A5120.

RESUME

Nous introduisons la matrice combinatoire d'un code et la notion de configuration de r-partition. En utilisant ces notions nous donnons une caracterisation des codes totalement reguliers et une interpretation combinatoire du fait que la matrice des distances d'un code non-lineaire comporte le plus petit nombre possible de lignes distinctes.

Keywords : Codes, association schemes, completely regular codes, coherent partitions.

INTRODUCTION

In this paper we introduce the combinatorial matrix of a code, the notion of r-partition-design and we relate these notions to fundamental concepts of coding theory.

Section 1. gives a combinatorial interpretation of the matrix $S = (\alpha_{ij})$ giving the basis $\{P_j^i(x)\}$ in terms of $\{P_j(x)\}$ the basis of the ring of polynomials over the finite field $F = GF(q)$ formed by the Krawtchouk polynomials $P_j(x)$. The element α_{ij} is the number of paths of length j joining two vectors of the Hamming space $\mathbb{F}^n$ at distance i apart. We then give a recurrence relation and the exponential generating function for these numbers α_{ij}.

In section 2. we introduce the combinatorial matrix $A = (A(x,j))$ of a code C:$A(x,j)$ is the number of paths of length j joining $x \in \mathbb{F}^n$ to the code C. This matrix A is related to the distance matrix B[2] by the relation $A = BS$ and the sequence of columns of A satisfy a recurrence of minimum order $s' + 1$ if and only if s' is the external distance of C. Moreover the characteristic polynomial of this minimum order recurrence admits as zeroes $P_1(l) = n(q-1) - ql$ being the dual distances of C. The preceding are extensions to non-linear codes of notions and results already obtained in [4], [5] and [14].

In section 3. we start the study of r-partition-designs (called coherent partitions by Higman [15]) which are partitions $\Pi = \{C_0, C_1, \ldots, C_r\}$ of $\mathbb{F}^n$ into

$r + 1$ classes such that for any $x \in C_u$ the number σ_{uv} of elements of C_v at distance one from x is independant of the choice of x in C_u. A code C is said to admit the partition Π if C is the union of some classes C_u. Perfect, uniformly packed and more generally completely regular codes are then characterized in terms of r-partition-designs. For example we prove the following result : Let C be a code with covering radius ρ. Then C is completely regular if and only if C admits a r-partition-design for $r = \rho$. Moreover $\rho = s'$ the external distance of C and the eigenvalues of the associated matrix $\sigma = (\sigma_{uv})$ are $P_1(l) = n(q-1) - ql$ for $l \in \{0, d'_1, \ldots, d'_{s'}\}$ where $d'_1, \ldots, d'_{s'}$ are the dual distances of C.

In general, if C admits a r-partition-design, then $r \geq s'$. The case $r = s'$ is characterized as follows : C admits a s'-partition-design if and only if the number of distinct rows in the distance matrix is $s' + 1$. This is an analogue of theorem 6.11 of [1] in the non linear case. On the other hand in the linear case, we may apply theorem 6.10 and 6.11 of [1] to obtain the result : the linear code C admits a s'-partition-design $\Pi = \{C_0, C_1, \ldots, C_{s'}\}$ if and only if the partition Π of the quotient group $C' = \mathbb{F}^n / C$ defines an association scheme over C' (called the coset scheme determined by Π) if and only if the restriction to C' of the Hamming scheme is a subscheme. The P-matrix of the coset scheme has been determined by A. Montpetit in-terms of the s'-partition-design Π : it is the left eigenmatrix of the matrix σ associated to Π. Finally in section 4. we give numerous examples of codes admitting r-partition-design for $r = s'$ and an example where there doesn't exist such a s'-partition-design.

1. - PATHS IN HAMMING SPACE

Let $\mathbb{F} = GF(q)$ be the field with q elements, q a prime power and $H(n,q)$ the Hamming space of dimension n over F that is the n-dimensional vector space F^n over F equipped with Hamming distance d defined by $d(x,y)=$ number of components in which the n-vectors x and y differ. $H(n,q)$ is a metric association scheme and we refer to [1,2] for all notions and results on association schemes that will be needed in the following.

Definition 1.1 **A path of length j** joining x to y in $\mathbb{F}^n$ is a sequence $x_{(0)}=x, x_{(1)}, \ldots, x_{(j)}=y$ of points in F^n such that $d(x_{(k-1)}, x_{(k)})=1$ for $k=1,\ldots,j$. The Hamming distance between x and y is the length of the shortest path joining x to y.

The $i-th$ adjacency matrix D_i is the $q^n \times q^n$ matrix with rows and columns indexed by $\mathbb{F}^n$ defined by

$$D_i(x,y)=\begin{cases}1 & \text{if } d(x,y)=i \\ o & otherwise.\end{cases}$$

Since $\{D_o=I,D_1,...,D_n\}$ is a basis of the Bose-Mesner algebra of $H(n,q)$, we have

$$D_1^j=\sum_{i=o}^{n}\alpha_{ij}D_i \qquad (1)$$

for uniquely defined complex numbers α_{ij}.

If $x,y \in \mathbb{F}^n$ are such that $d(x,y)=i$, then for $j \geq o$ we have $D_1^j(x,y)=\alpha_{ij}$. So α_{ij} is the number of paths of length j joining two points x and y at distance i apart and this number does not depend on the particular choice of x and y but only on the distance i between them.

Let $S=(\alpha_{ij})$ be the $n \times \infty$ non-negative integer matrix with α_{ij} in position (i,j).

Proposition 1.2

a) If $i>j$, then $\alpha_{ij}=0$. So S is a $n \times \infty$ upper triangular matrix.

b) If $i \leq j$, then $i!$ divides α_{ij}.

Proof : a) is evident. To prove b), remark that one passes from one element to the following in a path in $\mathbb{F}^n$ by modifying one and only one component of a n-vector. If $d(x,y)=i$, then there is exactly $i!$ paths of length i joining x to y. So $\alpha_{ii}=i!$. Moreover, any path of length j joining x to y must contain one and only one of these $i!$ minimal paths. Since these last paths play completely symmetric roles, the number of length j paths containing a given minimal path must be a constant α independant of the chosen minimal path. Hence $\alpha_{ij}=\alpha i!$.

Remark 1.3 If $P_i(l)$, $l=o,...,n$ are the eigenvalues of $D_i, i=o,...,n$, then by (1)

$$P_1^j(l)=\sum_{i=o}^{n}\alpha_{ij}P_i(l) \quad \text{for } j \geq 0. \qquad (2)$$

Since the Hamming scheme $H(n,q)$ is P-polynomial with respect to the class of Krawtchouk polynomials we may suppose that in (2) $P_i(l)$ is the evaluation on l of the $i-th$ Krawtchouk polynomial which shall be denoted by the same letter P_i. If P is the Krawtchouk matrix containing in position (l,i) the number $P_i(l)$, we may express equation (2) in matrix form as follows.

Proposition 1.4 $S=q^{-n}PV$ where the matrix V having in position (l,j) the number $P_1^j(l)$ is an infinite Vandermonde matrix.

