Pub. Mat. U.A.B.
Vol. 26 Nº 2 Juny 1982

CODING THEORY AS A MATHEMATICAL OBJECT: REGULAR CODES AND ASSOCIATION SCHEMES.

Llorenç Huguet i Rotger
Departament d'Informàtica, U.A.B

Rebut el 10 de desembre de 1981

Abstract:

Coding theory began as an engineering problem suggest by the Shannon, Golay and Hamming works and has developed by using more and more sophisticated mathematical techniques. This subject overlaps with so many other: group theory, number theory, switching functions, combinatorial geometries, association schemes, etc.

We present in this paper a sumary of some combinatorial properties of the family of regular codes, recently developed in (4), based on the coefficients of the dual weight enumerator of its cosets and the Krawtchouk polynomials. From the Goethals-va Tilborg's characterization (3) and from the Delsarte's work (1) we proof that for every s-weight linear code C(n,k), whose orthogonal code $C^{\perp}$ is regular, we can define a s-classes association scheme such that the rows of its eigenmatrix P are the coefficients of the dual weight enumerators of the orthogonal code and its cosets.

1.- ASSOCIATION SCHEME AND DESIGN STRUCTURE

An association scheme with n-classes on a set X consists of a partition of the set XxX into n+1 classes $\Gamma_0, \Gamma_1, \ldots, \Gamma_n$ satisfying the following conditions:

1: $\Gamma_0 = \{(x,x) \in X x X\}$

2: Given $x \in X$, the number $v_i := \# \{y \in X: (x,y) \in \Gamma_i\}$ depends only on y.

3: Given $(x,y)\in\Gamma_k$, the number $p_{ij}^k := \#\{z\in X: (x,z)\in\Gamma_i \text{ and } (y,z)\in\Gamma_j\}$ depends only on i,j and k.

(# denote the cardinal of the set)

If we denote by D_i the adjacency matrix of the graph (X,Γ_i) (the second condition asserts that each graph (X,Γ_i) is regular) which entries $D_i(x,y)$ are equal to 1 if $(x,y)\in\Gamma_i$ and 0 otherwise; we observe that the (x,y)-entry in the matrix product $D_i.D_j$ is p_{ij}^k if $(x,y)\in\Gamma_k$. Moreover the diagonal entries are equal to zero unless i=j, in which case they are equal to v_i. Then we can write:

$$D_i.D_j = D_j.D_i = \sum_{k=0}^{n} p_{ij}^k D_k \qquad -1-$$

where $p_{ij}^0=\delta_{ij}$ and $p_{i0}^k=p_{0i}^k=\delta_{ik}$.

This shows that the commuting symmetric matrices $D_0,D_1,\dots,D_n$ span a (n+1)-dimensional real algebra called the Bose-Mesner algebra of the scheme, which is semisimple (rf (1), Th. 2.1 and Th. 2.2) and hence admits a basis of mutually orthogonal idempotent matrices $J_0,J_1,\dots,J_n$; that is $J_i.J_k=\delta_{ik}.J_i$. Respect to the basis $\{J_0,J_1,\dots,J_n\}$, every D_k can be written as an expression of the form:

$$D_k = \sum_{i=0}^{n} p_k(i).J_i \quad \text{for } k=0,1,\dots,n \qquad -2-$$

where $p_k(i)$ are the eigenvelues of D_k, because $D_k.J_i=p_k(i).J_i$. The square matrix P of order n+1 whose (i,k)-entry is $p_k(i)$, $0\leq i,k\leq n$, is called the eigenmatrix of the scheme.

The matrix Q defined by $Q:= |X|.P^{-1}$, whose (i,k)-entry will be denoted by $q_k(i)$, is called the dual eigenmatrix of the scheme. Note that from -2- we obtain

$$J_k = |X|^{-1} \sum_{i=0}^{n} q_k(i).D_i \quad \text{for } k=0,1,\dots,n \qquad -3-$$

For every association scheme defined on a set X which has P and Q as eigenmatrix and dual eigenmatrix repectively, holds:

$$P^t = \Delta_v.Q.\Delta_\mu^{-1} \qquad -4-$$

where Δ_v and Δ_μ are diagonal matrices having the same order that P and Q and which diagonal entries are the valences v_i and multiplicities μ_i; that is, v_i is defined as 2: and μ_i is the dimension of the subspace V_k which has associated the eigenvalues $p_k(0)$,

$p_k(1),\ldots,p_k(n)$ of D_k. Moreover:

$$p_k(0)=v_k \quad\text{and}\quad q_k(0)=\mu_k \qquad -5-$$

being $p_k(0)$ the eigenvalue of D_k which is associated to the eigenvector $(1,1,\ldots,1)$.

