Send subscription orders to

B.V. UITGEVEVERSMAATSCHAPPIJ CENTREX
(Centrex Publishing Co.)
Cederlaan 4
P.O. Box 76
EINDHOVEN (Netherlands)

PHIL ESEARCH REPORTS SUPPLEMENTS 1973 No. 10

PHILIPS RESEARCH REPORTS SUPPLEMENTS

PHILIPS

PHILIPS RESEARCH LABORATORIES

Philips Res. Repts Suppl. 1973 No. 10

Printed in the Netherlands

AN ALGEBRAIC APPROACH TO THE ASSOCIATION SCHEMES OF CODING THEORY *)

BY

P. DELSARTE

*) Thesis, Université Catholique de Louvain, June 1973.
Promotor: Professor Dr J. M. Goethals.

Philips Res. Repts Suppl. 1973, No. 10.

Acknowledgment

I wish to express my deepest gratitude to Professor Dr J.-M. Goethals for his valuable advice and encouragement during the preparation of this thesis of which he accepted to be the promotor. Many thanks are also due to Professor Dr V. Belevitch, director of the MBLE Research Laboratory, who allowed me to carry on the research reported here and whose teaching had the greatest effect upon the conception of my work.

I am much indebted to Professor Dr J. J. Seidel, of the Technical University Eindhoven, for calling my attention to some combinatorial aspects of coding theory and I am pleased to thank him for his helpful assistance. Finally, I gratefully acknowledge valuable information brought to me by Dr P. J. Cameron, of Oxford University, by Dr J. Doyen, of the University of Brussels, and by Dr F. J. Mac Williams, of Bell Telephone Laboratories at Murray Hill.

Abstract

The present work is a contribution to the algebraic theory of association schemes, where special emphasis is put on concepts arising from the theory of error-correcting codes and of some combinatorial designs. The main idea is to characterize a subset in a given association scheme by its distribution with respect to the relations of the scheme. This yields some powerful methods for the study of subsets whose specific properties can be expressed in terms of their distribution. Various theorems are obtained in this way about generalized concepts of codes and t-designs.

CONTENTS

List of symbols

$\mathbf{a}$	inner distribution of Y
A	Bose–Mesner algebra of (X,R)
B	distribution matrix of Y
D_i	adjacency matrix of the relation R_i
d	minimum distance of a code
d_H	Hamming distance
d_J	Johnson distance
$E_k(u)$	Eberlein polynomial of degree k
G_k	matrix $[H_0, H_1, \ldots, H_k]$
H_k	characteristic matrix of Y
$H(n,q)$	Hamming scheme of length n over a q-ary alphabet
I	identity matrix
J	all-one matrix
J_k	minimal idempotent of A
$J(n,v)$	Johnson scheme of weight n and length v
$K_k(u)$	Krawtchouk polynomial of degree k
M	subset of N, containing zero
N	set of integers $0, 1, \ldots, n$
P	first eigenmatrix of (X,R)
$p_{i,j}^{(k)}$	intersection number of (X,R)
Q	second eigenmatrix of (X,R)
R	set of $n+1$ relations $R_0, R_1, \ldots, R_n$ on X
r	external distance of a code
S	orthogonal matrix diagonalizing A
s	degree of a design
T	subset of N, not containing zero
t	maximum strength of a design
v_i	valence of the relation R_i
w_H	Hamming weight
(X,R)	association scheme on the set X
Y	subset of X (code, design)
Y^0	dual of an additive code Y
(Y,R^Y)	restriction of (X,R) to Y
δ	designed distance
μ_k	rank of the matrix J_k
ϱ	distance function of a metric scheme
τ	designed strength
$\Phi_k(z)$	polynomial of degree k, specifying an eigenmatrix
ϕ_Y	vector characterizing Y as a subset of X
$\Psi_k(z)$	sum polynomial $\Phi_0(z) + \Phi_1(z) + \ldots + \Phi_k(z)$

$\lvert\ \rvert$	cardinality of a set, absolute value of a number
$[\ ]$	largest integer not exceeding the argument
$\lVert\ \rVert$	Hermitian norm of a vector or a matrix
$\langle , \rangle$	inner product on an Abelian group
D^{T}	transpose of a matrix D
$\bar{D}$	conjugate transpose of D
$\mathbf{F}(X)$	set of $\lvert X\rvert$-vectors over the field $\mathbf{F}$
$\mathbf{F}(X,X')$	set of $\lvert X\rvert \times \lvert X'\rvert$ matrices over $\mathbf{F}$
$\mathbf{F}[z]$	set of polynomials in z over $\mathbf{F}$
$\mathbf{F}_k[z]$	subset of polynomials of degree $\leqslant k$ in $\mathbf{F}[z]$

1. INTRODUCTION

Research in coding theory may be divided into three main parts. The first way, opened by Shannon [63]), consists in a study of the theoretical possibilities offered by the principle of coding for correction of errors in certain communication systems (cf. for instance Gallager [22])). At this level there already arise some algebraic concepts, such as the *minimum distance* between distinct codewords; among codes having the same *length* n and the same minimum distance d, the best is the one containing the largest number of words.

It is therefore natural that many authors applied themselves to construct "good" codes of fixed parameters n and d. In fact, for both theoretical and practical reasons, most researchers, following Slepian [66]) in that respect, restricted their interest to *linear codes* defined over finite fields.

The above aspects are certainly the most important if, adopting the point of view of information theory, one considers codes as devoted to the correction of errors occurring on a noisy channel. The reader will find an excellent treatment of *error-correcting codes* in Berlekamp's book [6]) and a recent survey of constructive coding theory in a paper by Sloane [67]), including a table of the best known binary codes.

It remains to be specified what constitutes the third approach, the one to which belongs the present work. In the most general sense, it is the *algebraic and combinatorial theory of codes* defined to be any subsets in some finite metric spaces, namely the Hamming spaces [29]). This covers subjects as various as the following ones: *upper bounds* to the number of words in codes of given length and minimum distance (cf. for instance Johnson [33])), the *duality* in linear codes, introduced by MacWilliams [46]), or also the theory of *perfect codes* (cf. Van Lint [42])) and of some other combinatorial configurations (cf. for instance Assmus and Mattson [4])). Let us already mention a rather precise question which appears throughout the theory: what can be said about a code when its *distance distribution* is known? (Cf. Delsarte [14,16]).)

The starting point of the present work was the simple observation that the distance relations in a Hamming space form an *association scheme* as defined by Bose and Shimamoto [10]). It turns out that this yields numerous results in classical coding theory. Moreover, many theorems obtained in this manner can be extended to more-general schemes than those of Hamming spaces; in particular to the "*Johnson schemes*", which are themselves interesting in coding theory for the study of constant weight codes considered by Johnson [34]).

These are the reasons why the author decides to use, from the beginning, the method of association schemes which really seems to be the most suitable for several aspects of algebraic and combinatorial theory of codes. Let us specify here that the combinatorial configurations in which one will be interested are the *orthogonal arrays* introduced by Rao [59]) and the *t-designs* de-

fined by Hanani [30]); these arise quite naturally in the study of Hamming and Johnson schemes, respectively.

After having briefly mentioned its background, let us now give a summarizing account of this thesis.

Chapter 2 is an introduction to the *association schemes* (for short, the schemes) *with n classes* on a finite set X. Adopting in sec. 2.1 a slightly more general definition of a scheme than the original concept, its *Bose–Mesner algebra* [9]) is described (sec. 2.2), that is, the $(n+1)$-dimensional commutative algebra generated by the adjacency matrices $D_0 = I, D_1, \ldots, D_n$ of the relations R_k of the given scheme.

One is led to consider the eigenvalues of the D_k and to define (sec. 2.3) the *eigenmatrices* P and Q of the scheme as follows: the element $P_{i,k}$ of the square matrix P, of order $n+1$, is the ith eigenvalue of D_k, for $i, k = 0, 1, \ldots, n$. Then Q is defined to be $|X| P^{-1}$. It turns out that the eigenmatrices play a very important role in the theory. For this reason, their properties are examined in detail; especially, it is shown that each of them satisfies a certain *orthogonality relation*.

Some examples are given in sec. 2.4; in particular, a short description of the case $n = 2$ which corresponds to the *strongly regular graphs* introduced by Bose [8]). Thereafter (sec. 2.5) it is indicated how a scheme with s classes on a set F can be *extended*, in a natural way, to produce a scheme with $\binom{m+s}{s} - 1$ classes on the set F^m. The simplest case, $s = 1$, yields the Hamming scheme of length m over the "alphabet" F. Other schemes of some interest in coding theory are also obtained in this manner.

Finally, in sec. 2.6, a concept of *duality* is introduced which applies to certain types of schemes; essentially, those whose automorphism group contains a regular Abelian subgroup. When applied to strongly regular graphs, this duality has the following property: a graph has the same parameters as its dual (or as the complement of its dual) if and only if it is of the Latin square type, in the sense of Mesner [52]).

In chapter 3 the concerns are already near to those occurring in coding theory: one examines the subsets Y of a set X on which an association scheme is defined. The way in which the pairs of points in Y^2 and in $X \times Y$ are distributed with respect to the relations R_i is the subject of sec. 3.1; first, the *inner distribution* of Y is defined to be the $(n+1)$-tuple $\mathbf{a} = (a_0, \ldots, a_n)$ where a_i is the average number of points of Y being ith associates of a fixed point of Y; next, the *distribution matrix* of Y is defined in a similar manner.

A result which turns out to be very fruitful is the fact that the product $\mathbf{a}Q$ of the inner distribution of Y by the eigenmatrix Q is an $(n+1)$-tuple o-nonnegative real numbers. This observation leads to certain *linear-programf ming problems* (sec. 3.2) defined by submatrices of P or Q.

The concept of a clique is the subject matter of sec. 3.3. For a given subset

M of $N = \{0, 1, \ldots, n\}$, with $0 \in M$, a subset Y of X is called an *M-clique* if the component a_i of its inner distribution is zero for all $i \notin M$. One takes the opportunity to generalize, in sec. 3.3.1, a theorem due to Elias (cf. Berlekamp [6]), p. 318) and to locate the place of the Johnson schemes in coding theory. Section 3.3.2 contains the application of the linear-programming method to the study of cliques: an upper bound is obtained to the number of points in an M-clique. An interesting consequence is that, when Y is an M-clique and Z an M-coclique (i.e. an $\bar{M}$-clique with $\bar{M} = N - M \cup \{0\}$), then $|Y|\,|Z| \leqslant |X|$ holds.

A "dual" concept is introduced in sec. 3.4. For a given subset T of $N - \{0\}$, a subset Y of X is called a *T-design* if its inner distribution $\mathbf{a}$ has the property that the components $(\mathbf{a}Q)_k$ of the product $\mathbf{a}Q$ are zero for all $k \in T$ (it turns out that this purely algebraic definition corresponds, in some cases, to interesting combinatorial configurations). The use of the linear-programming method yields a lower bound to the number of points in a T-design. The last point (sec. 3.6) concerns the *characteristic matrices* [16]) of a subset $Y \subseteq X$. These provide a useful tool especially in the theory of designs.

Chapter 4 is entirely devoted to coding theory; more specifically, to the Hamming schemes (sec. 4.1) and the Johnson schemes (sec. 4.2).

The *Hamming scheme* $H(n,q)$ is defined by the distance relations between n-tuples over a q-ary alphabet. In sec. 4.1.1 the explicit form of the eigenmatrices P and Q is obtained; it turns out that they are equal and that $P_k(i) = P_{i,k}$ can be considered as a *Krawtchouk polynomial* [37]) of degree k in the variable i. Equivalently, $P\ (= Q)$ is the matrix of the *MacWilliams transform* (cf. MacWilliams [46]); MacWilliams, Sloane and Goethals [48]); Delsarte [16])).

The linear-programming bound is then applied in sec. 4.1.2 to the codes of length n over a q-ary alphabet F; in particular, to the codes with a *designed minimum distance* δ, i.e. the M-cliques in $H(n,q)$ with $M = \{0, \delta, \delta+1, \ldots, n\}$. The binary case is examined more in detail and the method is illustrated by a numerical example.

Reformulating a previous result [14]), we exhibit in sec. 4.1.3 the meaning of T-designs in $H(n,q)$ for a set T of the form $\{1, 2, \ldots, \tau\}$: they are the *orthogonal arrays* of strength τ with n rows over F. This concludes the general study of Hamming schemes; the particular case of additive codes is postponed to the end of this work.

For $F = \{0,1\}$ and integers n, v such that $1 \leqslant n \leqslant v/2$, the set of v-tuples of weight n in $H(v,2)$ itself is an association scheme, with n classes, for the distance relations; one calls it a *Johnson scheme*, using the notation $J(n,v)$. In sec. 4.2.1 explicit formulas are derived for the eigenmatrices P and Q of $J(n,v)$. It turns out that these matrices have "polynomial properties" similar to those of the Hamming schemes: $Q_{i,k}$ and $P_{i,k}$ can be represented by means of

polynomials of degree k in the variables i and $i(v+1-i)$, respectively, which are in fact related to some formulas discovered by Eberlein [19]). Thereafter, the use of the linear-programming bound in the theory of binary constant-weight codes is briefly explained (sec. 4.2.2).

The combinatorial meaning of T-designs with $T = \{1, 2, \ldots, \tau\}$ appears to be at least as interesting in the Johnson schemes as in the Hamming schemes: it is proved in sec. 4.2.3 that they are nothing but the classical *τ-designs* $S_\lambda(\tau,n,v)$. So the linear-programming method yields a lower bound to the parameter λ of τ-designs with fixed τ, n and v; as an example, it is shown that 4-designs $S_5(4, 8, 17)$ do not exist.

Treating simultaneously the two types of schemes (Hamming and Johnson) we show in sec. 4.3 how certain classical inequalities of coding theory are implied by the linear-programming bound. Referring to the authors who discovered them for the Hamming spaces, the names are used of the Plotkin (sec. 4.3.1), Singleton (sec. 4.3.2) and Hamming (sec. 4.3.2) inequalities (cf. for instance Berlekamp [6]). The specific properties of codes achieving each of the three bounds are also briefly described.

Chapter 5 is central. Starting from polynomial properties which the Hamming and Johnson schemes have in common, in sec. 5.1 an axiomatic definition is given of "polynomial schemes". Roughly spoken, an association scheme is said to be *P-polynomial* if, for a fixed k and i running through N, the element $P_{i,k}$ of the eigenmatrix P is representable by means of a polynomial $\Phi_k(z_i)$ of degree k in a suitable variable z_i. The concept of a *Q-polynomial* scheme is defined analogously from the properties of the eigenmatrix Q.

The orthogonality relations satisfied by P and Q mean that, for a P- or Q-polynomial scheme, the set $\{\Phi_k(z)\}$ is a family of *orthogonal polynomials* (cf. Szegö [70]). Some results about this classical theory are recalled in sec. 5.1.1. It is also shown that the *sum polynomials* $\Psi_k(z) = \Phi_0(z) + \ldots + \Phi_k(z)$, which play an important role in the following, form themselves a family of orthogonal polynomials. Next (sec. 5.1.2) a generalization is obtained of an inequality due to MacWilliams [44]), which has a certain significance in theory of codes and designs.

A thorough study of P-polynomial and Q-polynomial schemes is undertaken in secs 5.2 and 5.3, respectively. Although both theories are formally similar, it is indeed better to treat them separately.

In sec. 5.2.1 it is first shown that a scheme of relations R_i is P-polynomial if and only if it is *metric*, in the sense that the mapping ϱ of X^2 onto N defined by $\varrho(x,y) = i$ for $(x,y) \in R_i$ is a "nondegenerate distance". The metric schemes are in fact a particular case of the so-called perfectly regular graphs (cf. Higman [31]). The inner distribution of a subset Y of X, or a "code", is called its *distance distribution*. Then two fundamental parameters of a code are introduced, from its distance distribution $\mathbf{a}$: the *minimum distance* d and the *external distance* r. The meaning of d is clear. As for r, defined to be the number of nonzero components $(\mathbf{a}Q)_k$ of index $k \neq 0$, its meaning appears afterwards. Application of the MacWilliams inequality yields $r \geqslant [(d-1)/2]$; it is shown later on that equality is a criterion for "perfect codes".

In the framework of metric schemes we examine in sec. 5.2.2 the straightforward extension of the *Hamming bound* [29]) for codes with given minimum distance d, and the corresponding concept of *perfect codes* of order $e = [(d-1)/2]$. The most interesting result is a generalization of the Lloyd theorem (cf. for instance Lenstra [39])): a perfect code of order e in a P-polynomial scheme can only exist if the sum polynomial $\Psi_e(z)$, called here the *Lloyd polynomial*, has e distinct zeros in the set $\{z_1, \ldots, z_n\}$. An explicit formula is also obtained for the distance distribution of a perfect code, only depending on e and on the "parameters" of the scheme.

The distribution matrix B of a code Y, examined in sec. 5.2.3, can be defined as follows: the rows and columns being numbered by the points $x \in X$ and the integers $i \in N$, respectively, the (x,i)-entry of B is the number of points $y \in Y$ at distance $\varrho(x,y) = i$ from x. It is shown that the knowledge of the distance distribution and of the columns $B_0, B_1, \ldots, B_{r-1}$ is sufficient to determine the whole matrix B. In addition, the result explains the meaning of the external distance r: each point of X is at distance less than or equal to r from at least one point of Y. Certain "regularity properties" of codes are also examined. In particular, it is proved that $d \geqslant 2r-1$ is a sufficient condition for a code to be *completely regular* in the sense that any row $B(x)$ of the distribution matrix B only depends on the minimum distance between the given x and the points of Y. An example concludes the section; the distribution matrix is computed for the Steiner system $S(5, 8, 24)$ in the Johnson scheme $J(8, 24)$.

The structure of sec. 5.3 on Q-polynomial schemes looks like that of the preceding one, the "designs of given maximum strength" playing here a similar role as the "codes of given minimum distance". We describe more in detail the concept of *Q-polynomial* schemes in sec. 5.3.1, without being able yet to give a combinatorial formulation of it.

The property of subsets Y of X in which one is most interested is that of being a T-design with $T = \{1, 2, \ldots, \tau\}$ for some integer τ. Then Y is simply said to be a *τ-design*, by extension of the usual notion. Two parameters, determined from the inner distribution $\mathbf{a}$, play an important role: the *maximum strength* t and the *degree* s. The first one is the largest integer τ such that Y is a τ-design, the latter is the number of nonzero components of the n-tuple $(a_1, \ldots, a_n)$. Application of the MacWilliams inequality yields $s \geqslant [t/2]$; it is shown later on that equality is a criterion for the so-called "tight designs".

Let us emphasize here the formal duality between the theories of secs 5.2 and 5.3 resulting from the following correspondence between the parameters: $d \leftrightarrow d' = t+1$, $r \leftrightarrow r' = s$. This duality was already present in a paper de-

voted by the author [14]), at least implicitly, to the Hamming spaces, for which the four parameters are well defined.

The inequality obtained by Rao [59]) for orthogonal arrays of strength t in $H(n,q)$ and, more recently, by Wilson and Ray-Chaudhuri [75]) for classical t-designs in $J(n,v)$ is extended, in sec. 5.3.2, to t-designs in any Q-polynomial scheme. By extension of Wilson's terminology [74]), a t-design is called a *tight design* of order $e = [t/2]$ whenever it achieves this generalized *Rao–Wilson bound*. In the case of Hamming schemes, the tight designs are in fact equivalent to the generalized Hadamard codes, as defined by the author [14]). A necessary condition is obtained for the existence of a tight design of order e, very similar to the Lloyd theorem on perfect codes, in terms of the sum polynomial $\Psi_e(z)$ called here the *Wilson polynomial*. The result reduces to theorems obtained by Wilson [74]) and by the author [14]) for the Johnson and Hamming schemes, respectively.

The discussion of Q-polynomial schemes ends, in sec. 5.3.3, with some results on regularity properties of a design Y of given maximum strength t and degree s. Essentially, it is shown that $t \geqslant 2s - 2$ is a sufficient condition for Y to define a *subscheme*. This result was known for $s = 2$ in the cases of Johnson schemes and Hamming schemes (for linear codes) with the following respective terminologies: the quasi-symmetric block designs (cf. Goethals and Seidel [25])) and the two-weight projective codes (cf. Delsarte [15])). A few examples are given to illustrate the theory; in particular, the remarkable codes discovered by Kerdock [36]) are examined in some detail.

Chapter 6 treats the *additive codes* (= group codes over an Abelian group F) in Hamming schemes, which are a generalization of the *linear codes* over finite fields (cf. Assmus and Mattson [2]) and MacWilliams [45]) for theoretical bases and fundamental results on linear codes). In the class of additive codes the formal duality emphasized above becomes quite precise.

A general concept of *duality among subgroups* of a finite Abelian group is given in sec. 6.1 by use of the group characters. As the additive codes of length n over F by definition are the subgroups of the Abelian group F^n, the concept applies to this class of codes. One obtains, in sec. 6.2, a version of the *MacWilliams identities* on the weight (or distance) distributions of dual additive codes (cf. MacWilliams [46]) and Pless [55]) for the original theorem on linear codes). The result implies that the values of the parameters $d' = t + 1$ and $r' = s$ of a code are nothing but those of d and r, respectively, for the dual code.

Finally, the question of deciding whether an additive code Y of degree s defines a subscheme of $H(n,q)$, with s classes, is examined in sec. 6.3. The result is the following: Y forms an association scheme for the distance relations if and only if the distribution matrix of its dual code contains exactly $s + 1$ distinct rows. Moreover, when this condition is satisfied, one obtains

an interesting representation of the dual scheme, in the sense of sec. 2.6, on the cosets of the dual code. The theory is applied to both Golay codes (cf. for instance Pless [56])) which define remarkable association schemes, including the strongly regular graphs discovered by Goethals and Seidel [25]), Berlekamp, Van Lint and Seidel [7]), and the author [13,15]).

2. ASSOCIATION SCHEMES

The present chapter contains elements of an algebraic theory of the association schemes defined by Bose and Shimamoto [10], which constitute a very particular case of the coherent configurations recently introduced by Higman [31].

2.1. Definitions

Let X be a finite set with at least two elements and, for any integer $n \geqslant 1$, let $R = \{R_0, R_1, \ldots, R_n\}$ be a family of $n+1$ relations R_i on X; in other words, $n+1$ subsets of the Cartesian square X^2. If (x, y) belongs to R_i, the *point* $y \in X$ will be said to be an i*th associate* of the point $x \in X$.

The pair (X,R) will be called an *association scheme with n classes* if the three following conditions are satisfied:

A1. The set R is a partition of X^2 and R_0 is the diagonal relation, i.e., $R_0 = \{(x,x) \mid x \in X\}$.

A2. For $i = 0, 1, \ldots, n$, the inverse $R_i^{-1} = \{(y,x) \mid (x,y) \in R_i\}$ of the relation R_i also belongs to R.

A3. For any triple of integers $i, j, k = 0, 1, \ldots, n$, there exists a number $p_{i,j}^{(k)} = p_{j,i}^{(k)}$ such that, for all $(x,y) \in R_k$:

$$|\{z \in X \mid (x,z) \in R_i, (z,y) \in R_j\}| = p_{i,j}^{(k)}. \tag{2.1}$$

The $p_{i,j}^{(k)}$ are called the *intersection numbers* of the scheme (X,R). Let us now consider a pair (R_i,R_j) with $R_j = R_i^{-1}$. The positive integer $v_i = p_{i,j}^{(0)}$ $(= v_j = p_{j,i}^{(0)})$ is called the *valence* of R_i (and of R_j). In fact v_i is the number of ith associates of a fixed point x:

$$v_i = |\{z \in X \mid (x,z) \in R_i\}|, \tag{2.2}$$

which is independent of x. Any relation $R_i \in X^2$ having this property will be called *regular*.

The above definition is slightly more general than the original one due to Bose and Shimamoto [10]; the latter is obtained when axiom A2 is replaced by the following.

A'2. The relations R_i are symmetric: $R_i^{-1} = R_i$ for $i = 0, 1, \ldots, n$.

In this case, the scheme (X,R) will itself be called *symmetric*. For an arbitrary association scheme (X,R), it is easy to show that the smallest partition $\bar{R}$ of X^2 satisfying A'2 and $\bar{R} \geqslant R$, namely

$$\bar{R} = \{R_i \cup R_i^{-1} \mid i = 0, 1, \ldots, n\},$$

yields a symmetric association scheme $(X,\bar{R})$, which could be called the *symmetric closure* of (X,R).

2.2. Bose–Mesner algebra

Let us first introduce some notations from matrix algebra. For two finite nonempty sets X and X', we shall denote by $\mathbf{C}(X,X')$ the set of matrices S of type $|X| \times |X'|$ over the complex field $\mathbf{C}$, where the rows and columns are numbered by the elements of X and X', respectively, the (x,x')-entry of S being written as $S(x,x')$ for $x \in X$, $x' \in X'$. In the case $|X'| = 1$ we shall omit X' in the notations, so $\mathbf{C}(X)$ denotes the set of column vectors ϕ of order $|X|$, the x-entry being $\phi(x)$. Similar notations will be used for the real field $\mathbf{R}$.

Partitions $\pi = \{X_i \mid i = 0, 1, \ldots, n\}$ and $\pi' = \{X_k' \mid k = 0, 1, \ldots, n'\}$ of the two sets X and X', respectively, induce an obvious decomposition of any matrix $S \in \mathbf{C}(X,X')$ into $(n+1)(n'+1)$ submatrices; we shall denote by $S_{i,k} \in \mathbf{C}(X_i,X_k')$, by $S_k \in \mathbf{C}(X,X_k')$ and by $S^{(i)} \in \mathbf{C}(X_i,X')$ the restrictions of S to the Cartesian products $X_i \times X_k'$, $X \times X_k'$ and $X_i \times X'$, respectively. Then, for a suitable numbering of rows and columns, we have

$$S = \begin{bmatrix} S_{0,0} & \cdots & S_{0,k} & \cdots & S_{0,n'} \\ \vdots & & & & \\ S_{i,0} & & S_{i,k} & & S_{i,n'} \\ \vdots & & & & \\ S_{n,0} & & S_{n,k} & & S_{n,n'} \end{bmatrix} = \begin{bmatrix} S^{(0)} \\ \vdots \\ S^{(i)} \\ \vdots \\ S^{(n)} \end{bmatrix} \tag{2.3}$$

$$= [\, S_0 \ \ldots S_k \ \ldots S_{n'} \,].$$

For X and X' with the same cardinality, any matrix $S \in \mathbf{C}(X,X')$ will be called *orthogonal* whenever it satisfies

$$S\bar{S} = |X|\, I, \tag{2.4}$$

where $\bar{S}$ denotes the conjugate transpose of S and I is the unit matrix of $\mathbf{C}(X,X)$. Then $\bar{S}$ is an orthogonal matrix in $\mathbf{C}(X',X)$. For the classical definitions of matrix sum and product, the set $\mathbf{C}(X,X)$ has the structure of an $|X|^2$-dimensional linear algebra over $\mathbf{C}$, having I as the multiplicative identity. As usual, a matrix $D \in \mathbf{C}(X,X)$ is called *normal* if it commutes with $\bar{D}$.

Any relation R_i is described by its *adjacency matrix* $D_i \in \mathbf{C}(X,X)$, defined as follows:

$$D_i(x,y) = \begin{cases} 1 & \text{for} \quad (x,y) \in R_i, \\ 0 & \text{for} \quad (x,y) \notin R_i. \end{cases}$$

Next, let J denote the all-one matrix: $J(x,y) = 1$ for all $x,y \in X$. Then R_i is a regular relation if and only if D_i commutes with J. In fact this is equivalent to the condition $D_i J = J D_i = v_i J$, where v_i is the valence of R_i.

The following theorem, essentially due to Bose and Mesner [9], gives an algebraic form of the axioms A2, A3 of an association scheme.

Theorem 2.1. Let $R = \{R_0, R_1, \ldots, R_n\}$ be a set of $n+1$ relations on X, satisfying A1, and define A to be the linear subspace of $\mathbf{C}(X,X)$ generated by the adjacency matrices D_i of R_i, $i = 0, 1, \ldots, n$. Then (X,R) is an association scheme, with n classes, if and only if A is a commutative $(n+1)$-dimensional subalgebra of $\mathbf{C}(X,X)$, all of whose elements are normal matrices.

Proof. Assuming that (X,R) is an association scheme, let us first prove the "only if" part of the theorem. Equation (2.1) can be written as follows:

$$D_i D_j = \sum_{k=0}^{n} p_{i,j}^{(k)} D_k, \qquad i,j = 0, 1, \ldots, n. \tag{2.5}$$

Indeed, for any $(x,y) \in X^2$, the (x,y)-entry of both members of (2.5) is equal to the number of points $z \in X$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$. Hence the linear space

$$\mathsf{A} = \{ \sum_{i=0}^{n} \alpha_i D_i \mid \alpha_i \in \mathbf{C} \} \tag{2.6}$$

is closed under matrix multiplication and, therefore, constitutes a subalgebra of $\mathbf{C}(X,X)$ whose dimension is $n+1$ since the D_i are linearly independent (by A1). It is clear that A is commutative since $p_{i,j}^{(k)} = p_{j,i}^{(k)}$ implies $D_i D_j = D_j D_i$, by (2.5). On the other hand, the matrix form of $R_j = R_s^{-1}$ is $D_j = D_s^T$. Hence the commutativity of A together with axiom A2 clearly implies that each matrix in A is normal.

Conversely, assuming that A is a commutative algebra of normal matrices, we now give the sketch of a proof for the "if" part. It can be shown that A admits a basis of Hermitian matrices (cf. the proof of theorem 2.2). Hence A is closed with respect to the transformation $D \to \bar{D}$ in $\mathbf{C}(X,X)$. From this, condition A2 readily follows. On the other hand, expressing the product $D_i D_j$ $(= D_j D_i)$ in the basis $\{D_0, \ldots, D_n\}$ of A, we obtain equations like (2.5). This being the matrix form of condition A3, we have shown that (X,R) is an association scheme.

The linear algebra (2.6) will be called the *Bose–Mesner algebra* (or BM algebra) of the association scheme (X,R). Axiom A1 implies that the matrices I and J belong to A, since $D_0 = I$ and $\sum D_i = J$. Before examining the structure of A (theorem 2.2), we need some notations and definitions. Given a partition $\pi' = \{X_k' \mid k = 0, 1, \ldots, n'\}$ of the finite set X', let us define diagonal matrices $\Gamma_k \in \mathbf{C}(X',X')$, for $k = 0, 1, \ldots, n'$, as follows:

$$\Gamma_k(x',x') = \begin{cases} 1 & \text{for} \quad x' \in X_k', \\ 0 & \text{otherwise,} \end{cases} \tag{2.7}$$

and $\Gamma_k(x',y') = 0$ for $x' \neq y'$. Obviously, the Γ_k generate a commutative $(n'+1)$-dimensional subalgebra of $\mathbf{C}(X',X')$, isomorphic to $\mathbf{C}^{n'+1}$. They form

the basis of *minimal, mutually orthogonal, idempotents* of this subalgebra; indeed, using the Kronecker symbol δ, we have

$$\Gamma_r \Gamma_s = \delta_{r,s} \Gamma_r, \qquad 0 \leqslant r,\ s \leqslant n'. \tag{2.8}$$

Definition. Let $S \in \mathbf{C}(X,X')$ be an orthogonal matrix. To the partition π' of X' correspond the following Hermitian matrices $J_k \in \mathbf{C}(X,X)$:

$$J_k = |X|^{-1} S \Gamma_k \bar{S} = |X|^{-1} S_k \bar{S}_k, \tag{2.9}$$

for $k = 0, 1, \ldots, n'$, where S_k is the restriction of S to $X \times X_k'$. Clearly, the J_k form the basis of minimal idempotents of a subalgebra of $\mathbf{C}(X,X)$, which is similar, under unitary transformation, to the subalgebra of $\mathbf{C}(X',X')$ generated by the Γ_k.

Theorem 2.2. Let (X,R) be an association scheme with n classes, and let X' be a set of the same cardinality as X. Then there exists a partition π' of X' into $n+1$ classes X_k', $0 \leqslant k \leqslant n$, with $|X_0'| = 1$, and an orthogonal matrix $S \in \mathbf{C}(X,X')$, with $S_0 = (1, \ldots, 1)^T$, such that the matrices $J_0, J_1, \ldots, J_n$ given by (2.9) form a basis of the Bose–Mesner algebra of the scheme.

Proof. Let A denote the BM algebra of (X,R). According to theorem 2.1 and a well-known result on commutative sets of normal matrices (cf. Marcus and Minc [49], p. 77), there exists an orthogonal matrix $S \in \mathbf{C}(X,X')$ diagonalizing A: to each $D \in \mathsf{A}$ corresponds a diagonal matrix $\Lambda \in \mathbf{C}(X',X')$ such that

$$D = |X|^{-1} S \Lambda \bar{S}, \tag{2.10}$$

the diagonal elements of Λ being the eigenvalues of D. When D runs through A, the matrix Λ runs through a subalgebra A' of $\mathbf{C}(X',X')$, which is isomorphic to A.

Let D be a matrix of A having the maximal number of distinct eigenvalues. We denote this number by $n'+1$ and the eigenvalues of D by $\lambda_0, \lambda_1, \ldots, \lambda_{n'}$. Then there exists a partition π' of X' into $n'+1$ classes X_k', $0 \leqslant k \leqslant n'$, such that the image $\Lambda \in \mathsf{A}'$ of D has the form

$$\Lambda = \sum_{k=0}^{n'} \lambda_k \Gamma_k, \tag{2.11}$$

where the Γ_k are defined by (2.7). Since the λ_k are distinct, there exist polynomials $f_i(z)$ over $\mathbf{C}$ satisfying $f_i(\lambda_k) = \delta_{i,k}$, for $i, k = 0, 1, \ldots, n'$. From (2.11) we deduce $f_k(\Lambda) = \Gamma_k$, using also (2.8). Therefore, the Γ_k belong to the algebra A' and this implies $n' \leqslant n$. In fact, by a similar argument, which will be omitted, it is not difficult to show that the Γ_k generate the whole algebra, i.e., equivalently, $n' = n$. Hence the images (2.9) of $\Gamma_0, \ldots, \Gamma_n$ in A form a basis of orthogonal idempotents of A.

Finally, we observe that the all-one matrix J, which belongs to A, admits $|X|$ as an eigenvalue of multiplicity 1 associated to the eigenvector $j = (1, \ldots, 1)^T$.

Hence it follows that one of the classes of π', which we shall assume to be X_0', contains a single element, the corresponding submatrix S_0 of S being equal to εj for some number ε with $\varepsilon\varepsilon^* = 1$. Since we may take $\varepsilon = 1$ without loss of generality, this concludes the proof.

Definitions. For an association scheme (X,R) and a fixed point $e \in X$, the partition $\tau(X,e)$ of X is defined to consist of the following $n+1$ classes:

$$X_i = \{x \in X \mid (x,e) \in R_i\}, \qquad 0 \leqslant i \leqslant n. \tag{2.12}$$

On the other hand, for a set X' of the same cardinality as X and for an orthogonal matrix $S \in \mathbf{C}(X,X')$ diagonalizing the BM algebra of the scheme, we shall denote by $\pi(X',S)$ a partition of X' into $n+1$ classes X_k', $0 \leqslant k \leqslant n$, with $|X_0'| = 1$, such that the column spaces of S_0 $(= j)$, $S_1, \ldots, S_n$ are the common eigenspaces of all matrices in the algebra.

In the proof of theorem 2.2, we have essentially established the existence and uniqueness of $\pi(X',S) = \pi'$. Let us also emphasize that the basis (2.9) of minimal idempotents of A is unique, although S is not unique.

Given a pair of partitions $\tau(X,e)$ and $\pi(X',S)$, we shall use the following notations for the cardinalities of the classes:

$$v_i = |X_i|, \qquad \mu_k = |X_k'|.$$

Clearly, v_i is the valence of R_i and the present notation agrees with (2.2). On the other hand, we have $\mu_k = \operatorname{rank}(S_k) = \operatorname{rank}(J_k)$. The μ_k are called the *multiplicities* of the BM algebra.

2.3. The eigenmatrices P and Q

Given the two "natural" bases $\{D_k\}$ and $\{J_k\}$ of the Bose–Mesner algebra of a scheme, let us consider the linear transformations of one of them into the other; first we write

$$D_k = \sum_{i=0}^{n} P_k(i)\, J_i, \qquad k = 0, 1, \ldots, n. \tag{2.13}$$

The complex numbers $P_k(0), P_k(1), \ldots, P_k(n)$ defined by (2.13) are the eigenvalues of D_k. From these we construct the square matrix P of order $n+1$ whose (i,k)-entry is $P_k(i)$:

$$P = [P_k(i); \qquad 0 \leqslant i,k \leqslant n]. \tag{2.14}$$

Since P is nonsingular, there exists a unique square matrix Q of order $n+1$ over $\mathbf{C}$ such that

$$P\,Q = Q\,P = |X|\, I. \tag{2.15}$$

The matrices P and Q will be called the *eigenmatrices* of the association scheme.