Remark 1.5 Definition of matrix S, proposition 1.2 a) and equation (2) hold in any metric scheme (X,R). In this general case the matrix equality in proposition 1.4 should be read $S=|X|^{-1}QV$ with $PQ=QP=|X|I$ where in the eigenmatrix P the Krawtchouk polynomials are replaced by another convenient class of orthogonal polynomials $\Phi_i(x)$. In the case of Hamming scheme, we have $Q=P$. Many of the following results may be extended to arbritrary metric schemes.

Using the order two recurrence satisfied by Krawtchouk polynomials written in the form

$$P_1(l)P_j(l)=(j+1)P_{j+1}(l)+(q-2)jP_j(l)+(q-1)(n-j+1)P_{j-1}(l) \tag{3}$$

we deduce from (2) the linear recurrence

$$\alpha_{i,j+1}=i\alpha_{i-1,j}+i(q-2)\alpha_{ij}+(n-i)(q-1)\alpha_{i+1,j} \tag{4}$$

In matrix form, this gives

$$S_{j+1}=MS_j$$

where $S_j=[\alpha_{0j},\ldots,\alpha_{nj}]^T$ is the $j-th$ column of $S(S_0=[1,0,\ldots,0]^T)$ and M is the following tridiagonal $(n+1)\times(n+1)$ matrix :

$$M=\begin{bmatrix} 0 & n(q-1) & 0 & 0 & 0 \\ 1 & q-2 & (n-1)(q-1) & \cdot & \cdot \\ 0 & 2 & 2(q-2) & \ddots & 0 & \cdot \\ \cdot & \cdot & 3 & \ddots & 2(q-1) & 0 \\ \cdot & \cdot & \cdot & \ddots & (n-1)(q-2) & (q-1) \\ 0 & \cdot & 0 & & n & n(q-2) \end{bmatrix} \tag{5}$$

So $S_j=M^jS_0$ is the first column of M^j and we note that the eigenvalues of

M are $P_1(0)=n(q-1),\ldots,P_1(l)=n(q-1)-lq,\ldots,P_1(n)$ and the associated eigenvectors are the corresponding columns in the Krawtchouk matrix P because the recurrence (3) may be written in matrix form as $PM=\Delta P$ which gives

$$P\ MP^{-1}=\Delta$$

where $\Delta = diag\{P_1(0),\ldots,P_1(l),\ldots,P_1(n)\}$.

Proposition 1.6 $S=[M^0S_0,MS_0,\ldots,M^jS_0,\ldots]$ where M the matrix given by (5) have $P_1(l)=n(q-1)-ql, l=0,\ldots,n$ as eigenvalues.

Remark 1.7 In the general case of a metric scheme we obtain a similar result by using in place of (3) the order two recurrence satisfied by orthogonal polynomials $\Phi_i(x)$ which are associated to the scheme [1].

We may also look at the numbers α_{ij} in matrix S by means of exponential generating functions. Here is the result.

Proposition 1.8

$$\sum_{j\geq 0}\alpha_{ij}\frac{Z^j}{j!}=q^{-n}\left[e^{(q-1)Z}-e^{-Z}\right]^i\left[e^{(q-1)Z}+(q-1)e^{-Z}\right]^{n-i},\quad i=0,\ldots,n \tag{6}$$

Proof : Let x and y be given in F^n such that $d(x,y)=i$ and let $\gamma=supp(x-y)=\{k \mid x_k-y_k\neq 0\}$ be the support of $x-y$. Consider the numbers

a_m = number of paths of length m joining two points at distance 1 apart obtained by modifying only the component where they differ (this component being in γ),

b_m = number of cycles of length m starting from a given point and obtained by modifying only one component (exterior to γ),

c_m = number of paths of length m joining the two points x and y (hence $c_m=\alpha_{im}$) and the associated exponential generating functions

$$a(Z)=\sum_{m\geq 0}a_m\frac{Z^m}{m!},\ b(Z)=\sum_{m\geq 0}b_m\frac{Z^m}{m!}\ \text{ and }\ c(Z)=\sum_{m\geq 0}\alpha_{im}\frac{Z^m}{m!}$$

Interpreting, as usual, the product of two exponential generating functions [3] as a kind of shuffle product, we may write

$$c(Z)=(a(Z))^i(b(Z))^{n-i}=\sum_{j\geq 0} a_{ij}\frac{Z^j}{j!}$$

and it remains to determine $a(Z)$ and $b(Z)$. Remark that $a_m=(q-2)a_{m-1}+b_{m-1}$ and $b_m=(q-1)a_{m-1}$ with $a_0=0, a_1=1, b_0=1, b_1=0$, so that we have the recurrence $a_m-(q-2)a_{m-1}-(q-1)a_{m-2}=0, a_0=0, a_1=1$ which gives in terms of generating functions the differential equation

$$a''(Z)-(q-2)a'(Z)-(q-1)a(Z)=0$$

with initial conditions $a(0)=0, a'(0)=1$. The solution of this problem is

$$a(Z)=\frac{e^{(q-1)Z}-e^{-Z}}{q}$$

By integration, we deduce from $b'(Z)=(q-1)a(Z)$

$$b(Z)=\frac{e^{(q-1)Z}+(q-1)e^{-Z}}{q} \quad \textit{since} \quad b(0)=1.$$

This completes the proof of proposition 1.8.

Remark 1.9 The preceding is a combinatorial proof. We may give a shorter algebraic proof by using the generating function of Krawtchouk polynomials $P_k(i)$ and proposition 1.4.

The generating function of polynomials $P_k(i)$ is

$$(X-Y)^i(X+(q-1)Y)^{n-i}=\sum_{0\leq k\leq n} P_k(i)X^{n-k}Y^k$$

Setting $X=e^{(q-1)Z}$ and $Y=e^{-Z}$ in this relation gives

$$(e^{(q-1)Z}-e^{-Z})^i(e^{(q-1)Z}+(q-1)e^{-Z})^{n-i}=\sum_{0\leq k\leq n} P_k(i)e^{(q-1)Z(n-k)-Zk}$$

$$=\sum_{0\leq k\leq n} P_k(i)e^{ZP_1(k)} \quad \textit{with} \quad P_1(k)=n(q-1)-qk$$

$$= \sum_{0\le k\le n} P_k(i) \sum_{j\ge 0} \frac{(ZP_1(k))^j}{j!} = \sum_{j\ge 0} \left[\sum_{0\le k\le n} P_k(i) P_1^j(k) \right] \frac{Z^j}{j!}$$

$$= q^n \sum_{j\ge 0} \alpha_{ij} \frac{Z^j}{j!}$$

by proposition 1.4.

2. - THE COMBINATORIAL MATRIX OF A CODE

Let $C \subset \mathbb{F}^n$ be an unrestricted code of length n over $\mathbb{F}$.

Definition 2.1 For any $x \in \mathbb{F}^n$, let $A_j(x)$ be the number of paths of length j joining x to an element of C. The **combinatorial matrix** of $\mathbb{F}^n$ **with respect to** C is then the $q^n \times \infty$ matrix A whose element in position (x,j) is

$$A(x,j) = A_j(x).$$

If $B_i(x)$ is the number of elements of C at distance i apart from x, then the **distance matrix** of $\mathbb{F}^n$ with **respect to** C [2] is the $(q^n \times (n+1))$ matrix B whose element in position (x,i) is

$$B(x,i) = B_i(x).$$

By the very definition of the numbers in question we have

$$A_j(x) = \sum_{i=0}^{n} \alpha_{ij} B_i(x) \tag{7}$$

giving in matrix form the following equality.

