© DISCRETE MATHEMATICS 3 (1972) 47–64. North-Holland Publishing Company

WEIGHTS OF LINEAR CODES AND STRONGLY REGULAR NORMED SPACES

Ph. DELSARTE

MBLE Research Laboratory, Avenue Van Becelaere 2, B 1170, Brussels, Belgium

Received 6 November 1971

Abstract. Starting from a theorem on the distance matrix of a projective linear code, one introduces an axiomatic definition of a strongly regular normed space. It is then shown that every such normed space admits a representation by means of a projective code. As a particular case, this yields a one-to-one correspondence between two-weight projective codes over prime fields and some strongly regular graphs.

§ 1. Introduction

The Hamming distance plays an important role in the study of linear codes, both for practical reasons, when codes are used for detecting or correcting errors on a noisy channel, and for more theoretical reasons. For instance, as shown by MacWilliams [9], two linear codes are equivalent under generalized permutation on their coordinates, if and only if they are isomorphic as normed spaces, when the Hamming weight is taken as the norm.

In this paper, we define the distance matrix of a code to be the matrix whose (i, j) entry is the Hamming distance between the i^{th} and the j^{th} code vectors. For some linear codes, called projective codes, it turns out that this matrix satisfies remarkable equations, very similar to those satisfied by the adjacency matrix of a strongly regular graph (cf. for instance Seidel [15]). Taking these properties as axioms, we introduce the concept of a strongly regular normed space, and we show that every such normed space is isomorphic to some projective code (when the Hamming weight is taken as the norm).

Some classes of two-weight cyclic codes have been discovered by McEliece [12] and Delsarte and Goethals [6]. However, no systematic investigation of such codes has yet been made. In §§3 and 5 of the present paper, we establish a one-to-one correspondence between two-weight projective codes over prime fields and a large class of strongly regular graphs; some results on that subject will appear in a forthcoming paper. In fact, our derivation of strongly regular graphs from two-weight codes is similar, especially in the binary case, to a method introduced by Goethals and Seidel [8] for quasi-symmetric designs.

The following notations are used throughout the text: the transpose of a matrix A is denoted by A^{T}; the matrices I_n and J_n are the unit matrix and the all-one square matrix of order n, respectively. The additive group of a linear space V is denoted by $(V, +)$. The notations for group characters are the same as in the author's recent paper on Abelian codes [5].

§2. Hamming metric of linear codes

We first introduce some definitions. Let $F = \mathrm{GF}(q)$ be the Galois field of q elements, where q is a prime power, and let F^n denote the n-dimensional linear space of all n-tuples over F. For a vector

$$a = (a^{(1)}, a^{(2)}, ..., a^{(n)}), \quad a^{(i)} \in F\,,$$

of F^n, and for an element λ in F, we define $N(\lambda, a)$ as the number of coordinates $a^{(i)}$, $1 \leq i \leq n$, being equal to λ. As usual, the number of nonzero coordinates

$$w_{\mathrm{H}}(a) = \sum_{\lambda \neq 0} N(\lambda, a) \tag{1}$$

is called the *Hamming weight* of a. This function w_{H} has the classical properties of a norm. For future use, we now recall them:

Let V be a linear space over F, and let w be a mapping from V into R^+, the set of nonnegative real numbers. Then w is called a norm if it satisfies the three following conditions:

(A1) $(w(a) = 0) \Longleftrightarrow (a = 0), \ \forall a \in V$,
(A2) $w(a + b) \leq w(a) + w(b), \ \forall a, b \in V$,
(A3) $w(\lambda a) = w(a), \ \forall a \in V, \ \lambda \in F, \ \lambda \neq 0$.

If k is a positive integer not exceeding n, we define an (n, k) *linear code over F* to be a k-dimensional subspace of F^n. The linear code C will be called a *projective code* if any two of its coordinates are linearly independent or, equivalently, if the minimum weight of the dual code of C is at least equal to three. A generator matrix for such a code is a $k \times n$ matrix, of rank k, whose columns correspond to n distinct projective points in PG$(k-1, q)$. Hence $k \leq n \leq (q^k - 1)/(q - 1)$ for any (n, k) projective code.

The *distance matrix* of a code C is the symmetric matrix D, of order $v = q^k$, given by

$$D = [d_{\mathrm{H}}(a, b); a, b \in C] ,$$

where $d_{\mathrm{H}}(a, b) = w_{\mathrm{H}}(a - b)$ is the Hamming distance between the code vectors a and b.

Theorem 1. *The distance matrix of any (n, k) projective code over $F = \mathrm{GF}(q)$ satisfies*

(2) $$DJ_v = mq^{k-1}J_v ,$$

(3) $$D^2 + q^{k-1}D = m(m+1)q^{k-2}J_v$$

with $v = q^k$, $m = n(q-1)$.

Proof. Let A be the $v \times n$ matrix over F whose rows are the vectors of a given (n, k) projective code C, and let B denote the $v \times m$ matrix

(4) $$B = [A, \omega A, \omega^2 A, \ldots, \omega^{q-2} A] ,$$

where ω is a primitive root in F.

For $q = p^e$, p prime, $e \geq 1$, we define ϕ to be a homomorphic mapping from $(F, +)$, the additive group of F, onto the group of complex p^{th} roots of unity, so that ϕ is a nonprincipal character of $(F, +)$. It is well known that one has

$$(5) \qquad \sum_{\alpha\in F} \phi(\alpha\lambda) = \begin{cases} q, \text{ if } \lambda = 0\,, \\ 0, \text{ if } \lambda \neq 0\,, \end{cases}$$

for any λ in F.

We first show that the column vectors of the matrix $\phi(B)$ are orthogonal to each other, and to the all-one vector, over the field of complex numbers, i.e.,

$$(6) \qquad \phi(-B^{\mathrm{T}})\,\phi(B) = v\,I_v\,,$$

$$(7) \qquad \phi(-B^{\mathrm{T}})\,J_v = 0\,,$$

where $\phi(X)$ is the matrix whose entries are the ϕ-images of the corresponding entries of X. Indeed, for $1 \leq i, j \leq m$, the (i, j) entry $g_{i,j}$ of the first member of (6) is equal to

$$g_{i,j} = \phi(b_{1,j} - b_{1,i}) + \phi(b_{2,j} - b_{2,i}) + \ldots + \phi(b_{v,j} - b_{v,i})\,,$$

where $b_{r,s}$ is the (r, s) entry of B. Since C is assumed to be a projective code, the columns of B are not zero, and are distinct from each other. On the other hand, the rows of B form a linear space over F. Hence, for fixed indices i and j, $i \neq j$, it is easily seen that each element of F appears v/q times among the differences $b_{r,j} - b_{r,i}$, $1 \leq r \leq v$. Eq. (6) then follows from the property (5) of ϕ. The proof of (7) is very similar.

Next, we show that the distance matrix D of the code C is given by

$$(8) \qquad \phi(B)\,\phi(-B^{\mathrm{T}}) = m\,J_v - q\,D\,.$$

Indeed, according to (4) and the definition of $N(\lambda; a)$, one has the following expression for the (i, j) entry $h_{i,j}$ of the first member of (8):

$$h_{i,j} = \sum_{\lambda\in F} N(\lambda, a_i - a_j)\,(\phi(\lambda) + \phi(\omega\lambda) + \ldots + \phi(\omega^{q-2}\lambda))\,,$$

where a_i is the i^{th} row of A, i.e., the i^{th} code vector of C. From (1) and (5), with $N(0, a) = n - w_{\mathrm{H}}(a)$, one readily obtains

$$h_{i,j} = n(q-1) - q\, w_H(a_i - a_j)\,,$$

which is equivalent to (8), with $m = n(q-1)$.

Finally, the desired formulas (2) and (3) follow from (6), (7) and (8), by straightforward matrix calculation.

A code C for which the Hamming weight $w_H(a)$ takes $s + 1$ distinct values, namely $w_0 = 0, w_1, w_2, \ldots, w_s$, is called an *s-weight code*, and $w_1, w_2, \ldots, w_s$ are called the weights of C. Let N_i be the number of code vectors of weight w_i in C; the following result is an immediate consequence of Theorem 1.

Corollary 1. (Assmus and Mattson [1], MacWilliams [10], Pless [13]). *The weight distribution of an s-weight (n, k) projective code satisfies*

$$\sum_{i=1}^{s} N_i w_i = m q^{k-1}\,,$$

$$\sum_{i=1}^{s} N_i w_i^2 = m(m+1) q^{k-2}\,.$$

Proof. Use (2) and the equality between the diagonal elements in both members of (3).

Let us denote by $\mathrm{ML}(k, q)$ any $((q^k - 1)/(q-1), k)$ projective code over F. It can be shown that $\mathrm{ML}(k, q)$ is equivalent to the so called maximal length FSR code (cf. Berlekamp [2]). In fact, as shown by MacWilliams [9], $\mathrm{ML}(k, q)$ can be defined, up to equivalence, as the unique 1-weight projective code of dimension k over F, the weight being $w_1 = q^{k-1}$.

For a subfield $F' = \mathrm{GF}(q')$ of F, with $q = q'^t$, let γ be an isomorphic mapping from the field F onto a code $\mathrm{ML}(t, q')$, both considered as t-dimensional spaces over F'. Then, if C is an (n, k) linear code over F, let $C' = \gamma(C)$ be the γ-image of C, i.e., the set of vectors

$$(\gamma(a^{(1)}), \gamma(a^{(2)}), \ldots, \gamma(a^{(n)}))\,,$$

where a is a code vector of C. It is easily seen that C' is an (n', k') linear code over F', with $n'(q' - 1) = n(q - 1)$, $k' = kt$. Moreover, the weights w_i' of C' are given by

$$w_i' = w_i q/q' , \qquad i = 1, 2, ..., s ,$$

when $w_1, w_2, ..., w_s$ are the weights of C. It can also be shown that C' is a projective code over F' whenever C is a projective code over F. In agreement with this, the reader could verify that the distance matrix $D' = qD/q'$ of C' satisfies (2) and (3), where q and k are replaced by q' and k', respectively, whenever D itself satisfies (2) and (3).

§3. Graphs derived from two-weight codes

First, we recall a definition due to Seidel [15] for the strongly regular graphs introduced by Bose [4]. The adjacency matrix of an undirected graph on v vertices (without loops and multiple edges) is the square matrix A, of order v, whose elements are $a_{i,i} = 0$, and $a_{i,j} = a_{j,i} = -1$ or $+1$, for $i \neq j$, according as the i^{th} and j^{th} vertices are adjacent or not. The graph is called *strongly regular* if its adjacency matrix satisfies the two following equations:

$$(9) \qquad AJ_v = \rho_0 J_v ,$$

$$(10) \qquad (A - \rho_1 I_v)(A - \rho_2 I_v) = (v - 1 + \rho_1 \rho_2) J_v ,$$

where ρ_0 is an integer, $1 - v < \rho_0 < v - 1$, and ρ_1, ρ_2 are some real numbers. It has been proved (cf. Seidel [15]) that, except for graphs with $\rho_0 = 0$, $\rho_1 = -\rho_2 = \pm v^{1/2}$, the eigenvalues ρ_1 and ρ_2 of A are odd integers of different signs. As usual, we assume $\rho_2 < 0 < \rho_1$.

Let C be a 2-weight linear code of dimension k over F, and let w_1, w_2 be the weights of C, with $w_1 < w_2$. To C we associate a graph $\Gamma(C)$, on $v = q^k$ vertices, as follows. The vertices of the graph are identified with the code vectors, and two vertices are taken as adjacent or not, according to the Hamming distance between the corresponding vectors being w_1 or w_2. The adjacency matrix A of $\Gamma(C)$ is clearly given by

(11) $$(w_2 - w_1)A = 2D - (w_1 + w_2)(J_v - I_v)\,,$$

where D is the distance matrix of the code C.

Theorem 2. *Let C be a 2-weight (n, k) projective code over F. Then the associated graph $\Gamma(C)$, on v vertices, is strongly regular; the eigenvalues ρ_i of its adjacency matrix are given by*

(12) $$(w_2 - w_1)\rho_0 = 2mv/q - (w_1 + w_2)(v - 1)\,,$$

(13) $$(w_2 - w_1)\rho_i = w_1 + w_2 - (1 + (-1)^i)v/q\,, \qquad i = 1, 2,$$

with $v = q^k$, $m = n(q - 1)$.

Proof. With the above values of ρ_0, ρ_1, ρ_2, equations (2) and (3) are transformed into (9) and (10), when A is defined by (11). This is easiest verified by identification of the corresponding eigenvalues in both members of (11). Hence Theorem 2 is a consequence of Theorem 1.

Corollary 2. *Let C be a 2-weight projective code over $F = \mathrm{GF}(p^e)$, p prime. Then the weights of C are of the form*

(14) $$w_1 = up^t\,, \qquad w_2 = (u + 1)p^t\,,$$

for suitable integers u and t, $u \geq 1$, $t \geq 0$.

Proof. From (13), with $q = p^e$, we get $(w_2 - w_1)(\rho_1 - \rho_2) = 2q^{k-1}$, where the ρ_i are the eigenvalues of the adjacency matrix of $\Gamma(C)$. Since $\frac{1}{2}(\rho_1 - \rho_2)$ is an integer, $w_2 - w_1$ has to be a power of p. Hence (14) follows from (13) with $u = \frac{1}{2}(\rho_1 - 1)$.

Example 1. Let n be an integer, $2 \leq n \leq q - 1$, and let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be n distinct nonzero elements of F. We take the matrix

$$K = \begin{bmatrix} 1 & 1 & & 1 \\ & & & \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{bmatrix}$$

as a generator matrix for an $(n, 2)$ code C over F. Obviously, C is a 2-weight projective code, with $w_1 = n - 1$, $w_2 = n$. Using Theorem 2, we get the following values for the parameters of the associated strongly regular graph $\Gamma(C)$ on $v = q^2$ vertices:

$$\rho_0 = (q-1)(q+1-2n), \ \rho_1 = 2n-1, \ \rho_2 = 2(n-q)-1 .$$

In fact, $\Gamma(C)$ is a Latin square graph $L_n(q)$ of order q (cf. Bose [4] and Mesner [12]).

Example 2. Let C be the $(11, 5)$ ternary Golay code, i.e., the "unique" $(11, 5)$ code over GF(3) having the weights $w_1 = 6$, $w_2 = 9$ only (cf. Pless [14]). Since C is a projective code, Theorem 2 produces a strongly regular graph, on $v = 243$ vertices, whose parameters are

$$\rho_0 = -22 , \quad \rho_1 = 5 , \quad \rho_2 = -49 .$$

In fact, $\Gamma(C)$ is closely related to another graph, on the same number of vertices, recently derived by Berlekamp et al. [3] from the $(11, 6)$ ternary Golay code. This relationship is a particular case of a nice duality existing among graphs associated with 2-weight projective codes; it will be examined in a forthcoming paper.

We conclude this section with two remarks:

Remark 1. For a 2-weight linear code C over F, the graph $\Gamma(C')$ associated to the image $C' = \gamma(C)$ of C over F' is exactly the same as $\Gamma(C)$, for every subfield F' of F. Hence considering linear codes over prime fields implies no loss of generality in our construction of graphs from 2-weight codes.

Remark 2. On the other hand, the additive group of an (n, k) linear code over $GF(p^e)$, p prime, is isomorphic to the elementary Abelian p-group G_v of order $v = p^{ek}$. Therefore, a strongly regular graph on v vertices cannot be the associated graph of some 2-weight linear code unless the automorphism group of the graph contains a regular subgroup isomorphic to G_v. In §5 of this paper, it will be shown that, in general, this is also a sufficient condition.

§4. Strongly regular normed spaces

Let V be a linear space of dimension $k \geq 1$ over $F = \mathrm{GF}(q)$. We make V a *normed linear space* by defining a norm w over V, i.e., a mapping from V into R^+, satisfying the classical axioms (A1), (A2), (A3). In analogy to the concept of a strongly regular graph, the normed space will be called *strongly regular* if the norm satisfies the following two conditions

$$\text{(A4)} \qquad \sum_{b \in V} w(a-b) = r\,, \quad \forall a \in V\,,$$

$$\text{(A5)} \qquad \sum_{c \in V} w(a-c)w(b-c) + sw(a-b) = t\,, \quad \forall a, b \in V\,,$$

where r, s and t are some fixed positive real numbers.

An arbitrary choice of one of these parameters implies no loss of generality in the problem, since it merely fixes the "scale" of the norm; here we set $s = q^{k-1}$. On the other hand, adding up both members of (A5), for b running through V, we get $r(r+s) = tq^k$, from (A4). Hence, one can write

$$\text{(15)} \qquad r = mv/q, \qquad s = v/q, \qquad t = m(m+1)v/q^2\,,$$

with $v = |V| = q^k$, for some positive number m. In that standard form, the parameter $n = m/(q-1)$ will be called the *length* of the normed space, which will now be denoted by (V, w, n).

With the definition (15) of r, s, t, eqs. (2) and (3) are the matrix form of (A4) and (A5), respectively (for $w = w_{\mathrm{H}}$, $V = C$). Hence Theorem 1 can be reformulated as follows:

Theorem 3. *Let C be an (n, k) projective code over F, and let w_{H} denote the Hamming weight. Then (C, w_{H}, n) is a strongly regular normed space over F.*

The rest of this section is essentially devoted to the proof of a converse of Theorem 3, asserting that any "abstract" strongly regular normed space admits an associated code C isomorphic to it, when the Hamming weight is taken as the norm.

Theorem 4. *Let (V, w, n) be a strongly regular normed space of length n and dimension k over F. Then n is an integer, with $k \leq n \leq (q^k - 1)/(q - 1)$, and there exists an (n, k) projective code C over F such that the normed spaces (V, w, n) and (C, w_H, n) are isomorphic to each other.*

Before we proceed to the proof, we need some material on the correspondence between F^k and the elementary Abelian p-group G_v of order $v = q^k$, with $q = p^e$, p prime. The *characters* of the group G_v are the homomorphic mappings ψ from G_v into the group C_p of complex p^{th} roots of unity. It is well known that the characters can be numbered with the elements x of G_v in such a way that $\psi_x(y) = \psi_y(x)$, $\forall x, y \in G_v$. As in [5], we adopt the notation of a symmetric inner product, that is

$$\langle x, y \rangle = \psi_x(y), \quad \forall x, y \in G_v .$$

Lemma 1. *Let ϕ be a fixed homomorphism from $(F, +)$ onto C_p. Then, for every isomorphism L from G_v onto $(F^k, +)$, there exists one and only one isomorphism M, from G_v onto $(F^k, +)$, such that*

$$(16) \qquad \langle x, y \rangle = \phi(L(x) M^{\mathrm{T}}(y)), \qquad \forall x, y \in G_v ,$$

where $M^{\mathrm{T}}(y)$ is the transpose of the row vector $M(y)$ in F^k.

Proof. Let N be any isomorphism from G_v onto $(F^k, +)$. Then the mapping ψ defined by

$$\psi(x) = \phi(L(x) N^{\mathrm{T}}(y)), \qquad x \in G_v ,$$

is a character of G_v, for every y in G_v. We denote this character by $\psi(x) = \langle x, A(y) \rangle$ since it only depends on y; it is readily seen that A is an automorphism of G_v. Hence the mapping M given by $M(A(y)) = N(y)$ is an isomorphism from G_v onto $(F^k, +)$ that satisfies (16). Finally, the uniqueness of M results from the fact that $\phi(ab^{\mathrm{T}}) = \phi(ac^{\mathrm{T}})$ cannot hold for all vectors a in F^k unless $b = c$.

Definition 1. Let ω be a primitive root in F, and let L be an isomorphism from G_v onto $(F^k, +)$. To L we associate the automorphism S of G_v defined by

$$L(S(x)) = \omega L(x) , \qquad \forall x \in G_v . \tag{17}$$

Obviously, S^{q-1} is the identity and the subsets of transitivity of $G_v \backslash \{1\}$ for the group generated by S have cardinality $q - 1$. They have the form

$$\{x, S(x), S^2(x), ..., S^{q-2}(x)\} ,$$

and are called the *S-classes* of G_v. (There are $(q^k - 1)/(q - 1)$ such S-classes and their L-images are the projective points of $\mathrm{PG}(k - 1, q)$).

Definition 2. Let A and A^{T} be two automorphisms of G_v satisfying

$$\langle x, A(y)\rangle = \langle y, A^{\mathrm{T}}(x)\rangle , \qquad \forall x, y \in G_v . \tag{18}$$

Then A^{T} is called the *transpose* of A. It is well known that each automorphism admits exactly one transpose. Moreover, according to (18), one has $(A^{\mathrm{T}})^{\mathrm{T}} = A$.

Lemma 2. *Let (L, M) be a pair of isomorphisms (from G_v onto $(F^k, +)$) satisfying* (16). *Then* (17) *is equivalent to*

$$M(S^{\mathrm{T}}(y)) = \omega M(y) , \qquad \forall y \in G_v , \tag{19}$$

and $G_v \backslash \{1\}$ can be divided into disjoint S^{T}-classes of order $q - 1$ as well as into S-classes.

Proof. This is an easy consequence of Lemma 1 and the definition (18) of the transpose.

Proof of Theorem 4. Let E be an isomorphism from F^k onto V, and L an isomorphism from G_v onto $(F^k, +)$. The code C will be defined by means of its generator matrix K, in such a manner as to make the following diagram

(20)
$$\begin{tikzcd}
 & F^k \arrow[dl, "E"'] \arrow[dr, "K"] & \\
V \arrow[dr, "w"'] & G_v \arrow[u, "L"'] \arrow[d, "\mu"] & C \arrow[dl, "w_H"] \\
 & R^+ &
\end{tikzcd}$$

commutative, i.e.,

(21) $$w_H(L(x)K) = \mu(x)\,, \qquad \forall x \in G_v\,,$$

with $\mu(x) = w(EL(x))$. The reasoning is rather long and is divided in four parts:

(i). Considering $\mu = \Sigma x\mu(x)$ as an element in the group algebra RG_v of the group G_v over the field R of real numbers, and using (15) with $m = n(q-1)$, one can write (A4), (A5) as

(22) $$\mu\sigma_v = n(q-1)q^{k-1}\sigma_v\,,$$

(23) $$\mu^2 + \mu q^{k-1} = t\,\sigma_v\,,$$

respectively, where σ_v stands for the sum of all elements of G_v over R. We now calculate the characters

(24) $$\langle y, \mu\rangle = \sum_{x\in G_v} \langle y, x\rangle \mu(x)\,, \qquad y \in G_v\,,$$

of $\mu \in RG_v$, in the field of complex numbers. By the well-known properties of group characters, we get both equations

(25) $$\langle 1, \mu\rangle = n(q-1)q^{k-1}\,,$$

(26) $$\langle y, \mu\rangle(q^{k-1} + \langle y, \mu\rangle) = 0\,, \qquad \forall y \neq 1\,,$$

from (22) and (23), respectively. Indeed, $\langle y, \sigma_v\rangle$ is equal to v or to zero, according as y is equal to 1 (the unit of G_v) or not. Let us examine the inversion formula for group characters, i.e.,

$$(27) \qquad \mu(x) = v^{-1} \left[\sum_{y \in G_v} \langle x, y^{-1} \rangle \langle y, \mu \rangle \right] .$$

According to (26), one has $\langle y, \mu \rangle = 0$ or $-q^{k-1}$, for $y \neq 1$. Hence (cf. also (25)), eq. (27) becomes

$$(28) \qquad \mu(x) = q^{-1} \left[n(q-1) - \sum_{y \in H} \langle x, y^{-1} \rangle \right] ,$$

where H is the set of elements y in $G_v \setminus \{1\}$ with $\langle y, \mu \rangle \neq 0$. In particular, for $x = 1$, (28) yields $q\mu(1) = n(q-1) - |H|$. Since $\mu(1) = w(0) = 0$, by (A1), this implies $n(q-1) = |H|$.

(ii). On the other hand, let ω be a primitive root in F. Defining S by (17), one verifies, using (A3), that $\mu(S(x)) = \mu(x)$, for any x in G_v. Therefore, one has

$$\langle S^{\mathrm{T}}(y), \mu \rangle = \sum_{x \in G_v} \langle y, S(x) \rangle \, \mu(x) = \langle y, \mu \rangle , \qquad \forall y \in G_v ,$$

by (18) and (24). Hence (cf. Lemma 2) $\langle y, \mu \rangle$ is constant over each S^{T}-class of G_v, so H must be the union of some of these classes. Therefore, the length $n = |H|/(q-1)$ of the normed space must be a positive integer, less than or equal to $(q^k - 1)/(q-1)$.

(iii). Next, noting that y^{-1} belongs to the same S^{T}-class $\bar{y}$ as y, one can write (28) as follows

$$(29) \qquad \mu(x) = q^{-1} \left[n(q-1) - \sum_{\bar{y} \in \bar{H}} \sum_{z \in \bar{y}} \langle x, z \rangle \right] ,$$

where $\bar{H}$ denotes the set of S^{T}-classes $\bar{y}$ in H. Remembering the definition of an S-class, and using Lemma 1, one has

$$(30) \qquad \sum_{z \in \bar{y}} \langle x, z \rangle = \sum_{i=0}^{q-2} \langle S^i(x), y \rangle = \sum_{i=0}^{q-2} \phi(\omega^i L(x) M^{\mathrm{T}}(y)) ,$$

for a suitable isomorphism M from G_v onto $(F^k, +)$. From (5) it follows that the third member of (30) is equal to $q - 1$ or -1 according as $L(x)M^{\mathrm{T}}(y)$ is zero or not, so (30) yields

$$\sum_{z \in \bar{y}} \langle x, z \rangle = q - 1 - q \, |L(x)M^{\mathrm{T}}(y)| ,$$

where $|\lambda| = 0$ or 1, according as λ equals zero or not, in F. Substituting this in (29), one obtains

$$\mu(x) = \sum_{i=1}^{n} |L(x)M^{\mathrm{T}}(y_i)| , \tag{31}$$

where $\{y_1, y_2, ..., y_n\}$ denotes any set of n elements of G_v obtained by taking exactly one element in each S^{T}-class $\bar{y}$ of $\bar{H}$.

(iv). Finally, we define C to be the linear code of length n over F generated by the $k \times n$ matrix

$$K = [M^{\mathrm{T}}(y_1), M^{\mathrm{T}}(y_2), ..., M^{\mathrm{T}}(y_n)] .$$

Since (31) is equivalent to (21), diagram (20) is commutative and it only remains to be shown that C is actually a projective code of dimension k. This is an easy consequence of (A1) and Lemma 2; the details are omitted.

Remark 3. Property (A2) has not been used in the proof of Theorem 4, so it can be omitted as an axiom for strongly regular normed spaces. In fact, (A2) becomes a consequence of Theorem 4, since the Hamming weight w_{H} satisfies it.

Remark 4. According to a theorem of MacWilliams [9] on the equivalence between linear codes, Theorems 3 and 4 establish a one-to-one correspondence between the classes of nonisomorphic strongly regular normed spaces of length n and dimension k over F, and the classes of inequivalent (n, k) projective codes over F.

§5. Two-weight codes derived from graphs

We first show that, in some cases, (A3) is a redundant axiom for strongly regular normed spaces.

Lemma 3. *Let V be a k-dimensional linear space over* GF(p), *p prime, and let w be a mapping from V into the nonnegative rational numbers, satisfying* (A1), (A4) *and* (A5). *Then* (V, w, n) *is a strongly regular normed space.*

Proof. According to Remark 3, we only need to show that w satisfies (A3). To that end, let us use the first part (depending on (A1), (A4) and (A5) only) of the proof of Theorem 4. The right hand member of (28) belongs to the cyclotomic field Z_p of p^{th} roots of unity and, for an integer i, $1 \leq i \leq p-1$, we readily get

$$\mu_i(x) = (\mu(x^i)) , \qquad \forall x \in G_v ,$$

where $\mu_i(x)$ denotes the i^{th} conjugate of $\mu(x)$ in Z_p. Since $\mu(x)$ is assumed to be rational, one must have $\mu_i(x) = \mu(x)$; whence $\mu(x^i) = \mu(x)$ or, equivalently,

$$w(a) = w(ia) , \qquad \forall a \in V , \qquad 1 \leq i \leq p-1 .$$

This is identical to (A3) for the prime field $F = \text{GF}(p)$, and the lemma is proved.

We now go back to strongly regular graphs and 2-weight codes. The following result is the converse of Theorem 2.

Theorem 5. *Let Γ be a strongly regular graph on $v = p^k$ vertices, p prime, whose adjacency matrix has integral eigenvalues ρ_0, ρ_1, ρ_2 with $\rho_1 > 1$. Assume the automorphism group of Γ contains a regular subgroup isomorphic to the elementary Abelian p-group G_v. Then Γ is the associated graph of some 2-weight (n, k) projective code, whose length n and whose weights w_i are given by*

$$(32)\qquad (\rho_1 - \rho_2)(p-1)n = \rho_0 + \rho_1(v-1)\,,$$

$$(33)\qquad (\rho_1 - \rho_2)w_i = (\rho_1 + (-1)^i)v/p\,, \qquad i = 1, 2\,.$$

Proof. Let V be a k-dimensional linear space over the prime field $F = \mathrm{GF}(p)$. Since G_v is isomorphic to $(V, +)$, it is possible to number the vertices of Γ with the elements of V in such a way that vertex v_a becomes adjacent to v_b if and only if v_{a-b} is adjacent to v_0, $\forall a, b \in V$. Indeed, this simply means that the additive group of V, acting as a regular permutation group on the vertices, transforms the graph Γ into itself.

Next, for the positive numbers w_i given by (33), one defines a mapping w from V into the nonnegative rational numbers as follows: one sets $w(0) = 0$, and $w(a) = w_1$ or w_2 according as v_a is adjacent to v_0 or not, for $a \in V$, $a \neq 0$. In other words, w is defined in such a manner that the matrix

$$(34)\qquad D = [w(a-b); a, b \in V]$$

satisfies (11), when A is the adjacency matrix of the given graph Γ. From eqs. (9) and (10) of a strongly regular graph, it easily follows that D satisfies (2) and (3) or, equivalently, (A4) and (A5), with $q = p$, if n, w_1 and w_2 are given by (32) and (33). Therefore, according to Lemma 3, (V, w, n) is a strongly regular normed space over F.

Finally, by Theorem 4, the length n is an integer and there exists a 2-weight (n, k) projective code C over F whose distance matrix is (34). This means that the given graph Γ is the associated graph of C, so the theorem is proved.

Remark 5. The restrictions on the eigenvalues in the assumptions of Theorem 5 only exclude graphs of one of the following two types: the ladder graphs, for which $\rho_1 = 1$ (cf. Seidel [15]), and the graphs with $v = p^k$, $k \equiv 1 \pmod 2$, $\rho_0 = 0$, $\mu_1 = -\mu_2 = v^{1/2}$. Graphs of the second type are known to exist if and only if $p \equiv 1 \pmod 4$; cf. for instance Goethals and Seidel [7].

We conclude with an illustration of Theorem 5. Goethals and Seidel [8] recently derived a strongly regular graph Γ on $v = 2048$ vertices from the Golay (24, 12) binary code. The eigenvalues of the adjacency matrix of Γ are

$$\rho_0 = 529\,, \qquad \rho_1 = 17\,, \qquad \rho_2 = -111\,.$$

Moreover, the automorphism group of Γ contains a regular subgroup isomorphic to G_v. Hence, according to Theorem 5, there exists a 2-weight projective code C over GF(2) whose associated graph is $\Gamma(C) = \Gamma$. Using (32) and (33), with $p = 2$, one obtains the following values for the parameters of C

$$n = 276\,, \qquad k = 11\,, \qquad w_1 = 128\,, \qquad w_2 = 144\,.$$

The reader familiar with the Golay code will easily find a "direct" construction for such a code.

Acknowledgment

The author is very grateful to J.J. Seidel who mentioned references on strongly regular graphs and suggested constructing two-weight codes from graphs.

References

[1] E.F. Assmus and H.F. Mattson, Error-correcting codes: an axiomatic approach, Inform. Control 6 (1963) 315–330.
[2] E.R. Berlekamp, Algebraic coding theory (McGraw Hill, New York, 1968).
[3] E.R. Berlekamp, J.H. van Lint and J.J. Seidel, A strongly regular graph derived from the perfect ternary Golay code, in: R.C. Bose Anniversary Volume, to be published.
[4] R.C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, Pacific J. Math. 13 (1963) 389–419.
[5] P. Delsarte, Automorphisms of Abelian codes, Philips Res. Rept. 25 (1970) 389–403.
[6] P. Delsarte and J.M. Goethals, Irreducible cyclic codes of even dimension, in: R.C. Bose and T.A. Dowlings, eds., Combinatorial mathematics and its applications (Univ. of North Carolina Press, Chapel Hill, N. Car., 1970) 100–113.
[7] J.M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal, Can. J. Math. 19 (1967) 1001–1010.

[8] J.M. Goethals and J.J. Seidel, Strongly regular graphs derived from combinatorial designs, Can. J. Math. 22 (1970) 597–614.
[9] F.J. MacWilliams, Error-correcting codes for multiple-level transmission, Bell Syst. Tech. J. 40 (1961) 281–308.
[10] F.J. MacWilliams, A theorem on the distribution of weights in a systematic code, Bell Syst. Tech. J. 42 (1963) 79–94.
[11] R.J. McEliece, A class of two-weight codes, Jet Propulsion Lab. Space Progr. Sum. 37–41, Vol. IV, 264–266.
[12] D.M. Mesner, A new family of partially balanced incomplete block designs with some Latin square design properties, Ann. Math. Statistics 38 (1967) 571–581.
[13] V. Pless, Power moment identities on weight distribution in error-correcting codes, Inform. Control 6 (1963) 147–152.
[14] V. Pless, On the uniqueness of the Golay codes, J. Combinatorial Theory 5 (1968) 215–228.
[15] J.J. Seidel, Strongly regular graphs of L_2-type and of triangular type, Indag. Math. 29 (1967) 188–196.