Writing $Q_k(i)$ for the (i,k)-entry of Q, as in (2.14), we derive from (2.13) and (2.15) the following system:

$$J_k = |X|^{-1} \sum_{i=0}^{n} Q_k(i)\, D_i, \qquad k = 0, 1, \ldots, n. \tag{2.16}$$

Using the partition $\tau(X,e)$ of X defined in (2.12), we obtain an equivalent form of (2.16), namely

$$J_k(x,e) = |X|^{-1}\, Q_k(i), \qquad \forall\, x \in X_i. \tag{2.17}$$

Since $|X|\, J_0$ is the all-one matrix, this yields $Q_0(i) = 1$ for all i, which is to be compared with the obvious identity $P_0(i) = 1$.

Let us now briefly examine the relations between the eigenmatrices and the parameters v_k, μ_k, $p_{i,j}^{(k)}$. Since $P_k(0)$ is the eigenvalue of D_k associated to the eigenvector $S_0 = j$, we have $P_k(0) = v_k =$ valence of R_k. On the other hand, considering equality of the traces in both members of (2.16) we deduce, since $\operatorname{tr}(J_k) = \mu_k$ and $\operatorname{tr}(D_i) = |X|\, \delta_{0,i}$:

$$Q_k(0) = \mu_k = \operatorname{rank}(J_k). \tag{2.18}$$

The intersection numbers $p_{i,j}^{(k)}$ can be expressed as "rational functions" of the eigenvalues $P_i(u)$. Indeed, the equality between the corresponding eigenvalues in both members of (2.5) gives

$$P_i(u)\, P_j(u) = \sum_{k=0}^{n} p_{i,j}^{(k)}\, P_k(u), \qquad u = 0, 1, \ldots, n. \tag{2.19}$$

Conversely, the numbers $P_i(u)$ are "algebraic functions" of the $p_{i,j}^{(k)}$. In order to show this fact, let us introduce the square matrix L_i of order $n+1$ whose (k,j)-entry is $p_{i,j}^{(k)}$ for $k,j = 0, 1, \ldots, n$ (cf. Bose and Mesner [9]). Then, as can be easily verified, (2.19) is equivalent to

$$P\, L_i\, P^{-1} = \operatorname{diag}(P_i(0), P_i(1), \ldots, P_i(n)).$$

Hence the $P_i(u)$ are the eigenvalues of L_i. (Moreover, we observe that the correspondence $D_i \to L_i$ gives an isomorphism between the BM algebra of the scheme and the algebra generated by $L_0, L_1, \ldots, L_n$.)

The derivation of the eigenmatrices from the parameters $p_{i,j}^{(k)}$ has been recalled only for completeness. In the present paper, for the two families of schemes that will be examined in detail (cf. ch. 4), we shall obtain the eigenmatrices in very different manners.

The following theorem describes some *orthogonality relations* satisfied by the eigenmatrices. We first introduce a notation: to an $(n+1)$-tuple $\mathbf{c} = (c_0, c_1, \ldots, c_n)$ of complex numbers c_i we associate the diagonal matrix

$$\Delta_{\mathbf{c}} = \operatorname{diag}(c_0, c_1, \ldots, c_n). \tag{2.20}$$

Theorem 2.3. Let P and Q be the eigenmatrices of an association scheme (X,R). Let v_k be the valence of R_k and μ_k the rank of J_k. Then the following two equations are satisfied:

$$P^{\mathrm{T}} \Delta_\mu P = |X| \Delta_v, \tag{2.21}$$

$$Q^{\mathrm{T}} \Delta_v Q = |X| \Delta_\mu. \tag{2.22}$$

Proof. For a point $e \in X$ and an orthogonal matrix $S \in \mathbf{C}(X,X')$ diagonalizing the BM algebra, let us consider the partitions $\tau(X,e)$ and $\pi(X',S)$ of X and X', respectively. They yield a decomposition (2.3) of S, with $n = n'$ and $S_0 = j$. From (2.9) and (2.17) we deduce

$$S_{i,k} \bar{S}_{0,k} = Q_k(i) S_{i,0}, \tag{2.23}$$

for $i,k = 0, 1, \ldots, n$. Using the symbol $\sum$ for the direct sum of matrices, we can write (2.23) as follows:

$$S\left(\sum_{k=0}^{n} \bar{S}_{0,k}\right) = \left(\sum_{i=0}^{n} S_{i,0}\right) Q.$$

Multiplying both members to the left by $\bar{S}$ and to the right by P, we readily obtain, by (2.4) and (2.15),

$$P_i(k) \bar{S}_{0,k} = \bar{S}_{i,k} S_{i,0}, \tag{2.24}$$

for $i,k = 0, 1, \ldots, n$. Using (2.23) and (2.24) we have two expressions for the numbers $S_{i,0}^{\mathrm{T}} S_{i,k} \bar{S}_{0,k}$; equality between them gives

$$P_i^*(k) S_{0,k} \bar{S}_{0,k} = Q_k(i) S_{i,0}^{\mathrm{T}} S_{i,0}.$$

Since $S_{i,0}^{\mathrm{T}} S_{i,0} = |X_i| = v_i$ and $S_{0,k} \bar{S}_{0,k} = Q_k(0) = \mu_k$, by (2.18) and (2.23) with $i = 0$, this can be written in matrix form as

$$P^{\mathrm{T}} \Delta_\mu = \Delta_v Q, \tag{2.25}$$

by use of the notation (2.20). The desired equations (2.21) and (2.22) then follow from (2.15) and (2.25).

The above proof has been adopted to show how the numbers $P_i(k)$ and $Q_k(i)$ can be derived from some partitioned form of an orthogonal matrix S (cf. (2.23) and (2.24)). However, there is a more direct proof: the orthogonality relations $J_r J_s = \delta_{r,s} J_r$ when expressed in the basis $\{D_i\}$ give, by (2.5) and (2.16),

$$\sum_{i,j} Q_r(i) Q_s(j) p_{i,j}^{(k)} = |X| \delta_{r,s} Q_r(k).$$

For $k = 0$ this is equivalent to (2.22), as can be readily verified.

By definition, the Bose–Mesner algebra is closed with respect to both transformations $D \to D^{\mathrm{T}}$ and $D \to D^*$. On the other hand, the idempotents J_k are Hermitian matrices. In fact, it is easy to show that the correspondence $J_k \to J_k^*$ $(= J_k^{\mathrm{T}})$ acts as a permutation on the set $\{J_0, J_1, \ldots, J_n\}$. Hence it is clear, by (2.16), that the conjugate of any given column Q_t of the eigenmatrix Q also is a column of Q: we have $Q_t = Q_k^*$ for $J_t = J_k^*$. Analogously, the columns P_t of P satisfy $P_j = P_i^*$ for $D_j = D_i^{\mathrm{T}}$, i.e. for $R_j = R_i^{-1}$.

For a symmetric association scheme (X,R) the eigenvalues of the adjacency matrices D_i are real. Hence the matrices P, Q, J_k are also real. In this case, it is sufficient to consider the BM algebra over the real numbers.

For given i,j, let us write the product $Q_i(u) Q_j(u)$ in the basis of the $Q_k(u)$:

$$Q_i(u) Q_j(u) = \sum_{k=0}^{n} q_{i,j}^{(k)} Q_k(u), \qquad u = 0, 1, \ldots, n, \tag{2.26}$$

for some complex numbers $q_{i,j}^{(k)}$ uniquely defined. Although these numbers have no clear "combinatorial" meaning, they have properties similar to those of the $p_{i,j}^{(k)}$ (cf. (2.19)), besides the obvious symmetry $q_{i,j}^{(k)} = q_{j,i}^{(k)}$:

Lemma 2.4. The $q_{i,j}^{(k)}$ are nonnegative real numbers. Moreover, they satisfy

$$q_{i,j}^{(0)} = \mu_i \delta_{i,t} \qquad \text{for} \qquad J_t = J_j^*. \tag{2.27}$$

Proof. To a given column vector $\phi \in \mathbf{C}(X)$ we associate the diagonal matrix $\Delta \in \mathbf{C}(X,X)$ defined by $\Delta(x,x) = \phi(x)$. On the other hand, let $S \in \mathbf{C}(X,X')$ be an orthogonal matrix diagonalizing the BM algebra. Then, for the partition $\pi(X',S)$ of X' and for given $i,j = 0, 1, \ldots, n$, the following identity holds:

$$\|\bar{S}_i \Delta S_j\|^2 = \sum_{k=0}^{n} q_{i,j}^{(k)} \|\bar{S}_k \phi\|^2 \qquad \text{for} \qquad Q_t = Q_j^*, \tag{2.28}$$

where $\|A\| = (\mathrm{tr}\,(\bar{A}A))^{1/2}$ denotes the Hermitian norm of a matrix A. This is obtained by straightforward verification, from (2.26), by use of $(S_k \bar{S}_k)(x,y) = Q_k(u)$ for $(x,y) \in R_u$ (cf. (2.23)). The details are left to the reader.

For fixed r, let ϕ be a nonzero vector in the column space of S_r. Since S is orthogonal, this implies $\bar{S}_k \phi = 0$ for $k \neq r$ and $\bar{S}_r \phi \neq 0$. Hence it follows from (2.28) that $q_{i,i}^{(r)}$ is real and nonnegative.

To show the second part of the lemma, we use (2.28) with $\phi = (1, \ldots, 1)^{\mathrm{T}} = S_0$ and $\Delta = I$. Since S is orthogonal, we obtain $|X|^2 \mu_i \delta_{i,j} = |X|^2 q_{i,i}^{(0)}$, which yields the desired result (2.27).

Concluding this rather technical section about eigenmatrices, we give in-

equalities that will be useful in the following: for all $i,k = 0, 1, \ldots, n$,

$$|P_i(k)| \leqslant v_i, \qquad |Q_k(i)| \leqslant \mu_k. \tag{2.29}$$

The first one simply follows from the fact that $v_i^{-1} D_i$ is a stochastic matrix, so that its eigenvalues have an absolute value less than or equal to unity. Then the second inequality follows from (2.25).

2.4. Examples

In ch. 4 some schemes connected with coding theory will be examined in detail. Here we briefly describe a few other "classical" examples.

Example 1. Let X be a finite set of cardinality $v \geqslant 2$ and let R_1 be a symmetric relation on X having no pair in common with the diagonal relation R_0. Then (X,R_1) is called a *graph of order* v. The graph is said to be *regular* if R_1 is regular, it is *strongly regular* if (X,R) is an association scheme with two classes for $R = \{R_0, R_1, R_2\}$, $R_2 = X^2 - (R_0 \cup R_1)$. This concept was first introduced by Bose [8]). Clearly, the *complementary graph* (X,R_2) of (X,R_1) is then also strongly regular.

According to theorem 2.3, the eigenmatrices P and Q of an association scheme with two classes can be expressed in terms of the valences v_i, the multiplicities μ_i and some real numbers r_i, s_i as follows:

$$P = \begin{bmatrix} 1 & v_1 & v_2 \\ 1 & r_1 & r_2 \\ 1 & s_1 & s_2 \end{bmatrix}, \qquad Q = \begin{bmatrix} 1 & \mu_1 & \mu_2 \\ 1 & \mu_1 r_1/v_1 & \mu_2 s_1/v_1 \\ 1 & \mu_1 r_2/v_2 & \mu_2 s_2/v_2 \end{bmatrix}. \tag{2.30}$$

The conditions (2.15) are classical identities on the parameters of strongly regular graphs; for instance the useful equation $(v_1 - s_1)(v_2 - r_2) = v s_1 r_2$. With only the following exceptions: $\mu_i = v_i = (v-1)/2$, $s_2 = r_1 = (-1 \pm \sqrt{v})/2$, $s_1 = r_2 = (-1 \mp \sqrt{v})/2$, it can be shown that the eigenvalues r_i, s_i are integers such that, for a suitable ordering, $r_1 \geqslant 0$, $s_1 \leqslant -1$. For this we refer to Seidel [61]).

To complete the description of association schemes with two classes, let us examine the nonsymmetric case, i.e. $R_2 = R_1^{-1}$. It is easy to show that the skew-symmetric matrix $D = D_1 - D_2$ then satisfies $D J = 0$ and $D^2 = J - v I$. In other words, D is the *kernel* of a *skew-symmetric Hadamard matrix* of order $v+1$ (cf. for instance Wallis [73])). In fact, the concept of a nonsymmetric association scheme with two classes on v points is equivalent to that of a skew-symmetric Hadamard matrix of order $v+1$.

Example 2. Let X be a finite group and denote by $X_0 = \{1\}, X_1, \ldots, X_n$ the conjugacy classes of X, i.e. the subsets of the form $\{z^{-1} a z \mid z \in X\}$ for some

$a \in X$. Then we define relations $R_0, R_1, \ldots, R_n$ on X as follows:

$$R_i = \{(x,y) \mid y^{-1} x \in X_i\}. \tag{2.31}$$

It is easy to check that (X,R) is an association scheme. The eigenmatrices of this scheme are closely related to the irreducible characters $\psi_0, \psi_1, \ldots, \psi_n$ of the group (cf. for instance Hall [28])): for any $x \in X_i$, the characters are given by

$$\psi_k(x) = v_i^{-1} \mu_k^{1/2} P_i(k) = \mu_k^{-1/2} Q_k^*(i).$$

The equations (2.21) and (2.22) here are the classical orthogonality relations of the theory of group characters. On the other hand, lemma 2.4 also reduces to a well-known result.

Example 3. Let X be a finite Abelian group of period ν and let $X_0 = \{1\}, X_1, \ldots, X_n$ be the central classes of X, i.e. the subsets of the form $\{a^t\}$, where a is a fixed element in X and t runs through the positive integers which are relatively prime to ν. Defining the relation R_i from X_i as in (2.31), one readily shows that (X,R) is a symmetric association scheme. Here the eigenmatrix P has integral entries and satisfies $P^2 = |X| I$, i.e. $P = Q$ (cf. Delsarte and Goethals [17])).

Example 4. For a prime power q, let ω be a primitive root in the Galois field $GF(q)$. Then, given an arbitrary divisor s of $q-1$, we consider the partition of $GF(q)$ into $s+1$ classes $C_0 = \{0\}, C_1, \ldots, C_s$ with the following definition, for $r = (q-1)/s$ and $0 \leqslant i \leqslant s-1$:

$$C_{i+1} = \{\omega^i, \omega^{s+i}, \omega^{2s+i}, \ldots, \omega^{(r-1)s+i}\}.$$

The classes $C_1, \ldots, C_s$ are the *cyclotomic classes* of $GF(q)$; they simply are the cosets of the subgroup of order r in the multiplicative group of $GF(q)$. Next, we define the set $K = \{K_0, \ldots, K_s\}$ of relations K_i on $GF(q)$ as follows: $K_i = \{(x,y) \mid x - y \in C_i\}$. It is easy to show that $(GF(q),K)$ is an association scheme; this will be called the *cyclotomic scheme* with s classes. Here the parameters $p_{i,j}^{(k)}$ are the so-called cyclotomic numbers (cf. Storer [69])).

2.5. Extensions of an association scheme

Let there be given an association scheme (F,K) with s classes $K_1, \ldots, K_s$ on a set F of cardinality q. For an integer $m \geqslant 1$, we consider two elements $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m)$ of the mth Cartesian power $X = F^m$. Let $\varrho_i(x,y)$ be the number of integers i, $1 \leqslant i \leqslant m$, such that $(x_i,y_i) \in K_i$ and define the following s-tuple: $\varrho(x,y) = (\varrho_1(x,y), \ldots, \varrho_s(x,y))$. The number n of distinct nonzero values assumed by $\varrho(x,y)$ in $\mathbf{R}^s$ when x and y run through X only depends on s and m. In fact, $n+1$ is the number of m-combinations with repetitions of $s+1$ distinct things, so that $n = \binom{m+s}{s} - 1$.

Let $\varrho^{(0)} = (0, \ldots, 0)$, $\varrho^{(1)}, \ldots, \varrho^{(n)}$ be the distinct values of $\varrho(x,y)$. Then we define the set $R = \{R_0, R_1, \ldots, R_n\}$ of relations R_j on X as follows:

$$R_j = \{(x,y) \mid \varrho(x,y) = \varrho^{(j)}\}. \tag{2.32}$$

It is not really difficult to show that (X,R) is an association scheme, with n classes. This will be called the *extension of length m* of the initial scheme (F,K).

The simplest case is $s = 1$, i.e. $K = \{K_0, K_1\}$. Then (F,K_1) is the complete graph of order q. The extension $(X = F^m, R)$ of the scheme (F,K) with one class will be denoted by $H(m,q)$ and will be called the *Hamming scheme* of length m over F. The number n of classes of (X,R) clearly is equal to m. The mapping ϱ_1 of X^2 onto $\{0, 1, \ldots, n\}$ is called the *Hamming distance* over X; it will be denoted by d_H in the rest of this work. By definition, $d_H(x,y) = \varrho_1(x,y)$ is the number of integers i for which x_i and y_i differ from each other. It is easily seen that d_H has the classical properties of a distance. An important part of the present work is devoted to the concept of "metric schemes" (cf. sec. 5.2), which is a natural generalization of the Hamming schemes (cf. sec. 4.1).

For $F = GF(q)$, q being a prime power, let us also consider the extensions $(X = F^m, R)$ of the cyclotomic schemes over F (cf. example 4 in sec. 2.4), for any divisor s of $q-1$. We shall briefly describe two interesting cases (besides $s = 1$, which leads to the Hamming schemes):

(i) For $s = q-1$, the scheme (X,R) will be called the *spectral scheme* of length m over F. The pairs (x,y) of vectors $x,y \in X$ belonging to a given relation (2.32) are those for which the difference $z = x - y$ has a specified "spectrum" $\varrho^{(j)}$, i.e. a fixed number of components z_i assuming each of the values of the field F. For given m and q, the spectral scheme is a "refinement" of the Hamming scheme $H(m,q)$, in the sense that the partition R of X^2 is finer for the first than for the second one.

(ii) For $q \equiv 1 \pmod 2$, $s = (q-1)/2$, the extension (X,R) of the cyclotomic scheme with s classes over $F = GF(q)$ will be called the *Lee scheme* of length m over F. Let us examine the connection with the Lee metric [38], when q is an odd prime. The *Lee distance* $d_L(x,y)$ between two vectors $x,y \in X$ is defined as follows:

$$d_L(x,y) = \sum_{i=1}^{m} |x_i - y_i|,$$

where $|\alpha|$ is the integer among $0, 1, \ldots, s$ which is congruent to $\pm\, \alpha$ modulo q. It is easily seen that we have $d_L(x,y) = \sum i_k \varrho_k(x,y)$, for a fixed permutation $(i_1, \ldots, i_s)$ of $(1, \ldots, s)$. Consequently, if two pairs (x,y) and (x',y') are in the same relation R_j of the Lee scheme, then they satisfy $d_L(x,y) = d_L(x',y')$. However, the distance relations in the sense of Lee do not yield, in general,

an association scheme. To give a scheme, these relations need to be refined; a suitable refinement is precisely that of the Lee scheme.

The above examples all have applications in coding theory. For instance, as will be examined in sec. 4.1, the Hamming scheme $H(m,q)$ is a convenient framework for studying the "distance distribution" of a code of length m over F (for the Hamming metric). We shall now examine another illustration of the concept of extension, leading to a scheme (X,R), defined on the set $X = F^{2m}$, which is a natural framework for investigating the "joint distance distribution" of two codes of length m over F (cf. MacWilliams, Mallows and Sloane [47]). First, let us consider the *direct product* of two copies of the scheme (F,K) with one class; we denote this simply by (F^2,K^2). The definition, rather obvious, is the following: for $i = 0, 1, 2, 3$, the relation $(K^2)_i$ over F^2 is the set of pairs $((\alpha,\alpha'), (\beta,\beta'))$ satisfying $\alpha = \beta$ and $\alpha' = \beta'$, $\alpha = \beta$ and $\alpha' \neq \beta'$, $\alpha \neq \beta$ and $\alpha' = \beta'$, $\alpha \neq \beta$ and $\alpha' \neq \beta'$, respectively. Then, for an integer $m \geqslant 1$, the extension of length m of (F^2,K^2) is a symmetric association scheme with $n = \binom{m+3}{3} - 1$ classes. In the binary case (i.e. $|F| = 2$), we point out that (X,R) is isomorphic to the spectral scheme of length m over $GF(4)$.

2.6. Duality in association schemes

In sec. 2.3 we have seen how a partitioned form (2.3), with $n' = n$, of an orthogonal matrix $S \in \mathbf{C}(X,X')$ corresponds to an association scheme with n classes. We shall now examine this correspondence more in detail and, using such partitions of orthogonal matrices, we shall introduce a concept of duality for certain association schemes.

2.6.1. *Partitions of orthogonal matrices*

Let X and X' be two finite sets, with the same cardinality, and let S be an orthogonal matrix in $\mathbf{C}(X,X')$. We consider a partition $\sigma = \{X_k' \mid k = 0, 1, \ldots, n'\}$ of X' into $n'+1$ classes, with $n' \geqslant 1$. Clearly, the matrices

$$J_k = |X|^{-1} S_k \bar{S}_k, \qquad k = 0, 1, \ldots, n', \tag{2.33}$$

are linearly independent and form a set of orthogonal idempotents in the algebra $\mathbf{C}(X,X)$. Using these matrices we define a mapping f of X^2 into $\mathbf{C}^{n'+1}$ as follows:

$$|X|^{-1} f(x,y) = (J_0(x,y), \ldots, J_{n'}(x,y)), \tag{2.34}$$

for all $x,y \in X$. Let $n+1$ be the number of distinct values assumed by f; the partition σ will be said to be of *type* (n,n') *with respect to* S. Let $Q^{(0)}, Q^{(1)}, \ldots, Q^{(n)}$ denote these values. To each $Q^{(i)}$ we attach a relation $R_i(\sigma)$ on X:

$$R_i(\sigma) = \{(x,y) \mid f(x,y) = Q^{(i)}\}, \qquad i = 0, 1, \ldots, n. \tag{2.35}$$

Before examining association schemes, we shall give in a lemma the first con-

sequences of the above definitions. This will lead us to the useful concept of "symmetric partitions".

Lemma 2.5. For any σ of type (n,n'), one has $n \geqslant n'$, and the idempotents J_k are linear combinations of the adjacency matrices of the relations $R_i(\sigma)$.
Proof. First we define the complex numbers $Q_k(i)$ to be the components of the $(n'+1)$-tuple $Q^{(i)}$, for $i = 0, 1, \ldots, n$:

$$Q^{(i)} = (Q_0(i), Q_1(i), \ldots, Q_{n'}(i)). \tag{2.36}$$

Then, if D_i stands for the adjacency matrix of $R_i(\sigma)$, we can write J_k in terms of $D_0, \ldots, D_n$ as follows, using (2.34) and (2.35):

$$J_k = |X|^{-1} \sum_{i=0}^{n} Q_k(i)\, D_i, \qquad k = 0, 1, \ldots, n'. \tag{2.37}$$

Since the J_k are linearly independent over $\mathbf{C}$, this is only possible if $n' \leqslant n$. Hence the lemma is proved.

Definitions. Let σ be a partition of a set X' which is of type (n,n') with respect to a given orthogonal matrix $S \in \mathbf{C}(X,X')$ and let f be the corresponding mapping (2.34). Then σ will be called *symmetric* if n is equal to n' and if $f(x,x)$ is constant for all x in X; it will be called *regular* if all relations $R_i(\sigma)$ are regular.

We now give two results, converse of each other, showing the equivalence between the concepts of association schemes and of symmetric partitions of orthogonal matrices. No proof will be given for the first theorem, which is essentially a new form of theorem 2.2.

Theorem 2.6. Let (X,R) be an association scheme with n classes and let $S \in \mathbf{C}(X,X')$ be an orthogonal matrix diagonalizing the Bose–Mesner algebra of the scheme. Then the partition $\sigma = \pi(X',S)$ of X' is regular and symmetric, of type (n,n), with respect to S. Moreover, $R = \{R_0(\sigma), \ldots, R_n(\sigma)\}$ holds.

Theorem 2.7. Let σ be a partition of X', which is symmetric of type (n,n) with respect to an orthogonal matrix $S \in \mathbf{C}(X,X')$. Then $(X,\{R_i(\sigma)\})$ is an association scheme with n classes and S diagonalizes the Bose–Mesner algebra of the scheme. Moreover, $\sigma = \pi(X',S)$ holds.
Proof. Let us first show that $R(\sigma) = \{R_0(\sigma), \ldots, R_n(\sigma)\}$ satisfies axiom A1 (sec. 2.1). By definition, $R(\sigma)$ is a partition of X^2. On the other hand, from (2.33), (2.34) and the orthogonality of S we readily deduce

$$f(x,y)\,(1, 1, \ldots, 1)^T = |X|\, \delta_{x,y}. \tag{2.38}$$

Hence two pairs (z,z) and (x,y) with $x \neq y$ cannot belong to the same $R_i(\sigma)$.

Therefore, since $f(z,z)$ is assumed to be constant, one of the relations, which we shall take to be $R_0(\sigma)$, must be the diagonal; so condition A1 is satisfied.

To prove that $(X,R(\sigma))$ is an association scheme, we use lemma 2.5 with $n' = n$. The adjacency matrices D_i of the $R_i(\sigma)$ can now be written as linear combinations of the idempotents J_k. Consequently, the D_i generate a commutative $(n+1)$-dimensional algebra of normal matrices in $\mathbf{C}(X,X)$. Hence, by theorem 2.1, $(X,R(\sigma))$ is an association scheme with n classes, whose BM algebra admits $J_0, J_1, \ldots, J_n$ as minimal idempotents (cf. theorem 2.2).

Finally, we observe that S diagonalizes the J_k and, therefore, the whole BM algebra. From this it also follows that the partition σ is identical to $\pi(X',S)$, which concludes the proof.

2.6.2. *Dual of a regular scheme*

Definition. Given an association scheme (X,R), let $S \in \mathbf{C}(X,X')$ be an orthogonal matrix diagonalizing the Bose–Mesner algebra and let e be a point of X. Then (X,R) is said to be *regular with respect to e and to S* if the partition $\tau(X,e)$ of X is regular with respect to $\bar{S}$ and if $S^{(0)}$ is equal to $(1, 1, \ldots, 1)$ for $X_0 = \{e\}$.

Without loss of generality (cf. theorem 2.2), we assume that S contains the column $S_0 = (1, \ldots, 1)^T$. Then we denote by e' the corresponding point of X', so that $X_0' = \{e'\}$ is one of the classes of the partition $\pi(X',S)$. We are now able to define a duality for regular schemes.

Theorem 2.8. Let (X,R) be an association scheme, with n classes, which is regular with respect to $e \in X$ and to $S \in \mathbf{C}(X,X')$. Then, for the partition $\tau = \tau(X,e)$ and for $R' = \{R_i(\tau)\}$, the pair (X',R') also is an association scheme with n classes, being itself regular with respect to e' and $\bar{S}$. The partitions corresponding to these schemes satisfy $\pi(X,\bar{S}) = \tau(X,e)$ and $\pi(X',S) = \tau(X',e')$. Moreover, the valences v_k', the multiplicities μ_k' and the eigenmatrices P', Q' of (X',R') can be derived from those of (X,R) by the formulas

$$v_k' = \mu_k, \qquad \mu_k' = v_k, \qquad P' = Q, \qquad Q' = P. \tag{2.39}$$

Proof. We shall use the method of sec. 2.6.1, interchanging the roles of X and X' and using the orthogonal matrix $\bar{S}$ instead of S. For the partition $\tau = \tau(X,e)$ into classes $X_0 = \{e\}, X_1, \ldots, X_n$ given by (2.12), we define like in (2.33) the idempotents

$$J_i' = |X|^{-1}\, \bar{S}^{(i)}\, S^{(i)}, \qquad i = 0, 1, \ldots, n, \tag{2.40}$$

in the algebra $\mathbf{C}(X',X')$. Let P be the first eigenmatrix (2.14) of (X,R) and let $X_0' = \{e'\}, X_1', \ldots, X_n'$ be the classes of $\pi(X',S)$. Then, since $S^{(0)}$ is the all-

one row vector, it follows from (2.24) that the (x',e')-entry of J_i', with $x' \in X_k'$, is equal to

$$J_i'(x',e') = |X|^{-1} (\bar{S}_{i,k} S_{i,0})(x') = |X|^{-1} P_i(k). \tag{2.41}$$

Next, we introduce the mapping f' of $(X')^2$ into $\mathbf{C}^{n+1}$, as in (2.34), using here the idempotents J_i':

$$|X|^{-1} f'(x',y') = (J_0'(x',y'), \ldots, J_n'(x',y')). \tag{2.42}$$

The regularity of $\tau(X,e)$ with respect to S implies that, for a fixed $y' \in X'$, the set of values assumed by $f'(x',y')$ for x' running through X' is independent of y'. Therefore, it follows from (2.41) that f' assumes exactly $n+1$ distinct values in $\mathbf{C}^{n+1}$, namely the $n+1$ rows $P^{(k)}$ of P. Since $f'(x',y')$ satisfies a condition similar to (2.38), this also shows that $f'(x',x')$ is constant. In other words, the partition $\tau(X,e)$ is symmetric of type (n,n) with respect to $\bar{S}$. Hence, by theorem 2.7, (X',R') is an association scheme with n classes, its BM algebra is diagonalized by $\bar{S}$, and the partitions $\tau(X,e)$ and $\pi(X,\bar{S})$ are equal.

Using the same numbering for the relations $R_k' = R_k(\tau)$ of R' as for the rows $P^{(k)}$ of P, we have

$$\{x' \in X' \mid (x',e') \in R_k'\} = X_k', \qquad k = 0, 1, \ldots, n.$$

Hence the partitions $\tau(X',e')$ and $\pi(X',S)$ are equal. Consequently, it follows from the definitions and from theorem 2.6 that (X',R') is regular with respect to e' and to $\bar{S}$.

Finally, let us prove (2.39). According to (2.17) the second eigenmatrix Q' of (X',R') is given by the following equation:

$$J_i'(x',e') = |X|^{-1} Q_i'(k), \qquad \forall\, x' \in X_k'.$$

Comparing this with (2.41), we have $Q' = P$ or, equivalently, $P' = Q$, which concludes the proof.

Definition. In the situation of theorem 2.8, the association scheme (X',R') will be called the *dual of* (X,R) *with respect to* $e \in X$ *and to* $S \in \mathbf{C}(X,X')$.

This duality is involutive in the sense that (X,R) is then itself the dual of (X',R') with respect to $e' \in X'$ and to $\bar{S} \in \mathbf{C}(X',X)$. The following theorem describes an interesting class of association schemes which actually have a dual. We shall use the convenient notation $\langle x,x' \rangle$ of a symmetric "inner product" for the irreducible complex group characters of an Abelian group. More details about this subject are given in sec. 6.2.

Theorem 2.9. Given a finite Abelian group X (written additively), let (X,R) be an association scheme which is invariant under translation in X:

$$((x,y) \in R_i) \Rightarrow ((x+z,\ y+z) \in R_i), \tag{2.43}$$

for each $z \in X$ and $i = 0, 1, \ldots, n$. Then (X,R) has a dual (X,R') with respect to $e = 0$ and to the symmetric matrix $S \in \mathbf{C}(X,X)$ of group characters of X, defined by $S(x,x') = \langle x,x' \rangle$ for $x,x' \in X$. Moreover, the dual itself is invariant under translation.

Proof. It is well known that S is an orthogonal matrix diagonalizing the adjacency matrix of any relation satisfying (2.43), and therefore, the BM albegra (2.6) of (X,R). It is also easy to prove that (X,R) is regular with respect to the unit $e = 0$ and to the matrix S. According to theorem 2.8, this shows the existence of a dual scheme (X,R'). Looking at the construction of the dual of an association scheme, the reader will readily check that (X,R') satisfies (2.43) where R_i is replaced by R_i'.

Remark. After discovery of this duality, the author became aware of the following fact (private communication with P. J. Cameron): The Bose–Mesner algebra of an association scheme of the type considered in theorem 2.9 is a particular case of a Schur ring. Moreover, Tamaschke [71] has defined a duality for certain Schur rings which is closely related to the above concepts; in fact, theorem 2.9 should be considered, essentially, as a particular case of Tamaschke's results.

2.6.3. *Duality in strongly regular graphs*

Let (X,R) and (X',R') be two symmetric association schemes, both with two classes, dual of each other. For $i = 1, 2$, the strongly regular graph (X',R_i') will be called a *dual graph* of (X,R_i). Using formulas (2.39), we can express the parameters v_1', r_1', s_1' of (X',R') in terms of v_1, r_1, s_1 as follows, with $v = |X|$:

$$\begin{aligned}
(r_1 - s_1)\, v_1' &= -(v_1 + s_1 (v-1)), \\
(r_1 - s_1)\, r_1' &= -r_1 (v_1 + s_1 (v-1))/v_1, \\
(r_1 - s_1)\, s_1' &= (1 + r_1)(v_1 + s_1 (v-1))/(v - 1 - v_1).
\end{aligned}$$

From the last two equations we obtain $(r_1 - s_1)(r_1' - s_1') = v$, by subtraction, using the orthogonality conditions. Hence, in the "normal" case where r_1 and s_1 are integers, a strongly regular graph (X,R_1) can have a dual only when $r_1 - s_1$ divides v. It is interesting to consider the cases of a graph having the same parameters as its dual (i) or as the complement of its dual (ii):

(i) First, we assume $r_i = r_i'$, $s_i = s_i'$, $v_i = v_i'$. Then we have $(r_1 - s_1)^2 = v$ and the parameters can be written in terms of two positive numbers t and q as follows: $v = q^2$, $r_1 = t$, $s_1 = t - q$, $v_1 = (q-t)(q-1)$.

(ii) Next, we assume $r_1 = s_2'$, $s_1 = r_2'$, $v_1 = v_2'$. Again we have

$(r_1 - s_1)^2 = v$ and the parameters are of the form $v = q^2$, $r_1 = t$, $s_1 = t - q$, $v_1 = t(q+1)$.

The graphs having such parameters are exactly those considered by Mesner [52]) under the names of pseudo Latin square graphs (i) and negative Latin square graphs (ii). Most of the known strongly regular graphs satisfying the duality conditions of theorem 2.9 belong to one of these classes. Two remarkable examples which are not of this "Latin square type" are treated in sec. 6.3 from the point of view of linear codes (cf. Delsarte [13])).

3. SUBSETS IN ASSOCIATION SCHEMES

Given a scheme (X,R) and a subset Y of X, we are interested here in the following question: how are the subsets Y^2 and $Y \times Y$ of X^2 distributed with respect to the relations R_i?

We shall use the notation $N = \{0, 1, \ldots, n\}$ throughout the rest of this work. The columns of a matrix $A \in \mathbf{C}(N,N)$ will be written $A_0, A_1, \ldots, A_n$, the ith component of A_k, i.e. the (i,k)-entry of A, being $A_k(i)$ like in (2.14). The symbols P and Q will always denote the eigenmatrices. Unless other specification, the summations Σ are taken over the set N.

3.1. Inner and outer distribution

Let $R = \{R_0, R_1, \ldots, R_n\}$ be a set of $n+1$ relations on X, satisfying the conditions A1 and A2 (sec. 2.1). For a nonempty subset Y of X, let us define the *inner distribution of Y with respect to R* to be the $(n+1)$-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_n)$ of nonnegative rational numbers a_i given by

$$a_i = |Y|^{-1} |R_i \cap Y^2|. \tag{3.1}$$

In explicit language, a_i is the average number of points of Y being ith associates of a fixed point of Y. Clearly, we have $a_0 = 1$, $\Sigma a_i = |Y|$ and $a_i = a_{i'}$ for $R_{i'} = R_i^{-1}$. We shall often consider $\mathbf{a}^T$ as a column vector in $\mathbf{R}(N)$.