Proposition 2.2 $A = BS$

As a consequence of proposition 1.8 and 2.2 we also have the following property generalizing theorem 3.3 of [4].

Proposition 2.3

$$q^n \sum_{j\ge 0} A_j(x) \frac{Z^j}{j!} = \sum_{i=0}^{n} B_i(x) \left[e^{(q-1)Z} - e^{-Z} \right]^i \left[e^{(q-1)Z} + (q-1)e^{-Z} \right]^{n-i} \tag{8}$$

Remark This result combined with proposition 1.4 may be viewed as generalized Pless identities. The classical Pless identities [6] are obtained when the code C is linear and $x=o$ in the formula. This is because, on the one hand

$$q^n A_j(x)=\sum_{i=0}^{n}\frac{d^j}{dZ^j}\Big[(e^{(q-1)Z}-e^{-Z})^i(e^{(q-1)Z}+(q-1)e^{-Z})^{n-i}\Big]_{Z=0}B_i(x)$$

and on the other hand, by proposition 2.2 and 1.4,

$$q^n A_j(x)=\sum_{i=0}^{n}\alpha_{ij}B_i(x)=\sum_{i=0}^{n}\sum_{l=0}^{n}P_l(i)P_1^j(l)B_i(x)$$

$$=\sum_{l=0}^{n}B'_l(x)[n(q-1)-ql]^j$$

Proposition 2.4 Let C be an unrestricted code in $\mathbb{F}^n$. Then the following two conditions are equivalent.

(i) s' is the external distance of C

(ii) s' is the minimum of the natural numbers t for which there exists a linear recurrence of order $t+1$

$$\sum_{j=0}^{t+1}c_j A_{j+m}(x)=0, \qquad x\in\mathbb{F}^n$$

where $c_0,c_1,\ldots,c_{t+1}$ are integers with $c_{t+1}\neq 0$.

Moreover, the recurrence of minimum order $s'+1$ with $c_{t+1}=1$ is unique and the coefficients c_j are determined by

$$\sum_{j=0}^{s+1}c_j Z^j=\prod_{l\in J}(Z-P_1(l)), \qquad J=\{0,d'_1,\ldots,d'_{s'}\}$$

where $d'_1,\ldots,d'_{s'}$ are the dual distances of C.

Proof : We shall work in the group algebra $\mathbb{C}[\mathbb{F}^n]$ of $\mathbb{F}^n$ over the complex numbers and use the polynomial notation

$$a=\sum_{x\in F^n}a_x Z^x, \qquad a_x\in\mathbb{C}$$

to represent an element $a\in\mathbb{C}[\mathbb{F}^n]$.

Remark that, if $C=\sum_{g\in C} Z^g$ and $Y_1=\sum_{w(h)=1} Z^h$ then in $\mathbb{C}[\mathbb{F}^n]$ we have

$$CY_1^j=\sum_{x\in\mathbb{F}^n} A_j(x)Z^x. \tag{7}$$

This is because, by definition of convolution product,

$$CY_1^j=\left(\sum_{g\in C} Z^g\right)\left(\sum_{w(h)=1} Z^h\right)^j=\sum_{x\in\mathbb{F}^n}\left[\sum_{x=g+h_1+\dots+h_j} 1\right]Z^x$$

where in the last sum $g\in C$ and $W(h_1)=1,\dots,W(h_j)=1$, and the fact that

$$A_j(x)=card\{(g,h_1,\dots,h_j)\mid x=g+h_1+\dots+h_j, g\in C, W(h_1)=\cdots=W(h_j)=1\}$$

Now we shall prove that if there exists a linear recurrence of order $t+1$

$$\sum_{j=0}^{t+1} c_j\, A_{j+m}(x)=0,\quad x\in\mathbb{F}^n,\quad m\geq 0 \tag{8}$$

then

$$\sum_{j=0}^{t+1} c_j[P_1(l)]^j=0 \tag{9}$$

for $l\in\{0,d'_1,\dots,d'_{s'}\}$, $d'_1,\dots,d'_{s'}$ being the dual distances of C.

From (8) and by (7) we may write

$$\sum_{x\in\mathbb{F}^n}\left(\sum_{j=0}^{t+1} c_jA_j(x)\right)Z^x=0$$

$$\sum_{j=0}^{t+1} c_j(CY_1^j)=0$$

$$C\left(\sum_{j=0}^{t+1} c_j\, Y_1^j\right)=0 \quad in \quad \mathbb{C}[\mathbb{F}^n] \tag{10}$$

Now, by theorem 7 p. 139 of [7], for all l such that $l=0$ or $l=d'_i$ $i=1,\dots,s'$, there exists $u\in\mathbb{F}^n$ such that $X_u(C)\neq 0$ and $w(u)=l$ where X_u is the character associated with u. For such an u, we have

$$X_u\left(\sum_{j=0}^{t+1} c_j\, Y_1^j\right)=0$$

i.e

$$\sum_{j=0}^{t+1} c_j \left[X_u(Y_1)\right]^j = 0.$$

i.e

$$\sum_{j=0}^{t+1} c_j \left[P_1(l)\right]^j = 0.$$

Hence the polynomial $c(Z)=\sum_{j=0}^{t+1} c_j Z^j$ is divisible by

$$p(Z)=\prod_{l\in J}(Z-P_1(l)), \quad J=\{0,d'_1,\ldots,d'_{s'}\} \text{ and } s'\le t.$$

Finally we shall exhibit a linear recurrence of order $s'+1$. Take the annihilator polynomial $\beta(Z)=Z\prod_{i=1}^{s'}(Z-d'_i)$ (up to a factor) decompose it in the basis $\{P_1^0(Z),P_1(Z),\ldots,P_1^j(Z),\ldots\}$

$$\beta(Z)=\sum_{j=0}^{s'+1} c_j P_1^j(Z)$$

and note that in the group algebra $\mathbb{C}[F^n]$

$$C\left(\sum_{j=0}^{s'+1} c_j Y_1^j\right) = 0$$

because for all character X_u either $X_u(C)=0$ or in case $w(u)=d'_i, i=1,\ldots,s'.X_u\left(\sum_{j=0}^{s'+1} c_j Y_1^j\right)=\sum_{j=0}^{s'+1} c_j\left[X_u(Y_1)\right]^j=\sum_{j=0}^{s'+1} c_j P_1^j(d'_i)=\beta(d'_i)=0$

Hence for all $m\ge 0$

$$Y_1^m\, C\left(\sum_{j=0}^{s'+1} c_j Y_1^j\right)=0$$

i.e

$$\sum_{j=0}^{s'+1} c_j C Y_1^{m+j}=0$$

and by (7)

$$\sum_{j=0}^{s'+1} c_j \left[\sum_{x \in F^n} A_{j+m}(x) Z^x \right] = 0$$

i.e

$$\sum_{x \in F^n} \left[\sum_{j=0}^{s'+1} c_j A_{j+m}(x) \right] Z^x = 0.$$

This gives the recurrence

$$\sum_{j=0}^{s'+1} c_j A_{j+m}(x) = 0.$$

To show how the preceding are generalization of notions introduced in [4,5], we specialize to the particular case where the code C is linear.