We define now a combinatorial structure, called design, over a subset Y of a point set X of an association scheme with n-classes.

The inner distribution of Y is the $(n+1)$-tuple $\underline{a}=(a_0,\ldots,a_n)$ which coordinate a_i is:

$$a_i := |Y|^{-1} \sum_{x\varepsilon Y} \sum_{y\varepsilon Y} D_i(x,y) \qquad -6-$$

and the dual distribution of Y is the $(n+1)$-tuple $\underline{b}=(b_0,b_1,\ldots,b_n)$ that consists of the inner distribution of $Y^{\perp}:=\{x\varepsilon X:\ (x|y)=0\ \forall y\varepsilon Y\}$ where $(.|.)$ is the scalar product.

A subset Y of a point set X of an association scheme with n-classes such that their inner and dual distribution satisfy:

$$s=\#\{a_k\neq 0;\ k\neq 0\}$$

and $\qquad -7-$

$$b_1=b_2=\ldots=b_\tau=0 \text{ and } b_{\tau+1}\neq 0$$

is called a design of degree s and maximum strenght τ.

theorem 1 (Delsarte)

Let $Y\subsetneq X$ be a design of degree s and maximum strenght τ which satisfies $\tau=2s-2$ or $2s-1$ or $2s$. Then we can define an association scheme with s-classes $\Gamma_0^Y,\Gamma_{i_1}^Y,\ldots,\Gamma_{i_s}^Y$

$$\Gamma_{i_j}^Y = Y\mathrm{x}Y\cap\Gamma_j \qquad -8-$$

where Γ_j is the j-th class of the association scheme on X which associated coordinate a_i of the inner distribution of Y is non-zero. Moreover, the dual eigenmatrix $Q=(q_k(i))$ of the association scheme (Y,Γ^Y) is given by the formula:

$$q_k(i_j)=\begin{cases} P_k(i_j) \text{ if } k=0,1,\ldots s-1 \\ \alpha(i_j)-\psi_{s-1}(i_j) \text{ if } k=s \end{cases} \qquad -9-$$

where $\alpha(z)$ is the annihilator polynomial of Y, that is: $\alpha(z)= |Y|^{-1} \prod_{j=0}^{n} (1- \frac{z}{i_j})$, being i_j the nonzero coordinates in the inner distribution of Y; and $\psi_{s-1}(z)= \sum_{k=0}^{s-1} P_k(z)$, being $P_k(z)$ the Krawtchouk polynomial (see -18-) of degree k in the variable z.

Remark: this theorem corresponds to theorem 5.25 and corolary 5.26 of Delsarte's work (1), and it is a crucial result for our theorem 5.

In the particular case where X is an additive finite abelian group, useful in coding theory, the (n+1)-classes $\Gamma_0,\Gamma_1,\ldots,\Gamma_n$ are invariant under translations; that is:

$$(x,y)\in\Gamma_i \implies (x+z,y+z)\in\Gamma_i \quad \forall z\in X \tag{-10-}$$

Thus we have a partition of X into n+1 classes $X_0,X_1,\ldots,X_n$ defined by

$$(x,y)\in\Gamma_i \iff \pm (y-x)\in X_i \quad \text{for } i=0,1,\ldots,n \tag{-11-}$$

