

An Introduction to Association Schemes and Coding Theory

N. J. A. Sloane

ABSTRACT

Association schemes originated in statistics, but have recently been used in coding theory and combinatorics by Delsarte, McEliece and others to obtain strong upper bounds on the size of codes and other combinatorial objects, and to characterize those objects (such as perfect codes) which meet these bounds. A central role is played by the eigenvalues of the association scheme, which in many cases come from a family of orthogonal polynomials. In the most important case these are the Krawtchouk polynomials. This paper gives an introduction to association schemes and the way they are used in coding theory and combinatorics.

§1 INTRODUCTION

Association schemes were first introduced by statisticians in connection with the design of experiments [6], [7], [39], [61], and have since proved very useful in the study of permutation groups [9], [33]-[38] and graphs [4], [10]. Recently, starting with the work of Delsarte [11]-[15], association schemes have been applied with considerable success in coding theory and in other combinatorial problems [16]-[21], [29].

One of the interesting features of this work is that to most of these association schemes there corresponds one or more families of orthogonal polynomials. For the Hamming association scheme, the most important

scheme for coding theory, these are the Krawtchouk polynomials $K_k(x;n)$, $k = 0, \dots, n$, which are orthogonal on the set $\{0, 1, \dots, n\}$ with respect to the weighting function $w(i) = \binom{n}{i}$.

There are two kinds of problems which are considered. The first is to find upper bounds on the size of a subset of an association scheme having certain desirable properties (a code, a t -design, an orthogonal array, etc). The second is to characterize those subsets which meet the bounds. The second problem includes the famous problem of finding all perfect codes - see §§2, 8 below.

The key result is a theorem published by Delsarte in 1972 [11] which states that certain linear combinations of the parameters of the subset must be nonnegative (Th 8 below). This theorem was independently discovered by McEliece, Rodemich, Rumsey and Welch [55] in the special case of error-correcting codes. Because of this result, the first problem can be stated as a linear programming problem. By converting to the dual problem, and using properties of Krawtchouk polynomials, Delsarte [11], [14] and McEliece et al. [55], [56] have obtained very good upper bounds on the size of codes - see §§2, 7 below. The same technique has been applied to other combinatorial problems including:

- (i) Codes of constant weight [14], [15]
 - (ii) t -designs and orthogonal arrays [14], [15]
 - (iii) Families of lines with a prescribed number of angles between them [21]
 - (iv) Bilinear and alternating bilinear forms over $GF(q)$ [19], [20].
- This gives a natural setting for subcodes of the second-order Reed Muller codes, including Kerdock codes. (See also [27].)

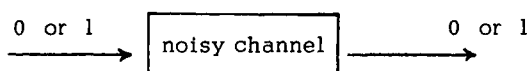
The linear programming approach is also useful in the second problem. For example, in this way Delsarte [11], [15] proved Lloyd's theorem (Cor. 15 below) which states that if a perfect error-correcting code exists then a certain Krawtchouk polynomial must have distinct integer zeros in a certain interval.

This paper assumes no previous knowledge of coding theory or

association schemes. Most of the results can be found in Delsarte [11]-[15]. Indeed an appropriate subtitle would be "an introduction to Delsarte's work".

§2 Error-Correcting Codes

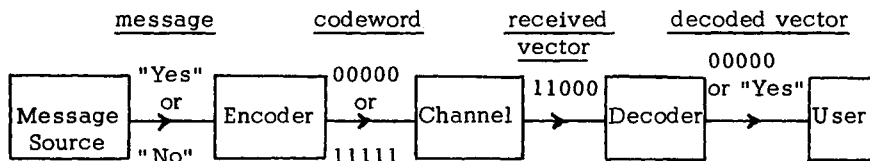
Error-correcting codes were invented to transmit data more accurately. Suppose there is a telegraph wire from Madison to New York down which 0's and 1's can be sent. Usually when a 0 is sent it is received as a 0, but occasionally a 0 will be received as a 1, or a 1 as a 0.



There are a lot of important messages to be sent down this wire, and they must be sent as quickly and reliably as possible. The messages are already written as strings of 0's and 1's - perhaps they are being produced by a computer.

The method we shall use is to encode the messages into codewords. Only codewords will be sent down the channel.

An example will make this clear. Suppose only two messages are to be sent, e.g. "Yes" or "No". "Yes" will be encoded as 00000 and "No" as 11111. This is a code with two codewords.



Suppose 11000 is received at the far end. The decoder argues that 00000 was more likely to have been sent than 11111, because 11000 is somehow closer to 00000 than to 11111.

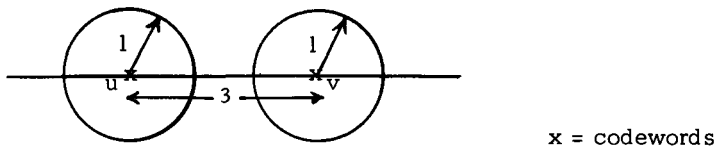
To make this precise we define the Hamming distance $\text{dist}(u, v)$ between two vectors $u = u_1 \dots u_n$ and $v = v_1 \dots v_n$ to be the number of places where they differ. Thus

$$\text{dist}(00000, 11000) = 2, \quad \text{dist}(11111, 11000) = 3 .$$

It is easy to check that this is a metric.

Then the decoder's strategy is to decode the received vector as the closest codeword (in Hamming distance). This is because a digit is more likely to be correct than in error.

Notice that in this example the decoder was able to correct two errors. This is because the Hamming distance between the codewords 00000 and 11111 is 5. The error correction procedure is perhaps best explained by a picture. Suppose we have a code in which any two distinct codewords differ in at least 3 places.



Then this code can correct one error. If the codeword u is transmitted and at most one error occurs, the received vector will still be within the "sphere" of radius 1 about u , and (by the triangle inequality) is closer to u than to any other codeword v . The "spheres" of radius 1 about each codeword are disjoint.

The same argument shows that a code in which any two distinct codewords have Hamming distance at least d apart can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. The "spheres" of Hamming radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ around the codewords are disjoint.

This motivates our definition. An (n, M, d) error-correcting code is a set of M vectors $u = u_1 \dots u_n$ of 0's and 1's of length n (called codewords) such that any two distinct codewords differ in at least d places. n is called the length of the code, M is the size and d is the minimum distance. This is a $\left\lfloor \frac{1}{2}(d-1) \right\rfloor$ -error-correcting code.

Examples of Codes

1. The preceding example $\{00000, 11111\}$ is a $(5, 2, 5)$ code.

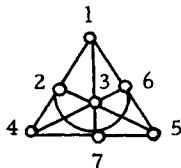
2. A $(3, 4, 2)$ code: $\{000, 011, 101, 110\}$. More generally, the $(n, 2^{n-1}, 2)$ even weight code consists of all vectors of even Hamming weight, where the Hamming weight $wt(u)$ of a vector $u = u_1 \dots u_n$ is the number of nonzero u_i . Clearly

$$\text{dist}(u, v) = wt(u-v) .$$

3. The Hamming $(7, 16, 3)$ code:

0000000	1111111
1101000	0010111
0110100	1001011
0011010	1100101
0001101	1110010
1000110	0111001
0100011	1011100
1010001	0101110

The reader will recognize codewords 2 through 8 as forming the incidence matrix of



the projective plane of order 2 .

These examples are all linear codes. That is, the sum (taken componentwise, modulo 2) of two codewords is again a codeword. They are also cyclic: if $u_1 \dots u_n$ is a codeword so is $u_2 \dots u_n u_1$.