Proposition 2.5 Let $C \subset F^n$ be a $(n,n-k)$ linear code with parity check matrix H and let $\Omega \subseteq F^k$ be the ordered set of columns (supposed distinct) of H.

If $x \in F^n$ and $h = Hx$ is the syndrome of x, then $A_j(x) = card\ \mathcal{E}_j(x)$ where

$$\mathcal{E}_j(x) = \left\{ (h_1, \ldots, h_j, \lambda_1, \ldots, \lambda_j) \mid h = \lambda_1 h_1 + \ldots + \lambda_j h_j, \lambda_i \in F^*, h_i \in \Omega, i = 1, \ldots, j \right\}$$

Proof :

Let $\mathcal{D}_j(x) = \left\{ (x = x_{(0)}, x_{(1)}, \ldots, x_{(j)}) \mid x_{(j)} \in C, d(x_{(i-1)}, x_{(i)}) = 1, x_{(i)} \in F^n, i = 1, \ldots, j \right\}$ be the set of paths of length j joining x to the code C.

Define $\rho: \mathcal{D}_j(x) \longrightarrow \mathcal{E}_j(x)$ by

$$\rho\left[(x, x_{(1)}, \ldots, x_{(j)})\right] = (h_1, \ldots, h_j, \lambda_1, \ldots, \lambda_j)$$

where $h = Hx = H\left[(x - x_{(1)}) + (x_{(1)} - x_{(2)}) + \ldots + (x_{(j-1)} - x_{(j)})\right]$

$$= \lambda_1 h_1 + \lambda_2 h_2 + \cdots + \lambda_j h_j.$$

This mapping ρ is well defined because $w(x_{(i-1)}-x_{(i)})=1$. In fact, the value of the non-zero component of $x_{(i-1)}-x_{(i)}$ gives λ_i and its index gives the index of h_i in Ω.

It is clear that ρ is onto. It is one-to-one because we have supposed the columns of H distinct. The inverse Ψ of ρ is defined by

$$\Psi\Big[(h_1,\ldots,h_j,\lambda_1,\ \ldots\ ,\lambda_j)\Big]=(x,x_{(1)},\ \ldots\ ,x_{(j)})$$

where $x_{(1)},\ldots,x_{(j)}$ are determined as follows :

$x_{(1)}=x-\lambda_1 e_{i_1}$ where i_1 is the unique index such that $H_{i_1}=h_1$.

This gives $Hx_{(1)}=\lambda_2 h_2+\ldots+\lambda_j h_j$. We then repeat the argument to obtain $x_{(2)},\ \ldots\ ,x_{(j)}$. Finally $Hx_{(j)}=0$ and $x_{(j)}\in C$.

3. - r-PARTITION DESIGNS

Definition 3.1 A **r-partition-design** of the Hamming scheme $H(n,q)$ is a partition of F^n into $r+1$ classes $C_0,C_1,\ \ldots\ ,C_r$ such that for any $x\in C_u$ the number σ_{uv} of elements in C_v at distance one from x is independant of the choice of x in its class C_u.

We shall say that a code C admits the r-partition-design $\{C_0,C_1,\ \ldots\ ,C_r\}$ if $C=\bigcup\{C_v \mid v\in J\},J\subseteq\{0,1,\ldots,r\}$. (We shall also say that the partition-design contains the code C).

Remark 3.2 If $\{C_0,C_1,\ \ldots\ ,C_r\}$ is a r-partition design, then for all $u,v\in\{0,\ldots,r\}$

$$(card\ \ C_u)\sigma_{uv}=(card\ \ C_v)\sigma_{vu}=card\{(x,y)\in C_u\times C_v \mid d(x,y)=1\}.$$

In matrix form this gives,

$$\sigma^T=K\sigma K^{-1}\ \ where\ \ K=diag\{card\ \ C_0,\ldots,card\ \ C_r\}.$$

Remark 3.3 Let C be a $(n,n-k)$*-linear* code admitting a r-partition-design $C_0,C_1,\ldots,C_r$ with associated matrix $\sigma=(\sigma_{uv})$ such that each C_u is an union of cosets of C. If $\Omega\subset F^k$ is the set of columns (supposed distinct) of a parity check matrix H for the code C, define the sets $\Omega_0=0,\Omega_1,\ \ldots\ ,\Omega_r$ as follows :

$$\Omega_u = \{Hx \mid x \in C_u\}, \qquad 0 \le u \le r$$

that is Ω_u is the set of syndromes of elements in C_u .

The set $\{\Omega_0, \Omega_1, \ldots, \Omega_r\}$ is a partition of F^k because rank $H=k$ and $\Omega_u \cap \Omega_v \neq 0$ implies $\Omega_u = \Omega_v$. ($h \in \Omega_u \cap \Omega_v ==> h = Hx = Hy$ for $x \in C_u$, $y \in C_v ==> x \in y + C ==> x \in C_v ==> C_u = C_v$.)

Then we have the following interpretation of the numbers σ_{uv} :

for $u,v \in \{0,1,\ldots,r\}$ and a $\in \Omega_u$

$$\sigma_{uv} = card\{(b,h) \in \Omega_v \times F^{*}\Omega \mid a = b + h\}. \tag{11}$$

This is because, if $\mathcal{E} = \{y \in C_v \mid d(x,y)=1\}$ for $x \in C_u$ and $\mathcal{D} = \{(b,h) \in \Omega_v \times F^{*}\Omega \mid a = b + h\}$ for a $\in \Omega_u$, then $\varphi : y \dashrightarrow (Hy, H(x-y))$ is a bijection of $\mathcal{E}$ *onto* $\mathcal{D}$.

We note that Ω is the union of some Ω_u because if $\Omega_u \cap \Omega \neq 0$ then $\sigma_{uo} \neq 0$ which implies that $\Omega_u \subset \Omega$.

Conversely, if $\Omega_0 = 0, \Omega_1, \ldots, \Omega_r$ is a partition of F^k satisfying (11) where $\Omega = \bigcup_{u \in J} \Omega_u$, then we may define the r-partiton design $\{C_0, C_1, \ldots, C_r\}$ by $C_u = \{x \in F^n \mid Hx \in \Omega_u\}$ where H is the matrix having Ω as columns set. Moreover each C_u is the union of some cosets of the code C having parity check matrix H.

This is a slightly more general definition of r-partition design than the one given in [4] for the case of linear codes. Note also that a 2-partition design is a partial difference set with two parameters [8]. So we may consider r-partition-design as some kind of generalized difference sets.

Remark 3.4 For any $u = 0,\ldots,r$, $\sum_{v=0}^{r} \sigma_{uv} = n(q-1)$. Hence $n(q-1)$ is an eigenvalue of σ.

Remark 3.5 Let C be any code in F^n. Then C always admits the **trivial** r-partition design $C_0, C_1, \ldots, C_r$ where $r=q^n-1$, the classes C_i consisting of only one element. In this case $\sigma=D_1$.