Next, let us introduce the *distribution matrix of Y with respect to R* (= outer distribution of Y) to be the matrix $B \in \mathbf{R}(X,N)$ whose (x,i)-entry is given by

$$B(x,i) = |R_i \cap (\{x\} \times Y)|, \tag{3.2}$$

for $x \in X$, $i \in N$. By definition, $B(x,i)$ is the number of points of Y being ith associates of x. Let $B(x)$ stand for the row of B corresponding to a given $x \in X$. If $B(y)$ is constant for all points $y \in Y$, then Y will be called a *regular subset* of X. In this case, $B(y)$ is equal to the inner distribution $\mathbf{a}$ of Y. Clearly, Y is regular if and only if, for each $i \in N$, the restriction $R_i \cap Y^2$ of R_i to Y is a regular relation on Y, the valence being $B_i(y) = a_i$. An interesting problem is to obtain sufficient conditions on $\mathbf{a}$ for a subset $Y \subseteq X$ to be regular. Some results on this question will be given in ch. 5 for the so-called "polynomial schemes".

In order to treat the above concepts by matrix methods, we shall characterize $Y \subseteq X$ by the vector $\phi_Y \in \mathbf{R}(X)$ defined as follows:

$$\phi_Y(x) = \begin{cases} 1 & \text{for} \quad x \in Y, \\ 0 & \text{for} \quad x \in X - Y. \end{cases}$$

Then the definitions (3.1) and (3.2) can be formulated in terms of the adjacency

matrices D_i of the R_i by eqs (3.3) and (3.4), respectively:

$$a_i = |Y|^{-1}\, \phi_Y{}^T D_i\, \phi_Y, \tag{3.3}$$

$$B = [D_0\, \phi_Y,\ D_1\, \phi_Y,\ \ldots,\ D_n\, \phi_Y]. \tag{3.4}$$

Clearly, $\mathbf{a}$ is obtained from B by the formula $\mathbf{a} = |Y|^{-1}\, \phi_Y{}^T B$. The next three results give, for the association schemes, more interesting relations between $\mathbf{a}$ and B.

Theorem 3.1. Let (X,R) be an association scheme and let Y be a subset of X. Then the inner and outer distributions of Y with respect to R satisfy

$$B^T B = |X|^{-1}\, |Y|\, \bar{P}\, \Delta_{\mathbf{a}Q} P, \tag{3.5}$$

where P and Q are the eigenmatrices of the scheme and Δ_v is defined as in (2.20).

Proof. For $i,j \in N$, let us calculate the (i,j)-entry of $B^T B$ from (3.4). Using (2.5) and (3.3) we readily obtain, for $R_t = R_t{}^{-1}$:

$$\begin{aligned}(B^T B)(i,j) &= \phi_Y{}^T D_i{}^T D_j\, \phi_Y \\ &= |Y| \sum_k p_{t,j}{}^{(k)}\, a_k.\end{aligned} \tag{3.6}$$

Defining $\mathbf{b} = \mathbf{a}Q$, we have $|X|\mathbf{a} = \mathbf{b}P$, by (2.15). Hence (3.6) becomes, according to (2.19):

$$(B^T B)(i,j) = |X|^{-1}\, |Y| \sum_u b_u\, P_t(u)\, P_j(u).$$

Since $P_t(u) = P_t{}^*(u)$ for $R_t = R_t{}^{-1}$, this is exactly the desired formula (3.5).

Corollary 3.2. The rank of the matrix B is equal to the number of nonzero components of $\mathbf{a}Q$.

Proof. Since P is nonsingular we have, by (3.5), rank (B) = rank $(B^T B)$ = rank $(\Delta_{\mathbf{a}Q})$, from which the corollary follows.

Theorem 3.3. The components $\mathbf{a}Q_k$ of the row vector $\mathbf{a}Q$ are nonnegative real numbers. Moreover, for a given k, the component $\mathbf{a}Q_k$ is zero if and only if $B\, Q_k$ is the zero vector.

Proof. Multiplying both members of (3.5) to the left by $\bar{Q}$ and to the right by Q we obtain $\bar{Q}\, B^T B\, Q = |X|\, |Y|\, \Delta_{\mathbf{a}Q}$, by (2.15). Equality between the corresponding diagonal entries can be written as follows:

$$\|B\, Q_k\|^2 = |X|\, |Y|\, \mathbf{a}\, Q_k, \qquad \forall\, k \in N, \tag{3.7}$$

where $\|\ \|$ stands for the Hermitian norm. This clearly leads to the conclusions of the theorem.

Remark. The inequalities $\mathbf{a}Q_k \geqslant 0$, which will play a very important role in this work, can be derived in a more direct way from the definition (3.3): using (2.9) and (2.16) we obtain

$$\mathbf{a}\, Q_k = |X|\, |Y|^{-1}\, \phi_Y{}^T J_k\, \phi_Y = |Y|^{-1}\, \|S_k\, \phi_Y\|^2, \tag{3.8}$$

for an orthogonal matrix S diagonalizing the BM algebra. These identities obviously imply $\mathbf{a}Q_k \geqslant 0$. Together with (3.7) they also show that, for a given k, the following four equations are simultaneously satisfied or not satisfied:

$$\mathbf{a}\, Q_k = 0, \qquad B\, Q_k = 0, \qquad S_k\, \phi_Y = 0, \qquad J_k\, \phi_Y = 0.$$

3.2. Linear programming

The conditions $\mathbf{a}Q_k \geqslant 0$ suggest using the linear-programming method for the study of subsets $Y \subseteq X$ whose specific properties are some linear equations (or inequalities) satisfied by the inner distribution $\mathbf{a}$. Such are the "cliques" and "designs" examined in secs 3.3 and 3.4.

First, we shall recall some well-known results about linear programming (cf. Simonnard [64]), with notations adapted to our problem. Let $A = [A_k(i)]$ be a matrix of $\mathbb{R}(N,N)$ such that $A_0(i) = 1$ and $A_k(0) > 0$ for all $i,k \in N$. On the other hand, let M be a subset of N, with $0 \in M$, and let $M^* = M - \{0\}$. Then we define the *linear-programming problem* (A,M), with $m = |M^*|$ real variables b_i, $i \in M^*$, and n inequalities, as follows:

$$(A,M)\begin{cases} \sum_{i \in M} b_i\, A_k(i) \geqslant 0, & k \in N^*, \quad (3.9) \\ b_i \geqslant 0, & i \in M^*, \quad (3.10) \\ \text{maximize } g = \sum_{i \in M} b_i. & (3.11) \end{cases}$$

An $(n+1)$-tuple $\mathbf{b} = (b_0, b_1, \ldots, b_n)$ is called a *program* of (A,M) if it satisfies (3.9) and (3.10) with $b_0 = 1$ and $b_i = 0$ for $i \in N - M$. For instance, $(1, 0, \ldots, 0)$ is a program with $g = 1$.

In our applications, the set of programs will always be bounded (cf. lemma 3.5); equivalently, it will be a convex polyhedron. In this situation there exists at least one *maximal program*, i.e. a program for which the function g is maximal. We shall denote by $g(A,M)$ the maximum value of g over the set of programs. (Clearly, $g(A,M) \geqslant 1$.)

It is useful to examine the *dual problem* $(A,M)'$ of (A,M), with n real variables β_k, $k \in N^*$, and m inequalities:

$$(A,M)'\begin{cases} \sum_{k\in N} \beta_k A_k(i) \leqslant 0, & i \in M^*, \quad (3.12)\\ \beta_k \geqslant 0, & k \in N^*, \quad (3.13)\\ \text{minimize } \gamma = \sum_{k\in N} \beta_k A_k(0). & (3.14)\end{cases}$$

An $(n+1)$-tuple $\boldsymbol{\beta} = (\beta_0, \beta_1, \ldots, \beta_n)$ is a program of $(A,M)'$ if it satisfies (3.12) and (3.13) with $\beta_0 = 1$; it is a *minimal program* if, besides, it gives the smallest value to the function γ.

The most important theoretical results about duality in linear programming can be summarized as follows, in the case of a bounded set of programs of (A,M):

Theorem 3.4. (i) The problems (A,M) and $(A,M)'$ admit at least one extremal program (i.e. a maximal and a minimal program, respectively). Each pair of programs $\mathbf{b}$ of (A,M) and $\boldsymbol{\beta}$ of $(A,M)'$ satisfies $g \leqslant \gamma$. Moreover, the extremal values of g and γ are equal.

(ii) For each pair $(\mathbf{b},\boldsymbol{\beta})$ of extremal programs, the following two sets of equations hold:

$$\beta_k\Big(\sum_{i\in M} b_i A_k(i)\Big) = 0, \qquad \forall k \in N^*, \quad (3.15)$$

$$b_i\Big(\sum_{k\in N} \beta_k A_k(i)\Big) = 0, \qquad \forall i \in M^*. \quad (3.16)$$

Conversely, if a pair $(\mathbf{b},\boldsymbol{\beta})$ of programs satisfies (3.15) and (3.16), then it is a pair of extremal programs.

To conclude this section, let us give two results about the problems (A,M) and $(A,M)'$ when A is taken to be one of the eigenmatrices, P or Q, of a symmetric association scheme with n classes.

Lemma 3.5. The set of programs of (P,M) is bounded by $b_i \leqslant \mu_i$ and the one of (Q,M) by $b_i \leqslant v_i$, for all $i \in M$.

Proof. We shall prove the second part. From (2.15) we readily obtain the following identity, for an arbitrary $(n+1)$-tuple $\mathbf{b}$:

$$\sum_k (v_i - P_i(k)) \sum_j b_j Q_k(j) = |X|\,(b_0 v_i - b_i).$$

By (2.29) and (3.9) the left-hand member is nonnegative when $\mathbf{b}$ is a program of (Q,M). Hence, with $b_0 = 1$, we deduce $b_i \leqslant v_i$.

Lemma 3.6. Each minimal program $\boldsymbol{\beta}$ of $(P,M)'$ satisfies $\beta_j \leqslant 1$ for all $j \in N$.

Moreover, it satisfies $\beta_j = 1$ for a given j if and only if the following conditions holds, for every maximal program $\mathbf{b}$ of (P,M):

$$p_{i,j}^{(k)}\,\beta_i\Big(\sum_u b_u P_k(u)\Big) = 0, \qquad \forall (i,k) \neq (j,0).$$

The same proposition remains valid when P is replaced by Q and $p_{i,j}^{(k)}$ by $q_{i,j}^{(k)}$.

Proof. Let $\mathbf{b}$ and $\boldsymbol{\beta}$ be two extremal programs of (P,M) and $(P,M)'$, respectively. By use of (3.14) and (3.16), with $A = P$, it is easy to check that we have

$$\gamma v_j = \sum_u b_u\Big(\sum_i \beta_i P_i(u)\Big) P_j(u)$$

$$= \sum_{i,k} p_{i,j}^{(k)}\,\beta_i\Big(\sum_u b_u P_k(u)\Big),$$

according to (2.19). Since $\mathbf{b}$ is a maximal program of (P,M), it satisfies $\sum b_u = g = \gamma$. Hence, using $p_{j,j}^{(0)} = v_j$, we obtain

$$\gamma v_j (1-\beta_j) = \sum_{(i,k)\neq(j,0)} p_{i,j}^{(k)}\,\beta_i\Big(\sum_u b_u P_k(u)\Big).$$

As each term of the right-hand sum is nonnegative, by (3.9) and (3.13), this yields the desired results about $(P,M)'$. The reasoning is exactly the same for $(Q,M)'$; it is essentially based on lemma 2.4.

3.3. Cliques in association schemes

Let $R = \{R_i \mid i \in N\}$ be a family of $n+1$ relations on X satisfying A1 and A'2 (sec. 2.1) and let M be a subset of N with $0 \in M$. Then a nonempty subset Y of X will be called an *M-clique with respect to R* if it satisfies

$$R_i \cap Y^2 = \emptyset, \qquad \forall i \in N - M, \quad (3.17)$$

i.e., equivalently, if any two points of Y are jth associates for some $j \in M$. The main problem we shall now consider is to find an upper bound to the number of points in M-cliques.

3.3.1. *The Elias theorem*

In this section, all relations R_i are assumed to be regular, although (X,R) not necessarily is an association scheme. Then it is possible to derive information about cliques $Y \subseteq X$ from results on cliques Y' in certain subsets X' of X. Essentially, the argument is due to Elias; it led to the important *Elias bound* in coding theory (cf. Berlekamp [6]), p. 318).

Let L be a nonempty subset of N. Then, for a point $e \in X$, we define a subset $C_L(e)$ of X as follows:

$$C_L(e) = \bigcup_{i \in L} \{z \in X \mid (e,z) \in R_i\}.$$

This could be called a *crown of centre e*. By assumption, the cardinality of $C_L(e)$ is independent of e: if v_i denotes the valence of R_i, then

$$|C_L(e)| = \sum_{i \in L} v_i. \tag{3.18}$$

Theorem 3.7. Let L and M be subsets of N, with $0 \in M$. If Y is an M-clique with respect to R, then there exists a crown $X' = C_L(e)$ and an M-clique $Y' \subseteq X'$ satisfying $|X|^{-1}|Y| \leqslant |X'|^{-1}|Y|'$.

Proof. Let us first establish the following identity, for an arbitrary subset Y of X:

$$\sum_{x \in X} |Y \cap C_L(x)| = |Y| \sum_{i \in L} v_i. \tag{3.19}$$

The left-hand member is the number of pairs (x,y) with $x \in X$, $y \in Y$, $y \in C_L(x)$. The relations R_i being symmetric, condition $y \in C_L(x)$ is equivalent to $x \in C_L(y)$. Hence the number of pairs to be counted is equal to the sum of $|C_L(y)|$ for y running through Y, that is, by (3.18), to the right-hand member of (3.19).

Next, from (3.19) we immediately deduce

$$|X| \max_{x \in X} |Y \cap C_L(x)| \geqslant |Y| \sum_{i \in L} v_i. \tag{3.20}$$

Let us choose a point $e \in X$ for which $|Y \cap C_L(e)|$ is maximal and define $X' = C_L(e)$, $Y' = Y \cap X'$. Then (3.20) becomes $|X|\,|Y'| \geqslant |Y|\,|X'|$. Since Y obviously is an M-clique whenever Y itself is an M-clique, this proves the theorem.

Example. Let $(F^n,R) = H(n,2)$ be the Hamming scheme of length n over a set F of two elements (cf. sec. 2.5). For some integer n', with $1 \leqslant n' \leqslant n/2$, we define $L = \{n'\}$; then the crown $C_L(e)$ is a sphere of centre e and radius n' in the Hamming metric space. The nonempty restrictions of the distance relations R_i to the sphere $X' = C_L(e)$ are the following subsets of $(X')^2$:

$$R_j' = \{(x',y') \in (X')^2 \mid d_H(x',y') = 2j\}, \qquad j = 0, 1, \ldots, n'.$$

It can be shown that $(X',\{R_j'\})$ is an association scheme, with n' classes, which, up to isomorphism, is independent of the centre e; this scheme will be examined in detail in sec. 4.2 under the name of Johnson scheme, with the notation $J(n',n)$. At the present, we only want to emphasize theorem 3.7: it shows how

upper bounds to the cardinality of cliques in the Johnson scheme $J(n',n)$ yield bounds of the same type for the Hamming scheme $H(n,2)$.

3.3.2. *The linear-programming bound*

It is obvious, by (3.1) and (3.17), that an M-clique is entirely specified in terms of its inner distribution $\mathbf{a}$ by the following condition:

$$a_i = 0, \qquad \forall\, i \in N - M. \tag{3.21}$$

Henceforth we assume (X,R) to be a symmetric association scheme. Then theorem 3.3 implies a strong necessary condition on the distribution $\mathbf{a}$ of an M-clique; in the terminology of sec. 3.2, it can be expressed as follows.

Theorem 3.8. Let Q be the second eigenmatrix of a symmetric association scheme. Then the inner distribution of every M-clique Y in the scheme is a program of (Q,M) such that $g = |Y|$.

Proof. This is an immediate consequence of definition (3.21), the inequalities $\mathbf{a}Q_k \geqslant 0$ of theorem 3.3 and the obvious identities $a_0 = 1$, $\sum a_i = |Y|$ satisfied by the inner distribution $\mathbf{a}$.

Since, by lemma 3.5, the programs of (Q,M) are bounded, the maximal value $g(Q,M)$ of g is well defined and theorem 3.8 yields

$$|Y| \leqslant g(Q,M), \tag{3.22}$$

for every M-clique Y with respect to R. Inequality (3.22) will be called the *linear-programming bound for cliques*. Theorem 3.4 will be used at several places for discussion of M-cliques achieving this bound.

Example. Let us apply (3.22) to the simplest nontrivial case, i.e. to strongly regular graphs (cf. sec. 2.4). For $n = 2$ and $M = \{0,1\}$ our definition of an M-clique with respect to $R = \{R_0, R_1, R_2\}$ reduces to the usual notion of a clique (= complete subgraph) in the strongly regular graph (X,R_1). It is left to the reader to verify, by use of (2.30), that the linear-programming bound (3.22) for such cliques is

$$|Y| \leqslant 1 + v_1/(-s_1). \tag{3.23}$$

Let us also check theorem 3.4. We observe that $\mathbf{a} = (1, -v_1/s_1, 0)$ and $\alpha = (1, 0, -v_1/s_1\mu_2)$ are programs of (Q,M) and $(Q,M)'$, respectively, satisfying (3.15) and (3.16) with $A = Q$. In agreement with theorem 3.4(ii), one has $g = \gamma = 1 - v_1/s_1$ for these extremal programs.

To conclude this section about cliques, we shall give a very general consequence of theorems 3.4 and 3.8, showing the strength of the method.

Theorem 3.9. Let M be a subset of N, with $0 \in M$, and let $\bar{M} = N - M^*$. If Y is an M-clique and Z an $\bar{M}$-clique in an association scheme, then $|Y||Z| \leqslant |X|$ holds.

Proof. Let $\mathbf{b}$ and $\mathbf{c}$ be the inner distributions of Y and Z, respectively. Then from the eigenmatrix Q and the multiplicities μ_k we define real numbers $\beta_0, \ldots, \beta_n$ as follows:

$$\beta_k = (|Z|\,\mu_k)^{-1} \sum_j c_j\, Q_k(j). \tag{3.24}$$

Clearly (cf. for instance theorem 3.8), the β_k are nonnegative with $\beta_0 = 1$. On the other hand, using (2.22) we readily obtain

$$\sum_k \beta_k\, Q_k(i) = |Z|^{-1}\,|X|\; v_i^{-1}\, c_i, \tag{3.25}$$

with v_i = valence of R_i. Since Z is an M-clique, c_i is zero for each i in M^*. Therefore, (3.25) shows that $\boldsymbol{\beta}$ is a program of $(Q,M)'$, the conditions (3.12) being satisfied with equality.

Next, we observe that $\mathbf{b}$ is a program of (Q,M) with $g = |Y|$, by theorem 3.8. Hence the inequality $g \leqslant \gamma$ for the programs $\mathbf{b}$, $\boldsymbol{\beta}$ becomes

$$|Y| \leqslant \sum_k \beta_k\, Q_k(0) = |Z|^{-1}\,|X|, \tag{3.26}$$

according to (3.25) with $i = 0$, and the theorem is proved.

Certain classical inequalities of coding theory can be derived from theorem 2.9, for instance the Hamming bound (cf. secs 4.3.3 and 5.2.2). The interesting point about the linear-programming method is the fact that it also gives necessary conditions on the distributions $\mathbf{b}$, $\mathbf{c}$ for pairs (Y = M-clique, Z = $\bar{M}$-clique) satisfying equality in (3.26). Indeed, the reasoning has shown that equality holds if and only if $(\mathbf{b},\boldsymbol{\beta})$ is a pair of extremal programs. Hence theorem 3.4(ii) with $A = Q$, when applied to this pair, yields, by (3.24):

$$\Big(\sum_i b_i\, Q_k(i)\Big)\,\Big(\sum_j c_j\, Q_k(j)\Big) = 0, \qquad k = 1, \ldots, n.$$

These conditions (to be compared with $b_k\, c_k = 0$) could be very useful in a study of pairs (Y,Z) achieving the bound of theorem 3.9; they would lead, for instance, to the Lloyd theorem on perfect codes (cf. sec. 5.2.2).

3.4. Designs in association schemes

Let (X,R) be a symmetric association scheme with n classes and let T be any subset of $N^* = \{1, 2, \ldots, n\}$. Then a nonempty subset Y of X will be called a *T-design with respect to R* if its inner distribution $\mathbf{a}$ satisfies

$$\sum_i a_i\, Q_k(i) = 0, \qquad \forall\, k \in T. \tag{3.27}$$

where Q is the second eigenmatrix of the scheme. In other words, a T-design

has the following extremal properties among the subsets of X: the general conditions $\mathbf{a}Q_k \geqslant 0$ of theorem 3.3 hold with equality for each k in T.

In general, we can give no clear "combinatorial" interpretation for the concept of T-design. However, as we shall see in ch. 4, some T-designs in the Hamming and Johnson schemes are among the most classical combinatorial configurations. This motivates the present general definition, the "conjecture" being that T-designs will often have interesting properties. Let us also emphasize the formal duality between the notions of cliques and designs (cf. definitions (3.21) and (3.27)). This duality will appear throughout the text.

Several equivalent forms of the conditions $\mathbf{a}Q_k = 0$ have been indicated in sec. 3.1. One of them leads to the following criterion for T-designs.

Theorem 3.10. Let $J_0, J_1, \ldots, J_n$ be the minimal idempotents of the Bose–Mesner algebra of (X,R). Then a subset Y of X is a T-design if and only if $J_k\, \phi_Y = 0$ holds for each k in T.

Proof. The defining equations of a T-design are $\mathbf{a}Q_k = 0$, $\forall\, k \in T$. Now, according to (3.8), the condition $\mathbf{a}Q_k = 0$ is equivalent to $\phi_Y{}^T J_k\, \phi_Y = 0$, i.e. to $J_k\, \phi_Y = 0$, since J_k is positive semi-definite. Hence the theorem is proved.

The condition $\phi_Y{}^T J_k\, \phi_Y = 0$ $(\forall\, k \in T)$ specifying a T-design is to be compared with the definition $\phi_Y{}^T D_i\, \phi_Y = 0$ $(\forall\, i \in N - M)$ of an M-clique. In analogy to sec. 3.2.2, let us now apply the linear-programming method in order to obtain a lower bound to the number of points in T-designs.

Theorem 3.11. Let Y be a T-design in an association scheme of eigenmatrices P and Q. If $\mathbf{a}$ denotes the inner distribution of Y, then the $(n+1)$-tuple

$$\mathbf{b} = |Y|^{-1}\, \mathbf{a}\, Q \tag{3.28}$$

is a program of $(P,\, N - T)$ such that $g = |Y|^{-1}\,|X|$.

Proof. From (2.15) and (3.28) we deduce $\mathbf{a} = |X|^{-1}\,|Y|\, \mathbf{b}\, P$ and, consequently, $\mathbf{b}\, P_k \geqslant 0$ for all k. On the other hand, we have $b_0 = 1$ and all components b_i of $\mathbf{b}$ are nonnegative, by theorem 3.3. Hence, for a T-design, $\mathbf{b}$ is a program of $(P,\, N - T)$. Finally, for this program we have $g = \mathbf{b}\, P_0 = |Y|^{-1}\,|X|$, which concludes the proof.

According to lemma 3.5, the programs of (P,M) are bounded, so that the maximal value $g(P,M)$ of g is well defined, and theorem 3.11 gives the *linear-programming bound for designs:*

$$|Y| \geqslant |X|/g(P,\, N - T). \tag{3.29}$$

Example. Let us examine the combinatorial meaning of designs for a strongly

regular graph (X,R_1) and apply the linear-programming bound in this simple case (cf. sec. 2.4). Let $\{Y,Z\}$ be a bipartition of X such that $(Y,R_1 \cap Y^2)$ and $(Z,R_1 \cap Z^2)$ are regular subgraphs of (X,R_1), and assume the valences satisfy $\mathrm{val}\,(R_1 \cap Y^2) + \mathrm{val}\,(R_1 \cap Z^2) \geqslant \mathrm{val}\,(R_1)$. Then $\{Y,Z\}$ will be called a *regular bipartition.*

On the other hand, for $T = \{2\}$, we consider the T-designs $Y (\neq X)$ in the association scheme (X,R) with $R = \{R_0, R_1, R_2\}$. It is not difficult to show that these two concepts are equivalent: Y is a T-design if and only if $\{Y, X - Y\}$ is a regular bipartition of X.

Using (2.30) we easily obtain the maximal value of g for the problem (P,M) with $M = \{0,1\}$; the result is $g(P,M) = 1 - v_2/r_2$. Hence, using the identity $(v_1 - s_1)(v_2 - r_2) = v\, s_1\, r_2$, we can write (3.29) as follows:

$$|Y| \geqslant 1 + v_1/(-s_1). \tag{3.30}$$

It turns out that the (unique) maximal program $\mathbf{b}$ of (P,M) satisfies $\mathbf{b}P_2 = 0$. Therefore, if a regular bipartition $\{Y, X - Y\}$ achieves (3.30), then the inner distribution of Y is $\mathbf{a} = (1, -v_1/s_1, 0)$, i.e., equivalently, Y is a clique in the graph (X,R_1) achieving the linear-programming bound (3.23).

Remark. The definition of T-designs in a symmetric association scheme (X,R) can be extended so as to admit the possibility of "repeated points". Let us briefly outline this generalization. For a nonzero vector $\phi \in \mathbf{R}(X)$ with integral nonnegative components $\phi(x)$, we define the *distribution of* ϕ to be the $(n+1)$-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_n)$ of rational numbers a_i given by

$$a_i = (\phi^T \phi)^{-1} (\phi^T D_i \phi), \tag{3.31}$$

where D_i is the adjacency matrix of R_i. In particular, when all components $\phi(x)$ are 0 or 1, this is exactly the concept of the inner distribution (3.3) for the subset $Y \subseteq X$ such that $\phi_Y = \phi$. For any ϕ, the same argument as the one leading to (3.8) shows that the numbers $\mathbf{a}Q_k$ are nonnegative when $\mathbf{a}$ is defined by (3.31).

Given a subset T of N^*, the vector ϕ will be called a T-design if its distribution $\mathbf{a}$ satisfies (3.27). In the case $\phi = \phi_Y$ for some subset $Y \subseteq X$, the design is said to be *simple* (without repeated points). In the general case, considering $\phi(x)$ as "the number of occurrences of a point x in the design", one is interested in the total number of points, i.e. the integer $h = \phi^T \phi_X$.

Given a T-design ϕ of distribution $\mathbf{a}$, it is not difficult to show, like in theorem 3.11, that the $(n+1)$-tuple $\mathbf{b} = h^{-2} (\phi^T \phi)\, \mathbf{a} Q$ is a program of $(P, N - T)$ with $g = h^{-2} (\phi^T \phi)\, |X|$. It follows that the linear-programming bound (3.29) is valid in the general case when $|Y|$ is replaced by h. Indeed we can write

$$h \geqslant h^2 (\phi^T \phi)^{-1} \geqslant |X|/g(P, N - T);$$

the right-hand inequality is simply $g \leqslant g(P, N - T)$; as for the left-hand inequality, it follows from the obvious property $\phi(x)\,[\phi(x) - 1] \geqslant 0$. As a consequence, we observe that a T-design achieving the linear-programming bound, i.e. $h = |X|/g(P, N - T)$, must satisfy $\phi(x) = 0$ or 1 for all x; equivalently, ϕ must be simple.

3.5. Characteristic matrices

For an association scheme (X,R) with n classes, let $S \in \mathbf{C}(X,X')$ be an orthogonal matrix diagonalizing the Bose–Mesner algebra and let $X_0', X_1', \ldots, X_n'$ be the classes of the partition $\pi(X',S)$ of X' (cf. sec. 2.2). Given a nonempty subset Y of X, we shall denote by H_k the restriction of S to the subset $Y \times X_k'$ of $X \times X'$. In particular, H_0 is the all-one vector. The matrices H_k, called the *characteristic matrices of* Y, will be a useful tool especially for the study of some T-designs (see sec. 5.3). We now give a few general results. We start with an equivalent formulation of theorem 3.10.

Theorem 3.12. Let $H_0, H_1, \ldots, H_n$ be the characteristic matrices of a subset Y of X for a symmetric association scheme (X,R). Then Y is a T-design with respect to R if and only if $H_k^T H_0 = 0$ holds for each k in T.

Next, we shall derive some formulas on the matrix products $H_k \bar{H}_k$ and $\bar{H}_t H_j$. We use the notation $D_i \mid Y$ for the adjacency matrix of $R_i \cap Y^2$, i.e. for the restriction of D_i to Y^2. For the rest, the notations are the same as in ch. 1.

Theorem 3.13. The characteristic matrices H_k of a given subset Y of X and the adjacency matrices $D_i \mid Y$ are related by

$$H_k \bar{H}_k = \sum_i Q_k(i)\,(D_i \mid Y). \tag{3.32}$$

Proof. This is an immediate consequence of the definition (2.16) of the eigenmatrix Q since, by (2.9), $H_k \bar{H}_k$ is the restriction of the matrix $|X|\, J_k$ to Y^2.

Lemma 3.14. Let $\mathbf{a}$ be the inner distribution of Y. Then the characteristic matrices of Y satisfy

$$\|\bar{H}_t H_j\|^2 = |Y| \sum_k q_{t,t}^{(k)} (\mathbf{a} Q_k), \qquad \text{for} \qquad Q_t = Q_j^*. \tag{3.33}$$

Proof. Let us substitute ϕ_Y for ϕ in the identity (2.28). Then we obtain immediately the desired result by using (3.8), remembering that H_t is the restriction of S_t to $Y \times X_t'$.

Theorem 3.15. For given integers $i, t \in N$, assume the inner distribution $\mathbf{a}$ of Y satisfies $q_{t,t}^{(k)} (\mathbf{a} Q_k) = 0$ for $k = 1, 2, \ldots, n$. Then the following equation

holds, for $Q_j = Q_i^*$:

$$\hat{H}_i H_j = \begin{cases} 0 & \text{if} \quad i \neq j, \\ |Y| I & \text{if} \quad i = j. \end{cases} \tag{3.34}$$

Conversely, (3.34) implies $q_{i,t}^{(k)}(\mathfrak{a} Q_k) = 0$ for $Q_t = Q_j^*$ and all $k \geqslant 1$.

Proof. Assuming $q_{i,t}^{(k)}(\mathfrak{a} Q_k) = 0$ for $k = 1, 2, \ldots, n$, we can write (3.33) as follows, using (2.27):

$$\| \hat{H}_i H_j \|^2 = |Y|^2 \mu_i \delta_{i,j}. \tag{3.35}$$

This proves (3.34) for $i \neq j$. Let us now examine the case $i = j$. By theorem 3.13 we have $\operatorname{tr}(\hat{H}_i H_i) = \operatorname{tr}(H_i \hat{H}_i) = \mu_i |Y|$. It is easily seen that this, together with (3.35), implies $\| \hat{H}_i H_i - |Y| I \| = 0$ and, consequently, $\hat{H}_i H_i = |Y| I$.

In order to prove the converse result, we first observe that all terms $q_{i,t}^{(k)}(\mathfrak{a} Q_k)$ of the sum Σ in (3.33) are nonnegative real numbers, by lemma 2.4 and theorem 3.3. On the other hand, condition (3.34) exactly means that Σ reduces to its term $|Y| \mu_i \delta_{i,j}$ of index $k = 0$. Hence all terms with $k \geqslant 1$ must be zero whenever (3.34) is satisfied.

To conclude this section let us indicate, without proof, how the distribution matrix B introduced in sec. 3.1 can be expressed in terms of the matrices S, P and H_k; it is given by

$$B = |X|^{-1} S (\hat{H}_0 H_0 \oplus \hat{H}_1 H_0 \oplus \ldots \oplus \hat{H}_n H_0) P,$$

where $\oplus$ stands for the direct sum. This equation, together with (3.8), could be used to give another proof of theorem 3.1.

4. AN INTRODUCTION TO ALGEBRAIC CODING THEORY

In the present chapter we shall examine in detail two types of finite metric spaces having the structure of association schemes: the Hamming schemes and the Johnson schemes, which we already mentioned in secs 2.5 and 3.3.1. These appear to be the natural frameworks for a theory of codes, especially for its combinatorial aspects.

4.1. The Hamming schemes

Let F be a finite set of cardinality $q \geqslant 2$ and let n be a positive integer. We make the nth Cartesian power $X = F^n$ of F a metric space by defining the *Hamming distance* $d_H(x,y)$ between two points $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ of X as follows:

$$d_H(x,y) = |\{j \mid 1 \leqslant j \leqslant n,\ x_j \neq y_j\}|. \tag{4.1}$$

In other words, the distance between two points is the number of coordinate places in which they differ. Next, we define the distance relations R_0, R_1, $\ldots$, R_n in an obvious way; two points of X are ith associates whenever they are at distance i:

$$R_i = \{(x,y) \in X^2 \mid d_H(x,y) = i\}. \tag{4.2}$$

It is easy to show, by verification of the axioms, that (X,R) is a symmetric association scheme for $R = \{R_0, R_1, \ldots, R_n\}$. An algebraic proof of this result is implicitly contained in the argument of theorem 4.2. For given n and q, we call (X,R) the *Hamming scheme of length n over F*, and denote it by $H(n,q)$.

4.1.1. *Eigenmatrices and Krawtchouk polynomials*

Let us provide F with the structure of an Abelian group, in an arbitrary way. We shall use an additive notation for the group operation and take the symbol 0 (zero) for the identity. The *Hamming weight* of an element x in the group $X = F^n$ then by definition is the number of nonzero components x_j of x. This allows to write (4.1) as follows:

$$d_H(x,y) = w_H(x - y), \qquad \forall\, x,y \in X. \tag{4.3}$$

Consequently, the distance relations (4.2) are invariant under translation in X, i.e. they satisfy (2.43), and it is well known that the matrix S of group characters of X diagonalizes the Bose–Mesner algebra of the scheme. Let us examine this more closely in order to obtain an explicit form of the eigenmatrices.

Let $(\alpha,\beta) \mapsto \langle \alpha,\beta \rangle$ be an *inner product* on the group F, i.e. a symmetric mapping of F^2 into $\mathbf{C}$ such that, when α runs through F, the mapping $\beta \mapsto \langle \alpha,\beta \rangle$ runs through the group of complex characters of F. The inner prod-

uct is described more in detail in sec. 6.1. We shall need the following result (cf. theorem 6.2):

$$\sum_{\beta \in F^n} \langle \alpha,\beta \rangle = \begin{cases} q-1 & \text{for} \quad \alpha = 0, \\ -1 & \text{for} \quad \alpha \in F^*, \end{cases} \tag{4.4}$$

with $F^* = F - \{0\}$. Next, keeping the same notation $\langle x,y \rangle$, let us extend the inner product to the group $X = F^n$ by defining, for $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n) \in X$,

$$\langle x,y \rangle = \prod_{i=1}^{n} \langle x_i,y_i \rangle, \tag{4.5}$$

from the inner product $\langle x_i,y_i \rangle$ of the components $x_i,y_i \in F$. It can easily be verified that (4.5) is then itself an inner product on X; we shall call it the *natural product on X*.

Let us briefly apply these notions to the binary case ($q = 2$), which might be more familiar to the reader. For $\alpha,\beta \in F = \{0,1\}$, we have $\langle \alpha,\beta \rangle = (-1)^{\alpha\beta}$. Hence the natural product of two binary n-tuples x and y can be written as $\langle x,y \rangle = (-1)^{[x,y]}$, where $[x,y] \equiv x_1y_1 + \ldots + x_ny_n \pmod 2$ is the scalar product of x and y considered as vectors over the binary field.

We now go back to an arbitrary $q \geqslant 2$ and define the *weight partition* $\sigma = \{X_0, X_1, \ldots, X_n\}$ to be formed by the classes of elements having a constant weight:

$$X_k = \{x \in X \mid w_H(x) = k\}, \qquad k = 0, 1, \ldots, n. \tag{4.6}$$

The cardinality of X_k (= valence of R_k) is equal to $v_k = \binom{n}{k}(q-1)^k$. On the other hand, with a normalization adapted to our problem, we introduce the Krawtchouk polynomials (cf. Szegö [70]) as follows: for given n and q, and an integer $k = 0, 1, \ldots, n$, the polynomial

$$K_k(u) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{u}{j}\binom{n-u}{k-j}, \tag{4.7}$$

in the indeterminate u, will be called the *Krawtchouk polynomial* of degree k. (We use the notation $\binom{u}{j} = u(u-1)\ldots(u-j+1)/j!$.) It is easy to check that $K_k(u)$ actually is a polynomial of degree k in the variable u. This fact appears even better from an equivalent expression of the Krawtchouk polynomials, the verification of which is left to the reader:

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

Before deriving the eigenmatrices of the Hamming scheme (theorem 4.2), we

give a relation between the concepts introduced above (natural product, weight partition and Krawtchouk polynomials).