The $(7, 16, 3)$ code has another nice property: it is perfect. An e -error-correcting code is called perfect if every binary vector of length n is within Hamming distance e of some codeword.

To state this another way, let $Q_n = \{u_1 \dots u_n : u_i = 0 \text{ or } 1\}$ be the set of all binary vectors of length n , i. e. the vertices of the unit n -cube.

An (n, M, d) code \mathcal{C} is a subset of Q_n of size M , with the property that the spheres

$$S_e(v) = \{u \in Q_n : \text{dist}(u, v) \leq e\}, \quad v \in \mathcal{C},$$

of radius $e = \lfloor \frac{1}{2}(d-1) \rfloor$ about the codewords are disjoint. In a perfect code these spheres include all the points of Q_n : they are both a packing and a covering of Q_n . We shall return to perfect codes in §8.

The Coding Theory Problem

In a good code n is small (for fast transmission), M is large (for efficiency), and d is large (to correct many errors).

The first thing one wants to know is how large M can be, for given values of n and d . Upper and lower bounds on the largest M (when n is large) due to Elias, Gilbert and Varshamov have been known for some time (see [1, Ch 13], [59, Ch 4]). Recently Levenshtein [47] and Sidel'nikov [64] have given small improvements on the Elias upper bound. One of the goals of this paper is to describe a new technique for obtaining upper bounds, discovered independently by Delsarte [11] and McEliece, Rodemich, Rumsey and Welch [55], and known as the linear programming method (see §7). Welch, McEliece and Rumsey [69] have recently used this method to improve the Elias bound when d/n is close to $\frac{1}{2}$. Finally, while this paper was being written, McEliece, Rodemich, Rumsey and Welch [56] have announced the following bound: if \mathcal{C} is any (n, M, d) code, then

$$\frac{\log_2 M}{n} \lesssim H_2 \left(\frac{1}{2} - \sqrt{\frac{d}{n} \left(1 - \frac{d}{n} \right)} \right), \quad \text{as } n \rightarrow \infty,$$

where $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$. This is a considerable improvement on the Elias bound over most of the range of d/n , and was obtained by using the linear programming method together with asymptotic properties of Krawtchouk polynomials. One expects that further upper bounds will be obtained using this method. However, the true upper

bound probably coincides with the Gilbert-Varshamov lower bound, and a proof of this seems a long way off.

For small values of n the story is similar. Upper and lower bounds are known [32], [41], [52], [67], and again the linear programming method has recently been used [55] to improve the upper bound in many cases.

The second main problem in coding theory is of course to find codes which come close to these bounds. This problem is still essentially unsolved, although a lot of constructions are known [1], [43], [48], [52], [59].

It is interesting to list a few of the best known codes and the mathematical techniques used to construct them:

Reed-Muller codes (Boolean functions, 1954),
 Bose-Chaudhuri-Hocquenghem codes (Galois fields, 1959),
 Quadratic residue codes (number theory, around 1960),
 Geometry codes (finite geometries, 1967),
 Goppa codes (alternating determinants, 1970 [30], [2], [31], [52]).

The latest technique to be introduced is that of association schemes (in 1973, by Delsarte [12]). This has led to the powerful linear programming bounds just mentioned, and to the other applications mentioned in the introduction.

§3 Association Schemes

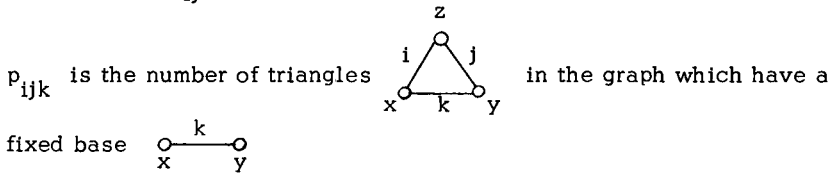
This section gives some of the basic theory, mostly following Delsarte [14], and then the next three §'s contain examples.

Definition (Bose and Shimamoto [7]) An association scheme with n classes consists of a finite set X of v points, together with $n + 1$ symmetric relations R_0, R_1, \dots, R_n defined on X which satisfy

- (i) For every $x, y \in X$, $(x, y) \in R_i$ for exactly one i .
- (ii) $R_0 = \{(x, x) : x \in X\}$ is the identity relation.
- (iii) If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(y, z) \in R_j$ is a constant $p_{i,j,k}$ depending on i, j, k but not on the particular choice of x and y .

Two points x and y are called ith associates if $(x, y) \in R_i$. In words, the definition states that if x and y are i th associates so are y and x ; every pair of points are i th associates for exactly one i ; each point is its own zeroth associate while distinct points are never zeroth associates; and finally if x and y are k th associates then the number of points z which are both i th associates of x and j th associates of y is a constant p_{ijk} .

An association scheme can be described by a complete graph having v nodes (corresponding to the points of X), in which the edge joining nodes x and y is labeled by i if x and y are i th associates. The numbers p_{ijk} are called the intersection numbers of the scheme.



The number of i th associates of any point x is

$$p_{ii0} = v_i \quad (\text{say}),$$

the valency of the i th relation. The p_{ijk} must satisfy the following identities:

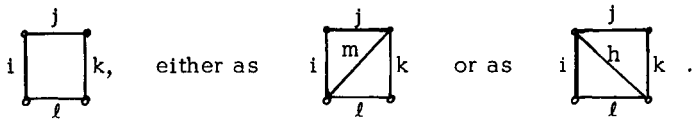
$$p_{ijk} = p_{jik}, \tag{1}$$

$$p_{0jk} = \delta_{jk}, \quad v_k p_{ijk} = v_i p_{kji},$$

$$\sum_{j=0}^n p_{ijk} = v_i,$$

$$\sum_{m=0}^n p_{ijm} p_{mkl} = \sum_{h=0}^n p_{ihl} p_{jkh}. \tag{2}$$

The last identity follows from counting the quadrilaterals



Let D_i be the adjacency matrix of R_i ($i = 0, \dots, n$). That is, D_i is the $v \times v$ matrix with rows and columns labeled by the points of X , defined by

$$(D_i)_{x,y} = \begin{cases} 1 & \text{if } (x, y) \in R_i, \\ 0 & \text{otherwise.} \end{cases}$$

The definition of an association scheme is equivalent to saying that the D_i are symmetric (0, 1)-matrices which satisfy

$$(i) \quad \sum_{i=0}^n D_i = J \quad (\text{the all-ones matrix}), \tag{3}$$

$$(ii) \quad D_0 = I,$$

$$(iii) \quad D_i D_j = \sum_{k=0}^n p_{ijk} D_k, \quad i, j = 0, \dots, n. \tag{4}$$

Indeed the $(x, y)^{\text{th}}$ entry of the left side of Eq. (4) is the number of paths $x \overset{i}{\circ} \overset{j}{\circ} y$ in the graph. Also

$$D_i J = J D_i = v_i J. \tag{5}$$

The Bose-Mesner Algebra

Let \mathcal{A} be the vector space consisting of all matrices of the form

$$\sum_{i=0}^n c_i D_i, \quad \text{where the } c_i \text{ are real.}$$

All the matrices in \mathcal{A} are symmetric. Equation (3) implies that D_0, \dots, D_n are linearly independent, and the dimension of \mathcal{A} is $n+1$. Furthermore Eq. (4) implies that \mathcal{A} is closed under multiplication, so \mathcal{A} is an algebra. Multiplication is commutative, from Eq. (1), and associative, since \mathcal{A} is an algebra of matrices and matrix multiplication is associative. (Alternatively, associativity follows from Eq. (2).) We call this associative, commutative algebra \mathcal{A} the Bose-Mesner algebra of the association scheme, after Ref. [6].

Since the matrices in \mathcal{A} are symmetric and commute with each other, they can be simultaneously diagonalized ([54, p. 77]). I. e. there is a matrix S such that to each $A \in \mathcal{A}$ there is a diagonal matrix Λ_A with

$$S^{-1}AS = \Lambda_A \quad (5')$$

Therefore \mathcal{A} is semisimple and has a unique basis of primitive idempotents J_0, \dots, J_n . These are real $n \times n$ matrices satisfying (see [58], [8], [68a])

$$J_i^2 = J_i, \quad i = 0, \dots, n, \quad (6a)$$

$$J_i J_k = 0, \quad i \neq k, \quad (6b)$$

$$\sum_{i=0}^n J_i = I. \quad (6c)$$

From Eqs. (3), (5), $\frac{1}{v} J$ is a primitive idempotent, so we shall choose

$$J_0 = \frac{1}{v} J.$$

Let D_k be expressed in terms of the basis J_0, \dots, J_n by

$$D_k = \sum_{i=0}^n P_k^{(i)} J_i, \quad k = 0, \dots, n, \quad (7)$$

for some uniquely determined real numbers $P_k(i)$. Equations (6), (7) imply

$$D_k J_i = P_k(i) J_i \quad (8)$$

Therefore the $P_k(i)$, $i = 0, \dots, n$, are the eigenvalues of D_k . Also the columns of the J_i span the common eigenspaces of all the matrices in \mathcal{A} . Let $\mu_i = \text{rank } J_i$ be the multiplicity of the i^{th} eigenspace.

Conversely, to express the J_k in terms of the D_i , let P be the real $(n+1) \times (n+1)$ matrix

$$P = \begin{bmatrix} P_0(0) & P_1(0) & \dots & P_n(0) \\ P_0(1) & P_1(1) & \dots & P_n(1) \\ \dots & \dots & \dots & \dots \\ P_0(n) & P_1(n) & \dots & P_n(n) \end{bmatrix} \quad (9)$$

and let

$$Q = v P^{-1} = \begin{bmatrix} Q_0(0) & Q_1(0) & \dots & Q_n(0) \\ Q_0(1) & Q_1(1) & \dots & Q_n(1) \\ \dots & \dots & \dots & \dots \\ Q_0(n) & Q_1(n) & \dots & Q_n(n) \end{bmatrix} \quad (\text{say}). \quad (10)$$

We call P and Q the eigenmatrices of the association scheme. Then

$$J_k = \frac{1}{v} \sum_{i=0}^n Q_k(i) D_i, \quad k = 0, \dots, n \quad (11)$$

Lemma 1

$$P_0(i) = Q_0(i) = 1, \quad P_k(0) = v_k, \quad Q_k(0) = \mu_k .$$

Proof Only the last equation is not immediate. Since J_k is an idempotent the diagonal entries of $S^{-1} J_k S$ (see Eq. (5')) are 0 and 1 .

Therefore

$$\text{trace } S^{-1} J_k S = \text{trace } J_k = \text{rank } J_k = \mu_k .$$

Since $\text{trace } D_i = v \delta_{0i}$, (11) implies $\mu_k = Q_k(0)$.

Q. E. D.

Theorem 2

The eigenvalues $P_k(i)$ and $Q_k(i)$ satisfy the following orthogonality conditions.

$$\sum_{i=0}^n \mu_i P_k(i) P_\ell(i) = v v_k \delta_{k\ell} , \tag{13}$$

$$\sum_{i=0}^n v_i Q_k(i) Q_\ell(i) = v \mu_k \delta_{k\ell} . \tag{14}$$

Also

$$\mu_j P_i(j) = v_i Q_j(i), \quad i, j = 0, \dots, n . \tag{15}$$

Proof To prove (14), expand $J_k J_\ell = J_k \delta_{k\ell}$ in the basis D_0, \dots, D_n , and equate the coefficients of D_0 . To prove (13), write (14) as $Q^T A Q = v B$, where $A = \text{diag}(v_0, \dots, v_n)$, $B = \text{diag}(\mu_0, \dots, \mu_n)$, and T denotes transpose. Then $v A = P^T B P$, which is (13). Finally (from (10)) $A Q = P^T B$, which proves (15). Q. E. D.

An Isomorphic Algebra of $(n+1) \times (n+1)$ Matrices

We briefly mention that there is an algebra of $(n+1) \times (n+1)$ matrices

which is isomorphic to \mathcal{A} , and is often easier to work with. Let

$$L_i = \begin{bmatrix} p_{i00} & p_{i10} & \cdots & p_{in0} \\ p_{i01} & p_{i11} & \cdots & p_{in1} \\ \cdots & \cdots & \cdots & \cdots \\ p_{i0n} & p_{i1n} & \cdots & p_{inn} \end{bmatrix}, \quad i = 0, \dots, n.$$

Then Eq. (2) implies

$$L_i L_j = \sum_{k=0}^n p_{ijk} L_k.$$

Thus the L_i multiply in the same manner as the D_i . Since $p_{ik0} = \delta_{ik}$, it follows that L_0, \dots, L_n are linearly independent. Therefore the algebra \mathcal{B} consisting of all matrices $\sum_{i=0}^n c_i L_i$ (c_i real) is an associative commutative algebra, which is isomorphic to \mathcal{A} under the mapping $D_i \rightarrow L_i$.

Equating eigenvalues on both sides of Eq. (4) gives

$$P_i(\ell) P_j(\ell) = \sum_{k=0}^n p_{ijk} P_k(\ell), \quad \ell = 0, \dots, n.$$

This implies that

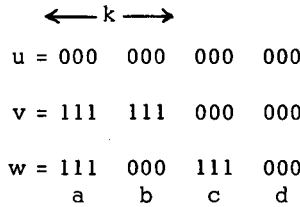
$$P L_k P^{-1} = \text{diag}(P_k(0), \dots, P_k(n)).$$

Thus the $P_k(i)$, $i = 0, \dots, n$, are also the eigenvalues of L_i . (Alternatively, since \mathcal{A} and \mathcal{B} are isomorphic, D_i and L_i have the same minimal polynomials and therefore the same eigenvalues.)

Further general properties of association schemes are given by Delsarte [14], [15]. But now it is time for some examples.

§4 The Hamming Association Scheme

The Hamming or hypercubic association scheme is the most important example for coding theory (see Delsarte [14], [15]). In this scheme $X = Q_n$, the set of binary vectors of length n , and two vectors $u, v \in Q_n$ are i th associates if they are Hamming distance i apart. Plainly conditions (i), (ii) of the definition of an association scheme are satisfied. To verify (iii), let $\text{dist}(u, v) = k$. Without loss of generality we may take $u = 00\dots 0$, $v = 11\dots 100\dots 0$. We show that the number of $w \in Q_n$ such that $\text{dist}(u, w) = i$, $\text{dist}(v, w) = j$ is a constant p_{ijk} independent of the choice of u, v, w . Consider the figure

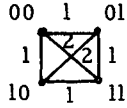


Then $a + c = i$, $b + c = j$, $a + b = k$. Hence $a = \frac{1}{2}(i-j+k)$, $c = \frac{1}{2}(i+j-k)$ and so

$$p_{ijk} = \begin{cases} \binom{k}{\frac{i-j+k}{2}} \binom{n-k}{\frac{i+j-k}{2}} & \text{if } i+j-k \text{ is even,} \\ 0 & \text{if } i+j-k \text{ is odd.} \end{cases}$$

Also $v_i = \binom{n}{i}$. The matrices in the Bose-Mesner algebra \mathcal{A} are $2^n \times 2^n$ matrices, with rows and columns labeled by vectors $u \in Q_n$. In particular the (u, v) th entry of D_k is 1 if and only if $\text{dist}(u, v) = k$.