Remark 3.6 Let ρ be the covering radius of C and $\bar{C}_0, \ldots, \bar{C}_\rho$ be the classes defined by

$$\bar{C}_i=\{x\in F^n \mid d(x,C)=i\}, \quad i=0,\ldots,\rho$$

If $\{C_0, C_1, \ldots, C_r\}$ is a r-partition design containing C, then

$$\bar{C}_i=\cup\{C_u \mid C_u\cap\bar{C}_i\neq 0\}, \quad i=0,\ldots,\rho.$$

This is proved by induction on i. Hence $\rho\leq r$. Naturally the extremal case $r=\rho$ is expected to show interesting combinatorial structures.

Remark 3.7 Consider the partition $\bar{C}_0=C, \bar{C}_1, \ldots, \bar{C}_\rho$ where the code C is e-error-correcting with covering radius ρ. Let $\sigma(x)=(\sigma_{ij}(x)), x\in F^n$, be the matrix defined by

$$\sigma_{ij}(x)=\begin{cases} card\{y\in\bar{C}_j \mid d(x,y)=1\} & \text{if } x\in\bar{C}_i \\ 0 & otherwise. \end{cases}$$

Then we have

1/ $\sigma_{ij}(x)=0$ for $|i-j|\geq 2$

2/ $\sigma_{i,i-1}(x)=i$ for $x\in\bar{C}_i$ and $1\leq i\leq e$

3/ $\sigma_{i,i}(x)=i(q-2)$ for $x\in\bar{C}_i$ and $0\leq i\leq e-1$

4/ $\sum_{j=o}^{\rho}\sigma_{ij}(x)=n(q-1)$ for $x\in\bar{C}_i$.

Hence for all i,j such that $|i-j|\geq 2$, $0\leq i\leq e-1$ and for $i=e, j=e-1$ the numbers $\sigma_{ij}(x)$ are independant of the choice of x into the class $\bar{C}_i$. From this we deduce the following results.

Proposition 3.8 Let C be an e-error-correcting code over $\mathbb{F}$. Then C is perfect if and only if C admits an e-partition design. Moreover this e-partition design is unique.

Proposition 3.9 Let C be an e-error-correcting quasi-perfect code over $\mathbb{F}$. Then

C is (λ,μ)-uniformly packed code [9] if and only if C admits an $(e+1)$-partition design. Moreover this $(e+1)$-partition design is unique and $\sigma_{ee}=(e+1)\lambda+e(q-2)$, $\sigma_{e+1,e}=(e+1)\mu$.

Example 3.10 If G is a subgroup of the group of Hamming isometries of $\mathbb{F}^n$ and if $C_0,C_1,\ldots,C_r$ are its orbits, then $\{C_0,C_1,\ldots,C_r\}$ is a r-partition design.

We now give some general results that show the interest of the combinatorial matrix A.

Proproposition 3.11 Let $C\subseteq\mathbb{F}^n$ be an unrestricted code of length n over the alphabet $\mathbb{F}$. If C admits a r-partition design $\{C_0,C_1,\ldots,C_r\}$ with associated matrix $\sigma=(\sigma_{uv})$, then

a) for all $x,y\in C_u$, $A_j(x)=A_j(y)=A_j(u)$, $j\geq 0$.

b) the numbers $A_j(u), u\in\{0,\ldots,r\}, j\geq 0$ satisfy the linear recurrence of order r

$$A_j(u)=\sum_{v=0}^{r}\sigma_{uv}A_{j-1}(v), \tag{11}$$

c) the number of distinct rows in the distance matrix B and in the combinatorial matrix A is less than or equal to $r+1$,

d) the external distance s' of C is less than or equal to r.

Proof (by induction on j). Let $C=\bigcup\{C_v \mid v\in J\}, J\subseteq\{0,1,\ldots,r\}$. If $x\in C_v, v\in J$, then $A_0(x)=1$ and if $x\in C_v, v\notin J$, then $A_0(x)=0$.

Now suppose that for $m\leq j-1$ the numbers $A_m(y)=A_m(v)$ only depends on the class C_v to which y belongs and let $x \in C_u$.

For any path γ of length j joining x to C, there exists one and only one v such that γ is obtained by concatenation of a path of length one joining x to $y \in C_v$ and a path of length $j-1$ joining y to C. Since the number σ_{uv} of length 1 paths joining x to C_v does not depend on the chosen x in C_u and that, by induction hypothesis, the number $A_{j-1}(v)$ of paths of length $j-1$ joining y to C does not depend on y, we deduce that $A_j(x)$ does not depend on the chosen x in C_u and moreover that

$$A_j(x)=A_j(u)=\sum_{v=0}^{r}\sigma_{uv}A_{j-1}(v)$$

This proves a) and b). Finally, condition a) means that the combinatorial matrix A has at most $r+1$ distinct rows. Proposition 2.2 then implies that the distance matrix B has also at most $r+1$ distinct rows proving part c). Part d) of the proposition is then an immediate consequence of theorem 3.1 of [2].

Corollary 3.12 Let C be an unrestricted code in F^n with external distance s', $d'_1, \ldots, d'_{s'}$ being the dual distances.

If C admits a s'-partition-design with associated matrix σ, then the eigenvalues of σ are $P_1(l)$ for $l \in \{0, d'_1, \ldots, d'_{s'}\}$.

Proof : First note that (11) may be written in matrix form

$$A_j=\sigma A_{j-1}, \quad j\geq 1$$

with initial vector A_0 defined by

$$A_0(u)=\begin{cases}1 & \text{if } C_u \subseteq C\\ 0 & \textit{otherwise}\end{cases}$$

This gives $A_j=\sigma^j A_0$ and

$$\underline{A}=[A_0, \sigma A_0, \ldots, \sigma^j A_0, \ldots]$$

where $\underline{A}$ is the restricted combinatorial matrix obtained from A by taking the $s'+1$ rows $A(u)$, $u=0,\ldots,s'$.

Since $\underline{A}=\underline{B}S$ by proposition 2.2, the rank of $\underline{A}$ is equal to the rank of $\underline{B}$ which is equal to $s'+1$ by [2,th.3.1]. Hence there exists a unique monic polynomial of degree $s'+1$ $p(Z)=\sum_{j=0}^{s'+1} p_j Z^j$ such that

$$p(\sigma)A_0=\sum_{j=0}^{s'+1} p_j \sigma^j A_0=0.$$

Multiplying by $\sigma^m, m\geq 0$ this yields

$$\sum_{j=0}^{s'+1} p_j \sigma^{j+m} A_0=0$$

and

$$\sum_{j=0}^{s'+1} p_j A_{j+m}=0.$$

The conclusion of corollary is then obtained by applying proposition 2.4.

Remark 3.13 This corollary yields strong necessary conditions for the existence of s'-partition-design containing a code of external distance s'. The characteristic polynomial of σ may replace Lloyd polynomial to obtain non-existence theorem concerning particular classes of codes for example perfect codes, uniformly packed codes etc. [10,11,12]. This is because the parameter e (and λ, μ in case of uniformly packed codes) completly determines the matrix σ for these classes of codes.

Proposition 3.14 Let $C\subseteq F^n$ be an unrestricted code over F and s' be the external distance of C. Then the three following conditions are equivalent.

(i) C admits a s'-partition design

(ii) The number of distinct rows in the distance matrix B is $s'+1$.

(iii) The number of distinct rows in the combinatorial matrix A is $s'+1$.

Moreover if it exists the s'-partition design containing C is unique.