Theorem 4.1. The natural product (4.5) and the Krawtchouk polynomials are related by the following equation, for $u,k = 0, 1, \ldots, n$:

$$\sum_{x' \in X_k} \langle x,x' \rangle = K_k(u), \qquad \forall\, x \in X_u. \tag{4.8}$$

Proof. First, we consider a fixed subset J of $\{1, 2, \ldots, n\}$, with $|J| = k$, and we compute the contribution $c(J)$ to the left-hand member of (4.8) afforded by the $(q-1)^k$ elements $x' \in X_k$ such that $x_i' \neq 0$ for all $i \in J$. Using (4.5) we obtain

$$c(J) = \prod_{i \in J} \left(\sum_{\beta \in F^*} \langle x_i,\beta \rangle \right).$$

By (4.4) we see that the number under brackets is equal to $q-1$ or -1 according to whether x_i is zero or not. Hence, denoting by j the number of non-zero components x_i with $i \in J$, we have $c(J) = (-1)^j (q-1)^{k-j}$.

On the other hand, the number of choices for J corresponding to a given j is equal to $\binom{n}{j}\binom{n-u}{k-j}$, for $w_H(x) = u$. Therefore, adding up all integers $c(J)$, we obtain exactly the right-hand member of (4.7), which concludes the proof.

Theorem 4.2. The eigenmatrices P and Q of the Hamming scheme $H(n,q)$ are given in terms of the Krawtchouk polynomials by

$$P_k(i) = Q_k(i) = K_k(i), \qquad i,k = 0, 1, \ldots, n.$$

Moreover, $H(n,q)$ is self-dual with respect to the zero of X and to the matrix $S \in \mathbf{C}(X,X)$ defined from the natural product by $S(x,x') = \langle x,x' \rangle$.

Proof. Let us consider the weight partition $\sigma = \{X_k\}$ of X' (= X) and the corresponding submatrices $S_k \in \mathbf{C}(X,X_k)$ of S. Using theorem 4.1 we obtain the following formula for the (x,y)-entry of $S_k \bar{S}_k$:

$$(S_k \bar{S}_k)(x,y) = \sum_{x' \in X_k} \langle x-y,x' \rangle$$

$$= K_k(w_H(x-y)). \tag{4.9}$$

According to (4.2) and (4.3), $w_H(x-y)$ is equal to i if and only if (x,y) belongs to R_i. Hence, using the incidence matrices D_i of the R_i, we can write (4.9) as follows:

$$S_k \bar{S}_k = \sum_{i=0}^{n} K_k(i)\, D_i. \tag{4.10}$$

On the other hand, the matrices $J_k = |X|^{-1} S_k \bar{S}_k$, for $k = 0, 1, \ldots, n$, form a set of mutually orthogonal idempotents of $\mathbf{C}(X,X)$. Since, by (4.10),

the J_k belong to the BM algebra of the scheme, they are the minimal idempotents of it. Comparing (4.10) to the definition (2.16) of the eigenmatrix Q, we deduce $Q_k(i) = K_k(i)$ for all i,k.

Finally, with the definitions of sec. 2.6, it can easily be shown that (X,R) is dual to itself with respect to $e = 0$ and to S, the partitions $\pi(X,S)$ and $\tau(X,e)$ being both the weight partition σ. The details of the argument are omitted. Then it follows from theorem 2.8 that the eigenmatrices P and Q are equal, which concludes the proof.

Applying theorem 2.3 to the Hamming scheme $H(n,q)$, we obtain the well-known orthogonality relations on the Krawtchouk polynomials:

$$\sum_{i=0}^{n} K_r(i)\,K_s(i)\binom{n}{i}(q-1)^i = q^n\binom{n}{s}(q-1)^s\,\delta_{r,s},$$

for $r,s = 0, 1, \ldots, n$. Consequently, the polynomials $K_0(u), K_1(u), \ldots, K_n(u)$ form "the" family of orthogonal polynomials on the set $N = \{0, 1, \ldots, n\}$ with respect to the weight function w defined by $w(i) = v_i = \mu_i = \binom{n}{i}(q-1)^i$. From a classical result about orthogonal polynomials (cf. Szegö [70], p. 42), we deduce the following useful recurrence relation on the $K_k(u)$:

$$(k+1)\,K_{k+1}(u) = (k+(q-1)(n-k)-qu)\,K_k(u) - (q-1)(n-k+1)\,K_{k-1}(u). \qquad (4.11)$$

4.1.2. *Codes in Hamming schemes*

A *code of length n over an alphabet F* by definition is a nonempty subset Y of $X = F^n$ provided with the Hamming distance (4.1). The elements of Y are called the *codewords*. The linear-programming bound (3.22) yields an upper bound to the number of codewords in codes submitted to restrictions of the following type: the distance between codewords can only assume some specified values. Indeed, if M is this set of values, such a code is nothing but an M-clique in the Hamming scheme.

Particular cases, being most important in theory of error detecting or correcting codes, are provided by sets M of the form

$$M = \{0, \delta, \delta+1, \ldots, n\}, \qquad (4.12)$$

for some integer δ with $1 \leqslant \delta \leqslant n$. An M-clique in $H(n,q)$ then is a q-ary code of length n having the property that the *minimum distance* between distinct codewords is at least equal to δ. Since the best code of given parameters n, q, δ is the one containing the largest number of words, many authors were interested in obtaining upper bounds to the number of codewords in such

codes. As for the binary case ($q = 2$), the most important from a practical point of view, let us especially refer to a paper by Johnson [33]).

The numerical values computed up to now for the linear-programming bound $|Y| \leqslant g(Q,M)$ lead to the hope that it will, in many cases, improve the known bounds (cf. also sec. 4.3). McEliece, Rumsey and Welsh, who discovered the linear-programming bound for codes independently of the author, have obtained more than promising results in this direction (private communication by R. J. McEliece). Unfortunately, a general explicit formula for $g(Q,M)$ seems to be out of the question; each case is a specific problem and, for relatively large values of n, one needs a computer.

Before giving an example treatable by hand, let us describe a method which allows to simplify the computation of $g(Q,M)$ in some important particular cases. A subset M of $N = \{0, 1, \ldots, n\}$,with $0 \in M$, will be called *even* if it contains only even numbers and *odd* if it has the following two properties:

$$(i \in M,\ \ i \equiv 0 \pmod 2,\ \ i \geqslant 1) \Rightarrow (i-1 \in M),$$
$$(i \in M,\ \ i \equiv 1 \pmod 2,\ \ i \leqslant n-1) \Rightarrow (i+1 \in M).$$

For instance, the set (4.12) is odd whenever δ is an odd integer.

Next, let us define the set $N' = \{0, 1, \ldots, n, n+1\}$. To a given odd subset M of N we associate the even subset M' of N' given by

$$M' = \{i \in N' \mid i \equiv 0 \pmod 2,\ \ i-1 \in M\} \cup \{0\}. \qquad (4.13)$$

It is easy to show that $M \mapsto M'$ is in fact a 1–1 correspondence between the odd subsets of N and the even subsets of N', with the following relation between cardinalities: $m' = [(m+1)/2]$ for $m = |M^*|$ and $m' = |M'^*|$.

Theorem 4.3. Let M be an odd subset of N, and M' be the corresponding even subset (4.13) of N'. On the other hand, let Q and Q' be the eigenmatrices of the Hamming schemes $H(n,2)$ and $H(n+1,2)$, respectively. Then $g(Q,M) = g(Q',M')$ holds, for $q = 2$.

Proof. The theorem follows from two remarks: (i) For a given program $\mathbf{b}$ of (Q,M), the $(n+2)$-tuple $\mathbf{b}' = (b_0', \ldots, b_{n+1}')$ defined by

$$b_i' = \begin{cases} b_{i-1} + b_i & \text{for} \quad i \equiv 0 \pmod 2, \\ 0 & \text{for} \quad i \equiv 1 \pmod 2, \end{cases}$$

with $b_{-1} = b_{n+1} = 0$, is a program of (Q',M'), satisfying $\Sigma b_i' = \Sigma b_i$. (ii) For any program $\mathbf{b}'$ of (Q',M') the $(n+1)$-tuple $\mathbf{b} = (b_0, \ldots, b_n)$ defined by

$$(n+1)\,b_i = \begin{cases} (n-i+1)\,b_i' & \text{for} \quad i \equiv 0 \pmod 2, \\ (i+1)\,b_{i+1}' & \text{for} \quad i \equiv 1 \pmod 2, \end{cases}$$

is a program of (Q,M), satisfying $\Sigma b_i = \Sigma b_i'$. Both results can be obtained

from the properties of Krawtchouk polynomials with $q = 2$; the details of the argument will not be given.

It is obvious that such a double correspondence with $\Sigma b_i = \Sigma b_i'$ between the programs of (Q,M) and (Q',M') suffices to prove that the maximal values of $g = \Sigma b_i$ and $g' = \Sigma b_i'$ are equal.

The above result shows that, for $q = 2$ and an odd subset M of N, we may replace the linear-programming problem (Q,M) by the simpler problem (Q',M'), provided we are only interested in knowing $g(Q,M)$ and at least one maximal program of (Q,M).

On the other hand, for $q = 2$ and an even subset M' of N', we observe the following: any $(n+2)$-tuple $\mathbf{b}'$ such that $b_i' = 0$ for all $i \in N' - M'$ satisfies $\mathbf{b}' Q_k' = \mathbf{b}' Q_{n+1-k}'$ for all $k \in N'$. Hence the even problem (Q',M') contains in fact only $[(n+1)/2]$ inequalities $\mathbf{b}' Q_k' \geqslant 0$ in the $[(m+1)/2]$ variables b_i'.

Example. Let us examine the binary codes Y of length $n = 13$ and designed minimum distance $\delta = 5$, i.e. the M-cliques in $H(13, 2)$ with $M = \{0, 5, 6, \ldots, 13\}$. To the odd subset M of N corresponds the even subset $M' = \{0, 5, 8, 10, 12, 14\}$ of N'. According to theorem 4.3, the linear-programming bound is $|Y| \leqslant g(Q',M')$. The inequalities $\mathbf{b}' Q_k' \geqslant 0$ of the problem (Q',M') are the following:

$$
\begin{array}{rrrrrcr}
2b_5' & -2b_8' & -6b_{10}' & -10b_{12}' & -14b_{14}' & \geqslant & -14, \\
-5b_5' & -5b_8' & +11b_{10}' & +43b_{12}' & +91b_{14}' & \geqslant & -91, \\
-12b_5' & +12b_8' & +4b_{10}' & -100b_{12}' & -364b_{14}' & \geqslant & -364, \\
9b_5' & +9b_8' & -39b_{10}' & +121b_{12}' & +1001b_{14}' & \geqslant & -1001, \\
30b_5' & -30b_8' & +38b_{10}' & -22b_{12}' & -2002b_{14}' & \geqslant & -2002, \\
-5b_5' & -5b_8' & +27b_{10}' & -165b_{12}' & +3003b_{14}' & \geqslant & -3003, \\
-40b_5' & +40b_8' & -72b_{10}' & +264b_{12}' & -3432b_{14}' & \geqslant & -3432,
\end{array}
$$

the function to be maximized being $g' = 1 + b_5' + \ldots + b_{14}'$. The easiest way for obtaining the coefficients $Q_k'(i)$ in the above system is to use the recurrence relation (4.11) on the Krawtchouk polynomials; this yields $(k+1)\,Q_{k+1}'(i) = (14-2i)\,Q_k'(i) - (15-k)\,Q_{k-1}'(i)$.

One can solve the problem (Q',M') by hand, using the simplex algorithm. It turns out that there is a unique maximal program, namely $\mathbf{b}' = (1, 0, 0, 0, 0, 0, 42, 0, 7, 0, 14, 0, 0, 0, 0)$. Hence we deduce $g(Q',M') = 64$. In fact the linear-programming bound $|Y| \leqslant 64$ is the best possible since there actually exists a binary code Y of length 13 and minimum distance 5 containing 64 codewords; such a code can be derived from the Nordstrom–Robinson code [53] (cf. also Goethals [23]).

4.1.3. *Orthogonal arrays*

Since the eigenmatrices P and Q of the Hamming scheme $H(n,q)$ are identical, the problem of codes with a designed minimum distance is related, at least formally, to the problem of T-designs (cf. sec. 3.4) for sets T of the form

$$T = \{1, 2, \ldots, \tau-1, \tau\}, \qquad 1 \leqslant \tau \leqslant n; \tag{4.14}$$

in particular, the linear-programming bound (3.29) for T-designs is $|Y| \geqslant q^n/g(Q,M)$ where M is the set (4.12) with $\delta = \tau + 1$.

In this section it will be shown that such T-designs are in fact classical combinatorial configurations, namely the orthogonal arrays (without repeated rows) introduced by Rao [59].

Definition. To a code Y of length n over F corresponds the array whose rows are the words of Y. Let τ and λ be positive integers, with $\tau \leqslant n$. Then Y is said to form an *orthogonal array of strength τ and index λ* if, in each τ-tuple of distinct columns of the array, all τ-tuples of symbols of F appear exactly λ times. Then, obviously, $|Y| = \lambda q^\tau$ holds.

Before showing the equivalence between this definition and the concept of T-design, we need some notations. For an integer τ, $1 \leqslant \tau \leqslant n$, let us consider a τ-tuple $(\omega_1, \omega_2, \ldots, \omega_\tau)$ of symbols $\omega_i \in F$ and a τ-tuple $L = (i_1, i_2, \ldots, i_\tau)$ of distinct integers i_s, with $1 \leqslant i_s \leqslant n$. For a given code Y of length n over F we shall denote by $m_L(\omega_1, \ldots, \omega_\tau)$ the number of codewords $x \in Y$ such that

$$x_{i_1} = \omega_1, \qquad x_{i_2} = \omega_2, \ \ldots, \qquad x_{i_\tau} = \omega_\tau. \tag{4.15}$$

The above definition means that Y forms an orthogonal array of strength τ if and only if the following equation holds:

$$m_L(\omega_1, \omega_2, \ldots, \omega_\tau) = |Y|\, q^{-\tau}, \tag{4.16}$$

for each choice of the $\omega_i \in F$ and of L. As in sec. 4.1, we shall assume F has the structure of an Abelian group.

Theorem 4.4. For a given set $T = \{1, 2, \ldots, \tau\}$, with $1 \leqslant \tau \leqslant n$, a code Y is a T-design in $H(n,q)$ if and only if it forms an orthogonal array of strength τ.

Proof. For a τ-tuple $L = (i_1, i_2, \ldots, i_\tau)$ of distinct integers i_s, with $1 \leqslant i_s \leqslant n$, and an integer k, with $0 \leqslant k \leqslant \tau$, we define the following subset of $X = F^n$:

$$X_k(L) = \{x' \in X_k \mid x_i' = 0 \quad \text{for} \quad i \neq i_1, i_2, \ldots, i_\tau\},$$

where X_k is the weight class (4.6) of X. Clearly, the union $X(L) = X_0(L) \cup X_1(L) \cup \ldots \cup X_\tau(L)$ of these sets is the subgroup of X consisting of the q^τ elements x' satisfying $x_i' = 0$ for $i \neq i_1, \ldots, i_\tau$.

Next, let $H_k \in \mathbf{C}(Y, X_k)$ be the characteristic matrix of Y deduced from the matrix S of the natural product on X (cf. sec. 3.5), i.e. $H_k(x,x') = \langle x,x' \rangle$ for $x \in Y$, $x' \in X_k$. Using (4.5) and (4.15) we have, for $x' \in X_k(L)$:

$$(H_k^T H_0)(x') = \sum_{x \in X} \langle x,x' \rangle$$

$$= \sum_{\omega_j \in F} m_L(\omega_1, \ldots, \omega_\tau) \langle \omega_1, x_{i_1}' \rangle \ldots \langle \omega_\tau, x_{i_\tau}' \rangle. \quad (4.17)$$

Let us first assume Y forms an orthogonal array of strength τ. Then, substituting (4.16) into (4.17), we obtain, by the well-known properties of the inner product:

$$(H_k^T H_0)(x') = |Y| \, \delta_{0,k}. \quad (4.18)$$

Now, for any given $x' \in X_k$, there exists an L such that $x' \in X_k(L)$. Hence (4.18) is valid for all $x' \in X_k$ and for $k = 0, 1, \ldots, \tau$. Therefore, it follows from theorem 3.12 that Y is a T-design.

Conversely, we assume eqs (4.18) are identically satisfied for $x' \in X_k$ and $k \leqslant \tau$, i.e. Y is a T-design. Then, for a fixed τ-tuple L, we deduce from (4.17) and (4.18) the following system of q^τ linear equations in the q^τ unknowns $m_L(\omega_1, \ldots, \omega_\tau)$:

$$\sum_{\omega_j \in F} m_L(\omega_1, \ldots, \omega_\tau) \langle \omega_1, x_{i_1}' \rangle \ldots \langle \omega_\tau, x_{i_\tau}' \rangle = |Y| \, \delta_{0,x'},$$

where x' is any element of the group $X(L)$. It is well known that the above system admits a unique solution, namely (4.16). Hence Y forms an orthogonal array of strength τ, which concludes the proof.

Owing to theorem 4.4, we may apply the linear-programming bound (3.29) to orthogonal arrays of a given strength τ. The example examined in sec. 4.1.2 gives, without extra computation, $\lambda \geqslant 8$ for the index λ of binary orthogonal arrays of strength 4 having 13 columns. Here also the bound is achieved. One may expect that the linear-programming bound will often be stronger than the few known results on the problem. In particular, as will be seen in sec. 5.3.2, it is always at least as good as the Rao bound [59]).

4.2. The Johnson schemes

Let n and v be integers, wit $1 \leqslant n \leqslant v$. In the Hamming space of length v over $F = \{0, 1\}$ let us consider the sphere of radius n centred at the point $(0, \ldots, 0)$, that is, the following subset X of F^v:

$$X = \{x \in F^v \mid w_H(x) = n\}. \quad (4.19)$$

Clearly, $|X| = \binom{v}{n}$. In the rest of this section, we always assume $1 \leqslant n \leqslant v/2$. This will imply no loss of generality, since the spheres of radius n and $v - n$ are equivalent under translation in F^v.

The Hamming distance $d_H(x,y)$ between two points $x,y \in X$ obviously is an even integer not exceeding $2n$. For convenience we define the *Johnson distance* $d_J(x,y)$ to be

$$d_J(x,y) = \tfrac{1}{2} d_H(x,y), \qquad \forall\, x,y \in X; \quad (4.20)$$

equivalently, $n - d_J(x,y)$ is the number of coordinate positions p in which the v-tuples x and y satisfy $x_p = y_p = 1$. Then $d_J(x,y)$ assumes all integral values between 0 and n. Next, like in sec. 4.1, we introduce the distance relations $R_0, R_1, \ldots, R_n$ from (4.20):

$$R_i = \{(x,y) \in X^2 \mid d_J(x,y) = i\}.$$

It is easy to show, and of course well known, that the partition $R = \{R_0, R_1, \ldots, R_n\}$ of X^2 yields a symmetric association scheme (X,R) with n classes. A rather indirect proof of this result will appear, implicitly, in lemma 4.5 below. We observe at this point, leaving the verification to the reader, that the valence of R_i is

$$v_i = \binom{n}{i}\binom{v-n}{i}. \quad (4.21)$$

For given n and v, with $1 \leqslant n \leqslant v/2$, we shall call (X,R) the *Johnson scheme* $J(n,v)$, by reference to the author who first considered codes in the metric space (X,d_J), i.e. binary codes of length v and constant weight n (cf. Johnson [34])). It turns out that the Johnson bound [32,33]) for binary codes of specified minimum distance in the space (F^v,d_H) depends on bounds of the same type for constant weight codes. (See also the Elias theorem in sec. 3.3.1.) Apart from this application in classical coding theory, the Johnson scheme provides an excellent framework for a study of the t-designs (cf. sec. 4.2.3), which here play a very similar role as the orthogonal arrays in the Hamming schemes.

4.2.1. *Eigenmatrices and Eberlein polynomials*

In order to apply the general theory, we first need explicit formulas for the eigenmatrices P and Q. The situation is not so simple as in Hamming schemes because here, at our starting point, we do not have an orthogonal matrix diagonalizing the adjacency matrices D_j of the relations R_j.

For a given integer i, with $0 \leqslant i \leqslant n$, let us define the following linear combination of the matrices D_j in $\mathbf{R}(X,X)$:

$$C_i = \sum_{k=i}^{n} \binom{k}{i} D_{n-k}. \quad (4.22)$$

Obviously, the C_i generate the same algebra as the D_j. To see what these C_i really are, it is convenient to introduce the mapping f of the set F^v onto the

Boolean algebra of the set $V = \{1, 2, \ldots, v\}$ given by

$$x = (x_1, x_2, \ldots, x_v) \mapsto f(x) = \{p \in V \mid x_p = 1\}. \tag{4.23}$$

Clearly, f is a bijection which maps the elements of a given Hamming weight u onto the u-subsets of V (i.e. the subsets of cardinality u); in particular, the images $f(x)$ of the points $x \in X$ are the n-subsets of V. It is easily seen that a pair (x,y) of X^2 belongs to R_{n-k} if and only if the intersection $f(x) \cap f(y)$ is a k-subset of V. Consequently, the integer $C_i(x,y)$ defined by (4.22) is the number of i-subsets of $f(x) \cap f(y)$.

The following lemma contains an implicit proof of the fact that (X,R) actually is an association scheme (cf. theorem 2.1). It gives a complete description of the Bose–Mesner algebra in the basis of the C_i.

Lemma 4.5. The matrices $C_0, C_1, \ldots, C_n$ satisfy

$$C_r C_s = \sum_{t=0}^{\min(r,s)} \binom{n-t}{r-t}\binom{n-t}{s-t}\binom{v-r-s}{v-n-t} C_t. \tag{4.24}$$

Proof. Let V_k be the set of k-subsets of V. For $\alpha = f(x)$, $\beta = f(y) \in V_n$ with $\alpha \cap \beta \in V_w$, it follows from the definitions that $(C_r C_s)(x,y)$ is equal to the number of triples $(\xi,\eta,\gamma) \in V_r \times V_s \times V_n$ satisfying $\xi \subseteq \alpha$, $\eta \subseteq \beta$ and $\xi \cup \eta \subseteq \gamma$. In order to calculate this number, let us first fix the values of $|\xi \cap \beta| = i$ and $|\xi \cap \eta| = j$. For given i, j, the number of choices for ξ, η and γ then is

$$\binom{n-u}{r-i}\binom{u}{i}, \quad \binom{n-i}{s-j}\binom{i}{j} \quad \text{and} \quad \binom{v-r-s+j}{v-n}, \tag{4.25}$$

respectively. The verification is left to the reader.

We now need the expansion of $\binom{n-u}{r-i}\binom{u}{i}$ in the basis of polynomials $\binom{u}{t}$ of the variable u. Starting from well-known combinatorial identities (cf. Riordan [60], p. 7), we obtain

$$\binom{n-u}{r-i}\binom{u}{i} = \sum_{t=0}^{r} (-1)^{t-i}\binom{t}{i}\binom{n-t}{r-t}\binom{u}{t}. \tag{4.26}$$

Hence, remembering $C_i(x,y) = \binom{u}{i}$ for $\alpha \cap \beta \in V_w$, we deduce from (4.25) and (4.26) that $C_r C_s$ is a linear combination of $C_0, C_1, \ldots, C_r$ in which the coefficient of C_t is

$$\binom{n-t}{r-t}\sum_{j=0}^{n}\binom{v-r-s+j}{v-n}\sum_{i=0}^{n}(-1)^{t-i}\binom{t}{i}\binom{i}{j}\binom{n-i}{s-j}.$$

To complete the proof it only remains to be shown that the coefficients are

the ones given by (4.24). This is easily checked by use of the identity (4.26) for the above summations in i and j.

Let us now examine the Bose–Mesner algebra $\mathfrak{A}$ of the Johnson scheme $J(n,v)$ and its three bases $\{C_i\}$, $\{D_i\}$, $\{J_i\}$. Lemma 4.5 shows that, for a given r, the products $C_r C_s$ are linear combinations of the C_t with $0 \leqslant t \leqslant r$. In other words, C_0 $(= J)$, $C_1, \ldots, C_r$ generate an $(r+1)$-dimensional ideal $\mathfrak{A}_r$ in $\mathfrak{A}$, with

$$\langle J \rangle = \mathfrak{A}_0 \subset \mathfrak{A}_1 \subset \ldots \subset \mathfrak{A}_n = \mathfrak{A}. \tag{4.27}$$

On the other hand, given a chain of ideals like (4.27), there exists a unique numbering of the minimal idempotents J_k of $\mathfrak{A}$ such that $\{J_0, J_1, \ldots, J_r\}$ is a basis of $\mathfrak{A}_r$, for $r = 0, 1, \ldots, n$.

Let us now calculate the components of C_r in this basis. For $0 \leqslant s \leqslant r \leqslant n$, we have

$$C_r = \sum_{t=0}^{r} \varrho_{r,t} J_t, \qquad C_s = \sum_{j=0}^{t} \varrho_{s,j} J_j,$$

for some real numbers $\varrho_{r,t}, \varrho_{s,j}$. Using the orthogonality relations $J_t J_j = \delta_{t,j} J_j$, we readily obtain the following expression for the product $C_r C_s$:

$$C_r C_s = \varrho_{r,s} C_s + \sum_{j=0}^{s-1} \varrho_{s,j}(\varrho_{r,j} - \varrho_{r,s}) J_j. \tag{4.28}$$

Comparing the coefficients of C_s in the right-hand members of (4.24) and (4.28) we deduce $\varrho_{r,s} = \binom{n-s}{r-s}\binom{v-r-s}{n-r}$, from which the desired expansion follows:

$$C_r = \sum_{t=0}^{r}\binom{n-t}{r-t}\binom{v-r-t}{n-r} J_t. \tag{4.29}$$

This shows, in particular, that the components of C_r in the basis $\{J_0, J_1, \ldots, J_r\}$ are all nonzero. Hence the rank of C_r is equal to the sum of ranks of the J_t for $i = 0, 1, \ldots, r$. So the following equation holds for the multiplicity $\mu_t = \operatorname{rank}(J_t)$:

$$\mu_t = \operatorname{rank}(C_t) - \operatorname{rank}(C_{t-1}). \tag{4.30}$$

In order to determine the rank of C_t, let us introduce the matrix $A_t \in \mathbb{R}(X, V_t)$ characterizing the inclusion of t-subsets in n-subsets of V. More precisely, using the mapping (4.23), we define

$$A_t(x,\xi) = \begin{cases} 1 & \text{for} \quad \xi \subseteq f(x), \\ 0 & \text{otherwise,} \end{cases} \tag{4.31}$$

for $x \in X$ and $\xi \in V_t$. Since the (x,y)-entry of C_t is the number of t-subsets ξ

being contained in both $f(x)$ and $f(y)$, we have $C_i = A_i A_i^T$, which shows that C_i and A_i have the same rank. Next, we use a result due to Kantor [35]) saying that A_i has maximal rank: rank $(A_i) = |V_i| = \binom{n}{i}$, for $i = 0, 1, \ldots, n$. Hence we know, by (4.30), the parameters μ_i of the Johnson scheme $J(n,v)$:

$$\mu_i = \binom{v}{i} - \binom{v}{i-1} = \frac{v-2i+1}{v-i+1}\binom{v}{i}. \tag{4.32}$$

We are now ready to give, in explicit form, the eigenmatrices P and Q. It turns out that the formulas can be written in terms of expressions discovered by Eberlein [19]). In fact, this is not accidental: the problem considered by Eberlein is equivalent to the computation of the eigenvalues and eigenvectors of the matrix $L_1 = [p_{1,j}^{(k)}]$ for the Johnson scheme (cf. sec. 2.3).

Given an integer k, with $0 \leqslant k \leqslant n$, we define the *Eberlein polynomial* $E_k(u)$, in the indeterminate u, as follows:

$$E_k(u) = \sum_{j=0}^{k} (-1)^{k-j} \binom{n-j}{k-j}\binom{n-u}{j}\binom{v-n+j-u}{j}. \tag{4.33}$$

It is easy to verify that $E_k(u)$, which has degree $2k$ in u, has in fact degree k in the indeterminate $z = u(v+1-u)$. We also give, without proof, another useful formula for the Eberlein polynomials:

$$E_k(u) = \sum_{j=0}^{k} (-1)^j \binom{u}{j}\binom{n-u}{k-j}\binom{v-n-u}{k-j}.$$

Theorem 4.6. The eigenmatrices P and Q of the Johnson scheme $J(n,v)$ are given by

$$P_k(i) = E_k(i), \qquad Q_i(k) = \mu_i v_k^{-1} E_k(i), \tag{4.34}$$

for $i,k = 0, 1, \ldots, n$, where $E_k(u)$ is the Eberlein polynomial (4.33), v_k is defined by (4.21) and μ_i by (4.32).

Proof. Let $D_0, D_1, \ldots, D_n$ be the adjacency matrices of the distance relations R_i. Using a well-known identity on binomial coefficients and, thereafter, eq. (4.29), we can solve the system (4.22) for the D_j as follows:

$$D_{n-k} = \sum_{r=0}^{n} (-1)^{r-k}\binom{r}{k} C_r$$

$$= \sum_{i=0}^{n}\Big[\sum_{r=i}^{n} (-1)^{r-k}\binom{r}{k}\binom{n-i}{r-i}\binom{v-r-i}{n-r}\Big] J_i.$$

By definition (2.13), $P_{n-k}(i)$ is equal to the number inside the square brackets in the latter expression. On the other hand, this number is precisely the value $E_{n-k}(i)$ given by (4.33). Hence the first part of (4.34) is proved. Then the second formula is obtained by use of the general relation (2.25) between P and Q.

Theorem 2.3, when applied to the eigenmatrix P of the Johnson scheme $J(n,v)$, implies that the $n+1$ Eberlein polynomials $\Phi_k(z) = E_k(u)$ in the variable $z = u(v+1-u)$ form "the" family of orthogonal polynomials on the set of $n+1$ numbers $z_i = i(v+1-i)$, $i = 0, 1, \ldots, n$, with respect to the weight function w given by $w(z_i) = \mu_i$. Indeed, (2.21) can be written as follows:

$$\sum_{i=0}^{n} \Phi_r(z_i)\,\Phi_s(z_i)\,\mu_i = \binom{v}{n} v_s\,\delta_{r,s},$$

for $r,s = 0, 1, \ldots, n$. Like any class of orthogonal polynomials, the Eberlein polynomials satisfy a three-term recurrence relation, which is very useful for computation. We give it here, without proof:

$$(k+1)^2 E_{k+1}(u) = (n(v-n) - k(v-2k) - u(v+1-u))\,E_k(u) +$$
$$-(n-k+1)(v-n-k+1)\,E_{k-1}(u). \tag{4.35}$$

Finally, let us examine the "functions" $Q_i(z)$ corresponding to the eigenmatrix $Q = [Q_i(k)]$. Clearly, for a given i, there is a unique polynomial $p(z)$ of degree not exceeding n, in the indeterminate z, such that $Q_i(k) = p(k)$ for $k = 0, 1, \ldots, n$. Using the second formula (4.34), we transform the recurrence relation (4.35) on the E_k into a "difference equation" on $p(z) = Q_i(z)$. Elementary computation yields, with $m = v - n$:

$$(n-z)(m-z)\,p(z+1) = [nm - z(v-2z) - i(v+1-i)]\,p(z) - z^2\,p(z-1).$$

It is easily verified that a polynomial $p(z)$ of degree less than or equal to n cannot be a solution of this equation unless it has degree i. Consequently, it follows from (2.22) that $\{Q_0(z), \ldots, Q_n(z)\}$ is "the" family of orthogonal polynomials on the set $\{0, 1, \ldots, n\}$ with respect to the weight function w given by $w(i) = v_i$.

4.2.2. *Binary codes with constant weight*

A *binary code of length v and constant weight n* by definition is a nonempty subset Y of the sphere (4.19) provided with the Johnson distance (4.20). Like in the Hamming scheme (sec. 4.1.2), the linear-programming bound $|Y| \leqslant g(Q,M)$ can be applied to such codes which are M-cliques in the Johnson scheme $J(n,v)$.

Example. Let us examine the binary codes Y of length $v = 8$ and weight $n = 4$ having the property that the Johnson distance between distinct codewords is either 2 or 4. In other words, Y is an M-clique in $J(4, 8)$ for the set $M = \{0, 2, 4\}$. The linear-programming problem (Q,M) is here very simple. It turns out that the unique maximal program is $\mathbf{a}' = (1, 0, 12, 0, 1)$. Hence $|Y| \leqslant 14$ holds for all codes Y in the family. In fact, this bound is tight since there exists a well-known code Y' containing 14 codewords and having $\mathbf{a}'$ as inner distribution, namely the set of incidence vectors of points and planes in the Euclidean geometry EG(3, 2).

As we have already mentioned, the cases $M = \{0, \delta, \delta + 1, \ldots, n\}$ are the most important ones for applications in classical coding theory: the M-cliques in $J(n,v)$ are the constant weight codes with designed minimum distance δ (in the sense of the Johnson distance). The best known upper bounds to the number of words in codes with given parameters v, n, δ are essentially due to Johnson [34]).

In sec. 4.3 it will be shown that the linear-programming bound $|Y| \leqslant g(Q,M)$ implies certain standard combinatorial or geometric inequalities. Hence one may expect it will often improve the known results. However, here is an example unfavourable to this bound: for $v = 12$, $n = 5$, $\delta = 3$, it gives $g(Q,M) = 15$, whereas the largest code having these parameters contains only 12 words (cf. Johnson [33])). The very few numerical results obtained by the author do not allow him any grounded conjecture about comparison between the linear-programming bound and Johnson's results; to progress further, one should use a computer.

4.2.3. *t-Designs*

To complete the parallelism with sec. 4.1, we shall now exhibit the intrinsic meaning of T-designs of type (4.14) in the Johnson schemes. Let us first give a definition, in terms of coding theory, of the t-designs introduced by Hanani [30]). Here we exclude repeated blocks.

Definition. To a binary code Y of length v and constant weight n corresponds the array, over $F = \{0, 1\}$, whose rows are the words of Y. Let τ and λ be positive integers, with $\tau \leqslant n$. Then Y is said to form a *τ-design* if, in each τ-tuple of distinct columns of the array, the τ-tuple of symbols 1 appears exactly λ times. Such a design is usually denoted by $S_\lambda(\tau,n,v)$.

It is convenient to include $\tau = 0$ in the definition: any code Y forms a 0-design $S_{\lambda_0}(0,n,v)$ with $\lambda_0 = |Y|$. It is easily seen that, if Y forms a τ-design $S_\lambda(\tau,n,v)$, then it also forms an i-design $S_{\lambda_i}(i,n,v)$, for $i = 0, 1, \ldots, \tau$, with

$$\binom{v}{n}\lambda_i = |Y|\binom{v-i}{n-i}. \tag{4.36}$$

Theorem 4.7. For a given set $T = \{1, 2, \ldots, \tau\}$ with $1 \leqslant \tau \leqslant n$, a code Y is a T-design in $J(n,v)$ if and only if it forms a τ-design $S_\lambda(\tau,n,v)$.

Proof. Using the matrices A_i defined by (4.31) we first observe that the following equations are sufficient and necessary conditions for a code $Y \subseteq X$ to form a τ-design:

$$A_i{}^T \phi_Y = |X|^{-1}\,|Y|\, A_i{}^T \phi_X, \qquad 0 \leqslant i \leqslant \tau. \tag{4.37}$$

Indeed, let ξ be an i-subset of $V = \{1, 2, \ldots, v\}$. Then the component $(A_i{}^T \phi_Y)(\xi)$ in the left-hand member of (4.37) is, by definition, the number $\lambda_i(\xi)$ of codewords $x \in Y$ such that $\xi \subseteq f(x)$. Now, the property of a τ-design is precisely the fact that $\lambda_i(\xi)$ is constant, for a fixed $i \leqslant \tau$, its value λ_i being given by (4.36). Hence the characterization (4.37) of a τ-design simply follows from the obvious identity $(A_i{}^T \phi_X)(\xi) = \binom{v-i}{n-i}$.

On the other hand, the system (4.37) is equivalent to the one obtained when $A_i{}^T$ is replaced by $C_i = A_i\, A_i{}^T$, that is, since $\{J_0, \ldots, J_\tau\}$ generate the same linear space as $\{C_0, \ldots, C_\tau\}$, to the following system:

$$\begin{aligned} J_k \phi_Y &= |X|^{-1}\,|Y|\, J_k \phi_X \\ &= |X|^{-1}\,|Y|\,\delta_{k,0}\,\phi_X, \qquad 0 \leqslant k \leqslant \tau, \end{aligned} \tag{4.38}$$

as J_k is orthogonal to $J_0 = |X|^{-1}\,\phi_X\,\phi_X{}^T$ for $k \geqslant 1$. Now, by theorem 3.10, the conditions (4.38) are the exact definition of a T-design Y in the Johnson scheme. Hence the theorem is proved.

Let us illustrate this result on the example of sec. 4.2.2. It turns out that the maximal program $\mathbf{a}' = (1, 0, 12, 0, 1)$ of (Q,M), with $v = 8$, $n = 4$, $M = \{0, 2, 4\}$, satisfies $\mathbf{a}'\,Q_k = 0$ for $k = 1, 2, 3$. So, by definition (3.27), the maximal code Y' is a T-design in $J(4, 8)$ for $T = \{1, 2, 3\}$. Hence theorem 4.7 is in agreement with a well-known result in finite geometry: Y' forms a 3-design $S_1(3, 4, 8)$.

According to theorem 4.7, the linear-programming bound (3.29) leads to a lower bound to the parameter λ of τ-designs $S_\lambda(\tau,n,v)$ with fixed values of τ,n,v. Indeed, using (4.36) with $i = \tau$, $\lambda_i = \lambda$, we obtain

$$\lambda \geqslant \binom{v-\tau}{n-\tau} \Big/ g(P,M) \qquad \text{for} \qquad M = \{0, \tau + 1, \tau + 2, \ldots, n\}. \tag{4.39}$$

(In fact, this inequality remains valid for the more general definition of τ-designs which admits the possibility of "repeated blocks"; see the remark at the end of sec. 3.4.)

Example. We shall consider the problem of 4-designs $S_\lambda(4, 8, 17)$, i.e. $\tau = 4$, $n = 8$, $v = 17$. It is easy to check that the parameters λ_i given by (4.36) are all integers if and only if λ is divisible by 5. Our next analysis will lead to the

conclusion that $\lambda = 5$ is impossible, so leaving $\lambda = 10$ as the first open question. In fact, the smallest λ for which a design has been constructed is $\lambda = 15$, the result being due to Alltop [1]).

Let us give explicitly the inequalities $\mathfrak{b} P_k \geqslant 0$ of the linear-programming problem (P,M'), with $M = \{0, 5, 6, 7, 8\}$, in the variables b_5, b_6, b_7, b_8:

$$\begin{array}{rrrrcr} 7\,b_5 & +0\,b_6 & -5\,b_7 & -8\,b_8 & \geqslant & -\ 72, \\ -32\,b_5 & -18\,b_6 & +7\,b_7 & +28\,b_8 & \geqslant & -1008, \\ 24\,b_5 & +52\,b_6 & +7\,b_7 & -56\,b_8 & \geqslant & -4704, \\ 45\,b_5 & -60\,b_6 & -35\,b_7 & +70\,b_8 & \geqslant & -8820, \\ -81\,b_5 & +24\,b_6 & +49\,b_7 & -56\,b_8 & \geqslant & -7506, \\ 38\,b_5 & +10\,b_6 & -35\,b_7 & +28\,b_8 & \geqslant & -2352, \\ 2\,b_5 & -12\,b_6 & +13\,b_7 & -8\,b_8 & \geqslant & -\ 288, \\ -4\,b_5 & +3\,b_6 & -2\,b_7 & +\,b_8 & \geqslant & -\ 9. \end{array}$$

The function to be maximized is $g = 1 + b_5 + b_6 + b_7 + b_8$. The best way for computing the coefficients $P_k(i) = E_k(i)$ appearing in the above system is of course to use the recurrence relation (4.35) on the Eberlein polynomials $E_k(u)$.

The problem can be treated by hand and the following values are obtained for the unique maximal program: $b_5 = 4752/175$, $b_6 = 7722/175$, $b_7 = 624/25$, $b_8 = 429/25$; whence $g = 572/5$. (In fact, $\mathfrak{b}$ is the solution of $\mathfrak{b} P_k = 0$ for $k = 1, 2, 7, 8$.) Therefore, applying the linear-programming bound (4.39), we deduce $\lambda \geqslant 25/4$, which shows the nonexistence of a 4-design $S_\lambda(4, 8, 17)$.

It will be shown in sec. 5.3.2 that the linear-programming bound (4.39) for τ-designs implies an inequality recently obtained by Wilson and Ray-Chaudhuri [75]), namely $|Y| \geqslant \binom{v}{e}$ for $e = [\tau/2]$. This reduces to Fisher's inequality [20]) for $e = 1$; the general result was conjectured by Petrenjuk [54]), who first proved it for $e = 2$. In the above example of $S_\lambda(4, 8, 17)$, the Petrenjuk–Wilson inequality becomes $\lambda \geqslant 4$, which leads to no conclusion.

4.3. Classical inequalities for codes

In this section we shall treat simultaneously the Hamming schemes $H(n,q)$ and the Johnson schemes $J(n,v)$ and indicate, without going into details of the proofs, how certain well-known "combinatorial" inequalities follow from the linear-programming method. We shall only consider the problem of M-cliques with $M = \{0, \delta, \delta + 1, \ldots, n\}$ for some positive integer $\delta \leqslant n$, i.e. the problem of codes with designed minimum distance δ.

As we have seen in secs 4.1.1 and 4.2.1, the second eigenmatrix Q of both types of schemes corresponds to well-defined polynomials $Q_0(z) = 1$, $Q_1(z)$, $\ldots$, $Q_n(z)$ over the rational numbers, with $\deg(Q_k(z)) = k$, such that $Q_k(i)$ is the (i,k)-entry of Q for $i,k = 0, 1, \ldots, n$. For example, the polynomials of degree $k = 1$ are

$$Q_1(z) = n(q-1) - q\,z \qquad \text{in } H(n,q),$$

$$Q_1(z) = \frac{v-1}{n(v-n)}\,(n(v-n) - v\,z) \qquad \text{in } J(n,v).$$

Given a polynomial $\alpha(z)$ in the indeterminate z, with rational coefficients, whose degree does not exceed n, we consider its expansion

$$\alpha(z) = \alpha_0\,Q_0(z) + \alpha_1\,Q_1(z) + \ldots + \alpha_n\,Q_n(z) \tag{4.40}$$

in the basis $\{Q_k(z)\}$. For a fixed integer δ, with $1 \leqslant \delta \leqslant n$, the polynomial $\alpha(z)$ will be said to be *δ-positive* if it satisfies $\alpha_0 = 1$, $\alpha_k \geqslant 0$ for all k, and $\alpha(i) \leqslant 0$ for $i = \delta, \delta + 1, \ldots, n$. In other words, $\alpha(z)$ is δ-positive if and only if the $(n+1)$-tuple $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ is a program of the linear-programming problem $(Q,M)'$. For this problem the function γ to be minimized is simply given by $\gamma = \alpha(0)$. Therefore, according to theorem 3.4, the linear-programming bound (3.22) for codes Y with designed minimum distance δ is equivalent to the following:

$$|Y| \leqslant \alpha(0) \qquad \text{for all } \delta\text{-positive } \alpha(z). \tag{4.41}$$

4.3.1. *The Plotkin bound*

Let us restrict ourselves to polynomials of degree one with $\alpha_0 = 1$, i.e. $\alpha(z) = 1 + \alpha_1\,Q_1(z)$. The largest value of α_1 for which $\alpha(z)$ can be δ-positive is the solution of $\alpha(\delta) = 0$. This choice leads to the *Plotkin bound*; its analytical expressions are easily obtained from (4.41) and the above formulas for $Q_1(z)$:

$$\begin{aligned} |Y| &\leqslant q\,\delta/(q\,\delta - n(q-1)) \quad \text{for} \quad q\,\delta > n(q-1), \\ |Y| &\leqslant v\,\delta/(v\,\delta - n(v-n)) \quad \text{for} \quad v\,\delta > n(v-n), \end{aligned} \tag{4.42}$$

in the schemes $H(n,q)$ and $J(n,v)$, respectively. In fact, the first inequality is essentially due to Plotkin [57]), the latter was discovered by Johnson [32]).

The second part of theorem 3.4 implies that a code Y achieving the Plotkin bound is necessarily *equidistant of distance* δ, in the sense that the distance between any two distinct codewords is equal to δ. Moreover, the same theorem also indicates that Y is a $\{1\}$-design.

In the case of a Johnson scheme $J(n,v)$ let us now translate these properties in more-usual combinatorial terminology. Given a binary code Y of length v and constant weight n, we define the incidence relation I between the set Y of "points" and the set $V = \{1, 2, \ldots, v\}$ of "blocks" (cf. Dembowski [18]), p. 1) to be:

$$I = \{(x,j) \in Y \times V \mid x_j = 1\}.$$

We are interested here in the incidence structure (Y,V,I) which is the dual of the one implicitly used in sec. 4.2.3 for defining τ-designs in $J(n,v)$.

The consequence of the above remarks about the Plotkin bound can be expressed as follows: For given parameters n,v,δ, with $v\,\delta > n\,(v-n)$, a code Y satisfies equality in (4.42) if and only if the incidence structure (Y,V,I) is a 2-design, which may have repeated blocks. Using the notation $S_{\lambda'}(2,n',v')$ for this design, one can derive the parameters n,v,δ of the code from n',v',λ' by the formulas $n\,(n'-1)=\lambda'\,(v'-1)$, $v\,n'=v'\,n$ and $\delta=n-\lambda'$.

4.3.2. *The Singleton bound*

Here we take for $\alpha(z)$ the polynomial of minimal degree $\tau=n-\delta+1$ vanishing at points $z=\delta,\ \delta+1,\ \ldots,\ n$ and satisfying $\alpha_0=1$. So, one has

$$\alpha(z)=c\,(1-z/\delta)\,(1-z/(\delta+1))\ldots(1-z/n),$$

for some nonzero rational number $c=\alpha(0)$. It is not difficult to find out explicit formulas for the components α_k/c of the polynomial $\alpha(z)/c$ in the basis $\{Q_k(z)\}$; it turns out that these components are all positive for $k=0,\ 1,\ \ldots,\ \tau$ (cf. Delsarte [16]) in the case $H(n,q)$). The only numerical value we really need is for $k=0$ since the condition $\alpha_0=1$ then fixes the value of c; the results are

$$c=q^{\tau} \qquad \text{in } H(n,q),$$

$$c=\binom{v}{\tau}\Big/\binom{n}{\tau} \qquad \text{in } J(n,v).$$

Since $\alpha(z)$ is δ-positive, we may apply (4.41), with $\alpha(0)=c$. For a Hamming scheme we obtain in this way the *Singleton bound* [65]) $|Y|\leqslant q^{\tau}$, with $\tau=n-\delta+1$. The same name will be given to the corresponding bound $|Y|\leqslant\binom{v}{\tau}/\binom{n}{\tau}$ for a Johnson scheme. It must be noticed that both results can be derived by means of very simple counting arguments.

Let us emphasize the combinatorial structure of codes achieving the Singleton bounds: In $H(n,q)$, these maximal codes are the orthogonal arrays of strength τ and index $\lambda=1$ (cf. theorem 4.4); in $J(n,v)$ they are the *Steiner systems* $S(\tau,n,v)$, i.e. the τ-designs with $\lambda=1$ (cf. theorem 4.7). Essentially, in our approach, these results are consequences of theorem 3.4(ii) and the fact that $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{\tau}$ are positive.

Explicit formulae can be obtained for the inner distribution $\mathbf{a}$ of the orthogonal arrays of index 1 in $H(n,q)$ and of the Steiner systems in $J(n,v)$, as solutions of the following equations:

$$\mathbf{a}\,Q_k=c\,\delta_{k,0} \qquad \text{for} \qquad k=0,\ 1,\ \ldots,\ \tau, \tag{4.43}$$

with $a_0=1$, $a_1=a_2=\ldots=a_{n-\tau}=0$. For a derivation of such formulas by combinatorial methods, the reader is referred to Goethals [24]) and to Marguinaud [50]).

It is interesting to observe the following fact about the linear-programming problem (Q,M) for the Hamming scheme $H(n,q)$ with $q\geqslant\max(\delta,\ n-\delta+2)$: the solution $\mathbf{a}$ of (4.43) with $a_0=1$ and $a_i=0$ for $1\leqslant i<\delta$ is always a program of (Q,M); this has been verified by Piret (private communication). So we have programs $\mathbf{a}$ and $\boldsymbol{\alpha}$ of (Q,M) and $(Q,M)'$, respectively, such that $g=\gamma=q^{\tau}$. Hence $(\mathbf{a},\boldsymbol{\alpha})$ is a pair of extremal programs. Consequently, in the very particular case $q\geqslant\max(\delta,\ n-\delta+2)$, we have an analytical expression for the linear-programming bound, namely $g(Q,M)=q^{\tau}$, with $\tau=n-\delta+1$.

4.3.3. *The Hamming bound*

For $e=[(\delta-1)/2]$ let us define $P_e'(k)=P_0(k)+P_1(k)+\ldots+P_e(k)$ from the eigenmatrix P and, then,

$$\alpha_k=(P_e'(k)/P_e'(0))^2, \qquad k=0,\ 1,\ \ldots,\ n.$$

It can be shown that the polynomial $\alpha(z)$ given by (4.40) vanishes for $z=\delta,\ \delta+1,\ \ldots,\ n$ and, therefore, that $\alpha(z)$ is δ-positive. Moreover, one has $\alpha(0)=|X|/P_e'(0)$; so (4.41) yields

$$|Y|\leqslant(v_0+v_1+\ldots+v_e)^{-1}\,|X|.$$

This inequality, which we shall call the *Hamming bound*, is the obvious "sphere-packing bound" in a finite metric space with regular distance relations (cf. Hamming [29]) and Freiman [21]). The codes achieving this bound are said to be *perfect*. The question of perfect codes in the more general "metric schemes" will be examined in detail later on (cf. sec. 5.2.2).

The perfect codes in Hamming schemes were investigated by several authors. Let us quote the strongest general result, due essentially to Van Lint [14]) and to Tietäväinen [72]): For $3<\delta<n$, and q being a prime power, the only triples (n,q,δ) for which there exists a perfect code in $H(n,q)$ are those of the two Golay codes, namely (23, 2, 7) and (11, 3, 5). The uniqueness of the binary Golay code has been recently proved by Snover [68]); an interesting open problem is the uniqueness of the ternary Golay code. The known results about perfect additive codes are summarized in theorem 6.6. For a survey of the whole question, the reader is referred to Van Lint [42]).

After having recalled there are "very few" perfect codes in the Hamming schemes, one must say that, for $1<\delta<n$, there is not a single one known in the Johnson schemes. It is tempting to risk the conjecture that such codes do not exist. Certain results contained in the present work could be useful to attack this problem; especially the generalized Lloyd theorem of sec. 5.2.2 and theorem 4.7 about t-designs.

5. POLYNOMIAL SCHEMES

In the preceding chapter we have exhibited several analogies between two types of association schemes which are important in coding theory: those of Hamming and of Johnson. Especially, let us emphasize the existence of families of orthogonal polynomials related to the eigenmatrices P and Q. In the present chapter we shall take these "polynomial properties" as axioms and undertake to set up a theory of the corresponding association schemes.

Let us point out, without going into details, that, apart from the above-mentioned "coding schemes", there exist other types of association schemes to which the theory can apply. Here are two interesting cases: (i) the scheme of alternating bilinear forms over the binary field (cf. Cameron and Seidel [12]), which is also of some use in coding theory; (ii) the scheme of finite projective geometries (cf. for instance Dembowski [18], p. 29). For both cases the author succeeded in obtaining explicit formulas for the eigenmatrices. In fact, the families (i) and (ii) are related, at least formally, to the Hamming schemes and to the Johnson schemes, respectively; some generalizations of the Krawtchouk and Eberlein polynomials follow from the theory.

5.1. Definitions and preliminaries

We shall denote by $\mathbf{R}[z]$ the linear algebra of polynomials, with real coefficients, in the indeterminate z and by $\mathbf{R}_k[z]$ the $(k+1)$-dimensional subspace of $\mathbf{R}[z]$ formed by all polynomials of degree less than or equal to a given integer $k \geqslant 0$. On the other hand, we shall use the notation $N = \{0, 1, \ldots, n\}$.

Definition. Let $P, Q \in \mathbf{R}(N,N)$ be the eigenmatrices of a symmetric association scheme with n classes. Let there be given $n+1$ distinct nonnegative real numbers $z_0 = 0, z_1, \ldots, z_n$. For a fixed $k \in N$ there exists a unique polynomial $\Phi_k(z) \in \mathbf{R}_n[z]$ such that

$$\Phi_k(z_i) = P_k(i), \qquad \forall\, i \in N, \tag{5.1}$$

where $P_k(i)$ is the (i,k)-entry of P. If $\Phi_k(z)$ has degree k, for all $k \in N$, then the association scheme will be said to be *P-polynomial* with respect to the z_i. A *Q-polynomial scheme* is defined analogously from the matrix Q.

Let us make two obvious remarks: (i) The condition $\deg(\Phi_k(z)) = k$ in the definition of a polynomial scheme can be replaced by $\Phi_k(z) \in \mathbf{R}_k[z]$. (ii) For a P-polynomial scheme, we have $z_i = c\,(P_1(0) - P_1(i))$ for some positive constant c which may be chosen arbitrarily.

5.1.1. *Orthogonal polynomials*

From theorem 2.3 it follows that the polynomials $\Phi_k(z)$ satisfy orthogonality relations. For future use we shall need some results and notations about such orthogonal polynomials. Except for one theorem, the matter is absolutely classical; the reader is referred to Szegö [70].

Let us consider a set $\{z_0 = 0, z_1, \ldots, z_n\}$ of $n+1$ distinct real numbers z_i, with $z_1, \ldots, z_n > 0$, and a *weight function* w, defined on this set, assuming only positive values $w(z_i)$. From these data we define the scalar product (f,g) of two real functions f,g of the variable z by the formula

$$(f,g) = \sum_{i=0}^{n} w(z_i) f(z_i) g(z_i). \tag{5.2}$$

The number $(f,f)^{1/2}$ is called the *norm* of f; it is zero if and only if $f(z)$ vanishes for $z = z_0, \ldots, z_n$.

Next, for an arbitrary choice of the norms $\sigma_k > 0$, we define the *family of orthogonal polynomials* $\Phi_0(z), \Phi_1(z), \ldots, \Phi_n(z)$, with $\deg(\Phi_k(z)) = k$ and $\Phi_k(0) > 0$, by the orthogonality relations:

$$(\Phi_k, \Phi_j) = \sigma_k^2\, \delta_{k,j}, \qquad 0 \leqslant k,j \leqslant n. \tag{5.3}$$

It is well known that these conditions determine uniquely the set $\{\Phi_k\}$. (The choice $\Phi_k(0) > 0$ is admissible since $\Phi_k(z)$ cannot vanish for $z = 0$; it is equivalent to $\Phi_k(-\infty) > 0$.) In the following, the normalization will be chosen such that

$$\Phi_k(0) = \sigma_k^2/\sigma_0^2, \qquad 0 \leqslant k \leqslant n, \tag{5.4}$$

which is always possible. The only remaining arbitrary parameter now is σ_0.

Before going further into the theory let us apply this to polynomial schemes. The next result simply is a reformulation of theorem 2.3 in the terminology of orthogonal polynomials.

Theorem 5.1. Let (X,R) be a P-polynomial scheme. Then the set $\{\Phi_k(z)\}$ deduced from P as in (5.1) is, for the normalization (5.4) with $\sigma_0^2 = |X|$, the family of orthogonal polynomials on the set $\{z_0, z_1, \ldots, z_n\}$ for the weight function $w(z_i) = Q_i(0)$. The same result holds when the roles of P and Q are interchanged.

Proof. For P-polynomial schemes, the orthogonality relations (5.3) follow from (2.21) and the normalization (5.4) follows from $P_k(0) = v_k$. The corresponding result for Q-polynomial schemes is a consequence of (2.22) and (2.18).

It is known (cf. Szegö [70], p. 42) that orthogonal polynomials satisfy a unique *recurrence relation* of the following type:

$$\gamma_{k+1}\, \Phi_{k+1}(z) = (\alpha_k - z)\, \Phi_k(z) - \omega_k\, \gamma_k\, \Phi_{k-1}(z), \tag{5.5}$$

where $\alpha_k, \gamma_k, \omega_k$ are real numbers, with $\omega_k = (\sigma_k/\sigma_{k-1})^2$ and $\gamma_k > 0$ for $k = 1, 2, \ldots, n$. For convenience, we also define $\gamma_0 = 0$. Substituting $z = 0$

into (5.5) we easily obtain, by use of (5.4),

$$\alpha_k = \gamma_k + \omega_{k+1}\,\gamma_{k+1}. \tag{5.6}$$

The reader could check this result for the formulas (4.11) and (4.35) given above for the Krawtchouk and Eberlein polynomials.

Next, let us introduce the *sum polynomial* $\Psi_k(z)$ of degree k, for $k = 0, 1, \ldots, n$, derived from the $\Phi_i(z)$ as follows:

$$\Psi_k(z) = \Phi_0(z) + \Phi_1(z) + \ldots + \Phi_k(z). \tag{5.7}$$

It is not difficult to show that $\Psi_n(z)$ vanishes for $z = z_1, \ldots, z_n$. On the other hand, we consider the scalar product $[f,g]$ associated to the weight function $w'(z_i) = z_i\, w(z_i)$ for $i = 1, 2, \ldots, n$:

$$[f,g] = \sum_{i=1}^{n} w'(z_i) f(z_i)\, g(z_i) = (zf,g).$$

Theorem 5.2. The polynomials $\Psi_0(z)$, $\Psi_1(z)$, $\ldots$, $\Psi_{n-1}(z)$ form the family of orthogonal polynomials on the set $\{z_1, \ldots, z_n\}$ for the weight function $w'(z_i)$. More precisely:

$$[\Psi_k,\Psi_j] = \gamma_{k+1}\,\sigma_{k+1}{}^2\,\delta_{k,j}, \qquad 0 \leqslant k,j \leqslant n-1.$$

Proof. We shall only give the sketch of the reasoning, without going into details. By use of (5.5) and (5.6) it is first shown that the sum polynomials (5.7) satisfy the following equations:

$$\gamma_{k+1}\,\Psi_{k+1}(z) = (\alpha_k' - z)\,\Psi_k(z) - \omega_k'\,\gamma_k\,\Psi_{k-1}(z), \tag{5.8}$$

with $\alpha_k' = \gamma_{k+1}\,(1 + \omega_{k+1})$ and $\omega_k'\,\gamma_k = \omega_{k+1}\,\gamma_{k+1}$. Next, we verify that $[\Psi_k,1] = 0$ holds for all $k \geqslant 1$. Owing to the recurrence relation (5.8), this implies $[\Psi_k,z^j] = 0$ for all $k > j$, which is equivalent to $[\Psi_k,\Psi_j] = 0$ for all $k \neq j$.

Finally, let us compute the norm σ_k' of Ψ_k, i.e. $\sigma_k'^2 = [\Psi_k,\Psi_k]$. From the recurrence relation (5.8) on the family of orthogonal polynomials $\Psi_k(z)$, we deduce, applying the general theory,

$$\frac{\sigma_k'^2}{\sigma_{k-1}'^2} = \omega_k' = \frac{\gamma_{k+1}\sigma_{k+1}{}^2}{\gamma_k\,\sigma_k{}^2}.$$

The solution obviously is $\sigma_k'^2 = \gamma_{k+1}\,\sigma_{k+1}{}^2$, which concludes the proof of the theorem.

As the polynomials $\Phi_k(z)$ and $\Psi_k(z)$ corresponding to the Johnson scheme are not really classical, we give for them, in table I, the values of the parameters appearing in the above formulas.

Going back to the general theory we finally apply to the family $\{\Psi_j\}$ two well-known results on the zeros of orthogonal polynomials.

TABLE I

Parameters of $J(n,v)$, with $m = v - n$

	P-polynomials	Q-polynomials
z_i	$i\,(v+1-i)$	i
$w(z_i)$	$\binom{v}{i}\dfrac{v-2i+1}{v-i+1}$	$\binom{m}{i}\binom{n}{i}$
γ_k	k^2	$\dfrac{k\,(m-k+1)\,(n-k+1)}{(v-2k)\,(v-2k+2)}$
$\sigma_k{}^2$	$\binom{v}{n}\binom{m}{k}\binom{n}{k}$	$\binom{v}{n}\binom{v}{k}\dfrac{v-2k+1}{v-k+1}$
α_k	$m\,n - k\,(v-2k)$	$\dfrac{m\,n\,(v+2) - v\,k\,(v-k+1)}{(v-2k)\,(v-2k+2)}$
$\sigma_k'^2$	$m\,n\binom{v}{n}\binom{m-1}{k}\binom{n-1}{k}$	$\binom{v}{n}\binom{v}{k}\dfrac{(m-k)\,(n-k)}{v-2k}$
α_k'	$m\,n + 1 - k\,(v-2k-2)$	$\dfrac{(v+1)\,(m-k)\,(n-k)}{(v-2k-1)\,(v-2k+1)}$
$\omega_k'\,\gamma_k$	$(m-k)\,(n-k)$	$\dfrac{(v-k+1)\,(m-k)\,(n-k)}{(v-2k)\,(v-2k+1)}$

Theorem 5.3. For a given $e \in \{1, 2, \ldots, n-1\}$, the polynomial $\Psi_e(z)$ has e distinct real zeros, located in the interior of the smallest interval containing $z_1, z_2, \ldots, z_n$.

Let us denote by $p_1, p_2, \ldots, p_e$ the zeros of $\Psi_e(z)$. To a given p_k corresponds the *Christoffel number* w_k defined as follows (cf. Szegö [70], p. 48), with $\sigma_j'^2 = [\Psi_j,\Psi_j]$:

$$w_k{}^{-1} = \sum_{j=0}^{e-1} (\Psi_j(p_k)/\sigma_j')^2, \qquad k = 1, 2, \ldots, e. \tag{5.9}$$

into (5.5) we easily obtain, by use of (5.4),

$$\alpha_k = \gamma_k + \omega_{k+1}\,\gamma_{k+1}. \tag{5.6}$$

The reader could check this result for the formulas (4.11) and (4.35) given above for the Krawtchouk and Eberlein polynomials.

Next, let us introduce the *sum polynomial* $\Psi_k(z)$ of degree k, for $k = 0, 1, \ldots, n$, derived from the $\Phi_i(z)$ as follows:

$$\Psi_k(z) = \Phi_0(z) + \Phi_1(z) + \ldots + \Phi_k(z). \tag{5.7}$$

It is not difficult to show that $\Psi_n(z)$ vanishes for $z = z_1, \ldots, z_n$. On the other hand, we consider the scalar product $[f,g]$ associated to the weight function $w'(z_i) = z_i\, w(z_i)$ for $i = 1, 2, \ldots, n$:

$$[f,g] = \sum_{i=1}^{n} w'(z_i) f(z_i)\, g(z_i) = (zf,g).$$

Theorem 5.2. The polynomials $\Psi_0(z), \Psi_1(z), \ldots, \Psi_{n-1}(z)$ form the family of orthogonal polynomials on the set $\{z_1, \ldots, z_n\}$ for the weight function $w'(z_i)$. More precisely:

$$[\Psi_k,\Psi_j] = \gamma_{k+1}\,\sigma_{k+1}^2\,\delta_{k,j}, \qquad 0 \leqslant k,j \leqslant n-1.$$

Proof. We shall only give the sketch of the reasoning, without going into details. By use of (5.5) and (5.6) it is first shown that the sum polynomials (5.7) satisfy the following equations:

$$\gamma_{k+1}\,\Psi_{k+1}(z) = (\alpha_k' - z)\,\Psi_k(z) - \omega_k'\,\gamma_k\,\Psi_{k-1}(z), \tag{5.8}$$

with $\alpha_k' = \gamma_{k+1}\,(1 + \omega_{k+1})$ and $\omega_k'\,\gamma_k = \omega_{k+1}\,\gamma_{k+1}$. Next, we verify that $[\Psi_k,1] = 0$ holds for all $k \geqslant 1$. Owing to the recurrence relation (5.8), this implies $[\Psi_k,z^j] = 0$ for all $k > j$, which is equivalent to $[\Psi_k,\Psi_j] = 0$ for all $k \neq j$.

Finally, let us compute the norm σ_k' of Ψ_k, i.e. $\sigma_k'^2 = [\Psi_k,\Psi_k]$. From the recurrence relation (5.8) on the family of orthogonal polynomials $\Psi_k(z)$, we deduce, applying the general theory,

$$\frac{\sigma_k'^2}{\sigma_{k-1}'^2} = \omega_k' = \frac{\gamma_{k+1}\sigma_{k+1}^2}{\gamma_k\,\sigma_k^2}.$$

The solution obviously is $\sigma_k'^2 = \gamma_{k+1}\,\sigma_{k+1}^2$, which concludes the proof of the theorem.

As the polynomials $\Phi_k(z)$ and $\Psi_k(z)$ corresponding to the Johnson scheme are not really classical, we give for them, in table I, the values of the parameters appearing in the above formulas.

Going back to the general theory we finally apply to the family $\{\Psi_j\}$ two well-known results on the zeros of orthogonal polynomials.

TABLE I

Parameters of $J(n,v)$, with $m = v - n$

	P-polynomials	Q-polynomials
z_i	$i\,(v+1-i)$	i
$w(z_i)$	$\binom{v}{i}\frac{v-2i+1}{v-i+1}$	$\binom{m}{i}\binom{n}{i}$
γ_k	k^2	$\frac{k\,(m-k+1)\,(n-k+1)}{(v-2k)\,(v-2k+2)}$
σ_k^2	$\binom{v}{n}\binom{m}{k}\binom{n}{k}$	$\binom{v}{n}\binom{v}{k}\frac{v-2k+1}{v-k+1}$
α_k	$m\,n-k\,(v-2k)$	$\frac{m\,n\,(v+2)-v\,k\,(v-k+1)}{(v-2k)\,(v-2k+2)}$
$\sigma_k'^2$	$m\,n\binom{v}{n}\binom{m-1}{k}\binom{n-1}{k}$	$\binom{v}{n}\binom{v}{k}\frac{(m-k)\,(n-k)}{v-2k}$
α_k'	$m\,n+1-k\,(v-2k-2)$	$\frac{(v+1)\,(m-k)\,(n-k)}{(v-2k-1)\,(v-2k+1)}$
$\omega_k'\,\gamma_k$	$(m-k)\,(n-k)$	$\frac{(v-k+1)\,(m-k)\,(n-k)}{(v-2k)\,(v-2k+1)}$

Theorem 5.3. For a given $e \in \{1, 2, \ldots, n-1\}$, the polynomial $\Psi_e(z)$ has e distinct real zeros, located in the interior of the smallest interval containing $z_1, z_2, \ldots, z_n$.

Let us denote by $p_1, p_2, \ldots, p_e$ the zeros of $\Psi_e(z)$. To a given p_k corresponds the *Christoffel number* w_k defined as follows (cf. Szegö [70], p. 48), with $\sigma_j'^2 = [\Psi_j,\Psi_j]$:

$$w_k^{-1} = \sum_{j=0}^{e-1} (\Psi_j(p_k)/\sigma_j')^2, \qquad k = 1, 2, \ldots, e. \tag{5.9}$$

Theorem 5.4. Let $f(z)$ vary through the set $\mathbf{R}_{2e-1}[z]$. Then the e-tuple $(w_1, w_2, \ldots, w_e)$ of Christoffel numbers associated to the zeros p_k of $\Psi_e(z)$ is the unique solution of the following system of linear equations:

$$\sum_{k=1}^{e} w_k f(p_k) = \sum_{i=1}^{n} z_i\, w(z_i) f(z_i). \tag{5.10}$$

5.1.2. *The Mac Williams inequality*

This section is devoted to a generalization of an inequality first discovered by MacWilliams [44]) in the theory of linear codes. It relates two parameters which will play a very important role in the rest of our study.

Definition. Let $\mathbf{a} = (a_0, a_1, \ldots, a_n)$ be an $(n+1)$-tuple of real numbers a_i. Then the integer $s(\mathbf{a})$ is defined to be the number of nonzero components a_i for $1 \leqslant i \leqslant n$ and $t(\mathbf{a})$ is defined to be the largest τ such that $a_1 = a_2 = \ldots = a_\tau = 0$. If a_1 is non-zero, $t(\mathbf{a})$ is taken to be zero.

Theorem 5.5. Let there be given a P-polynomial scheme. Then, for all $(n+1)$-tuples $\mathbf{a}$ with $a_0 \neq 0$, one has $s(\mathbf{a}Q) \geqslant [t(\mathbf{a})/2]$. The same proposition holds when the roles of P and Q are interchanged.

Proof. Using (2.15) we can write, for arbitrary $(n+1)$-tuples $\mathbf{a}$ and $\mathbf{b}$:

$$(\mathbf{a}\,Q)\,(\mathbf{b}\,P^T)^T = |X|\;\mathbf{a}\,\mathbf{b}^T. \tag{5.11}$$

For a P-polynomial scheme, we have $P_k(i) = \Phi_k(z_i)$ with $\deg(\Phi_k(z)) = k$. From $\mathbf{a}$ and $\mathbf{b}$ we construct the polynomial $\beta(z) = b_0\,\Phi_0(z) + \ldots + b_t\,\Phi_t(z)$, with $t = t(\mathbf{a})$. Since, by definition, $a_1 = \ldots = a_t = 0$, eq. (5.11) becomes

$$\sum_{i=0}^{n} (\mathbf{a}\,Q_i)\,\beta(z_i) = |X|\left(a_0\,b_0 + \sum_{j=t+1}^{n} a_j\,b_j\right). \tag{5.12}$$

We shall assume $s(\mathbf{a}Q) < [t/2]$. Then, obviously, there exists a polynomial $\gamma(z)$ of degree $[t/2]$ vanishing at each point z_i such that $\mathbf{a}Q_i \neq 0$, with $i = 0, 1, \ldots, n$. For a given $\mathbf{a}$ we now choose $\mathbf{b}$ such as to have $b_{t+1} = \ldots = b_n = 0$ and $\beta(z) = (\gamma(z))^2$. Then (5.12) can be written as follows:

$$0 = a_0 \sum_{i=0}^{n} (\gamma(z_i))^2\, Q_i(0). \tag{5.13}$$

Indeed, the components b_k of $\beta(z)$ in the basis $\{\Phi_k(z)\}$ are deduced from the values $\beta(z_i)$ by the formula $|X|\;b_k = \sum \beta(z_i)\,Q_i(k)$.

Since $Q_i(0) = \mu_i$ is positive, the right-hand member of (5.13) cannot be zero for $a_0 \neq 0$. Hence we are led to a contradiction and the first part of the theorem is proved. The second part is obtained by exactly the same argument.

5.2. *P*-polynomial (= metric) schemes and codes

The Hamming and Johnson schemes have at least two common properties: they are defined by the distance relations of some metric space and they are P-polynomial. More precisely, $H(n,q)$ and $J(n,v)$ are P-polynomial for $z_i = i$ and $z_i = i\,(v+1-i)$, respectively. In this section, it is first shown that the coincidence between metric and P-polynomial properties is quite general. Thereafter, the "codes" in these "metric schemes" are investigated in detail.

5.2.1. *Preliminary results*

Given a symmetric association scheme (X,R) with n classes, we define the mapping ϱ of X^2 onto $N = \{0, 1, \ldots, n\}$ as follows:

$$\varrho(x,y) = k \qquad \text{for} \qquad (x,y) \in R_k.$$

The scheme will be said to be *metric* if ϱ is a distance over X satisfying a condition of "nondegeneracy": for any two points x,y at distance $\varrho(x,y) = k$ from each other, with $1 \leqslant k \leqslant n$, there exists at least one point at distance 1 from x and at distance $k-1$ from y.

The graph (X,R_1) of a metric scheme could be called a *perfectly regular graph* in agreement with the definition of Higman [31]). In graph terminology, the distance $\varrho(x,y)$ is the length of the shortest path between x and y in (X,R_1).

It is obvious that the axioms of a metric scheme can be expressed in terms of the parameters $p_{i,j}^{(k)}$ by the following two conditions: $p_{i,j}^{(k)} \neq 0$ for $k = i + j$ and

$$(p_{i,j}^{(k)} \neq 0) \Rightarrow (|i-j| \leqslant k \leqslant i+j). \tag{5.14}$$

Theorem 5.6. A symmetric association scheme is P-polynomial if and only if it is metric.

Proof. First, let us assume the given scheme is metric. Using (5.14) and the general relation (2.19) on the eigenmatrix P, we have, for all $u \in N$,

$$P_1(u)\,P_k(u) = p_{1,k}^{(k+1)}\,P_{k+1}(u) + p_{1,k}^{(k)}\,P_k(u) + p_{1,k}^{(k-1)}\,P_{k-1}(u). \tag{5.15}$$

As $p_{1,k}^{(k+1)}$ is nonzero, this shows, by induction on k, that $P_k(u)$ is a polynomial of degree k in $P_1(u)$. Let us define $z_u = c\,(v_1 - P_1(u))$ for an arbitrary constant $c > 0$. By (2.29) the numbers z_u are nonnegative, with $z_0 = 0$. Moreover, they are distinct. Indeed, $z_i = z_j$ would imply $P_k(i) = P_k(j)$, for all k, which is impossible unless $i = j$ since P is nonsingular. Hence, by definition, the scheme is P-polynomial with respect to the z_u.

Next, we assume the scheme is P-polynomial with respect to some numbers z_u. From theorem 5.1 it follows that the corresponding polynomials $\Phi_k(z)$ satisfy a recurrence relation like (5.5). Writing it at point $z = z_u = c\,(v_1 - P_1(u))$ we obtain precisely (5.15) for suitable values of the

$p_{1,k}^{(i)}$, namely

$$p_{1,k}^{(k+1)} = c^{-1}\gamma_{k+1},\quad p_{1,k}^{(k)} = v_1 - c^{-1}\alpha_k,\quad p_{1,k}^{(k-1)} = c^{-1}\omega_k\gamma_k.$$

Hence we have $p_{1,k}^{(k+1)} \neq 0$ and $p_{1,k}^{(i)} = 0$ for $|k-i| \geqslant 2$. These are part of the conditions (5.14) for a metric scheme. In fact it can be easily shown, by induction, that this "part" is equivalent to the whole of the conditions, which concludes the proof.

Let Y be a nonempty subset of X for a metric scheme (X,R); we call Y a *code* in (X,R). The inner distribution $\mathbf{a}$ of Y with respect to R is called the *distance distribution* of the code. From $\mathbf{a}$ we define two fundamental parameters d and r as follows (cf. sec. 5.1.2):

$$d = t(\mathbf{a}) + 1 = \textit{minimum distance of } Y,$$

$$r = s(\mathbf{a}Q) = \textit{external distance of } Y.$$

The meaning of the first parameter is clear, at least for $|Y| \geqslant 2$: the integer d is the smallest value assumed by the distance $\varrho(x,y)$ for distinct points $x,y \in Y$. The significance of the concept of external distance will appear below.

A code Y will be said to be *trivial* when it is X itself or when it contains only one point. From now forth we shall only consider nontrivial codes. Then it is easy to show that the parameters satisfy $1 \leqslant r,\ d \leqslant n$.

On the other hand, using theorem 5.5, we have an interesting inequality on d and r, namely

$$r \geqslant [(d-1)/2]. \tag{5.16}$$

As will be shown in theorem 5.14, the codes satisfying equality are the perfect codes of which we now recall the definition in the terminology of metric schemes: A subset $Y \subset X$ is a *perfect code of order e*, for some integer $e \geqslant 1$, if the *spheres* $S_e(y)$ of radius e centred at the points $y \in Y$ form a partition of X, with the usual definition of a sphere:

$$S_e(y) = \{x \in X \mid 0 \leqslant \varrho(x,y) \leqslant e\}. \tag{5.17}$$

5.2.2. *The Hamming bound and the perfect codes*

An obvious "sphere-packing" bound for codes Y of a given minimum distance d in a metric scheme results from the following argument: the spheres (5.17) of radius $e = [(d-1)/2]$ centred at the points of Y have to be disjoint; this yields the inequality $|Y|\,|S_e(y)| \leqslant |X|$, which we call the *Hamming bound*. Clearly, the perfect codes of order e can be defined to be the ones achieving this bound.

In the present section, we shall obtain a very strong necessary condition on perfect codes in terms of the polynomials $\Phi_k(z)$ corresponding to the eigenmatrix P. It is a generalization of the Lloyd theorem [43]) on perfect codes in the Hamming schemes (cf. for instance Lenstra [39])).

Theorem 5.7. (i) Let Y be a code of minimum distance d in a metric scheme (X,R). Then the following inequality holds, with $e = [(d-1)/2]$:

$$|Y|\,(v_0 + v_1 + \ldots + v_e) \leqslant |X|. \tag{5.18}$$

(ii) Let $\mathbf{a}$ be the distance distribution of Y. If Y is a perfect code of order e, i.e. if it satisfies equality in (5.18), then its external distance r is equal to e and the sum polynomial

$$\Psi_e(z) = \Phi_0(z) + \Phi_1(z) + \ldots + \Phi_e(z) \tag{5.19}$$

vanishes at the e distinct points z_k, $1 \leqslant k \leqslant n$, such that $\mathbf{a}Q_k \neq 0$.

Proof. The first part is obvious, by the geometrical argument sketched above, as $v_0 + v_1 + \ldots + v_e$ is the volume $|S_e(y)|$ of the sphere (5.17). However, in order to show that the Hamming bound (5.18) is implied by the linear-programming bound, and to prepare the proof of the second part, we shall use an algebraic method.

By definition, Y is an M-clique in (X,R) for $M = \{0,\ d,\ d+1,\ \ldots,\ n\}$. Hence (cf. theorem 3.8) the distance distribution $\mathbf{a}$ of Y is a program of (Q,M) with $g = |Y|$. From the polynomial (5.19) we construct an $(n+1)$-tuple $\boldsymbol{\alpha} = (\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_n)$ as follows:

$$\alpha_k = (\Psi_e(z_k)/v_e')^2, \tag{5.20}$$

with $v_e' = \Psi_e(0) = v_0 + \ldots + v_e$. Let us show that $\boldsymbol{\alpha}$ is a program of $(Q,M)'$. Using (2.25) we can write the (i,k)-entry of Q in the form $Q_k(i) = \Phi_i(z_k)\,\mu_k/v_i$. So we have, by (5.20),

$$(\boldsymbol{\alpha}\,Q^T)_i = (v_i\,v_e'^2)^{-1} \sum_{k=0}^{n} \mu_k\,\Phi_i(z_k)\,(\Psi_e(z_k))^2. \tag{5.21}$$

Now the degree of $(\Psi_e(z))^2$ is $d-1$ or $d-2$. Hence from theorem 5.1 it follows that the right-hand member of (5.21) is zero for $i \geqslant d$. This shows that $\boldsymbol{\alpha}$ is a program of $(Q,M)'$, satisfying the conditions $(\boldsymbol{\alpha}\,Q^T)_i \leqslant 0$ with equality.

Let us compute $\gamma = (\boldsymbol{\alpha}\,Q^T)_0$ for this program. From (5.21) we readily obtain, by using the orthogonality relations (5.3),

$$\gamma = (v_e')^{-2}\,(\sigma_0^2 + \sigma_1^2 + \ldots + \sigma_e^2),$$

where σ_k is the norm of $\Phi_k(z)$. Since $\sigma_k^2 = |X|\,v_k$, this becomes $\gamma = |X|/v_e'$. Therefore, the general inequality $g \leqslant \gamma$ in linear programming yields the desired result (5.18).

Next, we assume Y is a perfect code of order e or, equivalently, Y satisfies equality in (5.18). This means that $\mathbf{a}$ and $\boldsymbol{\alpha}$ are extremal programs of (Q,M) and $(Q,M)'$, respectively. Let us apply theorem 3.4(ii) to the pair $(\mathbf{a},\boldsymbol{\alpha})$. Equation (3.15) gives, by (5.20),

$$\Psi_e(z_k) = 0 \qquad \text{for} \qquad \mathbf{a}\,Q_k \neq 0, \qquad 1 \leqslant k \leqslant n. \tag{5.22}$$

By definition, the external distance r is the number of integers k, with $1 \leqslant k \leqslant n$, such that $\mathbf{a}Q_k \neq 0$. Since $\Psi_e(z)$ cannot have more than e distinct zeros, (5.22) implies $e \geqslant r$. Comparing this to the MacWilliams inequality (5.16), we obtain $e = r$. Hence the second part of the theorem is proved.

The polynomial (5.19) will be called the *Lloyd polynomial of degree e*. By theorem 5.3, it always has e distinct real zeros in the interior of the smallest interval containing $z_1, \ldots, z_n$. According to theorem 5.7(ii), these zeros must all be among the z_i themselves if there exists a perfect code of order e. In the particular case of Hamming schemes, where $\Psi_e(z)$ is the Lloyd polynomial in the original sense, this condition was used successfully for nonexistence theorems on perfect codes (cf. especially Van Lint [40–42]).

Remark. For the Hamming and Johnson schemes, it turns out that the Lloyd polynomials are the $\Phi_e(z)$ themselves up to some "translation" on the indeterminates and parameters. Let us denote by $K_k(n,q;u)$ the Krawtchouk polynomial (4.7) and by $E_k(n,v;u)$ the Eberlein polynomial (4.33). Then, for the schemes $H(n,q)$ and $J(n,v)$, the Lloyd polynomials are given by the following expressions:

$$\Psi_e(z) = K_e(n-1, q; z-1),$$

$$\Psi_e(z) = E_e(n-1, v-2; u-1), \qquad \text{with} \qquad z = u\,(v+1-u),$$

respectively. The first formula is, implicitly, the one given by Van Lint [41] for the usual Lloyd polynomials.

We shall now derive a formula for the distance distribution of a perfect code of order e. We point out that the minimum distance of such a code has to be odd: $d = 2e + 1 = 2r + 1$.

Theorem 5.8. Let $p_1, p_2, \ldots, p_e$ be the zeros of the Lloyd polynomial $\Psi_e(z)$ of degree $e \leqslant [(n-1)/2]$ and let $w_1, w_2, \ldots, w_e$ be the corresponding Christoffel numbers. Then the distance distribution $\mathbf{a}$ of any perfect code Y of order e is given by

$$a_j = |X|^{-1} \sum_{k=1}^{e} p_k^{-1}\, w_k\, \Phi_j(p_k) + (\Psi_e(0))^{-1}\, \Phi_j(0). \tag{5.23}$$

Proof. Let us define $\mathbf{b} = \mathbf{a}\,Q$, whence $\mathbf{b}\,P = |X|\,\mathbf{a}$. The minimum distance of Y being $d = 2e + 1$, this yields $\mathbf{b}\,P_j = |X|\,\delta_{0,j}$ for $j = 0, 1, \ldots, 2e$. Using the orthogonality relations we can write these equations in terms of the polynomials $\Phi_j(z)$ as follows:

$$\sum_{i=0}^{n} (b_i - \mu_i)\, \Phi_j(z_i) = 0, \qquad 0 \leqslant j \leqslant 2e.$$

Consequently, since $\Phi_0(z), \ldots, \Phi_{2e}(z)$ form a basis of $\mathbf{R}_{2e}[z]$, we have, for an arbitrary polynomial $f(z) \in \mathbf{R}_{2e-1}[z]$,

$$\sum_{i=1}^{n} (b_i - \mu_i)\, z_i\, f(z_i) = 0. \tag{5.24}$$

On the other hand, by theorem 5.7(ii), the $(n+1)$-tuple $\mathbf{b}$ has exactly $e+1$ nonzero components $b_0, b_{i_1}, \ldots, b_{i_e}$, with the property that $z_{i_1}, \ldots, z_{i_e}$ are the zeros of the Lloyd polynomial $\Psi_e(z)$. Hence (5.24) becomes, for $p_k = z_{i_k}$:

$$\sum_{k=1}^{e} b_{i_k}\, p_k\, f(p_k) = \sum_{i=1}^{n} \mu_i\, z_i\, f(z_i).$$

Applying theorem 5.4 to the Lloyd polynomials, with $w(z_i) = \mu_i$, we deduce $b_{i_k} = p_k^{-1}\, w_k$. Substituting this value of $\mathbf{b}$ in the formula $a_j = |X|^{-1}\, \mathbf{b}\, P_j$ we obtain the desired result (5.23).

Example. Let us compute the distance distribution $\mathbf{a}$ of a perfect code Y of order $e = 2$ in the Hamming scheme $H(11, 3)$. In fact, there is exactly one linear code having these parameters (cf. Pless [56]), namely the ternary Golay code.

The Lloyd polynomial $\Psi_2(z)$ is expressed as follows in terms of the Krawtchouk polynomials (cf. theorem 4.2): $\Psi_2(z) = K_0(z) + K_1(z) + K_2(z)$. Using for instance (4.7), one readily obtains

$$\Psi_2(z) = 3^5\,(1 - z/6)\,(1 - z/9).$$

Moreover, (5.9) gives the values $w_1 = 3^8 \times 88$ and $w_2 = 3^8 \times 110$ for the Christoffel numbers corresponding to the zeros $p_1 = 6$ and $p_2 = 9$ of $\Psi_2(z)$. Finally, formula (5.23) yields

$$\mathbf{a} = (1, 0, 0, 0, 0, 132, 132, 0, 330, 110, 0, 24),$$

which is the well-known weight (or distance) distribution of the ternary Golay code.

5.2.3. *Distribution matrix of a code*

The distribution matrix $B \in \mathbf{R}(X,N)$ of a code Y in a metric scheme is defined as in sec. 3.1: if ϱ denotes the distance, then the element $B(x,i)$ of B is the number of points $y \in Y$ at distance $\varrho(x,y) = i$ from the given point $x \in X$. We shall consider the integer

$$\varrho(x,Y) = \min_{y \in Y} \varrho(x,y), \tag{5.25}$$

i.e. the distance from x to the code Y. Clearly, $\varrho(x,Y)$ is the smallest integer i such that $B(x,i) \neq 0$. In the following, the rows of B will be denoted by $B(x)$ and the columns by B_i, for $x \in X$, $i \in N$.

Specializing theorems 3.1 and 3.3 to metric schemes we shall now derive a result which is often very useful for actual computation of the distribution matrix. In case of Hamming schemes, cf. Delsarte [14]).

Theorem 5.9. For a code Y of external distance r in a metric scheme, the columns of indices $i = 0, 1, \ldots, r$ of the distribution matrix B generate its whole column space. More precisely, for an integer i between r and n, the column B_i is a linear combination of the all-one vector ϕ_X and of the columns $B_0, B_1, \ldots, B_{r-1}$, with coefficients only depending on the distance distribution of Y.

Proof. Let L be the set of values of i, $1 \leqslant i \leqslant n$, for which the distance distribution $\mathfrak{a}$ of Y satisfies $\mathfrak{a}Q_i \neq 0$. By definition, the external distance r is the cardinality of L. For an integer m, with $0 \leqslant m \leqslant n-r$, let us define the polynomial

$$\beta(z) = |X|\,|Y|^{-1} z^m \prod_{i \in L} (1 - z/z_i), \tag{5.26}$$

of degree $m + r \leqslant n$. We consider its expansion in the basis of polynomials $\Phi_k(z)$ corresponding to the eigenmatrix P:

$$\beta(z) = \beta_0 \Phi_0(z) + \beta_1 \Phi_1(z) + \ldots + \beta_n \Phi_n(z), \tag{5.27}$$

with $\beta_i = 0$ for $i > m + r$ and $\beta_{m+r} \neq 0$. Applying the identity

$$|X|\,\mathfrak{b}\,\mathfrak{b}^T = (\mathfrak{b}\,P^T)\,(\mathfrak{b}\,Q)^T$$

to the $(n+1)$-tuples $\mathfrak{b} = (\beta_0, \ldots, \beta_n)$ and $\mathfrak{b} = B(x) = (B(x,0), \ldots, B(x,n))$, we obtain, by (5.27),

$$\mathfrak{b}\,B^T(x) = |X|^{-1} \sum_{k=0}^{n} \beta(z_k)\,(B(x)\,Q_k).$$

It follows from theorem 3.3 that $B(x)\,Q_k$ is zero, for all x, whenever k belongs to $N^* - L$. Hence, remembering the definition (5.26) of $\beta(z)$, we deduce

$$\mathfrak{b}\,B^T(x) = |Y|^{-1}\,\delta_{0,m}\,(B(x)\,Q_0).$$

Finally, Q_0 being the all-one vector, we have $B(x)\,Q_0 = |Y|$ and the matrix form of the above equation becomes

$$\mathfrak{b}\,B^T = \delta_{0,m}\,\phi_X{}^T. \tag{5.28}$$

As β_{m+r} is not zero, this shows that the column B_{m+r} is a linear combination of $\delta_{0,m}\,\phi_X$ and of the B_i with $i < m + r$. By this argument, using induction on m, we readily obtain the desired results, remembering that the $(n+1)$-tuples $\mathfrak{b}$ only depend on the distance distribution.

We shall now derive several consequences of theorem 5.9. The following result tends to justify the terminology adopted for the parameter r.

Theorem 5.10. Let Y be a code of external distance r in a metric scheme (X,R). Then each point of X is at distance less than or equal to r from at least one point of Y.

Proof. Let us assume, on the contrary, there exists a point $x \in X$ such that $\varrho(x,Y) > r$, i.e., equivalently, such that $B_0(x) = \ldots = B_r(x) = 0$. Then theorem 5.9 leads to the absurd conclusion that the row $B(x)$ must be identically zero.

Given a code Y, we shall use the name of *true external distance* of Y for the following integer:

$$\varrho(X,Y) = \max_{x \in X} \varrho(x,Y). \tag{5.29}$$

Theorem 5.10 simply indicates that r is an upper bound to the true external distance. The interest of our concept of external distance lies in the fact that it can be determined from the distance distribution, whereas $\varrho(X,Y)$ cannot (in general).

Theorem 5.11. Let Y be a code of minimum distance d and external distance r. Then all rows $B(x)$ of the distribution matrix corresponding to a fixed value of $\varrho(x,Y)$ are identical in the following cases: $0 \leqslant \varrho(x,Y) \leqslant d-r$ and $\varrho(x,Y) = r$.

Proof. For a given integer j such that $0 \leqslant j \leqslant d-r$ or $j = r$, let x be any point of X satisfying $\varrho(x,Y) = j$. Using the inequality of the triangle in the metric space (X,ϱ) we easily obtain $B_i(x) = \delta_{i,j}$ for $i = 0, 1, \ldots, r-1$. So the first r components of $B(x)$ do not depend on x but only on j. Consequently, by theorem 5.9, the whole row $B(x)$ is independent of x.

According to the terminology of sec. 3.1, a code Y is *regular* in a metric scheme if and only if the number of points of Y at a given distance from a fixed $x \in Y$ does not depend on the choice of x. Specializing theorem 5.11 to $x \in Y$, i.e. $\varrho(x,Y) = 0$, we obtain the following sufficient condition for regularity.

Theorem 5.12. A code is regular if its minimum distance d is at least equal to its external distance r.

For instance, the perfect codes satisfy $d = 2r + 1$ and theorem 5.12 implies that these codes are regular. (Consequently, the components (5.23) of the distance distribution must be integers.) In fact, they are "completely regular" in the sense we shall now define.

A code having the property that, for all $x \in X$, the row $B(x)$ of the distribution matrix only depends on the distance $\varrho(x,Y)$ will be said to be *completely regular*. (This, of course, implies regularity.)

Theorem 5.13. If the parameters of a code Y satisfy $d = 2r-1$, $2r$ or $2r+1$, then Y is completely regular.

Proof. Assuming $d \geqslant 2r-1$ we deduce $\varrho(x,Y) \leqslant d-r$ or $\varrho(x,Y) = r$, for all $x \in X$, from theorem 5.10. Hence the complete regularity is an immediate consequence of theorem 5.11.

Let us mention two recent generalizations of the perfect codes (in binary Hamming schemes) which satisfy the condition $d \geqslant 2r-1$ for being completely regular: the uniformly packed codes introduced by Semakov, Zinov'ev and Zaitzev [62]) and the nearly perfect codes defined by Goethals and Snover [26]).

Theorem 5.10 implicitly contains a lower bound to the number of points in a code of a given external distance. We shall now combine it with theorem 5.7.

Theorem 5.14. Let Y be a code of minimum distance d and external distance r. Then the following inequalities hold, with $e = [(d-1)/2]$:

$$\sum_{i=0}^{e} v_i \leqslant |X|\,|Y|^{-1} \leqslant \sum_{i=0}^{r} v_i. \tag{5.30}$$

Moreover, if one of the bounds (5.30) is achieved, then so is the other one. This occurs if and only if Y is a perfect code of order e. A necessary condition for the existence of such a code is that all zeros of the Lloyd polynomial of degree e belong to the set $\{z_1, \ldots, z_n\}$.

Proof. Let us define $u = \varrho(X,Y)$, i.e. the true external distance (5.29). By definition, each point of X belongs to at least one sphere $S_u(y)$ of radius u centred at some point $y \in Y$. Hence we deduce $|X| \leqslant |S_u(y)|\,|Y|$. As we know, by theorem 5.10, that u is at most equal to r, this clearly yields the right-hand inequality in (5.30) since $v_0 + \ldots + v_r$ is the volume $|S_r(y)|$. Moreover, equality is only possible if $u = r$ and if the spheres $S_r(y)$ form a partition of X for y running through Y, which is precisely the definition of a perfect code of order r. The other results to be proved were already contained in theorem 5.7.

Let us now examine in more detail the properties of the polynomial (5.26) with $m = 0$, which we call the *minimal polynomial* of Y:

$$\beta(z) = |X|\,|Y|^{-1} \prod_{i \in L} (1 - z/z_i). \tag{5.31}$$

By definition of L and r, it has degree $r = |L|$ and vanishes at the r points z_i, with $1 \leqslant i \leqslant n$, such that $\mathbf{a}Q_i \neq 0$. So it only depends on the distance distribution $\mathbf{a}$ of Y. It turns out that, in many cases, a simple look at its minimal polynomial gives interesting information on a code:

Theorem 5.15. Let Y be a code of minimum distance d and external distance r. Let $\boldsymbol{\beta}$ be the $(n+1)$-tuple of components of the minimal polynomial $\beta(z)$ in the basis $\{\Phi_k(z)\}$. The following propositions hold:

(i) If $d-1 \geqslant r$, then $\beta_0 = \beta_1 = \ldots = \beta_{d-1-r} = 1$.

(ii) If $\beta_0 > 0$ and $\beta_1, \ldots, \beta_r \geqslant 0$, then $\beta_0 \leqslant 1$. If, besides, $\beta_0 = 1$, then $\beta_k \leqslant 1$ for all k, and Y achieves the linear-programming bound for $(N^* - L)$-designs.

(iii) If $\beta_0, \beta_1, \ldots, \beta_r > 0$, then the condition $\beta_0 = 1$ is equivalent to $d-1 \geqslant r$ and, in this case, $d-1-r$ is equal to the largest integer j such that $\beta_0 = \beta_1 = \ldots = \beta_j = 1$.

Proof. (i) Assuming $d-1 \geqslant r$, we use (5.28) with $m = 0$. For a point $x \in X$ such that $\varrho(x,Y) = k \leqslant d-1-r$, it is easily seen that the equation $\boldsymbol{\beta}\, B^T(x) = 1$ becomes simply $\beta_k = 1$. As $\varrho(x,Y)$ actually takes all values k between 0 and $d-1-r$, this shows the first result.

(ii) Let us assume $\beta_0, \ldots, \beta_r \geqslant 0$, with $\beta_0 \neq 0$. Then, for $M = L \cup \{0\}$, the $(n+1)$-tuple $\beta_0^{-1}\,\boldsymbol{\beta}$ is a program of $(P,M)'$ such that $\gamma = (\beta_0\,|Y|)^{-1}\,|X|$; this readily follows from the definition (5.31) of $\beta(z)$ and from (5.27). On the other hand, Y is an $(N-M)$-design. Hence, by theorem 3.11, the $(n+1)$-tuple $\mathbf{b} = |Y|^{-1}\,\mathbf{a}\,Q$ is a program of (P,M) with $g = |Y|^{-1}\,|X|$. The general inequality $g \leqslant \gamma$ becomes here $\beta_0 \leqslant 1$.

In case $\beta_0 = 1$, the programs $\mathbf{b}$ and $\boldsymbol{\beta}$ are extremal. This yields $g = \gamma = g(P,M)$, so that Y achieves the linear-programming bound (3.29) for T-designs with $T = N - M = N^* - L$. Moreover, by lemma 3.6, we have $\beta_k \leqslant 1$ for all k, and the second part is proved.

(iii) For $\beta_0 = 1$ and $\beta_1, \ldots, \beta_r \geqslant 0$ we just have seen that $\mathbf{b}$ and $\boldsymbol{\beta}$ form a pair of extremal programs of (P,M) and $(P,M)'$, respectively. Assuming $\beta_1, \ldots, \beta_r \neq 0$, and using theorem 3.4(ii), we obtain $\mathbf{b}\,P_k = 0$, i.e. $a_k = 0$, for $k = 1, \ldots, r$. Therefore, the minimum distance d is at least $r+1$.

Conversely, for $\beta_0 > 0$ and $\beta_1, \ldots, \beta_r \geqslant 0$, the condition $d \geqslant r+1$ implies that $(\mathbf{b}, \beta_0^{-1}\,\boldsymbol{\beta})$ is a pair of extremal programs; this is a consequence of theorem 3.4(ii). Hence we have $g = \gamma$ and, so, $\beta_0 = 1$. The last proposition follows from lemma 3.6; the details are left to the reader.

Example. To illustrate this chapter we finally investigate a remarkable code for which it will be possible to derive the complete distribution matrix, in a purely mechanical way. We consider the largest code Y in the Johnson scheme $J(8, 24)$ with minimum distance $d = 4$. It turns out that it is unique and achieves the Singleton bound (cf. sec. 4.3.2). In fact, Y contains 759 codewords and forms the celebrated Steiner system $S(5, 8, 24)$ whose uniqueness was shown by Witt [76]).

The distance distribution $\mathbf{a}$ of Y is well known (cf. for instance Goethals and Seidel [25])); it is given by $a_0 = 1$, $a_4 = 280$, $a_6 = 448$, $a_8 = 30$ and $a_i = 0$ for $i \neq 0, 4, 6, 8$. From the formulas for the eigenmatrix Q of a Johnson scheme (sec. 4.2.1) we compute

$$\mathbf{a}Q = 69\,(11, 0, 0, 0, 0, 0, 3808, 0, 6840).$$

Let us notice that the property $\mathfrak{a}\, Q_1 = \ldots = \mathfrak{a}\, Q_5 = 0$ is in agreement with the fact that Y forms a 5-design (cf. theorem 4.7). By definition, the external distance of Y is $r = s(\mathfrak{a}\, Q) = 2$. Hence from theorem 5.13 it follows that Y is completely regular: its distribution matrix B contains only three distinct rows $B(x)$ determined by the values (0, 1 and 2) taken by the Johnson distance $\varrho(x,Y) = d_1(x,Y)$.

Table II gives these three rows, together with the number of their occurrences in B. The computations have been performed by use of the polynomials (5.26) with $L = \{6, 8\}$ and $z_i = i\,(25 - i)$. In particular, the expansion of the minimal polynomial (5.31) in the basis of "modified Eberlein polynomials" $\Phi_k(z)$ is the following:

$$\beta(z) = \Phi_0(z) + \Phi_1(z) + \tfrac{1}{4}\,\Phi_2(z),$$

with $\Phi_k(u\,(25-u)) = E_k(u)$. We observe that this result agrees with theorem 5.15. From it we can compute the column B_2 of the matrix B by using (5.28) with $m = 0$; we deduce $B(x,2) = 4$ for $\varrho(x,Y) = 2$. The columns $B_3, \ldots, B_8$ can be calculated, successively, by the same method.

TABLE II

Outer distribution of $S(5, 8, 24)$

i / $\varrho(x,Y)$	0	1	2	3	4	5	6	7	8	multiplicity
0	1	0	0	0	280	0	448	0	30	759
1	0	1	0	35	140	231	252	85	15	128×759
2	0	0	4	32	130	256	228	96	13	840×759

5.3. Q-polynomial schemes and designs

Let us recall the definition: A symmetric association scheme with n classes, having Q as second eigenmatrix, is said to be *Q-polynomial* if there exist polynomials $\Phi_0(z), \ldots, \Phi_n(z)$, with $\Phi_k(z) \in \mathbf{R}_n[z]$, such that

$$\Phi_k(z_i) = Q_k(i), \qquad \forall\, i,k \in N = \{0, 1, \ldots, n\}, \tag{5.32}$$

for a fixed set $\{z_0 = 0, z_1, \ldots, z_n\}$ of distinct real numbers $z_i \geqslant 0$. In particular, we have seen in ch. 4 that the Hamming and Johnson schemes are Q-polynomial with $z_i = i$.

The present section looks like the preceding one. Essentially, we shall introduce and investigate the concept of t-designs of maximum strength t, which is a generalization of the classical notion. These "designs" play a similar role as the "codes" with given minimum distance d in the theory of metric schemes.

5.3.1. *Preliminary results*

We have seen in sec. 5.2.1 the intrinsic meaning of P-polynomial schemes, namely their metric properties. Unfortunately it seems difficult, in general, to attach such a precise combinatorial meaning to the dual concept of Q-polynomial schemes. Nevertheless, we shall give two algebraic characterizations of such schemes.

The first result is expressed in terms of the numbers $q_{i,j}^{(k)}$ defined by (2.26). It is to be compared with theorem 5.6; the proof, being quite similar, will not be repeated.

Theorem 5.16. A symmetric association scheme is Q-polynomial if and only if the parameters $q_{i,j}^{(k)}$ satisfy the following two conditions: $q_{i,j}^{(k)} \neq 0$ for $k = i + j$ and $(q_{i,j}^{(k)} \neq 0) \Rightarrow (|i-j| \leqslant k \leqslant i+j)$.

The second criterion uses the Bose–Mesner algebra A, over the reals, of the given symmetric scheme (X,R). Let $z_0 = 0, z_1, \ldots, z_n$ be $n+1$ distinct non-negative real numbers. To any polynomial $f(z) \in \mathbf{R}_n[z]$ corresponds a unique matrix $D^{(f)} \in \mathsf{A}$ such that

$$D^{(f)} = \sum_{i=0}^{n} f(z_i)\, D_i, \tag{5.33}$$

where D_i is the adjacency matrix of R_i. We define the operator $*$ over $\mathbf{R}_n[z]$ corresponding to the matrix product in A:

$$f(z) * g(z) = h(z) \qquad \text{for} \qquad D^{(f)}\, D^{(g)} = D^{(h)}.$$

The system $(\mathbf{R}_n[z], +, *)$ is an $(n+1)$-dimensional commutative algebra over $\mathbf{R}$; it is isomorphic to A and, therefore, to $\mathbf{R}^{n+1}$.

Theorem 5.17. A symmetric association scheme is Q-polynomial with respect to the z_i if and only if its Bose–Mesner algebra satisfies the following inequality, for all $f(z)$, $g(z) \in \mathbf{R}_n[z]$:

$$\deg\,(f(z) * g(z)) \leqslant \min\,(\deg f(z), \deg g(z)). \tag{5.34}$$

Proof. Let us first assume the algebra $\mathbf{R}_n[z]$ satisfies (5.34). This property can also be expressed as follows: the subspace $\mathbf{R}_k[z]$ is an ideal in $\mathbf{R}_n[z]$, for $k = 0, 1, \ldots, n$. Hence, denoting by A_k the image of $\mathbf{R}_k[z]$ in the BM algebra A, we have the following chain of ideals in A:

$$\langle J \rangle = \mathsf{A}_0 \subset \mathsf{A}_1 \subset \ldots \subset \mathsf{A}_n = \mathsf{A}.$$

For a suitable numbering of the minimal idempotents $J_0, J_1, \ldots, J_n$ of $\mathbf{A}$ we can assume J_k belongs to $\mathbf{A}_k - \mathbf{A}_{k-1}$, for all k, with $\mathbf{A}_{-1} = \{0\}$; then we shall denote by $\Phi_k(z)$ the image of $|X|\ J_k$ in $\mathbf{R}_k[z]$, i.e. the polynomial satisfying

$$|X|\ J_k = \sum_{i=0}^{n} \Phi_k(z_i)\, D_i. \tag{5.35}$$

Comparing this with the definition (2.16) of the eigenmatrix Q, we deduce $Q_k(i) = \Phi_k(z_i)$. Hence the given scheme is Q-polynomial with respect to the z_i.

Conversely, we assume $Q_k(i) = \Phi_k(z_i)$, for all i,k, with $\Phi_k(z) \in \mathbf{R}_k[z]$. The orthogonality relations on the idempotents J_k, given by (5.35), have the following image in the algebra $\mathbf{R}_n[z]$:

$$\Phi_k(z) *_{\mathbf{a}}^{\circ} \Phi_j(z) = |X|^{\circ} \delta_{k,j}\, \Phi_k(z). \tag{5.36}$$

Let us now consider any two polynomials $f(z)$, $g(z) \in \mathbf{R}_n[z]$ and their expansions $f = \sum \alpha_k \Phi_k$, $g = \sum \beta_k \Phi_k$ in the basis $\{\Phi_k\}$. Using (5.36) we obtain

$$f(z) * g(z) = |X| \sum_{k=0}^{n} \alpha_k \beta_k \Phi_k(z).$$

Since the degree of the right-hand member cannot exceed $\deg(f(z))$ or $\deg(g(z))$, this completes the proof of the theorem.

Example. Let us verify, using lemma 4.5, that the Johnson scheme $J(n,v)$ is Q-polynomial for $z_j = j$, in agreement with the result obtained at the end of sec. 4.2.1. The definition (4.22) of the matrix C_i can be written in the form (5.33) as follows:

$$C_i = D^{(p_i)}, \qquad \text{with} \qquad p_i(z) = \binom{n-z}{i}.$$

Since $p_i(z)$ has degree i, we deduce from lemma 4.5 that the degree of $p_r(z) * p_s(z)$ is equal to $\min(r,s)$. Hence, as $p_0(z), \ldots, p_n(z)$ form a basis of $\mathbf{R}_n[z]$, the inequality (5.34) is identically satisfied, so that, by theorem 5.17, the Johnson scheme is Q-polynomial.

Definition. Let (X,R) be a Q-polynomial scheme with n classes and let τ be an integer, $0 \leqslant \tau \leqslant n$. A nonempty subset Y of X will be called a *τ-design* (of strength τ) if its inner distribution $\mathbf{a}$ satisfies $\mathbf{a}\, Q_1 = \ldots \mathbf{a}\, Q_\tau = 0$. Equivalently, for $\tau \geqslant 1$, the subset Y is a T-design for $T = \{1, 2, \ldots, \tau\}$.

We have seen in theorem 4.7 that a τ-design in the Johnson scheme $J(n,v)$ is a τ-design $S_\lambda(\tau,n,v)$ in the usual sense; so the above definition is a generalization of the classical concept. The reader will also remember that, in Hamming schemes, the τ-designs are the orthogonal arrays of strength τ.

From the inner distribution $\mathbf{a}$ of Y we introduce two parameters t and s which play a similar role as the numbers $t' = d-1$ and $s' = r$, respectively, introduced in sec. 5.2.1 for P-polynomial schemes:

$$t = t(\mathbf{a}\, Q) = \textit{maximum strength} \text{ of } Y,$$
$$s = s(\mathbf{a}) = \textit{degree} \text{ of } Y.$$

The integer s is equal to the number of relations R_i whose restriction $R_i \cap Y^2$ is non-empty, for $1 \leqslant i \leqslant n$. As for the parameter t, it is equal to the largest τ such that Y is a τ-design.

Like in sec. 5.2, we shall only consider *nontrivial designs*, i.e. subsets of X with $1 < |Y| < |X|$. Then it is easily seen that the parameters satisfy $1 \leqslant s$, $t+1 \leqslant n$. Let us also apply the MacWilliams inequality (theorem 5.5); we obtain

$$s \geqslant [t/2], \tag{5.37}$$

which is the "dual" of (5.16). We shall examine in sec. 5.3.2, under the name of tight designs, the designs satisfying equality in (5.37). This is the dual of the concept of perfect codes.

The characteristic matrices $H_k \in \mathbf{C}(Y,X_k')$ defined in sec. 3.5 will be most useful in our theory of designs in Q-polynomial schemes. We shall also use the following matrices:

$$G_k = [H_0, H_1, \ldots, H_k], \qquad 0 \leqslant k \leqslant n. \tag{5.38}$$

Let us first show how the maximum strength t of Y depends on the properties of the characteristic matrices.

Theorem 5.18. Let e be the largest integer such that $\bar{G}_e G_e = |Y|\ I$, with $0 \leqslant e \leqslant n-1$. Then the maximum strength of the design Y is $t = 2e+1$ or $t = 2e$ according to whether the matrix $\bar{G}_e H_{e+1}$ is zero or not.

Proof. Let us assume $\bar{G}_e H_{e+1} = 0$. Then, by definition of e, the characteristic matrices satisfy

$$\bar{H}_i H_j = \begin{cases} 0 & \text{for} \quad i \neq j,\ i \leqslant e,\ j \leqslant e+1, \\ |Y|\ I & \text{for} \quad i = j \leqslant e. \end{cases}$$

On the other hand, by theorem 5.16, the numbers $q_{i,j}^{(k)}$ are distinct from zero for $k = i+j$. Therefore, using the second part of theorem 3.15, we readily obtain the following equations on the inner distribution $\mathbf{a}$ of the design: $\mathbf{a}\, Q_k = 0$ for $1 \leqslant k \leqslant 2e+1$, wich implies $t \geqslant 2e+1$.

Supposing $t \geqslant 2e+2$, one would have, besides, $\mathbf{a} Q_{2e+2} = 0$. Using now the first part of theorem 3.15 and theorem 5.16, with $i = j = e+1$, we deduce $\bar{H}_{e+1} H_{e+1} = |Y|\ I$ and, consequently, $\bar{G}_{e+1} G_{e+1} = |Y|\ I$. As this contradicts the definition of e, the only possibility is $t = 2e+1$. The reasoning is quite similar in the case $\bar{G}_e H_{e+1} \neq 0$.

5.3.2. *The Rao–Wilson bound and the tight designs*

We shall now derive an inequality for designs in Q-polynomial schemes which is the "dual" of the Hamming bound for codes in metric schemes.

Theorem 5.19. Let Y be a t-design of maximum strength t. Then the following inequality holds, with $e = [t/2]$:

$$|Y| \geqslant \mu_0 + \mu_1 + \ldots + \mu_e. \tag{5.39}$$

First proof. By theorem 5.18, the columns of G_e are pairwise orthogonal. This implies that the number of rows in G_e is at least equal to the number of columns, which was to be proved.

In particular, using formulas (4.32) for the multiplicities μ_i of the Johnson scheme $J(n,v)$, we obtain $|Y| \geqslant \binom{v}{e}$, a result due to Wilson and Ray-Chaudhuri [75] for t-designs in the usual sense. When applied to the Hamming scheme $H(n,q)$, with $\mu_i = \binom{n}{i}(q-1)^i$, (5.39) becomes the Rao bound [59] for orthogonal arrays of strength t. Let us give another proof of theorem 5.19, showing that the linear-programming bound for t-designs is always at least as good as the *Rao–Wilson bound* (5.39).

Second proof. From the polynomials $\Phi_k(z)$ corresponding to the eigenmatrix Q we define the sum polynomial of degree e, that is,

$$\Psi_e(z) = \Phi_0(z) + \Phi_1(z) + \ldots + \Phi_e(z). \tag{5.40}$$

Next, writing $\mu_e' = \mu_0 + \ldots + \mu_e$ for convenience, we consider the $(n+1)$-tuple $\beta = (\beta_0, \beta_1, \ldots, \beta_n)$ given by

$$\beta_k = (\Psi_e(z_k)/\mu_e')^2.$$

Using the same argument as in theorem 5.7, we can show that $(\beta P^T)_i$ is equal to zero for $i \geqslant t+1$ and to $|X|/\mu_e'$ for $i = 0$, whence β is a program of $(P,M)'$, with $M = \{0, t+1, \ldots, n\}$, such that $\gamma = |X|/\mu_e'$.

On the other hand, if $\mathbf{a}$ denotes the inner distribution of Y, we know from theorem 3.11 that the $(n+1)$-tuple $\mathbf{b} = |Y|^{-1}\,\mathbf{a}\,Q$ is a program of (P,M) with $g = |X|/|Y|$. Then the desired result $|Y| \geqslant \mu_e'$ follows from the inequalities $g \leqslant g(P,M) \leqslant \gamma$, satisfied by any pair $(\mathbf{b},\beta)$ of programs.

Definitions. (i) By extension of the concept introduced by Wilson [74], a t-design Y of maximum strength t will be said to be a *tight design of order e* if it satisfies equality in (5.39), i.e. $|Y| = \mu_0 + \ldots + \mu_e$ with $e = [t/2]$.

(ii) The polynomial $\Psi_e(z)$ defined in (5.40) will be called the *Wilson polynomial of degree e*.

In the case of Hamming schemes, the tight designs are equivalent to the *generalized Hadamard codes* [14] and the Wilson polynomials are the same as the Lloyd polynomials (cf. theorem 4.2).

Both arguments used in proving theorem 5.19 easily lead to a necessary condition for tight designs very similar to the Lloyd condition for perfect codes. However, to avoid useless repetition, we shall postpone this result after a study of the concept of degree.

Let us denote by $i_0 = 0, i_1, \ldots, i_s$ the values of i for which the restriction $R_i \cap Y^2$ of R_i to Y is non-empty. By definition, s is the degree of Y. We shall call the polynomial

$$\alpha(z) = |Y|\,(1 - z/z_{i_1})\,(1 - z/z_{i_2}) \ldots (1 - z/z_{i_s}), \tag{5.41}$$

of degree s, the *annihilator polynomial of Y*. One will have noticed the analogy with the minimal polynomial (5.31) defined for metric schemes.

Let us consider the expansion of $\alpha(z) \in \mathbf{R}_s[z]$ in the basis of polynomials $\Phi_k(z)$:

$$\alpha(z) = \alpha_0\,\Phi_0(z) + \alpha_1\,\Phi_1(z) + \ldots + \alpha_s\,\Phi_s(z). \tag{5.42}$$

From the real numbers α_k we construct the following diagonal matrix Γ, of order $\mu_s' = \mu_0 + \mu_1 + \ldots + \mu_s$:

$$\Gamma = \alpha_0\,I_0 \oplus \alpha_1\,I_1 \oplus \ldots \oplus \alpha_s\,I_s, \tag{5.43}$$

where I_k is the unit matrix of $\mathbf{C}(X_k',X_k')$ and $\oplus$ stands for the direct sum. The following theorem is a straightforward extension of a result of the author [14] about codes in Hamming schemes.

Theorem 5.20. Let $\alpha(z) = \sum \alpha_k\,\Phi_k(z)$ be the annihilitor polynomial of a design Y of degree s. Then the matrices G_s and Γ defined by (5.38) and (5.43), respectively, are related by

$$G_s\,\Gamma\,\bar{G}_s = |Y|\,I. \tag{5.44}$$

Moreover, the rank of G_s is equal to the number $|Y|$ of its rows, which implies $|Y| \leqslant \mu_s' = \mu_0 + \mu_1 + \ldots + \mu_s$.

Proof. Obviously, we have $G_s\,\Gamma\,\bar{G}_s = \sum \alpha_k\,H_k\,\bar{H}_k$. Therefore, we deduce from theorem 3.13, with $Q_k(i) = \Phi_k(z_i)$:

$$G_s\,\Gamma\,\bar{G}_s = \sum_{i=0}^{n} \Big(\sum_{k=0}^{s} \alpha_k\,\Phi_k(z_i)\Big)\,(D_i \mid Y),$$

where $D_i \mid Y$ denotes the adjacency matrix of $R_i \cap Y^2$. By definition of the annihilator polynomial, each term $\alpha(z_i)\,(D_i \mid Y)$ of the right-hand sum is zero, except for $i = 0$ in which case it is equal to $|Y|\,I$. This yields the desired formula (5.44).

In order to prove the second part of the theorem, it is sufficient to notice that, as $G_s\,\Gamma\,\bar{G}_s$ has rank $|Y|$, the matrix G_s, of type $|Y| \times \mu_s'$, must also have rank $|Y|$.

Remark. Let us denote by σ the smallest integer, with $0 \leqslant \sigma \leqslant n$, such that rank $(G_\sigma) = |Y|$. Theorem 5.20 shows that σ is less than or equal to s. In fact the degree s plays a similar role with respect to σ as the external distance r with respect to $\varrho(X,Y)$ in the theory of metric schemes (cf. sec. 5.2.3). In the particular case of additive codes, this analogy is more than formal (cf. sec. 6.3).

We shall now obtain a "dual" of theorem 5.14; essentially, it is a generalization of theorems due to Wilson [74]) for t-designs and to the author [14]) for codes, in the usual sense of both terms.

Theorem 5.21. Let Y be a t-design of maximum strength t and degree s. Then the following inequalities hold, with $e = [t/2]$:

$$\sum_{k=0}^{e} \mu_k \leqslant |Y| \leqslant \sum_{k=0}^{s} \mu_k. \tag{5.45}$$

Moreover, if one of the bounds (5.45) is achieved, then so is the other one. This occurs if and only if Y is a tight design of order e. A necessary condition for the existence of such a design is that all zeros of the Wilson polynomial of degree e belong to the set $\{z_1, \ldots, z_n\}$.

Proof. The two bounds were already given in theorems 5.19 and 5.20. We notice that they imply the Mac Williams inequality (5.37). Defining $\mu_k' = \mu_0 + \ldots + \mu_k$, we first assume $|Y| = \mu_s'$ with, necessarily, $s \leqslant n-1$ for a nontrivial design. Equation (5.44) clearly implies

$$\tilde{G}_s G_s = |Y|\, \Gamma^{-1}, \tag{5.46}$$

the square matrices G_s and Γ, of order μ_s', being nonsingular. Consequently, the diagonal entries α_k of Γ are positive and we deduce $\alpha_0 = 1$ since the column H_0 of G_s is the all-one vector.

This shows that the $(n+1)$-tuple $\alpha = (\alpha_0, \ldots, \alpha_s, 0, \ldots, 0)$ is a program of $(Q,M)'$, with $M = \{0, i_1, \ldots, i_s\}$; indeed we have $(\alpha\, Q^T)_i = \alpha(z_i)$, by (5.32) and (5.42), so that the conditions for a program of $(Q, M)'$ are trivially satisfied. For the program α, the function γ is given by $\gamma = \alpha(0) = |Y|$. Since, by definition, Y is an M-clique, α is in fact a minimal program (cf. the linear-programming bound (3.22)). Then, using lemma 3.6, we deduce $\alpha_k \leqslant 1$ for all k.

On the other hand, we may write

$$\sum_{k=0}^{s} \alpha_k \mu_k = |Y| = \sum_{k=0}^{s} \mu_k. \tag{5.47}$$

Indeed, the left-hand equation simply is $\alpha(0) = |Y|$, by (5.42) with $\Phi_k(0) = \mu_k$, and the right-hand equation is our assumption $|Y| = \mu_s'$. Obviously, (5.47) together with $\alpha_k \leqslant 1$ implies $\alpha_0 = \alpha_1 = \ldots = \alpha_s = 1$. In other words, the annihilator polynomial (5.42) is the Wilson polynomial $\Psi_s(z)$, which, consequently, must vanish for $z = z_{i_1}, \ldots, z_{i_s}$. Let us now go back to (5.46) with $\Gamma = I$. Owing to theorem 5.18, this implies $e \geqslant s$, whence, by the Mac Williams inequality, $e = s$. So we have $|Y| = \mu_e'$, which means, by definition, that Y is a tight design of order e.

Conversely, we assume $|Y| = \mu_e'$. From theorem 5.18 it follows that the square matrix G_e is orthogonal. By the same argument as in theorem 5.20, we can write the equation $G_e \tilde{G}_e = |Y|\, I$ in the form

$$\sum_{i=0}^{n} \Psi_e(z_i)\, (D_i \mid Y) = |Y|\, I,$$

using the Wilson polynomial (5.40). This clearly means that $\Psi_e(z)$ vanishes at points $z = z_{i_1}, \ldots, z_{i_s}$, which is only possible for $e \geqslant s$. From (5.37) we deduce $e = s$ and, so, $|Y| = \mu_s'$. This concludes the proof of the theorem.

Remark. The maximum strength of a tight design is always an even number $t = 2e = 2s$. Indeed, supposing $t = 2e+1$ we would deduce $\tilde{G}_e H_{e+1} = 0$ from theorem 5.18. This is impossible for a tight design since G_e is a nonsingular square matrix and H_{e+1} is not zero.

Using the fact that the Wilson polynomials form a family of orthogonal polynomials (cf. theorem 5.2), we shall now derive an explicit formula for the inner distribution of a tight design, only depending on the parameters of the scheme. This is to be compared with theorem 5.8 on perfect codes.

Theorem 5.22. Let $p_1, \ldots, p_e$ be the zeros of the Wilson polynomial $\Psi_e(z)$ of degree e, with $1 \leqslant e \leqslant (n-1)/2$, and let $w_1, \ldots, w_e$ be the corresponding Christoffel numbers. If there exists a tight design Y of order e, then $p_k = z_{i_k}$ holds for some integers $i_1, \ldots, i_e$ between 1 and n, and the nonzero components of the inner distribution $\mathbf{a}$ of Y are, apart from $a_0 = 1$,

$$a_{i_k} = |X|^{-1}\, \Psi_e(0)\, p_k^{-1}\, w_k, \qquad k = 1, 2, \ldots, e. \tag{5.48}$$

Proof. Let Y be a tight design of order e $(= s = t/2)$ and let $i_1, \ldots, i_e$ be the values of i, with $1 \leqslant i \leqslant n$, such that a_i is not zero. In the proof of theorem 5.21, we have seen that the zeros p_k of $\Psi_e(z)$ must be the numbers z_{i_k}.

Next, we shall derive the formula (5.48). By definition, Y is a T-design, with $T = \{1, 2, \ldots, 2e\}$, such that $|Y| = \mu_e' = \Psi_e(0)$. We can write the conditions (3.27) for a T-design in the form

$$\sum_{i=0}^{n} a_i\, \Phi_j(z_i) = |Y|\, \delta_{0,j}, \qquad 0 \leqslant j \leqslant 2e.$$

Equivalently, using the orthogonality properties (cf. theorem 5.1) of the polynomials $\Phi_j(z)$, we have

$$\sum_{i=0}^{n} (a_i - |X|^{-1}\, |Y|\, v_i)\, \Phi_j(z_i) = 0, \qquad 0 \leqslant j \leqslant 2e.$$

As $\{\Phi_0(z), \ldots, \Phi_{2e}(z)\}$ is a basis of $\mathbf{R}_{2e}[z]$, this equation remains satisfied when $\Phi_j(z)$ is replaced by $zf(z)$ for any polynomial $f(z) \in \mathbf{R}_{2e-1}[z]$. In this way we obtain, with $p_k = z_{i_k}$,

$$\sum_{k=1}^{e} a_{i_k} p_k f(p_k) = |X|^{-1} |Y| \sum_{i=1}^{n} v_i z_i f(z_i).$$

Consequently, theorem 5.4, when applied to the Wilson polynomials, yields $a_{i_k} p_k = |X|^{-1} |Y| w_k$, which is the desired result.

Example. In a Hamming scheme $H(n,q)$ the Lloyd and Wilson polynomials are identical. For $n = 11$, $q = 3$, we have seen in sec. 5.2.2 that the zeros of $\Psi_2(z)$ are $p_1 = 6$ and $p_2 = 9$, the corresponding Christoffel numbers being $w_1 = 3^8 \times 88$ and $w_2 = 3^8 \times 110$. So the inner distribution $\mathbf{a}$ of a tight design Y of order 2 in $H(11, 3)$ follows immediately from (5.48), with $|X| = 3^{11}$ and $\Psi_2(0) = 3^5$; we obtain $a_6 = 132$ and $a_9 = 110$, whereas for $i \neq 0, 6, 9$ all components a_i are zero. In specific terminology, Y forms an orthogonal array of length 11, strength 4 and index 3 over a ternary alphabet; it is also a generalized Hadamard code of order 2. In fact, there is a unique linear code Y of this type, namely the dual of the ternary Golay code (cf. theorem 6.6). As far as the author knows, the existence of a nonlinear code is an open problem.

It must be mentioned here that, in the Hamming and Johnson schemes, there are very few known tight designs of order e such that $1 < e < (n-1)/2$: there are exactly three. However, obtaining general nonexistence theorems seems to be a very hard problem, even more difficult than the corresponding problem for perfect codes.

Finally, let us examine more closely the properties of the annihilator polynomial $\alpha(z)$. The results are similar to those of theorem 5.15 about the minimal polynomial. Like before, we shall consider the set $M = \{0, i_1, \ldots, i_s\}$ of integers i such that $R_i \cap Y^2$ is non-empty.

Theorem 5.23. Let Y be a design of maximum strength t and degree s. Let $\boldsymbol{\alpha}$ be the $(n+1)$-tuple of components of the annihilator polynomial in the basis $\{\Phi_k(z)\}$. The following propositions hold:

(i) If $t \geqslant s$, then $\alpha_0 = \alpha_1 = \ldots = \alpha_{t-s} = 1$.

(ii) If $\alpha_0 > 0$ and $\alpha_1, \ldots, \alpha_s \geqslant 0$, then $\alpha_0 \leqslant 1$. If, besides, $\alpha_0 = 1$, then $\alpha_k \leqslant 1$ for all k and Y achieves the linear-programming bound for M-cliques.

(iii) If $\alpha_0, \alpha_1, \ldots, \alpha_s > 0$, then the condition $\alpha_0 = 1$ is equivalent to $t \geqslant s$ and, in this case, $t - s$ is equal to the largest integer j such that $\alpha_0 = \alpha_1 = \ldots = \alpha_j = 1$.

Proof. Let us prove the first part. For $t \geqslant s$, let k be an integer with $0 \leqslant k \leqslant t - s$. (Since $t \leqslant 2s$, this implies $k \leqslant s$.) By a similar reasoning as

in theorem 5.18 we readily obtain

$$\bar{H}_k G_s = |Y| \ (0, \ldots, 0, I, 0, \ldots, 0), \tag{5.49}$$

where $I = I_k$ is the unit matrix of $\mathbf{C}(X_k', X_k')$. On the other hand, multiplying both members of (5.44) to the left by $\bar{H}_k$ and to the right by H_k, we deduce, using $\bar{H}_k H_k = |Y| \ I$,

$$(\bar{H}_k G_s) \, \Gamma \, (\bar{G}_s H_k) = |Y|^2 \, I.$$

Substituting the expression (5.49) of $\bar{H}_k G_s$ in this equation, we simply obtain $\alpha_k = 1$, by definition (5.43) of Γ.

The two other propositions can be proved in the same way as in theorem 5.15, by examination of the linear-programming problems (Q,M) and $(Q,M)'$. The argument will not be repeated.

Example. From the Nordstrom–Robinson code [53]) there can be constructed a binary code Y, with 112 codewords, of length $v = 16$ and constant weight $n = 6$, having the following property: the Johnson distance between distinct codewords assumes exactly three values, namely $i_1 = 3$, $i_2 = 4$ and $i_3 = 5$. So the degree of Y in the Johnson scheme $J(6, 16)$ is $s = 3$ and its annihilator polynomial is

$$\alpha(z) = 112 \ (1 - z/3) \ (1 - z/4) \ (1 - z/5).$$

Computing the components α_k of $\alpha(z)$ in the basis of polynomials $\Phi_k(z) = Q_k(z)$ corresponding to $J(6, 16)$, we obtain $\alpha_0 = 1$, $\alpha_1 = 57/65$, $\alpha_2 = 3/13$ and $\alpha_3 = 24/143$. Therefore, it follows from theorem 5.23(iii) that the maximum strength t is equal to the degree $s = 3$. This shows that Y forms a 3-design $S_4(3, 6, 16)$, a result which is due to Goethals [23]). Moreover, theorem 5.23(ii) implies that Y is a maximal $\{0, 3, 4, 5\}$-clique in $J(6, 16)$.

5.3.3. *Regular designs and subschemes*

The question we shall now investigate is that of certain "symmetries" of designs in a Q-polynomial scheme (X,R). We shall derive sufficient conditions, depending on the parameters t and s only, for a design Y to be regular in (X,R) and, on the other hand, for Y to form a subscheme of (X,R).

Let us recall the definition of regularity (cf. sec. 3.1): a design Y is *regular* if all restrictions $R_i \cap Y^2$ of the R_i to Y are regular relations. On the other hand, let $i_0 = 0, i_1, \ldots, i_s$ be the $s+1$ integers i for which $R_i \cap Y^2$ is not empty; we shall consider the following partition of Y^2 into $s+1$ relations R_ν^Y:

$$R^Y = \{R_\nu^Y = R_{i_\nu} \cap Y^2 \mid \nu = 0, 1, \ldots, s\}. \tag{5.50}$$

Then (Y,R^Y) will be called the *restriction* of (X,R) to Y. If (Y,R^Y) is an association scheme (with s classes), it will be said to be a *subscheme* of (X,R). Obviously, this property implies that Y is regular.

The following result is to be compared with theorem 5.12. In the proof we shall make use of the distribution matrix B and of the characteristic matrices H_k.

Theorem 5.24. A design Y is regular if its maximum strength t is at least equal to $s-1$, where s denotes the degree.

Proof. The property of Y being a t-design can be expressed as follows, by use of theorem 3.12:

$$H_k \tilde{H}_k H_0 = |Y|\ \delta_{0,k}\, H_0, \qquad 0 \leqslant k \leqslant t. \tag{5.51}$$

Let x be a fixed point of Y. By definition, the element $B(x,i)$ of B is the number of points $y \in Y$ such that $(x,y) \in R_i$. Writing equality between the x-entries of both members of (5.51), we obtain, using theorem 3.13,

$$\sum_{i=0}^{n} B(x,i)\, Q_k(i) = |Y|\ \delta_{0,k}, \qquad 0 \leqslant k \leqslant t.$$

As each nonzero component $B(x,i)$ of the row $B(x)$ corresponds to some $i \in \{0, i_1, \ldots, i_s\}$, we have, equivalently,

$$\sum_{\nu=1}^{s} B(x,i_\nu)\, Q_k(i_\nu) = |Y|\ \delta_{0,k} - \mu_k, \qquad 0 \leqslant k \leqslant t. \tag{5.52}$$

This system determines uniquely the unknowns $B(x,i_\nu)$. Indeed it is easily verified that the first s equations ($k = 0, 1, \ldots, s-1$) are linearly independent. Hence the row $B(x)$ of B does not depend on the choice of $x \in Y$, which means that Y is regular.

We shall now obtain a sufficient condition for having a subscheme (Y,R^Y), with s classes. (It is the "dual" of the condition in theorem 5.13 for complete regularity in metric schemes.) In the particular case of strongly regular graphs ($s = 2$), the result was first obtained by Goethals and Seidel [25]) for the Johnson schemes and by the author [15]) for the Hamming schemes (under the restrictive hypothesis of linearity). The result for an arbitrary degree s has also been discovered, independently, by Cameron [11]) for the Johnson schemes.

Theorem 5.25. Let Y be a design of maximum strength t and degree s such that $t = 2s-2$, $2s-1$ or $2s$. Then (Y,R^Y) is a subscheme of (X,R), with s classes.

Proof. For $\nu = 0, 1, \ldots, s$, let $D_\nu' = D_{i_\nu} \mid Y$ be the adjacency matrix of $R_\nu{}^Y$. According to theorem 2.1, we only need to show that $D_0' = I, D_1', \ldots, D_s'$ generate a commutative $(s+1)$-dimensional subalgebra of $\mathbf{R}(Y,Y)$.

Let us consider the matrix G_{s-1}, defined as in (5.38). Since t is at least equal to $2s-2$, we have $\tilde{G}_{s-1} G_{s-1} = |Y|\ I$, by theorem 5.18. (The reader will also check that G_{s-1} is not a square matrix.) So we can construct an orthogonal matrix $G = [G_{s-1}, K]$, for a suitable choice of K. The row orthogonality

$G\tilde{G} = |Y|\ I$ can be written as follows:

$$K\tilde{K} = |Y|\ I - (H_0\tilde{H}_0 + H_1\tilde{H}_1 + \ldots + H_{s-1}\tilde{H}_{s-1}). \tag{5.53}$$

By theorem 3.13, each matrix $H_k\tilde{H}_k$ is a linear combination of the D_ν' and, consequently, so is $K\tilde{K}$ too.

On the other hand, the column orthogonality $\tilde{G}G = |Y|\ I$ implies that the $s+1$ following matrices:

$$J_s' = |Y|^{-1} K\tilde{K}, \qquad J_k' = |Y|^{-1} H_k\tilde{H}_k, \qquad 0 \leqslant k \leqslant s-1, \tag{5.54}$$

form a set of mutually orthogonal idempotents in $\mathbf{R}(Y,Y)$. Therefore, they are linearly independent and they generate a commutative $(s+1)$-dimensional subalgebra of $\mathbf{R}(Y,Y)$. Now the preceding argument shows that the D_ν' generate the same algebra as the J_k'. Hence the theorem is proved.

Corollary 5.26. In the situation of theorem 5.25, the second eigenmatrix $Q' = [Q_k'(\nu)]$ of the association scheme (Y,R^Y) is given by the following formulas, for $\nu = 0, 1, \ldots, s$:

$$Q_k'(\nu) = \begin{cases} \Phi_k(z_{i_\nu}), & 0 \leqslant k \leqslant s-1, \\ \alpha(z_{i_\nu}) - \Psi_{s-1}(z_{i_\nu}), & k = s, \end{cases}$$

where $\alpha(z)$ is the annihilator polynomial of Y and $\Psi_{s-1}(z)$ is the Wilson polynomial of degree $s-1$. In other words, (Y,R^Y) is Q'-polynomial with respect to the numbers z_{i_ν}, the corresponding polynomials being $\Phi_k'(z) = \Phi_k(z)$ for $0 \leqslant k \leqslant s-1$ and $\Phi_s'(z) = \alpha(z) - \Psi_{s-1}(z)$.

Proof. We have seen that the minimal idempotents of the BM algebra of (Y,R^Y) are the matrices $J_0', J_1', \ldots, J_s'$ given by (5.54). On the other hand, from theorem 3.13 we deduce

$$J_k' = |Y|^{-1} \sum_{\nu=0}^{s} \Phi_k(z_{i_\nu})\, D_\nu', \qquad k = 0, 1, \ldots, s-1.$$

This yields the formula for $k < s$, by definition (2.16) of the eigenmatrix Q'. As for J_s' ,we obtain, using the same argument,

$$J_s' = I - |Y|^{-1} \sum_{\nu=0}^{s} \Psi_{s-1}(z_{i_\nu})\, D_\nu'.$$

Consequently, this yields $Q_s'(\nu) = |Y|\ \delta_{\nu,0} - \Psi_{s-1}(z_{i_\nu})$, which, by definition (5.41) of the annihilator polynomial $\alpha(z)$, is the desired result.

Before describing some examples, let us briefly emphasize the particular case of tight designs, i.e. $t = 2s$. As we have seen in theorem 5.21, the annihilator polynomial is $\alpha(z) = \Psi_s(z)$. Hence corollary 5.26 shows that, for a tight design Y, the eigenmatrix Q' of (Y,R^Y) simply is the submatrix of $Q = [Q_k(i)]$ defined by the rows $i = i_0, i_1, \ldots, i_s$ and by the columns $k = 0, 1, \ldots, s$.

(This result can be obtained in a more natural way by use of $K = H_s$ and $G = G_s$ in the proof of theorem 5.25.)

Example 1. In the Hamming scheme (X,R) of length $n \geqslant 2$ over $F = \{0, 1\}$, let us consider the set Y of binary n-tuples having an even weight. It is easily seen that Y is a design (= orthogonal array) of maximum strength $t = n - 1$ and degree $s = [n/2]$. So the design is tight if and only if n is odd. From theorem 5.25 it follows that (Y,R^Y) is a subscheme of (X,R). This association scheme, which is metric and Q'-polynomial, provides a natural framework for a study of binary codes all of whose words have an even weight.

Example 2. We now consider the Hamming scheme $H(n,2)$ with $n = m^2 - 1$, $m \equiv 0 \pmod 2$, $m \geqslant 4$. We are interested in codes Y, of degree $s = 3$, such that the Hamming distance between distinct codewords only assumes one of the following three values:

$$i_1 = m(m-1)/2, \qquad i_2 = m^2/2, \qquad i_3 = m(m+1)/2.$$

Then, by elementary computation, we obtain the following expansion of the annihilator polynomial (5.41), with $z_i = i$, in the basis of Krawtchouk polynomials $\Phi_k(z) = K_k(z)$:

$$\alpha(z) = 2m^{-4}|Y|\left(\Phi_0(z) + \Phi_1(z) + \frac{3}{n}\Phi_2(z) + \frac{3}{n}\Phi_3(z)\right).$$

Hence from theorem 5.23(ii) we deduce $|Y| \leqslant m^4/2$.

A code Y achieving this bound, i.e. $|Y| = m^4/2$, will be called a *Kerdock code*, by reference to Kerdock [36]) who constructed such (nonlinear) codes for every m of the form $m = 2^c$ with $c \geqslant 2$. In fact, from results of Goethals and Snover [26]) on the Preparata codes [58]) it follows that a Kerdock code cannot be linear.

A simple look at the annihilator polynomial $\alpha(z)$ reveals, according to theorem 5.23(iii), that the maximum strength of the orthogonal array formed by a Kerdock code is equal to $t = s + 1 = 4$. Since $|Y|$ has to be divisible by 2^t, this yields the necessary condition $m \equiv 0 \pmod 4$.

Theorem 5.24 indicates that a Kerdock code Y is regular in the Hamming scheme. Solving the system (5.52) for the unknowns $a_i = B(x,i)$ we obtain the following values for the nonzero components of the distance distribution $\mathbf{a}$ of Y, apart from $a_0 = 1$:

$$a_{i_1} = m(m+1)(m^2-2)/4, \qquad a_{i_2} = m^2 - 1, \qquad a_{i_3} = m(m-1)(m^2-2)/4.$$

On the other hand, theorem 5.25 implies that (Y,R^Y) is a subscheme of $H(n,2)$. Let us give the eigenmatrices P' and Q' of such a "Kerdock scheme":

$$Q' = \begin{bmatrix} 1 & m^2-1 & (m^2-1)(m^2-2)/2 & (m^2-2)/2 \\ 1 & m-1 & -(m-1) & -1 \\ 1 & -1 & -(m^2-2)/2 & (m^2-2)/2 \\ 1 & -(m+1) & m+1 & -1 \end{bmatrix},$$

$$P' = \begin{bmatrix} 1 & m(m+1)(m^2-2)/4 & m^2-1 & m(m-1)(m^2-2)/4 \\ 1 & m(m^2-2)/4 & -1 & -m(m^2-2)/4 \\ 1 & -m/2 & -1 & m/2 \\ 1 & -m(m+1)/2 & m^2-1 & -m(m-1)/2 \end{bmatrix}.$$

The matrix Q' is first calculated by use of corollary 5.26. Thereafter, P' is deduced from it by the formulas (2.25), the valences being $P_\nu'(0) = a_{i_\nu}$, for $\nu = 0, 1, 2, 3$.

Examining the column P_2' of P', we see that (Y,R_2^Y) is a ladder graph (cf. Seidel [61]). In the terminology of coding theory, this means that any Kerdock code can be partitioned into $m^2/2$ subcodes which are Hadamard codes (cf. Berlekamp [6]), p. 316), i.e. equidistant codes of distance $i_2 = m^2/2$ containing $n + 1 = m^2$ words.

Example 3. Finally, let us give an example taken in the Johnson scheme $J(11, 47)$. Assmus and Mattson [4]) have shown the existence of a binary code Y, of length $v = 47$ and constant weight $n = 11$, forming a 4-design $S_3(4, 11, 47)$ of maximum strength $t = 4$ and degree $s = 3$. More precisely, the Johnson distance between distinct codewords assumes one of the three values $i_1 = 6$, $i_2 = 8$, $i_3 = 10$.

It follows from theorem 5.24 that Y is a regular design. Moreover, using theorem 5.25 with $t = 2s - 2$, we deduce that (Y,R^Y) is an association scheme with three classes. From the above data we could compute its eigenmatrices by means of corollary 5.26, in the same manner as we did for example 2.

6. ADDITIVE CODES IN HAMMING SCHEMES

We have seen, throughout the preceding chapter, the strong analogy between the theory of "codes" in P-polynomial schemes and of "designs" in Q-polynomial schemes. The role of the two pairs of parameters (d,r) and (d',r'), with $d' = t+1$, $r' = s$, is central in that respect.

It turns out that the analogy is more than formal in the case of additive codes (or designs) in a Hamming scheme: defining a duality among these codes, we shall especially show that the parameters d' and r' of a code simply are the parameters d and r of its dual.

Let us briefly recall the definition. For an "additive" Abelian group F of order $q \geqslant 2$ and for an integer $n \geqslant 1$, we shall consider the group $X = F^n$, i.e. the direct product of n copies of F. An *additive code* Y of length n over F then by definition is a subgroup of X provided with the Hamming distance d_H. In more standard terminology, it is an Abelian group code.

Before investigating these codes, we shall give some results about characters of Abelian groups and, thereafter, introduce the concept of duality among subgroups. The theorems are classical and the proofs will be omitted. The terminology and notations are the same as in a paper by the author [16]), where elementary proofs can be found.

6.1. Inner product and duality in Abelian groups

For an Abelian group X of finite order v, let $\langle x,y\rangle$ be a symmetric function of the variables $x,y \in X$, with complex values. Then, using an additive notation for the group operator, we shall call the function an *inner product on* X if it identically satisfies the following two conditions, besides $\langle x,y\rangle = \langle y,x\rangle$:

$$\langle x, y+z\rangle = \langle x,y\rangle\,\langle x,z\rangle$$

and

$$(\langle x,y\rangle = \langle x,z\rangle, \forall\, x \in X) \Leftrightarrow (y = z).$$

Clearly, for a given $x \in X$, the mapping ϕ_x of X into $\mathbf{C}$ defined by $\phi_x(y) = \langle x,y\rangle$ is a *character of* X, i.e. a homomorphic mapping of X into the multiplicative group of $\mathbf{C}$. More precisely, the correspondence $x \mapsto \phi_x$ is an isomorphism between X and the group of its characters, with $\phi_x(y) = \phi_y(x)$. In fact, it is well known that such an isomorphism exists; then the definition $\langle x,y\rangle = \phi_x(y)$ yields an inner product.

The orthogonality relations on group characters imply that the symmetric matrix $S \in \mathbf{C}(X,X)$ defined by $S(x,x') = \langle x,x'\rangle$ is orthogonal; a more general result is given in theorem 6.2.

Remark. If inner products have been defined on each of the n Abelian groups

$X^{(1)}, X^{(2)}, \ldots, X^{(n)}$, then we can construct an inner product on the group $X = \Pi\, X^{(i)}$ as follows: For $x = (x^{(1)}, \ldots, x^{(n)})$ and $y = (y^{(1)}, \ldots, y^{(n)})$ in X, with $x^{(i)}, y^{(i)} \in X^{(i)}$, we define

$$\langle x,y\rangle = \langle x^{(1)}, y^{(1)}\rangle\,\langle x^{(2)}, y^{(2)}\rangle \ldots \langle x^{(n)}, y^{(n)}\rangle, \tag{6.1}$$

using a unique notation $\langle a,b\rangle$ for the inner product on the group X and on each of the groups $X^{(i)}$.

We shall now examine the duality, with respect to a given inner product. If Y is a subgroup of X, then it is clear that the subset Y^0 of X defined by

$$Y^0 = \{x' \in X \mid \langle x,x'\rangle = 1, \quad \forall\, x \in Y\} \tag{6.2}$$

is itself a subgroup of X; it will be called the *dual* of Y in X. We shall need the following two results about duality:

Theorem 6.1. The dual of Y^0 is Y itself and Y^0 is isomorphic to the factor group X/Y.

Theorem 6.2. Given a pair (Y,Y^0) of dual subgroups of X, then

$$\sum_{x \in Y} \langle x,x'\rangle = \begin{cases} |Y| & \text{if} \quad x' \in Y^0, \\ 0 & \text{otherwise.} \end{cases}$$

Let us notice that, when applied to the trivial subgroups $Y = X$ and $Y^0 = \{0\}$, the latter result is equivalent to the orthogonality of the matrix S of group characters.

For a pair (Y,Y^0) of dual subgroups of X, with $|Y| = m$ and, so, $|Y^0| = v/m$, we shall consider the homomorphic image Y' of X whose elements are the cosets Y^j of Y^0:

$$Y' = X/Y^0 = \{Y^0, Y^1, \ldots, Y^{m-1}\}. \tag{6.3}$$

By theorem 6.1, the group Y' is isomorphic to Y. Let us choose an arbitrary element x_j in Y^j; so $Y^j = x_j + Y^0$ for $j = 0, 1, \ldots, m-1$. Then, if $y_0 = 0$, $y_1, \ldots, y_{m-1}$ are the elements of Y, we define the matrix $\Omega \in \mathbf{C}(Y,Y')$ as follows:

$$\Omega(y_i,Y^j) = \langle y_i,x_j\rangle, \qquad 0 \leqslant i,j \leqslant m-1. \tag{6.4}$$

It is easily seen that Ω is the matrix of group characters of Y, in the sense that the mappings ψ_j of Y into $\mathbf{C}$ defined by $\psi_j(y) = \langle y,x_j\rangle$ are the m distinct characters of Y. This implies that Ω is an orthogonal matrix: $\Omega\bar{\Omega} = m\,I$.

6.2. The MacWilliams identities on dual codes

Let X be the direct product of n copies of the Abelian group F. We shall always take as inner product $\langle x,y\rangle$ on X the one defined as in (6.1) from a

given inner product $\langle x^{(1)},y^{(1)}\rangle$ on $X^{(1)} = F$. In sec. 4.1.1, this was called the natural product on X.

The *Hamming weight* $w_H(x)$ of an element $x = (x^{(1)}, \ldots, x^{(n)})$ of X is defined to be the number of nonzero components $x^{(i)}$ in F. The Hamming distance between two points $x,y \in X$ is then given by $d_H(x,y) = w_H(x-y)$. Like in sec. 4.1.1, we shall use the notation X_k for the subset of X containing all elements of weight k ($k = 0, 1, \ldots, n$).

Given an additive code Y, i.e. a subgroup of X, we define the *weight distribution* of Y to be the $(n+1)$-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_n)$ of integers a_k given by

$$a_k = |Y \cap X_k|, \qquad k = 0, 1, \ldots, n. \tag{6.5}$$

In other terms, a_k is the number of codewords of weight k. It is easily seen that $\mathbf{a}$ also is the distance distribution of Y, that is, the inner distribution with respect to R for the Hamming scheme (X,R).

The minimum distance $d = t(\mathbf{a}) + 1$ of Y is often called the *minimum weight*: it is the smallest nonzero value of $w_H(y)$ for codewords y. A code of degree $s(\mathbf{a}) = s$ is said to be an *s-weight code*; in fact, the degree s is equal to the number of distinct nonzero values $i_1, i_2, \ldots, i_s$ (= the "weights" of Y) assumed by $w_H(y)$ for codewords $y \in Y$.

The *dual* of an additive code Y is defined, as in (6.2), to be the dual subgroup Y^0 of Y with respect to the natural product $\langle x,x'\rangle$. Let us make a short comment about duality. When q is a prime, additive codes are equivalent to linear codes over $GF(q)$. The dual of an additive code is then, in the terminology of linear codes, its *orthogonal complement* (cf. MacWilliams [44]). When q is a prime power, the linear codes over $GF(q)$ form a subclass of the additive codes over the elementary Abelian group of order q. In this case also, the orthogonal complement of a linear code can be defined to be its dual.

The following result on weight distributions of dual codes is essentially due to MacWilliams [46]. In fact, the original result only belongs to linear codes but the generalization to arbitrary additive codes is not difficult (cf. Delsarte [16]); it has also been obtained recently by McEliece [51]. We shall use the Krawtchouk polynomials $K_k(u)$ and the characteristic matrices $H_k \in \mathbf{C}(Y,X_k)$ defined from the matrix S of group characters, that is:

$$H_k(y,x') = \langle y,x'\rangle, \qquad y \in Y, \qquad x' \in X_k. \tag{6.6}$$

Theorem 6.3. The weight distribution $\mathbf{a}' = (a_0', a_1', \ldots, a_n')$ of the dual Y^0 of an additive code Y can be expressed in terms of the weight distribution $\mathbf{a}$ of Y itself as follows:

$$a_k' = |Y|^{-1} \sum_{i=0}^{n} a_i K_k(i), \qquad k = 0, 1, \ldots, n. \tag{6.7}$$

Proof. First, using for instance lemma 3.14, we can write, like for any association scheme,

$$||\hat{H}_k H_0||^2 = |Y|\ (\mathbf{a}\ Q_k). \tag{6.8}$$

On the other hand, owing to the fact that Y is a group, we readily deduce from the definition (6.6) the following formula:

$$||\hat{H}_k H_0||^2 = |Y| \sum_{x' \in X_k} \Big(\sum_{y \in Y} \langle y,x'\rangle \Big).$$

Now theorem 6.2 implies that the term under brackets is equal to $|Y|$ or to zero according to whether x' belongs to Y^0 or not. Therefore, the above equation becomes, by (6.5),

$$||\hat{H}_k H_0||^2 = |Y|^2 |Y^0 \cap X_k| = |Y|^2 a_k'.$$

Comparing this with (6.8), we obtain the desired formula (6.7), remembering the result $Q_k(i) = K_k(i)$ of theorem 4.2.

By use of the generating function for Krawtchouk polynomials (cf. Szegö [70], p. 36), we can derive another interesting form of the equations (6.7). Let us only give the result: From $\mathbf{a}$ we define the polynomial $a(\xi,\eta) = \sum a_i \xi^i \eta^{n-i}$ and, analogously, $a'(\xi,\eta)$ from $\mathbf{a}'$. Then (6.7) is equivalent to the following polynomial identity, called the *MacWilliams identity*:

$$a'(\xi,\eta) = |Y|^{-1} a(\eta - \xi, \eta + (q-1)\xi).$$

Corollary 6.4. Let Y and Y^0 be dual codes. Then the external distance of Y is the degree of Y^0 and the maximum strength of Y is one unit less than the minimum distance of Y^0.

Proof. This is an immediate consequence of the preceding result, written in the form $\mathbf{a}' = |Y|^{-1}\ \mathbf{a}\ Q$, and of the definitions of the four parameters given in secs 5.2.1 and 5.3.1.

Applying corollary 6.4 to perfect codes and tight designs (= generalized Hadamard codes [14]), we deduce the following consequence of the definitions (cf. theorems 5.14 and 5.21):

Theorem 6.5. An additive generalized Hadamard code of order e is the dual of a perfect code of order e.

In fact, the question of perfect additive codes or, equivalently, of additive generalized Hadamard codes, has been entirely solved lately, whenever the order is at least two:

Theorem 6.6. For orders e such that $1 < e < (n-1)/2$ there are exactly two

perfect additive codes, namely the Golay codes with $(n, q, e) = (11, 3, 2)$ and $(23, 2, 3)$.

Proof. Let us assume there exists a perfect additive code of length n and order e over an Abelian group F. From a theorem of Lenstra [39]) it follows that $q = |F|$ must be a prime power. Hence the general result of Tietäväien [72]) applies: the only possible values of the triple (n,q,e) are those indicated above, for $1 < e < (n-1)/2$. On the other hand, the uniqueness of the perfect additive codes discovered by Golay [27]) has been proved by Pless [56]).

Remark. Part of the results of this section and of the next one can be extended to arbitrary association schemes (X,R) satisfying the conditions of theorem 2.9. In order to illustrate this, let us now indicate, without proof, what would be the general form of the identity (6.7).

Let (X,R') be the dual scheme of (X,R) with respect to the zero of X and to the matrix S of group characters. For a pair of dual subgroups Y and Y^0 of X, let $\mathbf{a} = (a_i)$ be the inner distribution of Y with respect to R and let $\mathbf{a}' = (a_k')$ be the one of Y^0 with respect to R'. If P and Q are the eigenmatrices of (X,R), then we have

$$|Y|\,\mathbf{a}'\hat{} = \mathbf{a}\,Q, \qquad |Y^0|\,\hat{\mathbf{a}} = \mathbf{a}'\,P. \tag{6.9}$$

These equations yield necessary conditions for an $(n+1)$-tuple $\mathbf{a}$ of non-negative integers a_i to be the inner distribution of a subgroup Y with respect to R: the numbers $\mathbf{a}Q_k$ must be nonnegative integers divisible by $|Y|$.

For the spectral schemes or, more generally, for the extensions of cyclotomic schemes (cf. sec. 2.5), it is possible to derive explicit forms of the eigenmatrices (with $P = Q$; indeed these schemes are self-dual). Then (6.9) yields the generalized MacWilliams identities on the spectral distributions of dual codes (cf. Assmus and Mattson [3]) and MacWilliams, Sloane and Goethals [48])).

6.3. Weight distribution of cosets and subschemes

In the present section we shall examine the connections between, on the one hand, the restriction (Y,R^Y) of the Hamming scheme (X,R) to an additive code Y and, on the other hand, the distribution matrix B' of the dual code Y^0 (cf. sec. 3.1).

Like in (6.3), let $Y^0, Y^1, \ldots, Y^{m-1}$ be the cosets of Y^0 in the group X, with $m = |Y|$. Clearly, the row $B'(x)$ of B' only depends on the coset Y^j to which x belongs. Hence, choosing an element x_j in each Y^j, we only need to consider the restriction V of B' to its rows $B'(x_0), B'(x_1), \ldots, B'(x_{m-1})$. The (j,k)-entry $v_{j,k}$ of V can be written as follows:

$$v_{j,k} = B'(x_j,k) = |Y^j \cap X_k|, \qquad 0 \leqslant j \leqslant m-1, \qquad 0 \leqslant k \leqslant n.$$

So the row $(v_{j,0}, \ldots, v_{j,n})$ of V is the weight distribution of the coset code Y^j.

On the other hand, for an s-weight code Y, let $i_0 = 0, i_1, \ldots, i_s$ be the distinct values assumed by $w_H(y)$ over codewords $y \in Y$. We shall denote by $E_\nu \in \mathbf{R}(Y,Y)$ the adjacency matrix of the relation R_ν^Y, for $\nu = 0, 1, \ldots, s$, defined as in (5.50). Equivalently, E_ν is the restriction $D_{i_\nu} | Y$. We shall use the notation E for the $(s+1)$-dimensional subspace of $\mathbf{R}(Y,Y)$ generated by the matrices $E_0 = I, E_1, \ldots, E_s$.

An arbitrary matrix in E can be represented by means of a suitable polynomial $\alpha(z) \in \mathbf{R}_n[z]$ in the form

$$E^{(\alpha)} = \sum_{\nu=0}^{n} \alpha(i_\nu)\, E_\nu, \tag{6.10}$$

that is, equivalently, $E^{(\alpha)}(y,y') = \alpha(w_H(y-y'))$. We shall consider the $(n+1)$-tuple $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ of components α_k of $\alpha(z)$ in the basis of Krawtchouk polynomials:

$$\alpha(z) = \alpha_0\, K_0(z) + \alpha_1\, K_1(z) + \ldots + \alpha_n\, K_n(z). \tag{6.11}$$

Next, to $\alpha(z)$ we associate the m-tuple $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{m-1})$ defined as follows from the matrix V of weight distributions of the cosets Y^j:

$$\boldsymbol{\lambda} = m\,\boldsymbol{\alpha}\,V^T. \tag{6.12}$$

Finally, we construct the diagonal matrix $\Lambda^{(\alpha)} \in \mathbf{R}(Y',Y')$ whose elements are given by $\Lambda^{(\alpha)}(Y^j,Y^j) = \lambda_j$.

Theorem 6.7. For a given additive code Y, all matrices of E are diagonalized by the matrix Ω of group characters of Y as follows:

$$E^{(\alpha)} = m^{-1}\,\Omega\,\Lambda^{(\alpha)}\,\bar{\Omega}, \qquad \forall\, \alpha(z) \in \mathbf{R}_n[z]. \tag{6.13}$$

Proof. From theorem 3.13 and the definitions (6.10) and (6.11) we readily deduce the following identity:

$$E^{(\alpha)} = \sum_{k=0}^{n} \alpha_k\, H_k\, \bar{H}_k. \tag{6.14}$$

Let us examine closely the matrix H_k defined in (6.6). Assuming that the set $X_{j,k} = Y^j \cap X_k$ is not empty, we consider the restriction $H_{j,k}$ of H_k to $Y \times X_{j,k}$. Then, comparing with (6.4), we see that all $v_{j,k}$ columns of $H_{j,k}$ are identical to the column ω_j of Ω corresponding to the coset Y^j. Hence we can write (6.14) in the form

$$\begin{aligned} E^{(\alpha)} &= \sum_{k=0}^{n} \alpha_k \Big(\sum_{j=0}^{m-1} v_{j,k}\, \omega_j\, \bar{\omega}_j \Big) \\ &= \sum_{j=0}^{m-1} \Big(\sum_{k=0}^{n} \alpha_k\, v_{j,k} \Big)\, \omega_j\, \bar{\omega}_j. \end{aligned} \tag{6.15}$$

Defining λ as in (6.12), we see that the term under brackets in (6.15) is equal to λ_j/m. Hence the matrix form of (6.15) is the desired formula (6.13). As Ω is an orthogonal matrix, the λ_j are the eigenvalues of $E^{(\alpha)}$ and the theorem is proved.

Corollary 6.8. Let Y and Y^0 be additive codes, dual of each other. Then, for a given polynomial $\alpha(z) \in \mathbf{R}_n[z]$, the number

$$\delta(x) = \sum_{y \in Y} \alpha(w_H(y)) \langle y,x \rangle \tag{6.16}$$

only depends on the weight distribution $B'(x)$ of the coset Y^J of Y^0 to which the element x belongs.

Proof. From the numbers $\delta(x)$ we construct a diagonal matrix $\Delta \in \mathbf{C}(Y',Y')$ as follows: $\Delta(Y^J,Y^J) = \delta(x_j)$, for $x_j \in Y^J$. It is easily verified that (6.16) is equivalent to $E^{(\alpha)}\,\Omega = \Omega\,\Delta$; the details are left to the reader. Comparing this result with (6.13), we obtain $\Delta = A^{(\alpha)}$ and from theorem 6.7 it follows that $\delta(x)$ is equal to $m \sum \alpha_k v_{j,k}$, for all $x \in Y^J$, where $(v_{j,0}, \ldots, v_{j,n}) = B'(x)$ is the weight distribution of Y^J. Hence the theorem is proved.

Remark. Essentially, we have proved the following identity, for all $x \in X$ and all $\alpha(z) \in \mathbf{R}_n[z]$:

$$\sum_{y \in Y} \alpha(w_H(y)) \langle x,y \rangle = |Y| \sum_{k=0}^{n} \alpha_k B'(x,k).$$

When applied to $x \in Y^0$, this reduces to the MacWilliams identity on the weight distributions of the dual codes Y and Y^0.

After these preliminary results let us now examine the question of deciding whether the restriction (Y,R^Y) of the Hamming scheme to an additive code Y is a subscheme or not. We shall denote by A the commutative subalgebra of $\mathbf{R}(Y,Y)$ generated by the adjacency matrices E_v of the $R_v{}^Y$. (The commutativity of A follows from theorem 6.7.) By definition, if (Y,R^Y) is an association scheme, then A is its Bose-Mesner algebra.

Lemma 6.9. For an additive s-weight code Y the following two propositions hold: (i) The dimension $(= s+1)$ of E is equal to the rank of the distribution matrix B' of the dual code Y^0. (ii) The dimension of A is equal to the number of distinct rows in B'.

Proof. The first part is already contained in corollary 3.2 (cf. also corollary 6.4). However, let us give a more specific proof. From theorem 6.7 it is clear that E is isomorphic to the subspace of $\mathbf{R}(Y',Y')$ generated by the matrices $A^{(\alpha)}$ and, therefore, to the column space of V. Hence the dimension of E is equal to the rank of V, i.e. to the rank of B'.

We shall use a similar argument for the second part. Let $\mathbf{b}^{(1)}, \mathbf{b}^{(2)}, \ldots, \mathbf{b}^{(t)}$ be the distinct rows of B'. From theorem 6.7 we deduce that A is isomorphic to the subalgebra A' of $\mathbf{R}^t$ generated by the columns of B' restricted to the rows $\mathbf{b}^{(i)}$. So it only remains to be shown that A' is $\mathbf{R}^t$ itself.

For arbitrary real numbers $c_1, c_2, \ldots, c_t$ there exists a polynomial $f(\mathbf{z})$, in the $(n+1)$-tuple $\mathbf{z} = (z_0, \ldots, z_n)$ of variables z_k, satisfying $f(\mathbf{b}^{(i)}) = c_i$ for all i. Owing also to the obvious fact that A' contains the all-one vector, this exactly means that the vector $(c_1, \ldots, c_t)^T$ of $\mathbf{R}^t$ belongs to A', which is the desired result.

Theorem 6.10. The restriction (Y,R^Y) of the Hamming scheme to an additive s-weight code is a subscheme if and only if the distribution matrix of the dual Y^0 (which has rank $s+1$) contains $s+1$ distinct rows.

Proof. From theorem 2.1 it follows that (Y,R^Y) is an association scheme if and only if the vector space E itself constitutes a commutative algebra, i.e. if and only if $\mathsf{E} = \mathsf{A}$. Hence the desired result is an immediate consequence of lemma 6.9.

Example. Let us consider the binary code Y of length $n = 48$, containing $m = 2^{24}$ words, known under the name of extended quadratic residue code (cf. Berlekamp [6], p. 353). This code is a self-dual 8-weight code, the weights being 12, 16, 20, 24, 28, 32, 36 and 48. So the four parameters are $d = 12$, $r = 8$, $t = 11$ and $s = 8$ (cf. corollary 6.4).

From results of Assmus and Mattson [5]) the author [14]) showed, using theorem 5.9, that the 2^{24} cosets of Y^0 $(= Y)$ have exactly 14 distinct weight distributions. Therefore, by lemma 6.9, the algebra A generated by the adjacency matrices E_v has dimension 14 and theorem 6.10 implies that (Y,R^Y) is not an association scheme.

Before giving more "positive" examples we shall now examine the question of duality in association schemes derived from the Hamming scheme (X,R), in the sense of sec. 2.6 (cf. theorem 2.9).

For a given s-weight additive code Y, with $|Y| = m$, let us assume (Y,R^Y) is a subscheme of (X,R). Then, by theorem 6.10, we know that the number of distinct $(n+1)$-tuples among the weight distributions $B'(x_j)$ of the cosets Y^J is equal to $s+1$. Let us use the notations $\mathbf{a}^{(0)}, \mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(s)}$ for these $(n+1)$-tuples, specializing $\mathbf{a}^{(0)}$ to be the weight distribution of Y^0.

Next, we define the $(s+1)$-set $R' = \{R_0', R_1', \ldots, R_s'\}$ of symmetric relations R_i' on the group $Y' = X/Y^0$ as follows:

$$R_i' = \{(Y^J,Y^k) \mid B'(x_k - x_j) = \mathbf{a}^{(i)}\}, \qquad 0 \leqslant i \leqslant s,$$

where B' is the distribution matrix of Y^0. Clearly, R' is a partition of the Cartesian square $(Y')^2$ and R_0' is the diagonal relation.

Theorem 6.11. Let (Y,R^Y) be an association scheme for a given additive code Y. Then (Y',R') itself is an association scheme; it is the dual scheme of (Y,R^Y) with respect to the zero of Y and to the matrix Ω of group characters of Y.

Proof. By theorem 6.7, the orthogonal matrix Ω diagonalizes the BM algebra of (Y,R^Y). Let us consider the partition $\tau(Y,0)$ of Y, that is, the partition into the classes $Y_\nu = Y \cap X_{l_\nu}$ of codewords having a given weight i_ν, for $\nu = 0, 1, \ldots, s$; we shall denote by $\Omega^{(\nu)} \in \mathbf{C}(Y_\nu, Y')$ the restriction of Ω to $Y_\nu \times Y'$. The $s+1$ matrices

$$J_\nu' = m^{-1}\, \widetilde{\Omega}^{(\nu)}\, \Omega^{(\nu)}, \qquad \nu = 0, 1, \ldots, s, \tag{6.17}$$

are idempotent and pairwise orthogonal in the algebra $\mathbf{C}(Y',Y')$. Like in the general theory of duality (cf. theorem 2.8), we define from these idempotents the following mapping of $(Y')^2$ into $\mathbf{C}^{s+1}$:

$$f'(Y^j,Y^h) = m\,(J_0'(Y^j,Y^h), \ldots, J_s'(Y^j,Y^h)).$$

In order to prove that (Y',R') is the dual scheme of (Y,R^Y) with respect to 0 and Ω, all we need to show is that $f'(Y^j,Y^h)$ only depends on the relation R_i' to which (Y^j,Y^h) belongs, i.e. on the weight distribution $B'(x_h - x_j)$ of the coset $Y^h - Y^j$. Using (6.4) and (6.17) we obtain

$$J_\nu'(Y^j,Y^h) = m^{-1} \sum_{y \in Y_\nu} \langle y, x_h - x_j \rangle.$$

From corollary 6.8 it readily follows that, for a given ν, the right-hand member only depends on the weight distribution of the coset containing $x_h - x_j$. Hence the theorem is proved.

We shall now indicate two interesting illustrations of the above theorem on duality, based on the two Golay codes. Let us recall (cf. theorem 2.8) that, if $P^{(1)},Q^{(1)}$ and $P^{(2)},Q^{(2)}$ are the eigenmatrices of dual schemes (Y,R^Y) and (Y',R'), respectively, then we have $P^{(2)} = Q^{(1)}$ and $Q^{(2)} = P^{(1)}$.

Example 1. Let Z be the binary Golay code, i.e. the perfect linear code of order 3 and length 23 over $GF(2)$. The dual code $Y = Z^0$ is a generalized Hadamard code of maximum strength $t = 6$ and degree $s = 3$, the weights being $i_1 = 8$, $i_2 = 12$, $i_3 = 16$. By theorem 5.25, the restriction (Y,R^Y) of the Hamming scheme $H(23, 2)$ to Y is a subscheme with 3 classes. Using the formulas of corollary 5.26, we obtain the eigenmatrices $P^{(1)}$ and $Q^{(1)}$ of (Y,R^Y):

$$P^{(1)} = \begin{bmatrix} 1 & 506 & 1288 & 253 \\ 1 & 154 & -56 & -99 \\ 1 & 26 & -56 & 29 \\ 1 & -6 & 8 & -3 \end{bmatrix}, \qquad Q^{(1)} = \begin{bmatrix} 1 & 23 & 253 & 1771 \\ 1 & 7 & 13 & -21 \\ 1 & -1 & -11 & 11 \\ 1 & -9 & 29 & -21 \end{bmatrix}.$$

The fact that the adjacency matrix of R_2^Y has only three distinct eigenvalues ($= 1288, -56, 8$) means that (Y,R_2^Y) is a strongly regular graph, which was first proved by Goethals and Seidel [25]).

From theorem 6.11 it follows that (Y',R') is an association scheme with 3 classes. In fact, for a suitable numbering of the relations R_i', a pair (Y^j,Y^h) of cosets of the Golay code Z ($= Y^0$) belongs to R_i' if and only if the coset $Y^h - Y^j$ contains an element of weight i, for $i = 0, 1, 2, 3$. The eigenmatrices of the metric scheme (Y',R') are $P^{(2)} = Q^{(1)}$ and $Q^{(2)} = P^{(1)}$. As the last column of $Q^{(1)}$ has only 3 distinct elements, this implies that the graph (Y',R_3') is strongly regular; it is in fact the dual graph of (Y,R_2^Y) in the sense of sec. 2.6.3.

Example 2. Applying the same reasoning to the ternary Golay code Z of order $e = 2$ and length $n = 11$, we obtain two strongly regular graphs, on 243 points, dual of each other. For $Y = Z^0$, the eigenmatrices $P^{(1)}$ and $Q^{(1)}$ of (Y,R^Y) are the following:

$$P^{(1)} = \begin{bmatrix} 1 & 132 & 110 \\ 1 & 24 & -25 \\ 1 & -3 & 2 \end{bmatrix}, \qquad Q^{(1)} = \begin{bmatrix} 1 & 22 & 220 \\ 1 & 4 & -5 \\ 1 & -5 & 4 \end{bmatrix}.$$

The strongly regular graph (Y,R_1^Y) is in fact dual, in the sense of sec. 2.6.3, of the graph (Y',R_1'); the latter has been discovered by Berlekamp, Van Lint and Seidel [7]).

Let us examine more sharply the code Y, dual of the Golay code. It can be shown that the restriction to Y of the spectral scheme of length 11 over $F = GF(3)$ is a subscheme with 5 classes. We shall denote by $(Y,\bar{R})$ the symmetric closure of the spectral scheme on Y; it has 3 classes and the eigenmatrices are the following:

$$\bar{P} = \bar{Q} = \begin{bmatrix} 1 & 22 & 110 & 110 \\ 1 & 4 & -25 & 20 \\ 1 & -5 & 2 & 2 \\ 1 & 4 & 2 & -7 \end{bmatrix}.$$

The graph $(Y,\bar{R}_2)$ is identical to (Y,R_2^Y). Moreover, it can be shown that the graph $(Y,\bar{R}_1)$, which is also strongly regular, is isomorphic to (Y',R_1').

Finally, we shall elucidate, for additive codes in Hamming schemes, the connection between the true external distance introduced in (5.29) and the parameter σ considered in the remark after theorem 5.20.

Theorem 6.12. Let $H_0, H_1, \ldots, H_n$ be the characteristic matrices (6.6) of an additive code Y. Then the true external distance $d_H(X,Y^0)$ of the dual code Y^0 is equal to the smallest integer k, with $0 \leqslant k \leqslant n$, such that the rows of the matrix $G_k = [H_0, \ldots, H_k]$ are linearly independent.

Proof. As we already observed, the columns of G_k are certain columns of the matrix Ω of group characters of Y. Since Ω has rank $m = |Y|$, it is clear that G_k will itself be of rank m if and only if it contains Ω as a submatrix, that is, if and only if

$$(X_0 \cup X_1 \cup X_k) \cap Y^j \neq \emptyset, \tag{6.18}$$

for all cosets Y^j of Y^0 in X. The condition (6.18) means, in other words, that the distance $d_H(x,Y^0)$ is less than or equal to k whenever x belongs to Y^j. Hence the smallest value of k having this property for all j is equal to the maximum value of $d_H(x,Y^0)$, i.e. to the true external distance $d_H(X,Y^0)$.

Note added in proof

Since this work has been finished the author became aware of the following facts: The formulae of theorem 4.6 for the eigenmatrices of the Johnson schemes were first discovered by Ogasawara [78]) and by Yamamoto et al. [80]). On the other hand, it seems that the orthogonality relations of theorem 2.3, at least in the symmetric case, should be attributed to Ogawa [79]). Finally, the generalization of the Lloyd theorem on perfect codes in metric schemes (cf. theorem 5.7) has also been recently discovered by Biggs [77]), who used different methods.

REFERENCES

1) Alltop, W. O. (1972), An infinite class of 5-designs, J. combinatorial Theory Ser. A, 12, 390-395.
2) Assmus, E. F., Jr. and Mattson, H. F., Jr. (1963), Error-correcting codes: an axiomatic approach, Information and Control 6, 315-330.
3) Assmus, E. F., Jr. and Mattson, H. F., Jr. (1967), Research to develop the algebraic theory of codes, Air Force Res. Lab. Final Rept.
4) Assmus, E. F., Jr. and Mattson, H. F., Jr. (1969), New 5-designs, J. combinatorial Theory 6, 122-151.
5) Assmus, E. F., Jr. and Mattson, H. F., Jr. (1970), Algebraic theory of codes II, Air Force Res. Lab. Final Rept.
6) Berlekamp, E. R. (1968), Algebraic coding theory, Mc Graw-Hill, New York.
7) Berlekamp, E. R., Lint, J. H. van and Seidel, J. J. (1973), A strongly regular graph derived from the perfect ternary Golay code, In: "A survey of combinatorial theory" (J. N. Srivastrava et al., eds.), pp. 25-30, North Holland Publ. Co., Amsterdam.
8) Bose, R. C. (1963), Strongly regular graphs, partial geometries and partially balanced designs, Pacific J. Math. 13, 389-419.
9) Bose, R. C. and Mesner, D. M. (1959), On linear associative algebras corresponding to association schemes of partially balanced designs, Ann. Math. Statist. 30, 21-38.
10) Bose, R. C. and Shimamoto, T. (1952), Classification and analysis of partially balanced incomplete block designs with two associate classes, J. Amer. statist. Assoc. 47, 151-184.
11) Cameron, P. J., Near-regularity conditions for designs (to be published).
12) Cameron, P. J. and Seidel, J. J. (1973), Quadratic forms over GF(2), Indag. Math. 35, 1-8.
13) Delsarte, P. (1971), Two-weight linear codes and strongly regular graphs, Report R160, MBLE Res. Lab., Brussels.
14) Delsarte, P., Four fundamental parameters of a code and their combinatorial significance, Information and Control, to appear.
15) Delsarte, P. (1972), Weights of linear codes and strongly regular normed spaces, Discrete Math. 3, 47-64.
16) Delsarte, P. (1972), Bounds for unrestricted codes, by linear programming, Philips Res. Repts 27, 272-289.
17) Delsarte, P. and Goethals, J. M. (1971), On quadratic residue like sequences in Abelian groups, Report R168, MBLE Res. Lab., Brussels.
18) Dembowski, P. (1968), Finite geometries, Springer-Verlag, Berlin.
19) Eberlein, P. J. (1964), A two parameter test matrix, Math. Comp. 18, 296-298.
20) Fisher, R. A. (1940), An examination of the different possible solutions of a problem in incomplete blocks, Ann. Eugenics 10, 52-75.
21) Freiman, C. V. (1964), Upper bounds for fixed-weight codes of specified minimum distance, IRE Trans. Information Theory IT-10, 246-248.
22) Gallager, R. G. (1968), Information theory and reliable communication, Wiley, New York.
23) Goethals, J. M. (1971), On the Golay perfect binary code, J. combinatorial Theory Ser. A, 11, 178-186.
24) Goethals, J. M. (1970), On t-designs and threshold decoding, Univ. North Carolina Inst. Statistics, Mimeo Series n° 600.29.
25) Goethals, J. M. and Seidel, J. J. (1970), Strongly regular graphs derived from combinatorial designs, Canad. J. Math. 22, 597-614.
26) Goethals, J. M. and Snover, S. L. (1972), Nearly perfect binary codes, Discrete Math. 3, 65-88.
27) Golay, M. J. E. (1949), Notes on digital coding, Proc. IRE 37, 657.
28) Hall, M., Jr. (1959), The theory of groups, Macmillan, New York.
29) Hamming, R. W. (1950), Error detecting and error correcting codes, Bell Syst. tech. J. 29, 147-160.
30) Hanani, H. (1961), The existence and construction of balanced incomplete block designs, Ann. Math. Statist. 32, 361-386.
31) Higman, D. G. (1972), Combinatorial considerations about permutation groups, Lecture notes, Mathematical Institute, Oxford.
32) Johnson, S. M. (1962), A new upper bound for error-correcting codes, IRE Trans. Information Theory IT-8, 203-207.
33) Johnson, S. M. (1971), On upper bounds for unrestricted binary error-correcting codes, IRE Trans. Information Theory IT-17, 466-478.

[34]) Johnson, S. M. (1972), Upper bounds for constant weight error correcting codes, Discrete Math. 3, 109-124.
[35]) Kantor, W. M. (1972), On incidence matrices of finite projective and affine spaces, Math. Z. 124, 315-318.
[36]) Kerdock, A. M. (1972), A class of low-rate nonlinear binary codes, Information and Control 20, 182-187.
[37]) Krawtchouk, M. (1929), Sur une généralisation des polynômes d'Hermite, C.R. Acad. Sci. Paris 189, 620-622.
[38]) Lee, C. Y. (1958), Some properties of nonbinary error-correcting codes, IEEE Trans. Information Theory IT-4, 77-82.
[39]) Lenstra, H. W., Jr. (1972), Two theorems on perfect codes, Discrete Math. 3, 125-132.
[40]) Lint, J. H. van (1970), On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over GF(q), Information and Control 16, 396-401.
[41]) Lint, J. H. van (1971), Coding theory, Lecture notes in mathematics, Springer-Verlag, Berlin.
[42]) Lint, J. H. van, A survey of perfect codes, Rocky Mountain J. Math., to appear.
[43]) Lloyd, S. P. (1957), Binary block coding, Bell Syst. tech. J. 36, 517-535.
[44]) Mac Williams, F. J. (1961), Doctoral Dissertation, Harvard University (unpublished).
[45]) Mac Williams, F. J. (1961), Error-correcting codes for multiple-level transmission, Bell Syst. tech. J. 40, 281-308.
[46]) Mac Williams, F. J. (1963), A theorem on the distribution of weights in a systematic code, Bell Syst. tech. J. 42, 79-94.
[47]) Mac Williams, F. J., Mallows, C. L. and Sloane, N. J. A. (1972), Generalizations of Gleason's theorem on weight enumerators of self-dual codes, IEEE Trans. Information Theory IT-18, 794-805.
[48]) Mac Williams, F. J., Sloane, N. J. A. and Goethals, J. M. (1972), The Mac Williams identities for nonlinear codes, Bell Syst. tech. J. 51, 803-819.
[49]) Marcus, M. and Minc, H. (1964), A survey of matrix theory and matrix inequalities, Allyn and Bacon, Boston.
[50]) Marguinaud, A. (1970), Codes à distance maximale, Revue du CETHEDEC 22, 33-46.
[51]) Mc Eliece, R. J., A nonlinear, nonfield version of the Mac Williams identities (unpublished paper).
[52]) Mesner, D. M. (1967), A new family of partially balanced incomplete block designs with some Latin square design properties, Ann. Math. Statist. 38, 571-581.
[53]) Nordstrom, A. W. and Robinson, J. P. (1967), An optimum nonlinear code, Information and Control 11, 613-616.
[54]) Petrenjuk, A. Ja. (1968), Math. Zametski 4, 417-425.
[55]) Pless, V. (1963), Power moment identities on weight distributions in error-correcting codes, Information and Control 6, 147-152.
[56]) Pless, V. (1968), On the uniqueness of the Golay codes, J. combinatorial Theory 5, 215-228.
[57]) Plotkin, M. (1960), Binary codes with specified minimum distances, IRE Trans. Information Theory IT-6, 445-450.
[58]) Preparata, F. P. (1968), A class of optimum nonlinear double-error-correcting codes, Information and Control 13, 378-400.
[59]) Rao, C. R. (1947), Factorial experiments derivable from combinatorial arrangements of arrays, J. Roy. statist. Soc. 9, 128-139.
[60]) Riordan, J. (1968), Combinatorial identities, Wiley, New York.
[61]) Seidel, J. J. (1967), Strongly regular graphs of L_2-type and of triangular type, Indag. Math. 29, 188-196.
[62]) Semakov, N. V., Zinov'ev, V. A. and Zaitzev, G. V. (1971), Uniformly packed codes, Problemy Peredaci Informacii 7, 38-50.
[63]) Shannon, C. E. (1948), A mathematical theory of communication, Bell Syst. tech. J. 27, 379-423, 623-656.
[64]) Simonnard, M. (1962), Programmation linéaire, Dunod, Paris.
[65]) Singleton, R. C. (1964), Maximum distance Q-nary codes, IEEE Trans. Information Theory IT-10, 116-118.
[66]) Slepian, D. (1956), A class of binary signaling alphabets, Bell Syst. tech. J. 35, 203-234.
[67]) Sloane, N. J. A. (1972), A survey of constructive coding theory, and a table of binary codes of highest known rate, Discrete Math. 3, 265-294.
[68]) Snover, S. L., Doctoral dissertation, Michigan State Univ. (to be published).
[69]) Storer, T. (1967), Cyclotomy and difference sets, Markham, Chicago.

[70]) Szegö, G. (1959), Orthogonal polynomials, Amer. Math. Soc. Colloquium Publications, Vol. XXIII.
[71]) Tamaschke, O. (1963), Zur Theorie der Permutationsgruppen mit regulärer Untergruppe, Math. Z. 80, 328-352.
[72]) Tietäväinen, A. (1973), On the non-existence of perfect codes over finite fields, SIAM J. appl. Math. 24, 88-96.
[73]) Wallis, W. D., Street, A. P. and Wallis, J. S. (1972), Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture notes in mathematics, Springer-Verlag, Berlin.
[74]) Wilson, R. M., Lectures on t-designs at Ohio State University, communicated by J. Doyen.
[75]) Wilson, R. M. and Ray-Chaudhuri, D. K. (1971), Generalization of Fisher's inequality to t-designs, Amer. math. Soc. Notices 18, 805.
[76]) Witt, E. (1938), Über Steinersche Systeme, Abh. Math. Sem. Univ. Hamburg 12, 265-275.
[77]) Biggs, N., Perfect codes in graphs (to be published).
[78]) Ogasawara, M. (1965), A necessary condition for the existence of regular and symmetrical PBIB designs of T_m type, Univ. North Carolina Inst. Statistics, Mimeo Series No. 418.
[79]) Ogawa, J. (1959), The theory of the association algebra and the relationship algebra of a partially balanced incomplete block design, Univ. North Carolina Inst. Statistics, Mimeo Series No. 224.
[80]) Yamamoto, S., Fujii, Y. and Hamada, N. (1965), Composition of some series of association algebras, J. Sci. Hiroshima Univ. Ser. A-I 29, 181-215.