For example, if $n = 2$, $Q_2 = \{00, 01, 10, 11\}$, and we label the rows

and columns by 00, 01, 10, 11. The graph  shows that $v_0 = p_{000} = 1$, $v_1 = p_{110} = 2$, $v_2 = p_{220} = 1$, $p_{111} = 2$, $p_{112} = 1$, etc. The adjacency matrices are

$$D_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad D_1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad D_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

We shall need the following simple result.

Lemma 3

$$\sum_{u \in Q_n} (-1)^{u \cdot v} = 2^n \delta_{0,v},$$

where $u \cdot v$ denotes the real scalar product $\sum_{i=1}^n u_i v_i$.

Lemma 4 The primitive idempotent J_k is the matrix which has $(u, v)^{th}$ entry equal to

$$\frac{1}{2^n} \sum_{wt(w)=k} (-1)^{(u+v) \cdot w}, \quad k = 0, \dots, n. \quad (16)$$

Proof Let A_k be the matrix (16). We show that the $n+1$ matrices A_k satisfy (6a), (6b) and (6c), and therefore are the primitive idempotents. The $(u, w)^{th}$ entry of $A_k A_\ell$ is

$$\begin{aligned} & \frac{1}{2^{2n}} \sum_{v \in Q_n} \sum_{wt(x)=k} (-1)^{(u+v) \cdot x} \sum_{wt(y)=\ell} (-1)^{(v+w) \cdot y} \\ &= \frac{1}{2^{2n}} \sum_{wt(x)=k} \sum_{wt(y)=\ell} (-1)^{u \cdot x + v \cdot y} \sum_{v \in Q_n} (-1)^{v \cdot (x+y)} \end{aligned}$$

$$= \frac{1}{2^n} \delta_{k,\ell} \sum_{\text{wt}(\mathbf{x})=k} (-1)^{(u+v) \cdot \mathbf{x}}, \text{ by Lemma 3 ,}$$

which is the $(u, w)^{\text{th}}$ entry of $A_k \delta_{k,\ell}$ and proves (6a) and (6a). Equation (6c) follows from Lemma 3. Q. E. D.

For example, when $n = 2$,

$$J_0 = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \quad J_1 = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & - \\ 0 & 1 & - & 0 \\ 0 & - & 1 & 0 \\ - & 0 & 0 & 1 \end{bmatrix}, \quad J_2 = \frac{1}{4} \begin{bmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \\ - & 1 & 1 & - \\ 1 & - & - & 1 \end{bmatrix},$$

where - stands for -1. The ranks are $\mu_0 = 1, \mu_1 = 2, \mu_2 = 1$.

The eigenvalues $P_k(1)$ will turn out to be the values of Krawtchouk polynomials.

Definition For any positive integer n , the k^{th} Krawtchouk polynomial ([44], [68]) is defined by

$$K_k(x;n) = \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{n-x}{k-j}, \quad k = 0, 1, 2, \dots, \tag{17}$$

where x is an indeterminate, and

$$\binom{x}{m} = \begin{cases} \frac{x(x-1)\dots(x-m+1)}{m!} & \text{if } m \text{ is a positive integer,} \\ 1 & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Thus $K_k(x;n)$ is a polynomial in x of degree k . The first few Krawtchouk polynomials are

$$\begin{aligned} K_0(x;n) &= 1, \\ K_1(x;n) &= n - 2x, \\ K_2(x;n) &= \binom{n}{2} - 2nx + 2x^2. \end{aligned}$$

Theorem 5

If u is any vector of weight i ,

$$\sum_{wt(\mathbf{v})=k} (-1)^{u \cdot \mathbf{v}} = K_k(i;n) \quad (18)$$

Proof The figure

$$\begin{array}{cccc} \longleftarrow i \longrightarrow & & & \\ u = 111 & 111 & 000 & 000 \\ v = 111 & 000 & 111 & 000 \\ & j & & k-j. \end{array}$$

shows that the left hand side is

$$\sum_{j=0}^i (-1)^j \binom{i}{j} \binom{n-i}{k-j} = K_k(i;n) .$$

Q. E. D.

Theorem 6 The eigenvalues of the Hamming association scheme are

$$P_k(i) = Q_k(i) = K_k(i;n), \quad \text{for } i, k = 0, \dots, n .$$

Proof Since the expansion (7) is unique, $P_k(i) = K_k(i;n)$ will follow if we show that

$$D_k = \sum_{i=0}^n K_k(i;n) J_i, \quad k = 0, \dots, n .$$

This is now a routine calculation using Lemmas 3, 4 and Th. 5. Similarly for $Q_k(i)$. Q. E. D.

E. G., when $n = 2$

$$P = Q = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{pmatrix} .$$

From Th. 2 we obtain

$$\sum_{i=0}^n \binom{n}{i} K_k(i;n) K_\ell(i;n) = 2^n \binom{n}{k} \delta_{k,\ell} . \tag{19}$$

Thus the Krawtchouk polynomials $K_k(x;n)$, $k = 0, \dots, n$, are an orthogonal family on the set $\{0, 1, \dots, n\}$, with respect to the weighting function $w(i) = \binom{n}{i}$.

A generating function for these polynomials is

$$(1+z)^{n-x} (1-z)^x = \sum_{k=0}^{\infty} K_k(x;n) z^k . \tag{20}$$

If i is an integer in the range $0 \leq i \leq n$ this becomes

$$(1+z)^{n-i} (1-z)^i = \sum_{k=0}^n K_k(i;n) z^k . \tag{21}$$

From (20) it is not difficult to obtain the three-term recurrence

$$(k+1)K_{k+1}(x;n) = (n-2x)K_k(x;n) - (n-k+1)K_{k-1}(x;n) \tag{22}$$

for $k = 1, 2, \dots$, and the alternative expressions

$$\begin{aligned} K_k(x;n) &= \sum_{j=0}^k (-2)^j \binom{x}{j} \binom{n-j}{k-j} , \\ &= \sum_{j=0}^k (-1)^j 2^{k-j} \binom{n-k+j}{j} \binom{n-x}{k-j} \end{aligned} \tag{23}$$

Thus $K_k(x;n)$ is a polynomial in x of degree k , with leading coefficient $(-2)^k/k!$ and constant term $\binom{n}{k}$. Some other useful formulae are

$$\binom{n}{i} K_k(i;n) = \binom{n}{k} K_1(k;n) , \tag{24}$$

$$\sum_{i=0}^n K_k(i;n) K_1(\ell;n) = 2^n \delta_{k,\ell} \quad , \quad (25)$$

$$\sum_{i=0}^k K_1(x;n) = K_k(x-1;n-1), \quad k = 0, 1, \dots \quad (26)$$

$$\sum_{i=0}^n \binom{n-i}{n-j} K_1(x;n) = 2^j \binom{n-x}{j}, \quad j = 0, \dots, n \quad . \quad (27)$$

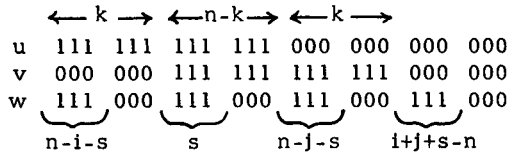
The usual classical definition of these polynomials is a bit more general than this (see [44], [45], [68], [24], [25]). Other generalizations have been used in coding theory (see [14]-[17], [53]).

§5 The Johnson Association Scheme

Upper bounds on the size of codes with a prescribed minimum distance and in which all codewords have the same weight have been given by Levenshtein [46] and Johnson [40]-[42]. Not only are these bounds important in themselves, but they often lead to improved bounds on unrestricted codes, see [40]-[42], [14, Th 3.7]. The appropriate association scheme is what we shall call the Johnson scheme, following Delsarte. (In the statistical literature this is called a triangular association scheme [57], [71]). As will be seen in §7, this scheme also has applications to t-designs.

Let V and n be fixed integers with $0 \leq n \leq \frac{1}{2} V$. In the Johnson scheme, X consists of all $\binom{V}{n}$ binary vectors of length V and weight n . Two vectors u, v are i th associates if $\text{dist}(u, v) = 2i$, for $i = 0, 1, \dots, n$.

The figure



shows that this is an association scheme, with intersection numbers

$$p_{ijk} = \sum_{s=0}^{n-k} \binom{k}{n-i-s} \binom{k}{n-j-s} \binom{n-k}{s} \binom{V-n-k}{i+j+s-n} ,$$

and valencies

$$v_i = \binom{n}{i} \binom{V-n}{i} .$$

It can be shown that the eigenvalues are given by $P_k(i) = E_i(i;V, n)$, where $E_k(x;V, n)$ is the Eberlein polynomial ([26], [14], [15], [18]) defined by

$$E_k(x;V, n) = \sum_{j=0}^k (-1)^{k-j} \binom{n-j}{k-j} \binom{n-x}{j} \binom{V-n+j+x}{j} . \quad (28)$$

In fact $E_k(x;V, n)$ is a polynomial $\Phi_k(z;V, n)$, say, of degree k in the indeterminate $z = x(V+1-x)$.

Theorem 2 implies that the Eberlein polynomials $\Phi_k(z;V, n)$ are an orthogonal family on the set $\{z_i = i(V+1-i): i = 0, \dots, n\}$ with respect to the weighting function $w(z_i) = \binom{V}{i} - \binom{V}{i-1}$.

The eigenvalues $Q_k(i) = Q_k(i;V, n)$ are also obtained from orthogonal polynomials $Q_k(x;V, n)$, where (see [14])

$$Q_0(x;V, n) = 1 ,$$

$$Q_1(x;V, n) = \frac{V-1}{n(V-n)} \{n(V-n) - Vx\} , \quad (29)$$

$Q_k(x;V, n)$ is a polynomial in x of degree k .

§6 Association Schemes Obtained from Graphs and Other Sources

Let Γ be a connected graph with v nodes, containing no loops or multiple edges. Let X be the set of nodes of Γ . The distance

$\rho(x, y)$ between nodes x and y is defined to be the number of edges on the shortest path joining them. The maximum distance n (say) between any two nodes is called the diameter of Γ .

Definition The graph Γ is called metrically regular [23] (or perfectly regular [36], or distance-regular [4], [10]) if the following condition is satisfied. For any pair of nodes x, y with $\rho(x, y) = k$, the number of nodes z such that $\rho(x, z) = i$ and $\rho(y, z) = j$ is a constant p_{ijk} depending on i, j, k but not on the particular choice of x and y .

Clearly we may obtain an association scheme with n classes from the nodes X of a metrically regular graph by calling x and y i th associates if $\rho(x, y) = i$, $i = 0, \dots, n$. This example explains why the p_{ijk} are called intersection numbers: let $\Gamma_i(x) = \{y \in X: \rho(x, y) = i\}$ be the nodes at distance i from x . Then if $\rho(x, y) = k$,

$$p_{ijk} = |\Gamma_i(x) \cap \Gamma_j(y)|.$$

Association schemes that can be obtained from graphs in this way are called metric schemes. To construct the graph from the scheme, one defines x and y to be adjacent if and only if $(x, y) \in R_1$.

Examples of Metrically Regular Graphs

1. The Hamming and Johnson Schemes are metric schemes.
2. Metrically regular graphs of diameter 2 are known as strongly regular graphs, and have been extensively studied ([5], [28], [62], [63]). Any association scheme with two classes is metric, and corresponds to a strongly regular graph.

But not all association schemes are metric. As pointed out by Delsarte [14], an association scheme is metric if and only if (i) $k = i + j \implies p_{ijk} \neq 0$, and (ii) $p_{ijk} \neq 0 \implies |i - j| \leq k \leq i + j$. Delsarte has also given an interesting characterization of metric schemes in terms of the eigenvalues $P_k(i)$, as follows.

Let z_0, \dots, z_n be distinct nonnegative real numbers, with $z_0 = 0$.

Suppose the entries of the eigenmatrix P can be written as

$$P_k(i) = \Phi_k(z_i), \quad i, k = 0, \dots, n,$$

where $\Phi_k(z)$ is a polynomial of degree k . Then the association scheme is called a P-polynomial scheme with respect to the z_i . A Q-polynomial scheme is defined similarly.

Theorem 2 implies that in a P-polynomial scheme, $\Phi_0(z), \dots, \Phi_n(z)$ are an orthogonal family on the set $\{z_0, \dots, z_n\}$ with respect to the weighting function $w(z_i) = \mu_i$. It can also be shown that the sum polynomials

$$\Psi_k(z) = \Phi_0(z) + \dots + \Phi_k(z), \quad k = 0, \dots, n-1 \quad (30)$$

form an orthogonal family on the set $\{z_1, \dots, z_n\}$ with respect to the weighting function $w(z_i) = \mu_i z_i$. The Hamming and Johnson schemes are both P- and Q-polynomial schemes.

Theorem 7 (Delsarte [14])

An association scheme is metric if and only if it is a P-polynomial scheme.

(No such characterization is known for Q-polynomial schemes.)

In a metric scheme, D_1 is the ordinary node-node adjacency matrix of the graph. Also it is easy to see that D_1 is a polynomial in D_i of degree i . Thus the Bose-Mesner algebra of a metric association scheme is the algebra of polynomials in D_1 . This algebra and its eigenvalues have been studied by several authors (see for example Biggs [3], [4], [4a]).

An interesting subclass of metrically regular graphs are distance-transitive graphs, defined as follows [4], [67a]. A graph is distance-transitive if, for any nodes u, v, x, y with $\rho(u, v) = \rho(x, y)$, there is a permutation of the nodes which preserves adjacency and which takes u to x and v to y . It is easy to see that a distance-transitive graph is metrically regular. The graphs corresponding to the Hamming and

Johnson schemes are distance-transitive.

Association Schemes from Permutation Groups

Metrically regular and distance-transitive graphs are important in studying permutation groups. In fact, many of the sporadic simple groups can be obtained as automorphism groups of such graphs. But we have already strayed too far from coding theory, and so just refer the reader to the extremely interesting references Higman [33]-[38], Cameron [9] and Biggs [3]. Wielandt [70] also contains much relevant material, although without using the terminology of association schemes.

Association Schemes in Statistics

Here again, space does not permit us to describe the role of association schemes in statistics. See Bose and Shimamoto [7], James [39], Ogasawara [57], Ogawa [58], Raghavarao [61], and Yamamoto et al. [71].

§7 The Linear Programming Bound

The definition of an error-correcting code given in §2 amounts to saying that a code is a subset of $X = Q_n$ in the Hamming association scheme. More generally, let us define a code Y in any association scheme to be a nonempty subset of the points X . Elements of Y are called codewords. We shall use the term error-correcting code to refer to a code as defined in §2.

The distance distribution of the code Y is defined to be the $(n+1)$ -tuple of rational numbers (B_0, \dots, B_n) , where

$$B_i = \frac{1}{|Y|} |R_i \cap Y^2|$$

is the average number of codewords which are i th associates of a given codeword. The distance distribution of an error-correcting code in the Hamming scheme gives the minimum distance d of the code and other useful information (see [52]).

Note that $B_0 = 1$, $\sum_{i=0}^n B_i = |Y|$, and of course $B_i \geq 0$. A much stronger result is

Theorem 8 (Delsarte [11], [15])

The distance distribution of any code $Y \subset X$ satisfies

$$B'_k \triangleq \frac{1}{|Y|} \sum_{i=0}^n B_i Q_k(i) \geq 0 ,$$

for $k = 0, \dots, n$. Note that $B'_0 = 1$, $\sum_{k=0}^n B'_k = |X|/|Y|$.

Proof Let $u = (u_x)_{x \in X}$ be the characteristic vector of Y , defined by $u_x = 1$ if $x \in Y$, $= 0$ if $x \notin Y$. Then $B_i = \frac{1}{|Y|} u D_i u^T$. Also

$$B'_k = \frac{1}{|Y|^2} u \left(\sum_{i=0}^n Q_k(i) D_i \right) u^T = \frac{|X|}{|Y|^2} u J_k u^T, \quad \text{from (11)} .$$

Now J_k has eigenvalues 0 and 1 (see the proof of Lemma 1), so is positive semi-definite. Therefore $B'_k \geq 0$. Q. E. D.

Remark For a linear error-correcting code in the Hamming scheme it turns out that B_i is the number of codewords of Hamming weight i , and (by the MacWilliams theorem [51], [52, Ch 5]) B'_i is the number of codewords of Hamming weight i in the dual code. So in this case Th. 8 is trivial. But the importance of Th. 8 comes from the fact that it applies to nonlinear error-correcting codes and more generally to codes in arbitrary association schemes.

The simultaneous linear inequalities in Th. 8 suggest the use of linear programming. Let us say that a code Y in an association scheme has minimum distance d if no codeword is an i th associate of any other codeword, for $0 < i < d$. The distance distribution of Y must satisfy

$$B_1 = B_2 = \dots = B_{d-1} = 0 .$$

This includes error-correcting codes with minimum distance d in the Hamming scheme as a special case.

The problem of finding the largest code of minimum distance d is related to:

Linear Programming Problem (I) Choose the real variables B_d, B_{d+1}, \dots, B_n so as to

$$\text{maximize } g = \sum_{i=d}^n B_i$$

subject to the inequalities

$$B_i \geq 0, \quad i = d, \dots, n, \quad (31)$$

$$Q_k(0) + \sum_{i=d}^n B_i Q_k(i) \geq 0, \quad k = 1, \dots, n. \quad (32)$$

An $(n+1)$ -tuple $B = (B_0, \dots, B_n)$ with $B_0 = 1, B_1 = \dots = B_{d-1} = 0$ is called a feasible solution to Problem (I) if it satisfies (31) and (32). A feasible solution is optimal if g is maximized. Let g_{\max} be the maximal value of g .

If a code Y with minimum distance d exists in this association scheme, its distance distribution (B_0, B_1, \dots, B_n) is (from Th. 8) a feasible solution to Problem (I). Therefore

$$|Y| \leq g_{\max} + 1$$

is an upper bound on the size of the code. This is the first version of the linear programming bound for codes.

Associated with this linear programming problem is the:

Dual Problem (II) Choose the real variables β_1, \dots, β_n so as to

$$\text{minimize } \gamma = \sum_{k=1}^n \beta_k Q_k(0)$$

subject to the inequalities

$$\beta_k \geq 0, \quad k = 1, \dots, n, \quad (33)$$

$$1 + \sum_{k=1}^n \beta_k Q_k(i) \leq 0, \quad i = d, \dots, n. \quad (34)$$

An $(n+1)$ -tuple $\beta = (\beta_0, \beta_1, \dots, \beta_n)$ with $\beta_0 = 1$ is called a feasible solution to Problem (II) if it satisfies (33) and (34), and an optimal solution if γ is minimized.

We now invoke the following theorem from linear programming theory:

Theorem 9 ([65])

- (a) If B is a feasible solution to Problem (I) and β is a feasible solution to Problem (II) then $g \leq \gamma$.
- (b) Optimal solutions exist to both Problems, and the optimal values of g and γ are equal (to g_{\max}).
- (c) If B is an optimal solution to (I) and β is an optimal solution to (II), then

$$\beta_k \left(Q_k(0) + \sum_{i=d}^n B_i Q_k(i) \right) = 0, \quad k = 1, \dots, n \quad (35)$$

and

$$B_i \left(\sum_{k=0}^n \beta_k Q_k(i) \right) = 0, \quad i = d, \dots, n. \quad (36)$$

- (d) Conversely, if a pair of feasible solutions B, β satisfy (35) and (36), then they are optimal solutions.

Suppose the association scheme is such that $Q_k(x)$ is a polynomial in x of degree k . (This includes the Hamming and Johnson schemes, as we have seen.) The $Q_k(x)$ are a family of orthogonal polynomials. Th. 9 can now be used to obtain another upper bound on $|Y|$.

Theorem 10 The second version of the linear programming bound for codes (Delsarte [11]).

Suppose a polynomial $\beta(x)$ of degree at most n can be found with the following properties. Let us write

$$\beta(x) = \sum_{k=0}^n \beta_k Q_k(x) . \quad (37)$$

Then $\beta(x)$ should satisfy

$$\beta_0 = 1 , \quad (38a)$$

$$\beta_k \geq 0 \quad \text{for } k = 1, \dots, n , \quad (38b)$$

$$\beta(i) \leq 0 \quad \text{for } i = d, \dots, n .$$

Then if Y is any code with minimum distance d ,

$$|Y| \leq \beta(0) .$$

Proof If such a $\beta(x)$ can be found, then $(\beta_0, \dots, \beta_n)$ is a feasible solution to Problem (II), since (33) and (34) hold, and $\gamma = \beta(0) - 1$. The theorem follows from Th. 9(a). Q. E. D.

Application to Error-Correcting Codes

Next we describe how these bounds have been applied to error-correcting codes in the Hamming and Johnson schemes. In the Hamming scheme, McEliece et al. [55] have obtained excellent numerical results by using the simplex algorithm and a computer. Delsarte et al. [22] have obtained preliminary numerical results for the Johnson scheme.

For theoretical purposes the second version of the linear programming bound is easier to use. This turns out to be a very powerful technique. For example Delsarte [11], [14] has derived the Plotkin, Singleton, sphere-packing and Grey bounds in this way. We illustrate the technique with three examples.

Theorem 11 The Plotkin bound [60]

If \mathcal{C} is an (n, M, d) error-correcting code with $n < 2d$, then

$$M \leq \frac{2d}{2d-n}$$

Proof We use Th. 9a, taking $\beta(x)$ to be a polynomial of degree 1. The polynomials $Q_k(x)$ in Eq. (37) are now Krawtchouk polynomials. Thus $\beta(x)$ has the form

$$\beta(x) = 1 + \beta_1 K_1(x; n) = 1 + \beta_1(n-2x) .$$

The best choice for β_1 to satisfy (38) is to make $\beta(d) = 0$, i. e., $\beta_1 = 1/(2d-n)$. Then $\beta(x) = (2d-2x)/(2d-n)$, and $\beta(0) = 2d/(2d-n)$. The theorem now follows from Th. 9a. Q. E. D.

Theorem 12 (Johnson [40, Th. 3]; Delsarte [14])

If \mathcal{C} is a (V, M, δ) error-correcting code in which every code-word has weight n , then

$$M \leq \frac{\delta V}{\delta V - n(V-n)} ,$$

provided $n(V-n) < \delta V$.

Proof \mathcal{C} is a code in the Johnson scheme, with minimum distance δ . The theorem is now proved in the same way as Th. 11, taking $\beta(x)$ to have degree 1 and using Eq. (29). Q. E. D.

Theorem 13 (The Singleton bound [66], [14])

If \mathcal{C} is an (n, M, d) error-correcting code then

$$M \leq 2^{n-d+1} .$$

Proof Let us use

$$\beta(x) = 2^{n-d+1} \prod_{i=d}^n \left(1 - \frac{x}{i}\right)$$

in Th. 10. Certainly (38c) is satisfied. Since the Krawtchouk polynomials are orthogonal, Eq. (25), the coefficients of the expansion

$$\beta(x) = \sum_{k=0}^n \beta_k K_k(x;n)$$

are given by

$$\begin{aligned} \beta_k &= \frac{1}{2^n} \sum_{i=0}^n \beta(i) K_1(k;n) \\ &= \frac{1}{2^{d-1}} \sum_{i=0}^n \binom{n-i}{n-d+1} K_1(k;n) / \binom{n}{d-1} \\ &= \binom{n-k}{d-1} / \binom{n}{d-1}, \quad \text{from Eq. (27) ,} \end{aligned}$$

for $k = 0, \dots, n-d+1$, and $\beta_k = 0$ for $k = n-d+2, \dots, n$. Thus (38a), (38b) are satisfied. The result follows from Th. 10, since $\beta(0) = 2^{n-d+1}$.

Q. E. D.

Applications to Designs

A code Y in an association scheme, with distance distribution (B_0, \dots, B_n) , will be called a t-design if

$$B_1^t = \dots = B_t^t = 0 .$$

Then t is called the strength of Y . The connection with the usual designs in statistics is given by:

Theorem 14 (Delsarte [14], [15])

A t -design Y in the Johnson association scheme is equivalent to

a classical t -(V, k, λ) design. (That is, a family of k -subsets, called blocks, of a V -set, such that any t -subset of the V -set is contained in exactly λ blocks.) Also a t -design in the Hamming association scheme is equivalent to an orthogonal array of strength t .

Again the linear programming approach has led to a number of bounds on t -designs (see [14], [15], [22]).

§8 Properties of Perfect Codes

Let Y be a code of minimum distance d in a metric association scheme (see §6). Then Y is called an e -perfect code if the spheres

$$S_e(y) = \{x \in X: \rho(x, y) \leq e\}, \quad y \in Y,$$

of radius $e = \lfloor \frac{1}{2}(d-1) \rfloor$ about the codewords include all points of X . (These spheres are disjoint by the definition of d .) This definition includes perfect error-correcting codes in the Hamming scheme as a special case. The distance distribution of an e -perfect code is an extremal solution to the linear programming Problem (I), and hence Th. 9c can be applied to give:

Theorem 15 (Delsarte [14])

If an e -perfect code exists in a metric association scheme, then the sum polynomial $\Psi_e(z)$ of Eq. (30) has e distinct zeros in the set $\{z_1, \dots, z_n\}$.

Corollary 16 (Lloyd [50])

If a perfect $(n, M, d=2e+1)$ error-correcting code exists, then the Krawtchouk polynomial $K_e(x-1; n-1)$ has e distinct zeros in the range $[1, n]$.

This theorem was the basis for the recent proof by Tietäväinen and Van Lint that we know all the perfect error-correcting codes, see [49]. Other applications of Th. 15 can be found in [14], [29], and [49]. Perfect codes in graphs have been studied by Biggs [3a], [4a].

Acknowledgments

I should like to thank Philippe Delsarte, Jean-Marie Goethals, Jessie MacWilliams and Colin Mallows for many helpful discussions.

REFERENCES

1. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, N. Y. 1968.
2. E. R. Berlekamp, Goppa codes, *IEEE Trans. Info. Theory*, 19 (1973), 590-592.
3. N. L. Biggs, *Finite Groups of Automorphisms*, London Math. Soc. Lecture Notes Series, No. 6, Cambridge Univ. Press, Cambridge, 1971.
- 3a. N. L. Biggs, Perfect codes in graphs, *J. Combinatorial Theory*, 15B (1973), 289-296.
4. N. L. Biggs, *Algebraic Graph Theory*, Cambridge Univ. Press, London, 1974.
- 4a. N. L. Biggs, Perfect codes and distance-transitive graphs, in *Combinatorics*, edited by T. P. McDonough and V. C. Mavron, London Math. Soc., Lecture Notes No. 13, Cambridge Univ. Press, Cambridge, 1974, pp. 1-8.
5. R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacif. J. Math.*, 13 (1963), 389-419.
6. R. C. Bose and D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Stat.*, 30 (1959), 21-38.
7. R. C. Bose and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, *J. Amer. Stat. Assoc.*, 47 (1952), 151-184.
8. M. Burrow, *Representation Theory of Finite Groups*, Academic Press, N.Y., 1965.

9. P. J. Cameron, Suborbits in transitive permutation groups, in *Combinatorics*, M. Hall, Jr., and J. H. Van Lint, editors, *Math. Centre Tracts* 57 (1974), 98-129 (Math. Centre, Amsterdam).
10. R. M. Damerell, On Moore graphs, *Proc. Comb. Phil. Soc.*, 74 (1973), 227-236.
11. P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Research Reports*, 27 (1972), 272-289.
12. P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control* 23 (1973), 407-438.
14. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Reports Supplements*, No. 10, 1973.
15. P. Delsarte, The association schemes of coding theory, in *Combinatorics*, edited by M. Hall, Jr., and J. H. Van Lint, *Math. Centre Tracts*, 55 (1974), 139-157 (Math. Centre, Amsterdam).
16. P. Delsarte, Association schemes in certain lattices, to appear.
17. P. Delsarte, Association schemes and t-designs in regular semi-lattices, to appear.
18. P. Delsarte, Properties and applications of the recurrence $F(i+1, k+1, n+1) = q^{k+1} F(i, k+1, n) - q^k F(i, k, n)$, *SIAM J. Appl. Math.* to appear.
19. P. Delsarte, The association scheme of bilinear forms over $GF(q)$, to appear.
20. P. Delsarte and J. M. Goethals, Alternating bilinear forms over $GF(q)$, *J. Combinatorial Theory*, to appear.
21. P. Delsarte, J. M. Goethals, and J. J. Seidel, Bounds for systems of lines, and Jacobi polynomials, to appear.
22. P. Delsarte, W. Haemers and C. Weug, Unpublished.
23. M. Doob, On graph products and association schemes, *Utilitas Mathematica*, 1 (1972), 291-302.
24. C. F. Dunkl, A Krawtchouk polynomial addition theorem and wreath products of symmetric groups, to appear.

25. C. F. Dunkl and D. E. Ramirez, Krawtchouk polynomials and the symmetrization of hypergroups, *SIAM J. Math. Anal.*, 5 (1974), 351-366.
26. P. J. Eberlein, A two parameter test matrix, *Math. Comp.* 18 (1964), 296-298.
27. J. M. Goethals, Two dual families of nonlinear binary codes, *Electronics Letters*, 10 (1974), 471-472.
28. J. M. Goethals and J. J. Seidel, Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.*, 22 (1970), 597-614.
29. J. M. Goethals and H. C. A. van Tilborg, Uniformly packed codes, to appear.
30. V. D. Goppa, A new class of linear correcting codes, *Problems of Information Transmission* 6 (1970), 207-212.
31. H. J. Helgert, Alternant codes, *Information and Control* 26 (1974), 369-380.
32. H. J. Helgert and R. D. Stinaff, Minimum-distance bounds for binary linear codes, *IEEE Trans. Info. Theory*, 19 (1973), 344-356.
33. D. G. Higman, Finite permutation groups of rank 3, *Math. Zeit.*, 86 (1964), 145-156.
34. D. G. Higman, Intersection matrices for finite permutation groups, *J. Algebra* 4 (1967), 22-42.
35. D. G. Higman, Characterization of families of rank 3 permutation groups by the subdegrees I and II, *Archiv. Math.* 21 (1970), 151-156 and 353-361.
36. D. G. Higman, Combinatorial Considerations about Permutation Groups, Lecture notes, *Math. Inst.*, Oxford, 1972.
37. D. G. Higman, Invariant relations, coherent configurations, and generalized polygons, in *Combinatorics*, edited by M. Hall, Jr., and J. H. van Lint, *Math. Centre Tracts*, 57 (1974), 27-43 (Math. Centre, Amsterdam).
38. D. G. Higman, Coherent configurations, part I: ordinary representation theory, *Geometriae Dedicata*, to appear.

39. A. T. James, The relationship algebra of an experimental design, *Ann. Math. Stat.*, 28 (1957), 993-1002.
40. S. M. Johnson, A new upper bound for error-correcting codes, *IEEE Trans. Info. Theory*, 8 (1962), 203-207.
41. S. M. Johnson, On upper bounds for unrestricted binary error-correcting codes, *IEEE Trans. Info. Theory*, 17 (1971), 466-478.
42. S. M. Johnson, Upper bounds for constant weight error correcting codes, *Discrete Math.*, 3 (1972), 109-124.
43. J. Justesen, A class of constructive asymptotically good algebraic codes, *IEEE Trans. Info. Theory*, 18 (1972), 652-656.
44. M. Kratchouk, Sur une généralisation des polynômes d'Hermite, *Comptes Rendus*, 189 (1929), 620-622.
45. M. Krawtchouk, Sur la distribution des racines des polynomes orthogonaux, *Comptes Rendus*, 196 (1933), 739-741.
46. V. I. Levenshtein, Upper bounds for fixed-weight codes, *Problems of Information Transmission*, 7 (1971), 281-287.
47. V. I. Levenshtein, On minimal redundancy of binary error-correcting codes (In Russian), *Problemy Peredachi Informatsii*, 10 (No. 2, 1974), 26-42.
48. J. H. van Lint, *Coding Theory*, Lecture Notes in Math. 201, Springer-Verlag, New York, 1971.
49. J. H. van Lint, Recent results on perfect codes and related topics, in *Combinatorics*, edited by M. Hall, Jr., and J. H. van Lint, *Math. Centre Tracts*, 55 (1974), 158-178 (Math. Centre, Amsterdam).
50. S. P. Lloyd, Binary block coding, *Bell Syst. Tech. J.*, 36 (1957), 517-535.
51. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.*, 42 (1963), 79-94.
52. F. J. MacWilliams and N. J. A. Sloane, *Combinatorial Coding Theory*, North-Holland, Amsterdam (in preparation).
53. F. J. MacWilliams, N. J. A. Sloane, and J. M. Goethals, The MacWilliams identities for nonlinear codes, *Bell Syst. Tech. J.*, 51 (1972), 803-819.

54. M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*, Allyn and Bacon, Boston, 1964.
55. R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, unpublished.
56. R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, private communication, March 14, 1975.
57. M. Ogasawara, *A necessary condition for the existence of regular and symmetrical PBIB designs of T_m type*, Inst. of Stat. Mimeo Series No. 418, Univ. of N. Carolina, Chapel Hill, N. C., Feb. 1965.
58. J. Ogawa, *The theory of the association algebra and the relationship algebra of a partially balanced incomplete block design*, Institute of Statistics, Mimeograph Series No. 224, Univ. of North Carolina, Chapel Hill, N. C., April 1959.
59. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd Ed., MIT Press, Cambridge, Mass., 1972.
60. M. Plotkin, *Binary codes with specified minimum distances*, IEEE Trans. Info. Theory, 6 (1960), 445-450.
61. D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*, Wiley, N.Y., 1971.
62. J. J. Seidel, *Strongly regular graphs*, pp. 185-198 of *Recent Progress in Combinatorics*, W. T. Tutte, ed., Academic Press, N.Y., 1969.
63. J. J. Seidel, *Graphs and two-graphs*, Proc. 5th Southeastern Conference on Combinatorics, Graph Theory, Computing, Boca Raton, Florida, 1974.
64. V. M. Sidelnikov, *Upper bounds for number of words in a binary code with given minimal distance (In Russian)*, Problemy Peredachi Informatsii, 10 (No. 2, 1974), 43-51.
65. M. Simonard, *Linear Programming*, Prentice-Hall, N.J., 1966 (Chapter 5).

66. R. C. Singleton, Maximum distance q -nary codes, *IEEE Trans. Info. Theory*, 10 (1964), 116-118.
67. N. J. A. Sloane, A survey of constructive coding theory, and a table of binary codes of highest known rate, *Discrete Math.*, 3 (1972), 265-294.
- 67a. D. H. Smith, Distance-transitive graphs, in *Combinatorics*, edited by T. P. McDonough and V. C. Mavron, London Math. Soc., Lecture Notes No. 13, Cambridge Univ. Press, Cambridge, 1974, pp. 145-153.
68. G. Szegő, *Orthogonal Polynomials*, Vol. 23, Amer. Math. Soc., Providence, R. I., 1967.
- 68a. J. H. M. Wedderburn, *Lectures on Matrices*, Dover, N.Y., 1964.
69. L. R. Welch, R. J. McEliece, and H. Rumsey, Jr., A low-rate improvement on the Elias bound, *IEEE Trans. Info. Theory*, 20 (1974), 676-678.
70. H. Wielandt, *Finite Permutation Groups*, Academic Press, N.Y., 1964.
71. S. Yamamoto, Y. Fujii and N. Hamada, Composition of some series of association algebras, *J. Sci. Hiroshima Univ., Ser. A-I*, 29 (1965), 181-215.

Bell Laboratories
Murray Hill, New Jersey 07974