Proof Proposition 3.11 and the fact that rank $B=s'+1$ [2] prove the implication (i) => (ii). Moreover (ii) <==> (iii) by proposition 2.2.

To prove the converse, consider the equivalence relation on F^n defined by

$x \equiv x'$ if and only if the rows $B(x)$ and $B(x')$ of B are equals and denote by $C_0, C_1, \ldots, C_{s'}$ the equivalence classes of this relation. By proposition 2.2, we may also say that $x, x' \in C_u$ if and only if $A_j(x) = A_j(x') = A_j(u)$ for all $j \geq 0$.

For $x \in C_u$ and $v \in \{0,1,\ldots,s'\}$, set

$$\sigma_{uv}(x) = card\{y \in C_v \mid d(x,y) = 1\}$$

Then we have that for all $j \geq 1$ and $x \in C_u$

$$A_j(x) = \sum_{v=0}^{s'} \sigma_{uv}(x) A_{j-1}(v).$$

Now, if $x' \in C_u$, this gives

$$A_j(x) = A_j(x') = A_j(u) = \sum_{v=0}^{s'} \sigma_{uv}(x) A_{j-1}(v) = \sum_{v=0}^{s'} \sigma_{uv}(x') A_{j-1}(v)$$

That is

$$\sum_{v=0}^{s'} \left[\sigma_{uv}(x) - \sigma_{uv}(x')\right] A_{j-1}(v) = 0, \quad j \geq 1.$$

Since $rank\ A = rank\ B = s'+1$, we conclude that

$$\sigma_{uv}(x) - \sigma_{uv}(x') = 0 \quad \text{for} \quad all \quad x, x' \in C_u$$

and $v \in \{0,1,\ldots,s'\}$. Hence $\{C_0, C_1, \ldots, C_{s'}\}$ is a s'-partition design. If C is distance-invariant then C will be one of the classes C_u, otherwise it will be the union of some classes C_u. Finally this s'-partition design is unique by proposition 3.11.

Corollary 3.15 Let C be a code with covering radius ρ. Then C is completely regular if and only if C admits a r-partition-design for $r = \rho$. Moreover $\rho = s'$ and the eigenvalues of the associated matrix σ are $P_1(l)$ for $l \in \{0, d'_1, \ldots, d'_{s'}\}$ where $P_1(x) = n(q-1) - qx$ is the degree one Krawtchouk polynomial of parameter n and $d'_1, \ldots, d'_{s'}$ are the dual distances of C.

In the particular case where the code C is additive we may use theorems

6.10 and 6.11 of [1] to obtain the following results.

Proposition 3.16 Let $C \subset F^n$ be a additive code and s' be the number of non-zero weights of the dual C^- of C. Then the following conditions are equivalent.

(i) C admits a s'partition-design $\pi=\{C_0, C_1, \ldots, C_{s'}\}$.

(ii) The partition $\pi=\{C_0, C_1, \ldots, C_s\}$ of the quotient group $C'=F^n/C$ defines an association scheme over C'

(iii) The restriction to C^- of the Hamming scheme $H(n,q)$ is a subscheme.

The association scheme (ii) whose relations R'_i are well defined by

$$(x+C)R'_i(y+C)$$

if and only if

$$x-y \in C_i$$

because, by definition, C_i is an union of cosets of C, is called the **coset scheme** determined by the partition π.

The P-matrix of the coset scheme has been determined by A Montpetit [13].

Let P_σ be the **left eigenmatrix** of σ whose row number i is the vector v_i with first component 1 such that

$$v_i\sigma = P_1(d'_i)v_i, \qquad 0 \le i \le s'.$$

Proposition 3.17 [13]

The P matrix of the coset association scheme is P_σ the left eigenmatrix of σ.

4. - EXAMPLES

We shall give the matrices σ and P_σ for perfect codes, some uniformly packed codes and some other codes not of these types.

4.1. - Perfect codes

4.1.1. - One-error-correcting perfect codes

If C is a perfect one-error-correcting q-ary code of length n, then by proposition 3.8 there exists a 1-partition-design $\{C_0=C, C_1\}$ in F_q^n with associated matrix

$$\sigma=\begin{bmatrix}0 & n(q-1)\\ 1 & n(q-1)-1\end{bmatrix}.$$

By remark 3.2

$$|C_1|=\sigma_{10}|C_1|=\sigma_{01}|C_0|=n(q-1)|C|$$

where $|X|=$ card X denotes the cardinality of X. Hence

$$q^n=|C_0|+|C_1|=|C|[1+n(q-1)]$$

so that $n=(q^m-1)/(q-1)$ and $|C|=q^{n-m}$ for some natural number m. The dual distances are by corollary 3.12

$$d'_0=[n(q-1)-n(q-1)]/q=0 \text{ and } d'_1=[n(q-1)-(-1)]/q=q^{m-1}$$

because the eigenvalues of σ are $n(q-1)$ and -1. Thus the matrices σ and P_σ for one-error-correcting codes over F_q are

$$\sigma=\begin{bmatrix}0 & q^m-1\\ 1 & q^m-2\end{bmatrix} \text{ and } P_\sigma=\begin{bmatrix}1 & q^m-1\\ 1 & -1\end{bmatrix}$$

4.1.2. - Golay code of length n=11

The parameters are $e=2, q=3$. So matrices σ and P_σ are

$$\sigma=\begin{bmatrix}0 & 22 & 0\\ 1 & 1 & 20\\ 0 & 2 & 20\end{bmatrix} \text{ and } P_\sigma=\begin{bmatrix}1 & 22 & 220\\ 1 & 4 & -5\\ 1 & -5 & 4\end{bmatrix}$$

the eigenvalues of σ being $P_1(0)=n(q-1)=22, P_1(d'_1)=n(q-1)-qd'_1=4$ and $P_1(d'_2)=n(q-1)-qd'_2=-5$ from which we deduce the two non-zero weights of the orthogonal. $d'_1=6$ and $d'_2=9$.

4.1.3. - Golay code of length n = 23

The parameters are $e=3$, $q=2$. So matrices σ and P_σ are

$$\sigma=\begin{bmatrix}0 & 23 & 0 & 0\\ 1 & 0 & 22 & 0\\ 0 & 2 & 0 & 21\\ 0 & 0 & 3 & 20\end{bmatrix} \text{ and } P_\sigma=\begin{bmatrix}1 & 23 & 253 & 1771\\ 1 & 7 & 13 & -21\\ 1 & -1 & -11 & 11\\ 1 & -9 & 29 & -21\end{bmatrix}$$

the eigenvalues of σ being $P_1(0)=n(q-1)=23$, $P_1(d'_1)=n(q-1)-qd'_1=7$, $P_1(d'_2)=-1$ and $P_1(d'_3)=-9$ from which we deduce the three non-zero weights of the orthogonal : $d'_1=8, d'_2=12, d'_3=16$.

4.2 - Some uniformly packed codes

4.2.1. - BCH 2-error-correcting code of length $n=2^{2m+1}-1$.

