Weight distribution of translates of linear codes and generalized Pless identities

Paul Camion, B. Courteau, G. Fournier, S.V. Kanetkar

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.: 954 90 20

Rapports de Recherche

N° 213

WEIGHT DISTRIBUTION OF TRANSLATES OF LINEAR CODES AND GENERALIZED PLESS IDENTITIES

Paul CAMION
Bernard COURTEAU
Gilles FOURNIER
S. V. KANETKAR

Mai 1983

WEIGHT DISTRIBUTION OF TRANSLATES OF LINEAR CODES AND GENERALIZED PLESS IDENTITIES

by

P. Camion[1], B. Courteau[2], G. Fournier[2],
S. V. Kanetkar[3]

---

(1) Institut national de recherche en informatique et en automatique, Domaine de Voluceau-Rocquencourt 78150 LeChesnay, France.

(2) Département de mathématiques et d'informatique, Université de Sherbrooke Québec, Canada, J1K 2R1. This research was supported in part by FCAC grants #EQ 1886 and by CRSNG grants #A 5120 and #

(3) Department of Electrical Engineering, Old Dominion University, Norfolk, VA 23508, U.S.A. This research was supported in part by CRSNG grant #A4402.

ABSTRACT

Using group algebra and Fourier transform, we introduce a combinatorial matrix of which a factorization into integer matrices is investigated. The combinatorial signification of that factorization is exhibited. This leads in particular to show the relation between the work of several authors and the fundamental results of Delsarte.

RESUME

A l'aide d'une algèbre de groupe et d'une transformation de Fourier, nous introduisons une matrice dont nous étudions une factorisation en matrices à coefficients entiers. L'interprétation combinatoire de cette factorisation est mise en évidence. Ceci permet en particulier d'établir un lien entre les travaux de plusieurs auteurs et les résultats fondamentaux de Delsarte.

1.- INTRODUCTION

The aim of this paper is to introduce a combinatorial approach to the distance matrix of Delsarte in the case of a linear code over any finite field F_q. This will be done by using systematically group algebra and Fourier transform. Considering the i-th convolution power of an element of a group algebra closely related to the code C, we naturally introduce the combinatorial matrix. The Fourier transform is then use to obtain some results about the orthogonal code and two linear recurrences for the rows of the combinatorial matrix.

In section 3 we established a relationship between the distance matrix B of Delsarte and the combinatorial matrix A first by using Fourier transform and a result of Delsarte about Krawtchouk polynomials and secondly by using generating functions. These two approach give identities which contain the Pless'ones. Furthermore, the relation $A = q^{-n}B(PV)$ introduces the matrix $S = q^{-n}PV$ where P is the Krawtchouk matrix and V is an infinite Vandermonde matrix. The combinatorial approach implies that S is upper triangular. This matrix defines a transform which may be usefull even in the non linear case.

Finally, solving a recurrence on the rows of the combinatorial matrix we obtain a formula to evaluate the distance matrix in terms of the possible initial data $[x_{0h} \ldots x_{s'h}]$ where s' is the number of non zero weights of the orthogonal code.

2. A COMBINATORIAL MATRIX

2.1 GENERALITIES

Let $\mathbb{F} = \mathbb{F}_q$ be the q elements field, where q is a power of a prime p. Set $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. We refer to [8] for the fundamental concepts of coding theory needed in this paper.

Let $\Omega = \{g_1, \ldots, g_n\} \subseteq \mathbb{F}^k$ be the set of columns of a parity check matrix of a linear e-error correcting $(n, n-k')$-code C with $e \geq 1$ and $k' = \text{rank } \Omega \leq k$. We shall denote this parity check matrix by the same letter Ω. The syndrom of $u \in \mathbb{F}^n$ with respect to C is then $s(u) = \Omega u$ and the orthogonal code $C^\perp$ (also called the projective code associated to Ω) of C is is $C^\perp = \{c(g) = g^T\Omega \mid g \in \mathbb{F}^k\}$ where g^T is the transposed of the column vector g:

$$c(g) = [g^T g_1, \ldots, g^T g_n] = [g \cdot g_1, \ldots, g \cdot g_n]$$

where $g.g_i$ is the usual dot product of g and g_i in $\mathbb{F}^k$.

2.2 GROUP ALGEBRA AND THE COMBINATORIAL MATRIX

If $G = \mathbb{F}^k$, the elements x of the group algebra $\mathbb{C}[G]$ of G over the complex numbers will be expressed in the polynomial notation

$$x = \sum_{g \in G} x_g X^g \quad \text{where} \quad x_g \in \mathbb{C}.$$

The multiplication in $\mathbb{C}[G]$ is the convolution

$$xy = \sum_{g \in G} \left(\sum_{h+\ell=g} x_h \, y_\ell \right) X^g$$

The i - th convolution power of x will be denoted

$$x^i = \sum_{h \in G} x_{ih} X^h = x \ldots x \quad (i \text{ times}).$$

Set $\tilde{\Omega} = \mathbb{F}^* \Omega$ and let $x = \sum_{g \in \tilde{\Omega}} X^g$ be the characteristic function of $\tilde{\Omega}$ as an element in the group algebra $\mathbb{C}[G]$. It is easy to see [4] that in this case

$$(1) \qquad x_{ih} = \text{card}\{(a_1, \ldots, a_i) \mid h = \sum_{m=1}^{i} a_m,\ a_m \in \tilde{\Omega}\}$$

for all $h \in \mathbb{F}^k$.