In the other way, let S denote the square matrix of order $|X|$ with $\chi_y(x)$ its entries indexed by the elements $x,y\in X$ (χ_y is the associated character to y on X). The orthogonality relations satisfied by them can be expressed by the matrix equation

$$\tilde{S}.S=S.\tilde{S}=|X|.I \tag{-12-}$$

where $\tilde{S}$ is the conjugate transpose of S. They follow from $\tilde{\chi}_y(x)=\chi_y(-x)$ and from the relations $\sum_{x\in X} \chi_y(x)=\begin{cases}|X| \text{ if } y=0\\ 0 \text{ otherwise}\end{cases}$ that the columns of S are the eigenvectors of all the matrices in the Bose-Mesner algebra of the association scheme (rf. (1),(2)), hence we can write a new partition of X into n+1 classes $X_0',X_1',\ldots,X_n'$ where X_i' is the set of indices $z\in X$ for which the corresponding column of S is in the i-th eigenspace V_i. In this way, we have:

$$X_0'=\{0\} \quad \text{and} \quad |X_i'|=\mu_i \tag{-13-}$$

From these partition of X we can define a new partition $\Gamma_0',\Gamma_1',\ldots,\Gamma_n'$ on XxX as follows:

$$(x,y)\in\Gamma_i' \iff \pm(y-x)\in X_i' \tag{-14-}$$

resulting that the n+1 classes Γ_i' form an association scheme on

X, called the dual scheme from the constructed one by the classes Γ_i (rf(2)).

The respective eigenmatrices and parameters satisfy (rf. (1) th 2.8):

$$P=Q' \quad \text{and} \quad Q=P' \qquad -15-$$

$$v_k=\mu'_k \quad \text{and} \quad \mu_k=v'_k$$

Let $X=(F_q^n,+)$ be the set of all the n-tuples $\underline{x}=(x_1,\ldots,x_n)$ from a Galois field F_q of order $q=p^r$ for a prime number p. We make X a metric space by definning the Hamming distance $d_H(\underline{x},\underline{y})$ betwen two n-tuples to be the number of coordinates in which they are different.

For $i=0,1,\ldots,n$ we define Γ_i by the set of all pairs of n-tuples at distance i, that is:

$$\Gamma_i= \{(\underline{x},\underline{y})\varepsilon X\text{x}X:\ d_H(x,y)=i\} \qquad -16-$$

which constitutes an association scheme, called the Hamming scheme. This one is a self-dual association scheme (P=Q) and its eigenmatrix elements are given by:

$$p_k(i)=q_k(i)=P_k(i) \qquad -17-$$

where $P_k(i)$ denotes the Krawtchouk polynomial of degree k in the variable i, which is defined in (5) by

$$P_k(i)=\sum_{j=0}^{n}(-1)^j(q-1)^{k-j}\binom{i}{j}\binom{n-k}{k-j} \qquad -18-$$

for two orefix numbers: n and q.

From the expressions -5-,-17- and -18- we can write the parameters of a Hamming scheme by

$$\mu_k=v_k=\binom{n}{k}(q-1)^k \qquad -19-$$

Remark: For the design structure defined by -7- over a subset Y of the point set X of a Hamming scheme; that is, Y can be considered as a linear code, the inner and dual distribution coincide with the enumerator weight coefficients $(A_0,A_1,\ldots,A_n)$ of Y and the enumerator weight coefficients $(B_0,B_1,\ldots,B_n)$ of its dual code $Y^{\perp}$ respectively.

2.- REGULAR CODES

A linear code $C(n,k)$. over F_q, is a k-dimensional subspace of the n-dimensional vectorial space that consists on all the n-tuples with the elements of F_q: $V=\{\underline{u}=(u_1,u_2,\dots,u_n): u_i \in F_q\}$. The orthogonal code $C^{\perp}(n,n-k)$ is the (n-k)-dimensional subspace of V consisting on all the n-tuples $\underline{v} \in V$ which inner product with every codeword of C is zero.

The weight enumerator of a code C is the polynomial in the variable z:

$$A_C(z) = \sum_{\underline{u} \in C} z^{w(\underline{u})} = \sum_{i=0}^{n} A_i . z^i \qquad -20-$$

where $w(\underline{u})$ denotes the weight of the codeword $\underline{u}$, that is the number of nonzero coordinates u_i, and A_i is the number of codewords of weight i.

Let $B_C(z)=A_{C^{\perp}}(z)= \sum_{j=0}^{n} B_j . z^j$ be the weight enumerator of $C^{\perp}$. Between the weight enumerator of a linear code and the one of its orthogonal code, there exist the following relation:

$$B_C(z)=|C|^{-1}(1+(q-1)z)^n A_C\left(\frac{1-z}{1+(q-1)z}\right) \qquad -21-$$

called the <u>MacWilliams identity</u>; or equivanlently:

$$A_C(z)=|C^{\perp}|^{-1} \sum_{j=0}^{n} B_j . (1-z)^j (1+(q-1)z)^{n-j} \qquad -22-$$

where the right hand is called the <u>dual form of the weight enumerator</u> of C, (rf.(5)).

In order to generalize expression -22- for the weight enumerator of any coset $C_j := C + \underline{u}_j$ of C, we write :

$$A_{C_j}(z) = \sum_{i=0}^{n} A_i(C_j) . z^i \qquad -23-$$

where $A_i(C_j)$ denotes the number of vectors of weight i into the coset C_j, for $j=0,1,\dots,q^{n-k}-1$.

<u>Remark:</u> $V=C_0 \cup C_1 \cup \dots \cup C_{q^{n-k}-1}$ is the partition given by the equivalence relation $R_C=\{(u,v) \in VxV: \underline{u}-\underline{v} \in C\}$, and the leader $\underline{u}_j$ is a minimum weight vector into C_j. Obviously, $C_0=C$ itself.

Taking the complex algebra of all the polynomials in the variables $X_{q_i,j}$ for $q_i \in F_q$ and $1 \leqslant j \leqslant n$, denoted by A, we can define the two following applications:

$$f: V \longrightarrow A$$
$$\underline{a}=(a_1,\ldots,a_n) \longrightarrow f(\underline{a})= \prod_{i=1}^{n} X_{a_i,i} \qquad -24-$$

and

$$g: V \longrightarrow A$$
$$\underline{a}=(a_1,\ldots,a_n) \longrightarrow g(\underline{a})= \sum_{\underline{b}\in V} \chi_{\underline{a}}(\underline{b}).f(\underline{b}) \qquad -25-$$

where $\chi_{\underline{a}}$ denotes a character defined on the additive group $(V,+)$.

From definitions of f and g, and from the characters properties, we can write (rf. (4)):

<u>lemma 2</u>

For any coset C_j of a linear code $C(n,k)$ the following identity holds:

$$\sum_{\underline{u}\in C_j} g(\underline{u}) = |C| \sum_{\underline{b}\in C^{\perp}} \chi_{\underline{u}_j}(\underline{b}).f(\underline{b}) \qquad -26-$$

Identifying $X_{0,i}=1$ and $X_{a_i,i}=z$ if $a_i\neq 0$, into -24- and -25-; the duality of the MacWilliams identity -21- and our lemma 2 proves (rf(4)):

<u>theorem 3</u>

The weight enumerator of any coset $C_j:=C+\underline{u}_j$ of a linear code $C(n,k)$ can be written under the dual form:

$$A_{C_j}(z)=|C^{\perp}|^{-1} \sum_{h=0}^{n} B_h(C_j)(1-z)^h(1+(q-1)z)^{n-h} \qquad -27-$$

where the coefficients $B_h(C_j)$ are defined as:

$$B_h(C_j)= \sum_{\substack{\underline{v}\in C^{\perp} \\ \overline{w}(\underline{v})=h}} \chi_{\underline{u}_j}(\underline{v}) \qquad -28-$$

<u>Remarks</u>: When the coset C_j is the code itself, this theorem is equivalent to MacWilliams identity -22- because we have, from the properties of characters: $B_h(C)=B_h$.

The coefficients $B_h(C_j)$ are easily obtained if C is a regular code, through the Krawtchouk polynomials.

Let "s" be the number of distinct nonzero weights in the orthogonal code $C^{\perp}$ of a given code C; s is usually called <u>external distance of C</u>. A linear code C is named <u>r-regular</u>,

$0 \leqslant r \leqslant s$, if and only if the weight enumerators of their cosets C_j, which have minimum weight $i \leqslant r$, depends only on i. When $r=s$, C is called completely regular.

Goethals-van Tilborg give the characterization of the regular codes as a function of the minimum weight d and the external distance s of the code (rf.(3) th.7) as follows:

1) if $s<d\leqslant 2s-1$, then C is $(d-s)$-regular -29-
2) if $d>2s-1$, then C is completely regular

theorem 4

For every coset $C_j:=C+\underline{u}_j$ having minimum weight i, $i \leqslant r \leqslant t$, of a r-regular t-error correcting code ($d \geqslant 2t+1$), we have:

$$B_h(C_j) = \left(\binom{n}{i}(q-1)^i\right)^{-1}.P_i(h).B_h \qquad \text{-30-}$$

where $P_i(h)$ is the Krawtchouk polynomial of degree i in the variable h (rf.-18-) and B_h is the number of the n-tuples of weight h into $C^{\perp}$.

proof:

By the duality of -27- we can write:

$$\sum_{h=0}^{n} B_h . z^h = |C|^{-1} \sum_{m=0}^{n} A_m(C_j)(1-z)^m(1+(q-1)z)^{n-m} \qquad \text{-31-}$$

and since $A_m(C_j)$ depends only on i, we have for $i \leqslant r$:

$$\sum_{\substack{C_j \\ w(\underline{u}_j)=i}} \left(\sum_{m=0}^{n} A_m(C_j)(1-z)^m(1+(q-1)z)^{n-m}\right)$$

$$= \binom{n}{i}(q-1)^i \sum_{m=0}^{n} A_m(C_j)(1-z)^m(1+(q-1)z)^{n-m}$$

$$= \binom{n}{i}(q-1)^i \left(\sum_{h=0}^{n} B_h(C_j).z^h\right)|C| \qquad \text{-32-}$$

By the character property: $\displaystyle\sum_{\substack{\underline{u}\in V \\ w(\underline{u})=i}} \chi_{\underline{v}}(\underline{u}) = P_i(w(\underline{v}))$

where $P_i(w(\underline{v}))$ is the Krawtchouk polynomial of degree i in the variable $w(\underline{v})$; we can write , in the other way:

$$\sum_{\substack{C_j\\ w(\underline{u}_j)=i}} |C| \sum_{h=0}^{n} B_h(C_j).z^h = \sum_{\substack{C_j\\ w(\underline{u}_j)=i}} |C| \sum_{h=0}^{n} \Big(\sum_{\substack{\underline{v}\in C^{\perp}\\ w(\underline{v})=h}} \chi_{\underline{u}_j}(\underline{v}) \Big).z^h$$

$$= |C| \sum_{\underline{v}\in C^{\perp}} z^{w(\underline{v})} \sum_{\substack{\underline{u}\in V\\ w(\underline{u})=i}} \chi_{\underline{v}}(\underline{u})$$

$$= |C| \sum_{\underline{v}\in C^{\perp}} z^{w(\underline{v})} \; P_i(w(\underline{v}))$$

$$= |C| \sum_{h=0}^{n} B_h.P_i(h).z^h \qquad -33-$$

From -31-, the equality between -32- and -33- holds and so -30- is proved. ##

<u>Remark</u>: The particular case when $s\leqslant t+1$ is very interesting since the coefficients $B_h(C_j)$ can be found for every coset of a regular code. (If $i\leqslant t$, following the above theorem, and if $i=t+1$ following the next corolary).

<u>corolary</u>: (rf.(4))

a) With the same assumptions of the theorem 3 we have:

$$\sum_{j=0}^{M-1} B_h(C_j) = \begin{cases} 0 \text{ if } h\neq 0 \\ M=q^{n-k} \text{ if } h=0 \end{cases} \qquad -34-$$

b) With the same assumptions of the theorem 4 we have:

$$\sum_{h=0}^{n} B_h(C_j) = \begin{cases} 0 \text{ if } 0<i\leqslant r \\ |C^{\perp}|=q^{n-k} \text{ if } i=0 \end{cases} \qquad -35-$$

3.- <u>REGULAR CODES AND ASSOCIATION SCHEMES</u>

A linear code is said to be <u>projective</u> if its generator matrix has not a linear dependence between any two columns. Let $C(n,k)$ be a linear projective code with "s" distinct nonzero weights $w_1,w_2,\dots,w_s$ and such that the minimum weight in the orthogonal code d' satisfies: $d'\geqslant 2s-1$; that is $C^{\perp}$ is completely regular (rf-29-), then we can define two dual association scheme on the additive group associated to code C.

Let $X=(C,+)$ be the additive group associated to the projective code $C(n,k)$, that is, the set of all the codewords with the componentwise modulo q addition. We define the partition Γ_0, $\Gamma_1,\ldots,\Gamma_s$ by:

$$\Gamma_0=\{(x,x)\in X\times X\} \quad\text{and}\quad \Gamma_i=\{(x,y)\in X\times X:\ w(x-y)=w_i\} \qquad -36-$$

which constitutes an association scheme with s-classes on X where $v_i=|X_i|=A_{w_i}$ for $0\leqslant i\leqslant s$ being X_i a class of the partition induced by Γ_i on X. (rf.(1) and (2)).

In the other way, we can consider $C={}^{V}/_{C^{\perp}}$ as a quotient of additives groups and consequently the decomposition of V into $N=q^k$ cosets of $C^{\perp}$, that is $C=Y_0\cup Y_1\cup\ldots\cup Y_N$ where $Y_0=C^{\perp}$ and $Y_j=C^{\perp}+\underline{v}_j$ for $j\neq 0$. Since $C^{\perp}$ is a completely regular code all its cosets, having the same minimum weight at most s, have the same weight enumerator. Moreover, since $d'\geqslant 2s-1$, $C^{\perp}$ is a (s-1)-error correcting code and each codeword of C with weight at most s-1 belong to distinct cosets Y_j of $C^{\perp}$. In this way, we can write a new partition $\Gamma'_0,\Gamma'_1,\ldots,\Gamma'_s$ over X as follows:

$$\Gamma'_0=\{(Y_j,Y_j)\in C\times C\} \quad\text{and}\quad \Gamma'_i=\{(Y_j,Y_k)\in C\times C:\ W_H(Y_j-Y_k)=i\} \quad -37-$$

where $W_H(Y_j-Y_k)$ denotes the minimum weight in the coset $Y_j-Y_k:=C^{\perp}+(\underline{v}_j-\underline{v}_k)$. This partition defines an association scheme with s-classes on C, this one considered as the set of all the cosets Y_i of $C^{\perp}$, and constitutes the dual scheme of the one defined by -36-. In this case, $\mu_i=|X'_i|=\binom{n}{i}(q-1)^i$ for $0\leqslant i\leqslant s-1$ and $\mu_s=q^k-\sum_{k=0}^{s-1}\mu_k$

Using the theorem 1 we can show an important combinatorial result, explained in the following:

<u>theorem 5</u>:

For every linear projective code C(n,k) with "s" distinct nonzero weights such that the minimum weight d' of the orthogonal code satisfies: $2s-1\leqslant d'\leqslant 2s+1$; we can define an association scheme with s-classes on C such that the rows of its eigenmatrix P coincide with the coefficients of the dual weight enumerators of $C^{\perp}$ and of its cosets.

proof:

According with definition -7- and remark of page 5; this code C is a design of degree "s" and maximum strenght $\tau=d'-1$, which satisfies the assumptions of theorem 1. Then (C,Γ^{C}) is an association scheme whose dual eigenmatrix Q is obtained by -9-.

From -29- we claim that $C^{\perp}$ is completely regular and moreover that is a (s-1)-error correcting code ($d'>2t+1$ being $t=s-1$ the capacity of error correction). In this way, we can apply the theorem 4 for every coset of $C^{\perp}$ having minimum weight $i\leq t$ and -34- for them which minimum weight is t+1.

If we arrange those results in a (s+1)x(s+1) matrix B whose entries (i,w_i) are the coefficients $B_{w_i}(C+\underline{v}_j)$, where this coset has minimum weight i, i=0,1,..,s and $w_0=0$; we can write:

$$B = C^{-1}.Q^{t}.A \qquad -38-$$

where A and C are diagonal matrices whose entries are, respectively; $a_{ii}=A_{w_i}$ (the coefficients of the weight enumerator of $C=(C^{\perp})^{\perp}$)

and $c_{ii}=\begin{cases} \binom{n}{i}(q-1)^{i} & \text{for } 0\leq i\leq s-1 \\ q^{n-(n-k)}-\sum_{j=0}^{s-1} c_{jj} & \end{cases}$ (the number of cosets of C with minimum weight i)

From definitions -36- and -37- we assure that the right hand in -38- coincide with the transpose of the right hand in -4-. Then, B=P and this proof is end. ##

<u>example 1</u>:

For the perfect binari Golay code with a weight enumerator (rf.(5)):

$$A_G(z)=1+253z^{7}+506z^{8}+1288z^{11}+1288z^{12}+506z^{15}+253z^{16}+z^{23}$$

from which we know it is completely regular and that its orthogonal code has three nonzero weights:

$$A_{G^{\perp}}(z)=1+506z^{8}+1288z^{12}+253z^{16}$$

we can obtain easily all the coefficients $B_h(G_j)$ of the dual weight enumerator of all the cosets $G_j:=G+\underline{u}_j$ through theorem 4 and from the three-term recurrence of the Krawtchouk polynomial (rf.(4)), and we have the next table where B is the central piece:

i	$B_0(G_j)$	$B_8(G_j)$	$B_{12}(G_j)$	$B_{16}(G_j)$	N° of cosets with minimum weight i
0	1	506	1288	253	1
1	1	154	-56	-99	23
2	1	26	-56	29	253
3	1	-6	8	-3	1771

Consequently, let C be this three weight linear code which orthogonal code is the binary Golay code with minimum weight d'=7. By theorem 5, we can define an association scheme with 3-classes on C whose eigenmatrix P is:

$$P = \begin{pmatrix} 1 & 506 & 1288 & 253 \\ 1 & 154 & -56 & -99 \\ 1 & 26 & -56 & 29 \\ 1 & -6 & 8 & 3 \end{pmatrix}$$

<u>remark</u>: We refer to the reader to exemple 6.1 in (1) where this eigenmatrix is constructed in a different way.

<u>example 2</u>:

In the same work (1) Delsarte gives an association schema, with two classes, on the orthogonal code at the ternary Golay code $G_3(11,6)$, where the corresponding eigenmatrix P is given by:

$$P= \begin{pmatrix} 1 & 132 & 110 \\ 1 & 24 & -25 \\ 1 & -3 & 2 \end{pmatrix}$$

Applying the inverse reasoning to example 1, we can obtain from theorem 5, since the ternary Golay code is perfect (rf.(5)), that is completely regular (rf.(3)); that the two non-zero weights of the ternary Golay code are $w_1=6$ and $w_2=9$. Those results are obtaineds from -30- and from the Krawtchouk polynomials $P_1(x)=22-3x$ and $P_2(x)=220-\frac{129}{2}x+\frac{9}{2}x^2$ (rf.(5)) (e.g. $B_{w_1}=132$; and $24=\frac{1}{\binom{11}{1}.2}.P_1(w_1).132$ in second column of P, then $w_1=6$).

In this way, our theorem 3 permits give the dual weight enumerator for the ternary Golay code and for its 243 cosets:

$$A_{G_3}(z) = \frac{1}{243}\left((1+2z)^{11}+132(1-z)^6(1+2z)^5+110(1-z)^9(1+2z)^2 \right)$$

For $w(\underline{u}_j)=1$; there are $\binom{11}{1}.2=22$ cosets with the same minimum weight, we have:

$$A_{G_3+\underline{u}_j}(z)=\frac{1}{243}\left((1+2z)^{11}+24(1-z)^6(1+2z)^5-25(1-z)^9(1+2z)^2 \right)$$

And for $w(\underline{u}_j)=2$; there are $\binom{11}{2}.2^2=220$ cosets with the same minimum weight, we have:

$$A_{G_3+\underline{u}_j}(z)=\frac{1}{243}\left((1+2z)^{11}-3(1-z)^6(1+2z)^5+2(1-z)^9(1+2z)^2 \right)$$

References:

(1) P. DELSARTE: An Algebraic Approach to the Association Schemes of Coding Theory.
These Doctorat, Université Catholique de Louvain, Belgium (1973)

(2) J.M. GOETHALS: Association Schemes
Lectures given at International Centre of Mechanical Sciences. Udine (1978)

(3) J.M. GOETHALS and H.C.A. Van TILBORG: Unifromly Packed Codes
Philips Res. Report, 30, (1975) R. 879

(4) LL. HUGUET: Códigos Regulares: Aspectos Combinatóricos y Aplicaciones al Wire-Tap Channel.
These Doctorat: Universitat Autonoma de Barcelona, Spain (1981)

(5) F.J. MACWILLIAMS and NJA. Sloane: The Theory of Error-Correcting Codes.
North-Holland Mathematical Library (1977).