Here we have a (λ,μ)-uniformly packed code with $\lambda=\frac{n-7}{6}$ and $\mu=\lambda+1=\frac{n-1}{6}$. The matrices σ and P_σ are

$$\sigma=\begin{bmatrix} 0 & 2^{2m+1}-1 & 0 & 0 \\ 1 & 0 & 2^{2m+1}-2 & 0 \\ 0 & 2 & 2^{2m}-4 & 2^{2m}+1 \\ 0 & 0 & 2^{2m}-1 & 2^{2m} \end{bmatrix}$$

$$\text{and } P_\sigma=\begin{bmatrix} 1 & 2^{2m+1}-1 & (2^{2m}-1)(2^{2m+1}-1) & (2^{2m}+1)(2^{2m+1}-1) \\ 1 & 2^{m+1}-1 & (2^m-1)^2 & -(2^{2m}+1) \\ 1 & -1 & -(2^{2m}-1) & 2^{2m}-1 \\ 1 & -(2^{m+1}+1) & (2^m+1)^2 & -(2^{2m}+1) \end{bmatrix}$$

the eigenvalues of σ being $P_1(0)=2^{2m+1}-1, P_1(d'_1)=2^{m+1}-1, P_1(d'_2)=-1$ and $P_1(d'_3)=-(2^{m+1}+1)$ from which we deduce the three non zero weights of the orthogonal : $d'_1=2^{2m}-2^m, d'_2=2^{2m}$ and $d'_3=2^{2m}+2^m$.

4.2.2. - Golay code of length 24

It is the only (λ,μ)-uniformly packed 3-error-correcting code [12]. The parameters are $e=3$, $q=2$, $\lambda=0, \mu=6$.

The matrices σ and P_σ are

$$\sigma=\begin{bmatrix} 0 & 24 & 0 & 0 & 0 \\ 1 & 0 & 23 & 0 & 0 \\ 0 & 2 & 0 & 22 & 0 \\ 0 & 0 & 3 & 0 & 21 \\ 0 & 0 & 0 & 24 & 0 \end{bmatrix}$$

$$P_\sigma=\begin{bmatrix} 1 & 24 & 276 & 2024 & 1771 \\ 1 & 8 & 20 & -8 & -21 \\ 1 & 0 & -12 & 0 & 11 \\ 1 & -8 & 20 & 8 & -21 \\ 1 & -24 & 276 & -2024 & 1771 \end{bmatrix}$$

the eigenvalues being $P_1(0)=24, P_1(d'_1)=8, P_1(d'_2)=0, P_1(d'_3)=-8, P_1(d'_4)=-24$ from which we deduce the four non-zero weights of the orthogonal : $d'_1=8, d'_2=12, d'_3=16, d'_4=24$.

4.2.3. - Preparata codes of length $n=2^{2m}-1$, $m\geq 2$.

These are binary 2-error-correcting non-linear (λ,μ)-uniformly packed codes with $\lambda=\frac{1}{3}[2^{2m}-4]$ and $\mu=\frac{1}{3}[2^{2m}-1]$. The matrices σ and P_σ are

$$\sigma=\begin{bmatrix} 0 & 2^{2m}-1 & 0 & 0 \\ 1 & 0 & 2^{2m}-2 & 0 \\ 0 & 2 & 2^{2m}-4 & 1 \\ 0 & 0 & 2^{2m}-1 & 0 \end{bmatrix}$$

$$P_\sigma=\begin{bmatrix} 1 & 2^{2m}-1 & (2^{2m}-1)(2^{2m-1}-1) & 2^{2m-1}-1 \\ 1 & 2^m-1 & -(2^m-1) & -1 \\ 1 & -1 & -(2^{2m-1}-1) & 2^{2m-1}-1 \\ 1 & -(2^m+1) & 2^m+1 & -1 \end{bmatrix}$$

The eigenvalues of σ are $P_1(0)=2^{2m}$, $P_1(d'_1)=2^m-1$, $P_1(d'_2)=-1$, $P_1(d'_3)=-(2^m+1)$, so that the dual distances are $d'_1=2^{m-1}(2^m-1)$, $d'_2=2^{2m-1}$ and $d'_3=2^{m-1}(2^m+1)$.

4.2.4. - Van Lint code of length $n=11$ [12]

This is a binary non-linear 2-error-correcting (λ,μ)-uniformly packed code with $\lambda=2$ and $\mu=3$. The matrices σ and P_σ are

$$\sigma=\begin{bmatrix} 0 & 11 & 0 & 0 \\ 1 & 0 & 10 & 0 \\ 0 & 2 & 6 & 3 \\ 0 & 0 & 9 & 2 \end{bmatrix}$$

$$P_\sigma=\begin{bmatrix} 1 & 11 & 55 & 55/3 \\ 1 & 3 & -1 & -3 \\ 1 & -1 & -5 & 5 \\ 1 & -5 & 7 & -3 \end{bmatrix}$$

The eigenvalues of σ are $P_1(0)=11$, $P_1(d'_1)=3$, $P_1(d'_2)=-1$ and $P_1(d'_3)=-5$. So the non-zero dual distances are $d'_1=4, d'_2=6, d'_3=8$.

4.3 - Some non-uniformly packed codes admitting s'-partition-design

We shall use remark 3.3 to define a s'-partition design of F^n by means of subset $\Omega_0=0,\Omega_1,\Omega_2,\ldots,\Omega_{s'}$, of F^k.

4.3.1. -

Set

$$\Omega_0=\begin{bmatrix}0\\0\\0\end{bmatrix},\quad \Omega_1=\begin{bmatrix}1100\\0110\\0011\end{bmatrix}\quad \Omega_2=\begin{bmatrix}0\\1\\0\end{bmatrix}\quad \Omega_3=\begin{bmatrix}11\\01\\11\end{bmatrix}$$

$$C=\mathit{Ker}\ H \ \mathit{where}\ H=\begin{bmatrix}11000\\01101\\00110\end{bmatrix}\quad i.e.\ \ \Omega=\Omega_1\cup\Omega_2$$

We have here

$$\sigma=\begin{bmatrix}0&4&1&0\\1&1&1&2\\1&4&0&0\\0&4&0&1\end{bmatrix},\quad P_\sigma=\begin{bmatrix}1&4&1&2\\1&0&1&-2\\1&0&-1&0\\1&-4&1&2\end{bmatrix}$$

and the eigenvalues of σ are $5,+1,-1,-3$ that is $n(q-1)-qw_i$ for $n=5,q=2,w_i\in\{0,2,3,4\}$, the w_i being the weights of C.

4.3.2. -

Set

$$\Omega_0=\begin{bmatrix}0\\0\\0\\0\end{bmatrix},\ \Omega_1=\begin{bmatrix}100101\\011001\\010110\\010101\end{bmatrix},\ \Omega_2=\begin{bmatrix}1\\1\\1\\1\end{bmatrix},\ \Omega_3=\begin{bmatrix}101010\\100101\\011001\\010110\end{bmatrix},\ \Omega_4=\begin{bmatrix}01\\01\\01\\10\end{bmatrix}\quad C=C_0=\mathit{Ker}\,\Omega_1.$$

We have here

$$\sigma=\begin{bmatrix} 0 & 6 & 0 & 0 & 0 \\ 1 & 0 & 1 & 4 & 0 \\ 0 & 6 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 2 \\ 0 & 0 & 0 & 6 & 0 \end{bmatrix},\quad P_\sigma=\begin{bmatrix} 1 & 6 & 1 & 6 & 2 \\ 1 & 2 & 1 & -2 & -2 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & -2 & 1 & -2 & 2 \\ 1 & -6 & 1 & 6 & -2 \end{bmatrix}$$

and the eigenvalues of σ are 6, 2 , 0, -2, -6 that is $n(q-1)-qw_i$ for $n=6$ and $w_i \in \{0,2,3,4,6\}$, the w_i being the weights of C .