DEFINITION 2.2.1

The combinatorial matrix of $\mathbb{F}^k = G$ with respect to the subset Ω is the $(q^k \times \infty)$ matrix A whose rows and columns are numbered with G and $\mathbb{N}$ respectively, the (h, i)-entry being x_{ih}:

$$A = \left(x_{ih} \ ; \ h \in \mathbb{F}^k, \ i \in \mathbb{N} \right).$$

2.3 FOURIER TRANSFORM

To obtain connections between the combinatorial matrix A and the projective code associated to Ω we need the Fourier transform.

Let $f: \mathbb{F} \to \mathbb{F}_p$ be a fixed non zero linear form of $\mathbb{F}$ considered as a vector space over its prime field $\mathbb{F}_p$ and let ζ be a primitive p - th root of unity in $\mathbb{C}$. The Fourier transform [2]

$\hat{x} = F(x)$ of the element $x = \sum_{g\in G} x_g X^g \in \mathbb{C}[G]$ is

$$F(x) = \sum_{h\in G} \hat{x}_h X^h$$

where $\hat{x}_h = \sum_{g\in G} x_g \zeta^{f(h\cdot g)}$ is called the Fourier coefficient of x associated to h.

The following property is proved in [2] : F is a linear isomorphism of the group algebra $\mathbb{C}[G]$ onto the Hadamard algebra that is the vector space $\mathbb{C}[G]$ provided with the Hadamard product

$$x \times y = \sum_{g\in G} (x_g y_g) X^g.$$

Thus $F(xy) = F(x) \times F(y)$ and

$$F(x^i) = F(x) \times \ldots \times F(x) \quad (i \text{ times}) = F(x)^{[i]} .$$

Furthermore, we have an inversion formula

$$FF(x) = q^k \tilde{x}$$

where $\tilde{x} = \sum_{g\in G} x_{-g} X^g$ is the reciproqual of $x = \sum_{g\in G} x_g X^g$. Now let $x = \sum_{g\in\tilde{\Omega}} X^g$ be as above the characteristic function of $\tilde{\Omega} = \mathbb{F}^*\Omega$. The connection between de Fourier transform of x and the weights of the projective code associated to Ω is | 2,4 |

$$\hat{x}_h = n(q-1) - q\, w(c(h)) \tag{2}$$

where $w(c(h))$ is the Hamming weight of the codeword $c(h) = (h\cdot g)_{g\in\Omega} \in C^t$.

LEMMA 2.3.1

Let $K \subset \mathbb{F}^k$ be a subspace. Then

$$F\Big(\sum_{g\in K} X^g\Big) = (\text{card } K) \sum_{g\in K^\perp} X^g.$$

PROOF

If $y = \sum_{g\in K} X^g$, then $\hat{y}_h = \sum_{g\in K} \zeta^{f(g\cdot h)}$. If $h \in K^\perp$, then

$\hat{y}_h = \text{card } K$ and if $h \notin K^\perp$ then

$$\hat{y}_h = \sum_{j=0}^{p-1} \sum_{\substack{g\in K \\ f(g.h)=j}} \zeta^j = q^{k'-1} \sum_{j=0}^{p-1} \zeta^j = 0$$

because

$$\text{card}\{g \in K \mid f(g\cdot h) = j\} = q^{k'-1}$$

the equation $f(g.h)=j$ defining an affine hyperplane of K.

We shall now reformulate and extend some results of [4].

THEOREM 2.3.2

Let $\Omega \subset \mathbb{F}^k$ be the column set of a parity check matrix of an e-error correcting $(n, n-k')$-code C with $e \geq 1$ and $k' = \text{rank } \Omega$. Let $K = \{h \in \mathbb{F}^k \mid h\ \Omega = 0\}$. Then $C^\perp$ admits s' non zero weights implies that there exists integers $c_0, \ldots, c_{s'}, b$ with $c_{s'} \neq 0$, $b \neq 0$ such that for all $h \in K^\perp$

$$\sum_{i=0}^{s'} c_i x_{ih} = b. \tag{3}$$

PROOF

Let $w_1, \ldots, w_{s'}$ be the non zero weights of $C^{\perp}$ and by(2) $r_i = n(q-1)-qw_i$ $(i = 1, \ldots, s')$ be the corresponding Fourier coefficients of $x = \sum_{g\in\tilde{\Omega}} X^g$, $\tilde{\Omega} = \mathbb{F}^*\Omega$.

Taking the Fourier transform of the product

$$(x - r_1X^\circ) \ldots (x - r_{s'}X^\circ) \quad \text{we obtain}$$

$$F((x - r_1X^\circ)\ldots(x - r_{s'}X^\circ)) = F(x - r_1X^\circ)\times\ldots\times F(x - r_{s'}X^\circ)$$

$$= (F(x) - r_1F(X^\circ))\times\ldots\times (F(x) - r_{s'}F(X^\circ))$$

$$= \Big(\sum_{h\in G} (\hat{x}_h - r_1)X^h\Big)\times\ldots\times \Big(\sum_{h\in G} (\hat{x}_h - r_{s'})X^h\Big)$$

$$= \sum_{h\in G} \left[(\hat{x}_h - r_1) \ldots (\hat{x}_h - r_{s'})\right] X^h$$

$$= \sum_{h\in K} (n(q-1)-r_1) \ldots (n(q-1) - r_{s'})X^h$$

$$= \prod_{i=1}^{s'} (n(q-1) - r_i) \sum_{h\in K} X^h$$

$$= q^{s'} \prod_{i=1}^{s'} w_i \sum_{h\in K} X^h$$

Taking again the Fourier transform gives

$$q^k(x - r_1X^\circ)\ldots(x - r_{s'}X^\circ) = q^{s'} \prod_{i=1}^{s'} w_i \,(\text{card } K) \sum_{h\in K^\perp} X^h$$

by the lemma. Hence

(4) $$\sum_{i=0}^{s'} c_i x^i = b \sum_{h \in K^\perp} X^h$$

where c_i is the coefficient of Z^i in the polynomial

$$(z - r_1)\ldots(z-r_{s'}) \quad \text{and} \quad b = q^{s'-k'} \prod_{i=1}^{s'} W_i.$$

Finally

$$\sum_{i=0}^{s'} c_i \sum_{h \in G} x_{ih} X^h = b \sum_{h \in K^\perp} X^h$$

i.e. $$\sum_{h \in G} \left[\sum_{i=0}^{s'} c_i x_{ih} \right] X^h = b \sum_{h \in K^\perp} X^h$$

and the result follows.

REMARK 2.3.3

If $h \notin K^\perp$, then there does not exist any sequence $a_1, \ldots, a_i$ of elements from $\tilde{\Omega}$ summing up to h since $K^\perp$ is the vector space spanned by Ω. Hince if $h \notin k^\perp$, then $x_{ih} = 0$ for all $i \in \mathbb{N}$.

THEOREM 2.3.4

Let Ω and K as in the preceeding theorem. If there exists complex numbers $c_0, \ldots, c_t$, b not all zero such that for all $h \in K^\perp$

$$\sum_{i=0}^{t} c_i x_{ih} = b$$

then $C^\perp$ admits at most t non zero weights.

PROOF

We have

$$\sum_{i=0}^{t} c_i x^i = \sum_{h\in G}\left[\sum_{i=0}^{t} c_i\, x_{ih}\right] X^h$$

$$= \sum_{h\in K^\perp} b\, X^h + \sum_{h\notin K^\perp}\left(\sum_{i=0}^{t} c_i x_{ih}\right) X^h$$

$$= b \sum_{h\in K^\perp} X^h \qquad \text{by remark 2.3.3}$$

Taking the Fourier Transform, we obtain

$$\sum_{i=0}^{t} c_i\, F(x)^{[i]} = b \text{ card } K \sum_{h\in K} X^h \qquad \text{by Lemma 2.3.1}$$

i.e.
$$\sum_{h\in G}\left[\sum_{i=0}^{t} c_i\, \hat{x}_h^i\right] X^h = b\, q^{k-k'} \sum_{h\in K} X^h$$

Hence

$$\sum_{i=0}^{t} c_i\, \hat{x}_h^i = b\, q^{k-k'} \qquad \text{for all } h \in K$$

$$\sum_{i=0}^{t} c_i\, \hat{x}_h^i = 0 \qquad \text{for all } h \notin K.$$

Thus the numbers $\hat{x}_h = n(q-1) - w(c(h))$ being solutions to a degree t polynomial equation may take at most t values and this is the same for the weights $w(c(h))$ for $h \notin K$. Note that if $h \in K$, then $c(h) = 0$ and the corresponding weight is zero.

2.4 A LINEAR RECURRENCE FOR THE NUMBERS x_{ih}

THEOREM 2.4.1

$\Omega \subseteq \mathbb{F}^k$ being as in theorem 2.3.2, for all $h \in \mathbb{F}^k$ and $m \in \mathbb{N}$, we have

$$(5) \qquad \sum_{i=0}^{s'+1} d_i \; x_{i+m,h} = 0$$

where s' is the number of non zero weights of the projective code $C^{\perp}$ associated to Ω and the $d'_i s$ are such that

$$\sum_{i=0}^{s'+1} d_i z^i = (z - n(q-1))(z - r_1) \ldots (z - r_{s'})$$

with $r_j = n(q-1) - q\, w_j$ the Fourier coefficients of the characteristic function of $\tilde{\Omega} = \mathbb{F}^* \Omega$.

PROOF

If $0, w_1, \ldots, w_s$, are weights of $C^{\perp}$ and $n(q-1), r_1, \ldots, r_s$, are the corresponding Fourier coefficients of $x = \sum_{g \in \tilde{\Omega}} X^g$, then we have for all natural number m

$$x^m (x - n(q-1)X^{\circ})\,(x - r_1 X^{\circ}) \ldots (x - r_{s'} X^{\circ}) = 0$$

in the group algebra of $G = \mathbb{F}^k$. To see this take the Fourier transform of the left hand member as in the proof of Theorem 2.3.2 and observe that it is zero. The relation follows then from the fact that the Fourier transform is bijective.

Expanding the product, we obtain

$$\sum_{h\in G}\left[\sum_{i=0}^{s'+1} d_j \; x_{i+m,h}\right]X^h = 0$$

and the result follows.

The following lemma is easily verified.

LEMMA 2.4.2

Let

$$x = \sum_{g\in G} x_g \, X^g.$$

Then

$$x\left(\sum_{h\in G} X^h\right) = \left(\sum_{g\in G} x_g\right) \sum_{h\in G} X^h.$$

In the case where $x = \sum_{g\in \Omega} X^g$, we have

$$x^m \sum_{h\in G} X^h = (\text{card } \Omega)^m \sum_{g\in G} X^g = (n(q-1))^m \sum_{g\in G} X^g.$$

Applying this relation to equation (4) (multiplying in by x^n) in the particular case $K^\perp = G$ (that is rank Ω = k) we obtain the following non homogeneous linear recurrence of order s'

$$\sum_{i=0}^{s'} c_i \, x_{i+m,h} = (n(q-1))^m \, b \tag{6}$$

where the c_i are as in (4).

3. RELATIONS BETWEEN THE DISTANCE MATRIX AND THE COMBINATORIAL MATRIX

In [6] Delsarte consider the distance matrix of $\mathbb{F}^n$ with respect to C : $B = (B_{ui})$, $u \in \mathbb{F}^n$, $0 \le i \le n$ where

$$B_{ui} = B_i(u) = \text{card}\{c \in C \mid d(u, c) = i\}.$$

The u-th row $[B_0(u), B_1(u), \ldots, B_n(u)]$ of B is then the weights distribution of the coset $C + u$. Note that in the linear case the coset $C + u = s^{-1}(h) = C_h$ where $h = s(u) = \Omega u \in \mathbb{F}^k$ is the syndrom of u and that $B_i(v) = B_i(u)$ for all $v \in C + u$. Denoting $B_i(h)$ the common value $B_i(v)$ for $v \in C + u = C_h$ i.e. for the v's having the same syndrom h, we may consider the $q^k \times n$ restricted distance matrix $B = (B_i(h))$ $h \in \mathbb{F}^k$, $0 \le i \le n$. We note with the same symbol B this restricted distance matrix . Recal that the combinatorial matrix of F^k with respect to $\Omega \subseteq F^k$ is the matrix $A = (A_{hi})$, $h \in F^k$ $0 \le i$ where

$$A_{hi} = x_{ih} = \text{card}\{(a_1, \ldots, a_i) \mid h = \sum_{\ell=1}^{i} a_\ell,\ a_\ell \in \tilde{\Omega}\} \text{ with } \tilde{\Omega} = \mathbb{F}^* \Omega .$$

A relationship between submatrices of A and B has been obtained in [5] by elementary combinatorial argument. The following two theorems give a connection between the matrices A and B or the numbers x_{ih} and $B_i(h)$ from which we may deduce, in particular, the Pless identities.

THEOREM 3.1

Let Ω be the columns of a parity check matrix of the $(n, n-k)$ linear e-error-conecting code C over the field $\mathbb{F}_q$ with $e \ge 1$. If A is the combinatorial matrix associated to Ω and B is the restricted

distance matrix, then

$$A = q^{-n} B\, PV \tag{7}$$

where P is the Krawtchouk matrix [6] and $V = (V_{\ell i})$, $V_{\ell i} = (n(q-1)-q\ell)^i$ is an infinite Vandermonde matrix.

PROOF

We have to prove the formula

$$x_{ih} = q^{-n} \sum_{0\le\ell\le n} \left[\sum_{0\le j\le n} B_j(h)\, P_\ell(j) \right] (n(q-1)-q\ell)^i \tag{8}$$

for all $h \in \mathbb{F}^k$ and $i \ge 0$.

a) Consider in the group algebra of $G = \mathbb{F}^k$ the characteristic function

$$x = \sum_{g\in\widetilde{\Omega}} X^g \quad \text{of} \quad \widetilde{\Omega} = \mathbb{F}^*\Omega \quad \text{and} \quad x^i = \sum_{h\in G} x_{ih} X^h$$

it's i-th convolution power.

Taking the Fourier transform of x^i twice we obtain by the inversion formula [2.4]

$$F(F(x^i)) = q^k x^i = \sum_{h\in G} q^k x_{ih} X^h. \tag{9}$$

On the other hand, we have by the fact that the Fourier transform gives an isomorphism of the group algebra of G onto its Hadamard algebra,

$$F(x^i) = \hat{x}^{[i]} = \hat{x} \times \ldots \times \hat{x} \quad (i \text{ Hadamard factors})$$

$$= \sum_{h\in G} \hat{x}_h^i X^h.$$

Then by definition

$$(10) \qquad F(F(x^i)) = \sum_{h\in G} \left(\sum_{g\in G} \hat{x}_g^i \cdot \zeta^{f(g\cdot h)} \right) X^h$$

But by (2) $\hat{x}_g = n(q-1) - q\, w(c(g))$, whence by (9) and (10)

$$(11) \qquad q^k x_{ih} = \sum_{0\le \ell \le n} (n(q-1)-q\,\ell)^i \sum_{w(c(g))=\ell} \zeta^{f(g\cdot h)}$$

b) Let us show finally that

$$(12) \qquad \sigma(h) = \sum_{w(c(g))=\ell} \zeta^{f(g\cdot h)} = q^{k-n} \sum_{0\le j\le n} B_j(h)\, P_\ell(j)$$

We shall use theorem 2.4 of Delsarte [6] which says in our notations that if $a \in \mathbb{F}^n$ is such that $w(a) = j$, then

$$\sum_{b\in Y_\ell} \zeta^{f(a\cdot b)} = P_\ell(j)$$

where

$$Y_\ell = \{b \in \mathbb{F}^n \mid w(b) = \ell\}$$

and $P_\ell(x)$ is the Krawtchouk polynomial of degree ℓ.

Using matricial notation, we may write

$$c(g) = g^T\Omega \quad \text{and} \quad g\cdot h = g^T h = g^T\Omega u = (g^T\Omega)u = v\cdot u$$

where $v = g^T\Omega \in C^\perp$ and $u \in C_h$ (i.e. $\Omega u = h$). Then

$$\sigma(h) = \sum_{w(c(g))=\ell} \zeta^{f(g\cdot h)} = \sum_{v\in C^\perp \cap Y_\ell} \zeta^{f(v\cdot u)}$$

with $\Omega u = h$. Noting that this sum is independant of u in C_h, we have

$$\sigma(h) = q^{k-n} \sum_{u \in C_h} \sum_{v \in C^{\perp} \cup Y} \zeta^{f(v \cdot u)}$$

But

$$\sum_{u \in C_h} \sum_{\substack{v \notin C^{\perp} \\ v \in Y_\ell}} \zeta^{f(v \cdot u)} = \sum_{\substack{v \notin C^{\perp} \\ v \in Y_\ell}} \sum_{c \in C} \zeta^{f(v \cdot (u_0 + c))} \quad \text{for any } u_0 \in C_h$$

$$= \sum_{\substack{v \notin C^{\perp} \\ v \in Y_\ell}} \zeta^{f(v \cdot u_0)} \sum_{c \in C} \zeta^{f(v \cdot c)} = 0$$

because

$$\sum_{c \in C} \zeta^{f(v \cdot c)} = \sum_{i=0}^{p-1} \sum_{\substack{f(v \cdot c) = i \\ c \in C}} \zeta^i = p^{k-1} \sum_{i=0}^{p-1} \zeta^i = 0$$

since $\{c \mid f(v \cdot c) = i\}$ is an affine hyperplane of C and ζ is a primitive p-th root of unity.

Hence

$$\sigma(h) = q^{k-n} \sum_{u \in C_h} \sum_{v \in Y_\ell} \zeta^{f(v \cdot u)}$$

$$= q^{k-n} \sum_{0 \le j \le n} \sum_{\substack{w(u) = j \\ u \in C_h}} P_\ell(j) \quad \text{by Delsarte theorem 2.4}$$

$$= q^{k-n} \sum_{0 \le j \le n} B_j(u) \, P_\ell(j).$$

REMARK 3.2

If $\Omega^{(\ell)} = \{g \in \mathbb{F}^k | w(c(g)) = \ell\}$ and $x^{(\ell)} = \sum_{g \in \Omega^{(\ell)}} X^g$ is the characteristic function of $\Omega^{(\ell)}$ in the group algebra of $G = \mathbb{F}^k$, then by (12) $\sigma(h)$ is the Fourier coefficient $\hat{x}_h^{(\ell)}$ of $x^{(\ell)}$. By (2) the weights $w_h^{(\ell)}$ of the projective code $C^{(\ell)} = C(\Omega^{(\ell)*})$ defined by $\Omega^{(\ell)}$ are then given by the formula.

$$(13) \qquad w_h^{(\ell)} = q^{-1}\left[A'_\ell - q^{k-n} \sum_{0 \le j \le n} B_j(h)\, P_\ell(j)\right] \qquad h \in \mathbb{F}^k$$

where $[A'_0, A'_1, \ldots, A'_n]$ is the weights distribution of the code $C^\perp = C(\Omega)$.

COROLLARY

If $A'_\ell = 0$, then $B'_\ell(h) = 0 \quad \forall\, h \in \mathbb{F}^k$.

The following theorem gives the exponential generating function of the numbers x_{ih} in terms of the numbers $B_j(h)$.

THEOREM 3.3

$$\sum_{i \ge 0} x_{ih} \frac{t^i}{i!} = q^{-n} \sum_{0 \le j \le n} B_j(h)\left[e^{(q-1)t} - e^{-t}\right]^j \left[e^{(q-1)t} + (q-1)e^{-t}\right]^{n-j}$$

PROOF

Remark first that

$$B_j(h) = \text{card}\{u \in \mathbb{F}^n | \Omega u = h \text{ and } w(u) = j\}$$

is the number of linear combinations of j elements of Ω which are equal to h.

Let $(a_1, \ldots, a_i)$ be a sequence of elements of $\tilde{\Omega} = \mathbb{F}^*\Omega$ such that $a_1 + \ldots + a_i = h$. The number of such sequences is by definition x_{ih}. Define the core of the sequence $(a_1, \ldots, a_i)$ to be the unique linear combination u of elements of Ω obtained by collecting the elements of the sequence by parallel bunches and expressing these in term of the corresponding unique element of Ω.

Consider now a fixed linear combination u of elements of Ω which is equal to h and such that $w(u) = j$. To form a sequence of elements of $\tilde{\Omega}$ whose sum is h and whose core is u, we may replace each of the j terms "a" appearing in the linear combination u by parallel elements in $\tilde{\Omega}$ that is $\alpha_1 a, \ldots, \alpha_m a$ such that $\sum_{i=1}^{m} \alpha_i = 1$, each of the $n-j$ elements b of Ω not appearing in u by parallel elements in $\tilde{\Omega}$ that is $\beta_1 b, \ldots, \beta_r b$ such that $\sum_{i=1}^{r} \beta_i = 0$ and finally permute all these elements.

This may be expressed more conveniently by using generating functions [3]. If

$$A(t) = \sum_{m\geq 0} A_m \frac{t^m}{m!}, \quad B(t) = \sum_{m\geq 0} B_m \frac{t^m}{m!}, \quad C^u(t) = \sum_{m\geq 0} C^u_m \frac{t^m}{m!}$$

are the exponential generating functions of the numbers

$$A_m = \text{card}\{(\alpha_1, \ldots, \alpha_m) \mid \alpha_i \in \mathbb{F}^* \text{ and } \sum_{i=1}^{m} \alpha_i = 1\}$$

$$B_m = \text{card}\{(\beta_1, \ldots, \beta_m) \mid \beta_i \in \mathbb{F}^* \text{ and } \sum_{i=1}^{m} \beta_i = 0\}$$

$$C^u_m = \text{card}\{(a_1, \ldots, a_m) \mid a_i \in \tilde{\Omega}, \sum_{i=1}^{m} a_i = h, \text{ core } (a_1, \ldots, a_m) = u\}$$

then we have $C^u(t) = (A(t))^j \, (B(t))^{n-j}$. Hence

$$(14) \qquad \sum_{i\geq 0} x_{ih} \frac{t^i}{i!} = \sum_{0\leq j\leq n} B_j(h)(A(t))^j(B(t))^{n-j}$$

It remains to determine the functions $A(t)$ and $B(t)$. Remark that

$$B_m = (q-1)\, A_{m-1}$$

$$A_{m+1} = (q-2)A_m + B_m$$

so that A_m satisfies the difference equation

$$A_{m+2} - (q-2)A_{m+1} - (q-1)A_m = 0$$

with the initial conditions $A_0 = 0$, $A_1 = 1$. In terms of generating functions this gives the differential equation

$$A''(t) - (q-2)A'(t) - (q-1)A(t) = 0$$

with the initial condition $A(0) = 0$, $A'(0) = 1$. The solution of this problem is

$$A(t) = \frac{e^{(q-1)t} - e^{-t}}{q}$$

on the other hand $B_m = (q-1)A_m$ gives

$$B'(t) = (q-1)A(t)$$

and thus

$$B(t) = \frac{e^{(q-1)t} + (q-1)e^{-t}}{q}$$

since $B(0) = B_0 = 1$.

COROLLARY 3.4

If

$$\alpha^{n}_{qji} = \frac{d^i}{dt^i}\left(\frac{e^{(q-1)t}-e^{-t}}{q}\right)^j \left(\frac{e^{(q-1)t}+(q-1)e^{-t}}{q}\right)^{n-j}\Bigg|_{t=0}$$

then

$$x_{ih} = \sum_{0\le j\le n} B_j(h)\ \alpha^{n}_{qji} \qquad i \ge 0,\ h \in \mathbb{F}^k.$$

REMARK 3.5

By the proof of the theorem 3.3 the number α^{n}_{qji} is the cardinality of i-sequences of elements of $\tilde{\Omega}$ whose sum is h constructed from a given j non zero term linear combination of elements of Ω which is equal to h. Hence $\alpha^{n}_{qji} = 0$ for all $j > i$. This fact may also be verified analytically. Furthermore, we have $\alpha^{n}_{qii} = i!$ The formula (14) then gives

$$B_i(h) = \frac{1}{i!}\left[\sum_{j=0}^{i-1} B_j(h)\ \alpha^{n}_{qji} - x_{ih}\right]$$

which is to be compared to the formulas obtained by Karpovsky [7].

REMARK 3.6

Using the generating function of the Krawtchouk polynomials in the form [6]

$$(15) \qquad (X - Y)^j(X + (q-1)Y)^{n-j} = \sum_{0\le \ell\le n} P_{\ell}(j)X^{n-\ell}\,Y^{\ell}$$

we can easily verify the formula (7) given in theorem 3.1. Thus we obtain the relation $\alpha^{n}_{qji} = q^{-n} \sum_{0\le \ell\le n} P_{\ell}(j)(n(q-1) - q\ell)^i$ and by the preceeding remark,

$$S = (\alpha^n_{qji}) = q^{-n}\, PV$$

is a $(k \times \infty)$ upper triangular matrix.

We may express the above in the following manner to obtain some identities of Pless type, putting (8) with 3.4.

THEOREM 3.7

If $[B_0(h), \ldots, B_n(h)]$ is the weight distribution of the coset C_h of the linear e-error-correcting (n,k)-code C over $\mathbb{F}_q$, with $e \geq 1$ then

$$\sum_{0\leq \ell \leq n} B'_\ell(h)(n(q-1)-q\ell)^i = q^n \sum_{0\leq \ell \leq n} B_\ell(h)\ \alpha^n_{q\ell i}$$

where

$$\left[B'_\ell(h) = \sum_{0\leq j\leq n} B_j(h)\ P_\ell(j)\right]_{0\leq \ell \leq n}$$

is the MacWilliam transform (see [6]) of $[B_\ell(h)]_{0\leq \ell\leq n}$ and $\alpha^n_{q\ell i}$ is as in 3.4.

REMARK 3.8

In the particular case $q = 2$ and $h = 0$ we obtain the power moments of the weight distribution of $C^\perp$ about the mean [8 , p. 132 eq(24)] , 9] Here

$$\alpha^n_{2ji} = \frac{d^i}{dt^i}\ (\sinh^j(t)\ \cosh^{n-j}(t))\Big|_{t=0}.$$

REMARK 3.9

Assmus and Mattson in [1] give the following relation

$$(q-1) \sum_{0\le i\le n} B_i(h) Z^i = q^{k-n} \sum_{0\le i\le n} (qb_i - A_i') (1 + (q-1)Z)^{n-i} (1 - Z)^i$$

where $B(h) = [B_0(h), \ldots, B_n(h)]$ is the weight distribution of the translate $C_h = C + u$ of u, $[A_0', \ldots, A_n']$ is the weight distribution of $C^\perp$ and b_i is the number of i-weight elements of $C^\perp$ that are orthogonal to u.

This result yields in fact a combinatorial interpretation of the MacWilliams transform $B'(h)$ of $B(h)$. Putting $Z = \frac{Y}{X}$ and introducing Krawtchouk polynomials using (15), we obtain

$$(q-1) B_\ell(h) = q^{k-n} \sum_{0\le i\le n} (q b_i - A_i') P_\ell(i)$$

and by the MacWilliams transform

$$B_j'(h) = q^k (q-1)^{-1} (q b_j - A_j')$$

The formula (13) then gives

$$W_h^{(\ell)} = q^{-1} [(1+q^{2k-n} (q-1)^{-1}) A_\ell' - q^{2k-n+1} (q-1) b_\ell]$$

which is a relation between some parameters associated with the set of projective points Ω.

4. Weight distribution of translates of the orthogonal of a two-weights code

Let $\Omega \subseteq \mathbb{F}^k$ be as in theorem 2.3.2 the column set of a parity check matrix of a $(n, n-k')$-code C whose orthogonal $C^\perp$ admits $s' = 2$ non zero weights w_1 and w_2.

To determine $B(h) = [B_0(h), \ldots, B_n(h)]$ we have to solve the linear recurrence (5)

$$d_0 x_{ih} + d_1 x_{i+1,h} + d_2 x_{i+2,h} + d_3 x_{i+3,h} = 0 \tag{16}$$

for the possible initial data $[x_{0h}, x_{1h}, x_{2h}]$, $h \in \mathbb{F}^k$ and then to solve the triangular linear system (14) to obtain

$$B_i(h) = \frac{1}{i!}\left[\sum_{j=0}^{i-1} B_j(h)\, \alpha^n_{qji} - x_{ih}\right] \quad \text{for} \quad i = 0, \ldots, n.$$

Here the possible initial data are

$$[1 \quad 0 \quad n(q-1)] \qquad \text{for} \quad h = 0$$

$$[0 \quad 1 \quad \lambda_1] \qquad \text{for} \quad h \in \tilde{\Omega} = \mathbb{F}^*\Omega$$

$$[0 \quad 0 \quad \lambda_2] \qquad \text{for} \quad h \notin \Omega \quad h \neq 0$$

where by (2) and (4)

$$\lambda_1 = q^{2-k'} w_1 w_2 + 2n(q-1) - q(w_1+w_2) = x_{2h} \quad \text{for} \quad h \in \tilde{\Omega}$$

$$\lambda_2 = q^{2-k'} w_1 w_2 = x_{2h} \qquad \text{for} \quad h \notin \tilde{\Omega},\ h \neq 0.$$

(in this case $\tilde{\Omega}$ is called a partial difference set with the two parameters λ_1 and λ_2, the case $\lambda_1 = \lambda_2$ being the classical (Mann) difference set).

The solution of the recurrence (16) is

$$x_{ih} = a_0(h)\ \tilde{n}^i + a_1(h) r_1^i + a_2(h) r_2^i \qquad \forall\ i \geq 0$$

where $\tilde{n} = n(q-1)$ and the coefficients $a_j(h)$ depends of the initial data. In fact,

$$\begin{bmatrix} a_0(h) \\ a_1(h) \\ a_2(h) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \tilde{n} & r_1 & r_2 \\ \tilde{n}^2 & r_1^2 & r_2^2 \end{bmatrix}^{-1} \begin{bmatrix} x_{0h} \\ x_{1h} \\ x_{2h} \end{bmatrix}$$

The numbers $B_i(h)$ may then be calculated by (14) in terms of the initial data $[x_{0h}\ \ x_{1h}\ \ x_{2h}]$.

REMARK 4.1

In general, the recurrence (5) has the solution

$$x_{ih} = \sum_{j=0}^{s'} a_j(h) r_j^i$$

where $r_0 = \tilde{n} = n(q-1)$ and

$$\begin{bmatrix} a_0(h) \\ \cdot \\ \cdot \\ \cdot \\ a_{s'}(h) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ r_0 & \cdots & r_{s'} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ r_0^{s'} & & r_{s'}^{s'} \end{bmatrix}^{-1} \begin{bmatrix} x_{0h} \\ \cdot \\ \cdot \\ \cdot \\ x_{s'h} \end{bmatrix}$$

Hence

$$B_i(h) = \frac{1}{i!} \left[\sum_{j=0}^{i-1} B_j(h)\ \alpha_{qji}^n - \sum_{j=0}^{s'} a_j(h) r_j^i \right]$$

REFERENCES

1.- E.F. Assmus, Jr., H.F. Mattson, Jr., The Weight-Distribution of a Coset of a Linear Code, IEEE Trans. Inform. Theory, p. 497, 1978.

2.- P. Camion, Difference Sets in Elementary Abelian Groups, Les Presses de l'Université de Montréal, Montréal, 1979.

3.- L. Comtet, Advanced Combinatorics, D. Reidel Publishing Co., 1974.

4.- B. Courteau, G. Fournier, R. Fournier, A Characterization of N-Weight Projective Codes, IEEE Trans. Inform. Theory, vol. IT-27, 808-812, 1981.

5.- B. Courteau, G. Fournier, R. Fournier, Etude de certains paramètres associés à un code linéaire, Annals of Discrete Math., Combinatoire 81, to appear.

6.- P. Delsarte, Four Fundamental Parameters of a Code and their combinatorial Significance, Inform. and Control, vol. 23, 407-438, 1973.

7.- M. Karpovsky, Weight Distribution of Translates, covering Radius, and Perfect Codes Correcting Errors of Given Weights, IEEE Trans. Inform. Theory, vol. IT-27, 462-472, 1981.

8.- F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes. North-Holland 1977.

9.- V. Pless, Power moment identities on weight distributions in error correcting codes, Inform. Contr., vol. 6, 147-152, 1963.

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