Note : If we merge C_0 and C_2 because $\sigma_{0\nu}=\sigma_{2\nu}$ and $\sigma_{\nu 0}=\sigma_{\nu 2}$ for all $\nu=0,\ldots,5$, then $C'_0=C_0 \cup C_2, C_1, C_3, C_4$ form a 3-partition design but it doesn't contain C.

4.3.3. -

Set

$$\Omega_0=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix},\quad \Omega_1=\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix},$$

$$\Omega_4=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

and let the columns of Ω_3 be the complements of $\Omega_0 \cup \Omega_1 \cup \Omega_4$ in $\mathbb{F}_2^6$.

If $C=Ker\ \Omega_1$ then

$$\sigma=\begin{bmatrix} 0 & 15 & 0 & 0 \\ 1 & 2 & 12 & 0 \\ 0 & 4 & 10 & 1 \\ 0 & 0 & 15 & 0 \end{bmatrix},\quad P_\sigma=\begin{bmatrix} 1 & 15 & 45 & 3 \\ 1 & 3 & -3 & -1 \\ 1 & -1 & -3 & 3 \\ 1 & -5 & 5 & -1 \end{bmatrix}$$

and the eigenvalues of σ are 15,3,−1,−5 that is $n(q-1)-qw_i$ for $n=15$, $q=2$ and $w_i \in \{0,6,8,10\}$ the w_i being the weights of C.

4.3.4. - Nordstrom-Robinson of length 16 [MacWilliams-Sloane p. 171]

This is a **non-linear** formally self-dual code C with distances $d_1=6, d_2=8, d_3=10, d_4=16$. C admits the 4-partition design C_0, C_1, C_2, C_3, C_4 where $C_i=\{x \in F_2^{16} \mid d(x,C)=i\}$. The matrices σ and P_σ are

$$\sigma=\begin{bmatrix} 0 & 16 & 0 & 0 & 0 \\ 1 & 0 & 15 & 0 & 0 \\ 0 & 2 & 0 & 14 & 0 \\ 0 & 0 & 15 & 0 & 1 \\ 0 & 0 & 0 & 16 & 0 \end{bmatrix}$$

$$\text{and } P_\sigma=\begin{bmatrix} 1 & 16 & 120 & 112 & 7 \\ 1 & 4 & 0 & -4 & -1 \\ 1 & 0 & -8 & 0 & 7 \\ 1 & -4 & 0 & 4 & -1 \\ 1 & -16 & 120 & -112 & 7 \end{bmatrix}$$

The eigenvalues of σ are 16, 4, 0, -4, -16 that is $n(q-1)-qd_i$ with $n=16, q=2$ and $d_i \in \{0,6,8,10,16\}$ as it should be.

4.3.5. - An exemple [13] where there doesn't exist a s'partition design : **First** order Reed-Muller code of length 16.

If C denotes the first order Reed-Muller code of length 16, then the covering radius is $\rho=6$ and $s'=6$ because the extended Hamming code has weights 0,4,6,8,10,12,16. C admits the 7-partition-design $\{C_0, C_1, C_2, \ldots, C_7\}$ where the C_i are the equivalence classes for the relation over F_2^{16} $x \equiv y$ if and only if the cosets $x + C$ and $y + C$ have the same weight distributions.

The matrices σ and P_σ are here

$$\sigma=\begin{bmatrix} 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 15 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 14 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 & 12 & 0 & 0 \\ 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 15 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 \end{bmatrix}$$

$$P_\sigma=\begin{bmatrix} 1 & 16 & 120 & 560 & 35 & 840 & 448 & 28 \\ 1 & 8 & 24 & 24 & 3 & -24 & -32 & -4 \\ 1 & 4 & 0 & -20 & -5 & 0 & 16 & 4 \\ 1 & 0 & -8 & 0 & 0 & 14 & 0 & -7 \\ 1 & 0 & -8 & 0 & 1 & 12 & 0 & -6 \\ 1 & -4 & 0 & 20 & -5 & 0 & -16 & 4 \\ 1 & -8 & 24 & -24 & 3 & -24 & 32 & -4 \\ 1 & -16 & 120 & -560 & 35 & 840 & -448 & 28 \end{bmatrix}$$

The eigenvalues of σ are 16,8,4,0,-4,-8,-16 ; 0 being a double eigenvalue. Note that there doesn't exist a 6-partition-design containing C because B has 8 distinct rows. We may also note that the eigenvalues are $n(q-1)-qw_i$ with w_i the weights of C .

Acknowledgment : The second author wishes to express his sincere thanks to INRIA for his kind hospitally, P. Sole' and A. Montpetit for numerous stimulating discussions on the subject of this paper.

REFERENCE

[1] Delsarte P.,
An algebraic approach to the association schemes of coding theory,
Philipps Research Reports Supplements 10 (1973).

[2] Delsarte P.,
Four Fundamental Parameters of a Code and Their Combinatorial Significance,
Inform and Control 23, 407-438 (1973).

[3] Comtet L.,
Advanced Combinatorics,
D. Reidel Publishing co., 1974.

[4] Camion P., Courteau B., Fournier G., Kanetkar S.V.,
Weight Distribution of Translates of Linear Codes and Generalized Pless Identities,
To appear in Journal of information & optimization Sciences
(No 183/85).

[5] Courteau B., Fournier G., Fournier R.,
Etude de certains parame'tres associe's a' un code line'aire,
Ann. Discrete Math. 17, 225-233, 1983.

[6] Pless V.,
Power Moment Identities on weight distribution in error-correcting Codes.
Inform. and Control, 6, 147-152, 1963.

[7] MacWilliams F.J., and Sloane N.J.A.,
The Theory of Error-Correcting Codes
North-Holland, Amsterdam, 1977.

[8] Camion P.,
Difference sets in elementary abelian groups,
Les presses de l'Universite' de Montre'al, Montre'al, 1979.

[9] Goethals J.M., and Van Tilborg H.C.A.,
Uniformly packed codes,
Philips Research Reports 30, 9-36, (1975)

[10]Tietavainen A.,
A short proof for the non-existence of unknown perfect codes over GF (q), q > 2,
Ann. Acad. Sc. Fenn., Ser. AI Math., 580, 1-6, (1974).

[11]Van Lint J.H.,
A Survey of Perfect Codes,
Rocky Mountain J. Math., 5, 199-224 (1975).

[12]Van Tilborg H.C.A.,
Uniformly packed codes,
Thesis, Tech. Univ. Eindhoven, 1976.

[13]Montpetit A.,
Determination of the eigenmatrices of the coset scheme of an uniform linear code,
Unpublished.

[14]Courteau B., Fournier G., Fournier B.,
A Characterization of N-weight projective codes,
IEEE Trans. Inform. Theory 27 (1981) 808-812

[15]Higman D.G.,
Coherent configurations,
Geometrical Dedicata 4 (1975) 1-32.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique