

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: PROFESSOR I. M. JAMES, Mathematical Institute,
24-29 St Giles, Oxford

Already published in this series

1. General cohomology theory and K-theory, PETER HILTON.
4. Algebraic topology: A student's guide, J. F. ADAMS.
5. Commutative algebra, J. T. KNIGHT.
7. Introduction to combinatory logic, J. R. HINDLEY, B. LERCHER, and J. P. SELDIN.
8. Integration and harmonic analysis on compact groups, R. E. EDWARDS.
9. Elliptic functions and elliptic curves, PATRICK DU VAL.
10. Numerical ranges II, F. F. BONSALL and J. DUNCAN.
11. New developments in topology, G. SEGAL (ed.).
12. Symposium on complex analysis Canterbury, 1973, J. CLUNIE and W. K. HAYMAN (eds.).
13. Combinatorics, Proceedings of the British combinatorial conference 1973, T. P. McDONOUGH and V. C. MAVRON (eds.).
14. Analytic theory of abelian varieties, H. P. F. SWINNERTON-DYER.
15. An introduction to topological groups, P. J. HIGGINS.
16. Topics in finite groups, TERENCE M. GAGEN.
17. Differentiable germs and catastrophes, THEODOR BRÖCKER and L. LANDER.
18. A geometric approach to homology theory, S. BUONCRISTIANO, C. P. ROURKE and B. J. SANDERSON.
19. Graph theory, coding theory and block designs, P. J. CAMERON and J. H. VAN LINT.
20. Sheaf theory, B. R. TENNISON.
21. Automatic continuity of linear operators, ALLAN M. SINCLAIR.
22. Presentations of groups, D. L. JOHNSON.
23. Parallelisms of complete designs, PETER J. CAMERON.
24. The topology of Stiefel manifolds, I. M. JAMES.
25. Lie groups and compact groups, J. F. PRICE.
26. Transformation groups: Proceedings of the conference in the University of Newcastle upon Tyne, August 1976, CZES KOSNIOWSKI.
27. Skew field constructions, P. M. COHN.
28. Brownian motion, Hardy spaces and bounded mean oscillation, K. E. PETERSEN.
29. Pontryagin duality and the structure of locally compact abelian groups, SIDNEY A. MORRIS.
30. Interaction models, N. L. BIGGS.
31. Continuous crossed products and type III von Neumann algebras, A. VAN DAELE.
32. Uniform algebras and Jensen measures, T. W. GAMELIN.
33. Permutation groups and combinatorial structures, N. L. BIGGS and A. T. WHITE.
34. Representation theory of Lie groups, M. F. ATIYAH.
35. Trace ideals and their applications, BARRY SIMON.

- 36. Homological group theory, edited by C. T. C. WALL.
- 37. Partially ordered rings and semi-algebraic geometry, GREGORY W. BRUMFIEL.
- 38. Surveys in combinatorics, edited by B. Bollobas.
- 39. Affine sets and affine groups, D. G. NORTHCOTT.
- 40. Introduction to H_p spaces, PAUL KOOSIS.
- 41. Theory and applications of Hopf bifurcation, B. D. HASSARD, N. D. KAZARINOFF and Y. H. WAN.
- 42. Topics in the theory of group presentations, D. L. JOHNSON.

Graphs, Codes and Designs

P. J. Cameron

Fellow and Tutor,
Merton College, Oxford

J. H. van Lint

Professor of Mathematics,
Technological University, Eindhoven, The Netherlands

CAMBRIDGE UNIVERSITY PRESS

CAMBRIDGE

LONDON NEW YORK NEW ROCHELLE

MELBOURNE SYDNEY

CAMBRIDGE UNIVERSITY PRESS

Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press

The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org

Information on this title: www.cambridge.org/9780521231411

© Cambridge University Press 1980

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 1980

Re-issued in this digitally printed version 2008

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-23141-1 paperback

Contents

	Preface	vii
1.	A brief introduction to design theory	1
2.	Strongly regular graphs	16
3.	Quasi-symmetric designs	25
4.	Partial geometries	32
5.	Strongly regular graphs with no triangles	37
6.	Polarities of designs	45
7.	Extensions of graphs	49
8.	1-factorisations of K_6	56
9.	Codes	61
10.	Cyclic codes	68
11.	Threshold decoding	74
12.	Finite geometries and codes	76
13.	Self-orthogonal codes, designs and projective planes	84
14.	Quadratic residue codes	95
15.	Symmetry codes over $GF(3)$	107
16.	Nearly perfect binary codes and uniformly packed codes	113
17.	Association schemes	124
	References	136
	Index	145

Preface

The predecessor of this book (London Mathematical Society Lecture Note Series 19) had its origin in several short courses of lectures given by the authors at Westfield College, London, in 1973. The audience for the lectures consisted mainly of design theorists, and the aim was to present developments in graph theory and coding theory having a bearing on design theory. An introductory chapter on designs was added, for the benefit of readers without the background of the Westfield audience.

For the present volume, the format has been kept, but extensive revisions and updatings have been made. New material includes ovals in symmetric designs (Chapters 1 and 13), the inequalities of Ray-Chaudhuri and Wilson (Chapter 1), partial geometries, with the Hoffman-Chang and Hall-Connor theorems (Chapter 4), 1-factorisations of K_6 (Chapter 8), equidistant codes (Chapter 12), planes and biplanes (Chapter 13), generalised quadratic residue codes and inversive planes (Chapter 14), two-weight projective codes (Chapter 16), and the Krein bound (Chapter 17).

1 · A brief introduction to design theory

These lectures were given to an audience of design theorists; for those outside this class, the introductory chapter describes some of the concepts of design theory and examples of designs to which we shall refer.

A t-design with parameters (v, k, λ) (or a $t - (v, k, \lambda)$ design) is a collection \mathcal{D} of subsets (called blocks) of a set S of v points, such that every member of \mathcal{D} contains k points, and any set of t points is contained in exactly λ members of \mathcal{D} . Various conditions are usually appended to this definition to exclude degenerate cases. We assume that S and \mathcal{D} are non-empty, and that $v \geq k \geq t$ (so $\lambda > 0$). A t -design with $\lambda = 1$ is called a Steiner system. Alternatively, a t -design may be defined to consist of a set of points and a set of blocks, with a relation called incidence between points and blocks, satisfying the appropriate conditions.

Sometimes a t -design is defined so as to allow 'repeated blocks', that is, \mathcal{D} is a family rather than a set, and the same subset of S may occur more than once as a block. (This is more natural with the 'relation' definition; simply omit the condition that any k points are incident with at most one block.) In these notes, we normally do not allow repeated blocks; where they are permitted, we shall say so. There are 'non-trivial' t -designs with repeated blocks for every value of t ; but the only known examples without repeated blocks with $t > 5$ are those in which every set of k points is a block. The existence of non-trivial t -designs with $t > 5$ is the most important unsolved problem in the area; even 5-designs are sufficiently rare that new constructions are interesting. Of course, for Steiner systems the question of repeated blocks does not arise.

Only finitely many Steiner systems with $t > 3$ are known. Four of these, the 5 - (24, 8, 1) and 5 - (12, 6, 1) designs and their contractions, are particularly important, and will be described later. The others were

constructed by Denniston [45].

Remark. A 0-design is simply a collection of k -element subsets of a set.

In a t -design, let λ_i denote the number of blocks containing a given set of i points, with $0 \leq i \leq t$. Counting in two ways the number of choices of $t - i$ further points and a block containing all t distinguished points, we obtain

$$(1.1) \quad \lambda_i \binom{k-i}{t-i} = \binom{v-i}{t-i} \lambda.$$

It follows that λ_i is independent of the i points originally chosen; that is, a t -design is also an i -design for $0 \leq i \leq t$. The parameters λ_0 (the total number of blocks) and λ_1 (the number of blocks containing a given point) are usually denoted by b and r respectively. With $t = 1$, $i = 0$, (1.1) shows that, in any 1-design,

$$(1.2) \quad bk = vr.$$

A 2-design is often called a block design, or simply a design; in the literature the term 'balanced incomplete block design', abbreviated to BIBD, is used in the case where not every k -subset is a block. In a 2-design we have

$$(1.3) \quad r(k-1) = (v-1)\lambda.$$

An incidence matrix of a design is a matrix M whose rows and columns are indexed by the blocks and points of the design respectively, the entry in row B and column p being 1 if $p \in B$, 0 otherwise. (The reader is warned that a different convention is often used, for example in the books by Dembowski [44] and Hall [60], with the result that our incidence matrix is the transpose of that appearing in these books. The present convention is adopted because we shall wish to regard the characteristic functions of blocks, or rows of M , as row vectors, and consider the subspace they span.)

The conditions that any block contains k points, any point lies in r blocks, and any pair of points lies in λ blocks, can be expressed in

terms of M :

$$\begin{aligned}(1.4) \quad & MJ = kJ, \\ & JM = rJ, \\ & M^T M = (r - \lambda)I + \lambda J.\end{aligned}$$

(Here, as throughout this book, I is the identity matrix, and J the matrix with every entry 1, of the appropriate size.) It is not difficult to show that

$$\det((r - \lambda)I + \lambda J) = rk(r - \lambda)^{v-1};$$

so, if $r > \lambda$, the matrix $M^T M$ is non-singular, from which follows Fisher's inequality:

(1.5) **Theorem.** In a 2-design with $k \leq v - 1$, we have $b \geq v$.

Furthermore, if $b = v$, then $MJ = JM$; thus M commutes with $(r - \lambda)I + \lambda J$, and so with $((r - \lambda)I + \lambda J)M^{-1} = M^T$. So $MM^T = (r - \lambda)I + \lambda J$, from which we see that any two blocks have λ common points.

(1.6) **Theorem.** In a 2-design with $k \leq v - 1$, the following are equivalent:

- (i) $b = v$;
- (ii) $r = k$;
- (iii) any two blocks have λ common points.

A 2-design satisfying the conditions of (1.6) is called symmetric. Its dual is obtained by reversing the roles of points and blocks, identifying a point with the set of blocks containing it; the dual is a symmetric 2-design with the same parameters, having incidence matrix M^T . A polarity of a symmetric design \mathcal{D} is a self-inverse isomorphism between \mathcal{D} and its dual, that is, a one-to-one correspondence σ between the points and blocks of \mathcal{D} such that, for any point p and block B , $p \in B$ if and only if $B^\sigma \in p^\sigma$. A point p (resp. a block B) is absolute with respect to the polarity σ if $p \in p^\sigma$ (resp. $B^\sigma \in B$).

(1.5) and (1.6) follow from a more general result, which we will need in chapter 5.

(1.7) Theorem. In a 2-design, the number of blocks not disjoint from a given block B is at least $k(r-1)^2/((k-1)(\lambda-1) + (r-1))$. Equality holds if and only if any block not disjoint from B meets it in a constant number of points; if this occurs, the constant is $1 + (k-1)(\lambda-1)/(r-1)$.

Proof. Let d be the number of blocks different from but not disjoint from B ; suppose n_i of these blocks meet B in i points. Counting in two ways the number of choices of j points of B and another block incident with these j points, for $j = 0, 1, 2$, we obtain (with summations over i running from 1 to k):

$$\begin{aligned}\sum n_i &= d, \\ \sum i n_i &= k(r-1), \\ \sum i(i-1)n_i &= k(k-1)(\lambda-1).\end{aligned}$$

So

$$\sum (i-x)^2 n_i = dx^2 - 2k(r-1)x + k((k-1)(\lambda-1) + (r-1)).$$

This quadratic form in x must be positive semi-definite, proving the inequality. It vanishes only if $d = k(r-1)^2/((k-1)(\lambda-1) + (r-1))$ and $n_i = 0$ for all $i \neq 1 + (k-1)(\lambda-1)/(r-1)$.

Remark. Now (1.5) follows from $b-1 \geq k(r-1)^2/((k-1)(\lambda-1)+(r-1))$ on applying (1.2) and (1.3). Also, if $b = v$, then $r = k$, and $1 + (k-1)(\lambda-1)/(r-1) = \lambda$.

The Bruck-Ryser-Chowla theorem gives necessary conditions for the existence of symmetric designs with given parameter sets (v, k, λ) satisfying $(v-1)\lambda = k(k-1)$.

(1.8) Theorem. Suppose there exists a symmetric 2 - (v, k, λ) design. Put $n = k - \lambda$. Then (i) if v is even then n is a square; (ii) if v is odd, then the equation

$$z^2 = nx^2 + (-1)^{(v-1)/2} \lambda y^2$$

has a solution in integers (x, y, z) , not all zero.

The incidence equation $M^T M = nI + \lambda J$ shows that the matrices I and $nI + \lambda J$ are rationally cogredient; (1.8) can then be verified by applying the Hasse-Minkowski theorem to them, though more elementary proofs are available. The Hasse-Minkowski theorem guarantees the existence of a rational matrix M satisfying the incidence equation whenever the conditions of (1.8) are satisfied; but this does not mean that a design exists, and indeed it is not known whether these conditions are sufficient for the existence of a design. We shall have more to say about the case $(v, k, \lambda) = (111, 11, 1)$ in chapter 11.

A Hadamard matrix is an $n \times n$ matrix H with entries ± 1 satisfying $HH^T = H^T H = nI$. (It is so called because its determinant attains a bound due to Hadamard.) Changing the signs of rows and columns leaves the defining property unaltered, so we may assume that all entries in the first row and column are $+1$. If we then delete this row and column and replace -1 by 0 throughout, we obtain a matrix M which (if $n > 4$) is the incidence matrix of a symmetric $2 - (n-1, \frac{1}{2}n-1, \frac{1}{4}n-1)$ design. Such a design is called a Hadamard 2-design. From a design with these parameters, we can recover a Hadamard matrix by reversing the construction. However, a Hadamard matrix can be modified by permuting rows and columns, so from 'equivalent' Hadamard matrices it is possible to obtain different Hadamard 2-designs.

Examples of Hadamard 2-designs include the Paley designs, with $n-1 = q$ a prime power ($q \equiv 3 \pmod{4}$). The points of the design are the elements of $GF(q)$, and the blocks are the sets $Q + a$ ($a \in GF(q)$), where Q is the set of nonzero squares in $GF(q)$.

Let H be a Hadamard matrix with $n > 4$, in which every entry in the first row is $+1$. Any row other than the first has $\frac{1}{2}n$ entries $+1$ and $\frac{1}{2}n$ entries -1 , thus determining two sets of $\frac{1}{2}n$ columns. (This partition is unaffected by changing the sign of the row.) If we take columns as points, and the sets determined in this way as blocks, we obtain a $3 - (n, \frac{1}{2}n, \frac{1}{4}n-1)$ design called a Hadamard 3-design. Any design with these parameters arises from a Hadamard matrix in this way.

It should be pointed out that Hadamard matrices are very plentiful.

Examples are known for many orders n divisible by 4 (the smallest unsettled case at present is $n = 268$), and for moderately small n there are many inequivalent matrices.

A projective geometry over a (skew) field F is, loosely speaking, the collection of subspaces of a vector space of finite rank over F . The points of the geometry are the subspaces of rank 1. A projective geometry is often regarded as a lattice, in which points are atoms and every element is a join of atoms. We shall identify a subspace with the set of points it contains, regarded as a subset of the point set. The dimension of a subspace is one less than its vector-space rank (so points have dimension 0); the dimension of the geometry is that of the whole space. Lines and planes are subspaces of dimension 1 and 2 respectively; hyperplanes are subspaces of codimension 1. Thus, familiar geometric statements hold: two points lie in a unique line, a non-incident point-line pair lies in a unique plane, etc.

If F is finite, the subspaces of given positive dimension are the blocks of a 2-design. The hyperplanes form a symmetric 2-design, which we shall denote by $PG(m, q)$, where m is the dimension and $q = |F|$; its parameters are $((q^{m+1} - 1)/(q - 1), (q^m - 1)/(q - 1), (q^{m-1} - 1)/(q - 1))$. These facts can be verified by counting arguments, or by using the transitivity properties of the general linear group. Note that $PG(m, 2)$ is a Hadamard 2-design for all $m \geq 2$.

A projective plane is a symmetric 2-design with $\lambda = 1$. This agrees with the previous terminology, in that $PG(2, q)$ is a projective plane; by analogy, the blocks of a projective plane are called lines. We will modify our notation and use $PG(2, q)$ to represent any projective plane with $k = q + 1$; q is not even restricted to be a prime power (though it is in all known examples). Thus $PG(2, q)$ may denote several different designs; however, the symbol $PG(m, q)$ is unambiguous for $m > 2$. This is motivated by various characterisations; we mention one due to Veblen and Young [117]:

(1.9) Theorem. A collection of subsets (called 'lines') of a finite set of points is the set of lines of a projective geometry or projective plane if the following conditions hold:

- (i) any line contains at least three points, and no line contains every point;
- (ii) any two points lie on a unique line;
- (iii) any three non-collinear points lie in a subset which, together with the lines it contains, forms a projective plane.

Projective planes can be axiomatised in a way which permits the extension of the definition (and of (1.9)) to infinite planes; the requirements are that any two points lie on a unique line, any two lines have a unique common point, and there exist four points of which no three are collinear. Projective planes over fields are called Desarguesian, since they are characterised by the theorem of Desargues.

An affine (or Euclidean) geometry of dimension m is the collection of cosets of subspaces of a vector space of rank m over a field F . Here, the geometric dimension of a coset is equal to the vector-space dimension of the underlying subspace; points are just vectors (or cosets of the zero subspace). Again, we identify a subspace with the set of points it contains. If F is finite, the subspaces of given positive dimension form a 2-design. If $|F| = 2$, then any line has two points (and any set of two points is a line), while the subspaces of given dimension $d > 1$ form a 3-design. We denote the design of points and hyperplanes by $AG(m, q)$, where $q = |F|$. $AG(m, 2)$ is a Hadamard 3-design.

An affine plane $AG(2, q)$ can be defined to be a $2 - (q^2, q, 1)$ design. (It is also possible to give an axiomatic definition of an affine plane, in terms of the concept of 'parallelism'.) Again our notation is ambiguous. The exact analogue of the Veblen-Young theorem has been proved by Buekenhout [23] under the restriction that each line has at least four points; Hall [59] has given a counterexample with three points on any line. Again, affine planes over fields are characterised by Desargues' theorem.

We note that an affine geometry can be obtained from the corresponding projective geometry by deleting a hyperplane (the 'hyperplane at infinity') together with all of its subspaces, while the projective geometry can be recovered from the affine geometry. The same is true for projective and affine planes.

A similar question can be asked about more general designs. Let \mathcal{D} be a symmetric $2 - (V, K, \lambda)$ design, and B a block of \mathcal{D} . If B and all its points are deleted from \mathcal{D} , the resulting structure \mathcal{D}^B is a $2 - (V-K, K-\lambda, \lambda)$ design. If we put $v = V-K$, $k = K-\lambda$, then we have $v = k(k + \lambda - 1)/\lambda$. We call \mathcal{D}^B the residual design of \mathcal{D} relative to the block B . An arbitrary $2 - (v, k, \lambda)$ design with $v = k(k + \lambda - 1)/\lambda$ is called quasi-residual. The question is: which quasi-residual designs are residual?

A quasi-residual design with $\lambda = 1$ is a $2 - (k^2, k, 1)$ design, that is, an affine plane. The familiar procedure of adjoining a line at infinity to an affine plane shows that any such design is residual. For $\lambda = 2$, the same assertion is true, by a theorem of Hall and Connor [61]. We will prove this theorem, and state a theorem of Bose, Shrikhande and Singhi [19] concerning quasi-residual designs with $\lambda > 2$, in Chapter 4. There are quasi-residual designs which are not residual: see van Lint [82].

We shall consider briefly in chapter 5 the affine symplectic geometry of dimension 4 over $GF(2)$. Here the vector space carries a symplectic bilinear form, and the blocks of the design are the cosets of those subspaces of rank 2 which are totally isotropic with respect to the form.

Given a t -design \mathcal{D} , the derived design \mathcal{D}_p with respect to a point p is the $(t-1)$ -design whose points are the points of \mathcal{D} different from p , and whose blocks are the sets $B - \{p\}$ for each block B of \mathcal{D} which contains p . The residual design \mathcal{D}^p with respect to p has the same point set as \mathcal{D}_p , but its blocks are the blocks of \mathcal{D} not containing p ; it is also a $(t-1)$ -design.

A converse question, which is very important in design theory and permutation groups, is that of extendability:

given a t -design, is it isomorphic to \mathcal{D}_p for some $(t+1)$ -design \mathcal{D} ? \mathcal{D} is called an extension of the given design. An extension may not exist, or there may be more than one. (To construct the extension, we must find a suitable design \mathcal{D}^p .) By applying (1.2) to the extension, we obtain a simple necessary condition for extendability:

(1.10) **Proposition.** If a $t - (v, k, \lambda)$ design with b blocks is extendable, then $k + 1$ divides $b(v + 1)$.

The 2-design $PG(2, q)$ has $v = q^2 + q + 1 = b$, $k = q + 1$. Applying (1.10), we obtain a result of Hughes [70]:

(1.11) **Theorem.** If $PG(2, q)$ is extendable, then $q = 2, 4$, or 10 .

Much effort has been devoted to these projective planes and their extensions. Further application of (1.10) shows that $PG(2, 2)$ and $PG(2, 10)$ can be extended at most once, and $PG(2, 4)$ at most three times. In fact, $PG(2, 2)$ is unique, and has a unique extension, namely $AG(3, 2)$. $PG(2, 4)$ is also unique, and can be extended three times, each successive extension being unique (up to isomorphism). The existence of $PG(2, 10)$ is still undecided (we will discuss this further in chapter 11) and its extendability appears rather remote at present.

Hughes showed further that there are only finitely many extendable symmetric $2 - (v, k, \lambda)$ designs with any given value of λ . The strongest result in this direction is due to Cameron [25].

(1.12) **Theorem.** If a $3 - (v, k, \lambda)$ design \mathcal{D} is an extension of a symmetric 2-design, then one of the following occurs:

- (i) \mathcal{D} is a Hadamard 3-design;
- (ii) $v = (\lambda + 1)(\lambda^2 + 5\lambda + 5)$, $k = (\lambda + 1)(\lambda + 2)$;
- (iii) $v = 112$, $k = 12$, $\lambda = 1$;
- (iv) $v = 496$, $k = 40$, $\lambda = 3$.

Proof. First we note that a 3-design \mathcal{D} is an extension of a symmetric 2-design if and only if any two blocks of \mathcal{D} meet in 0 or $\lambda + 1$ points. A $3 - (v, k, \lambda)$ design with these properties has $r = v - 1$, $\lambda_2 = k - 1$, and $(v - 2)\lambda = (k - 1)(k - 2)$.

Let B be a block of \mathcal{D} . If $p, q \notin B$, then there are $k\lambda/(\lambda + 1)$ blocks containing p and q and meeting B in $\lambda + 1$ points, and hence $(k - \lambda - 1)/(\lambda + 1)$ blocks disjoint from B . This shows that the incidence structure \mathcal{D}_0 , where points are those outside B and whose blocks are those disjoint from B , is a $2 - (v - k, k, (k - \lambda - 1)/(\lambda + 1))$ design. By (1.2) and (1.3) (or by (1.7) applied to \mathcal{D}), the number of blocks of \mathcal{D}_0 is

$$\frac{(v-k)(v-k-1)(k-\lambda-1)}{k(k-1)(\lambda+1)}.$$

If \mathcal{D}_0 is degenerate (having but a single block), then $v = 2k$, whence $v = 4(\lambda + 1)$, $k = 2(\lambda + 1)$, and \mathcal{D} is a Hadamard 3-design. Otherwise, we may apply Fisher's inequality to \mathcal{D}_0 , yielding

$$(v - k - 1)(k - \lambda - 1) \geq k(k - 1)(\lambda + 1),$$

$$(k - 1)(k - (\lambda + 1)(\lambda + 2)) \geq 0,$$

and so $k \geq (\lambda + 1)(\lambda + 2)$.

However, $b = v(v - 1)/k = (k^2 - 3k + 2\lambda + 2)(k^2 - 3k + \lambda + 2)/k\lambda^2$; so k divides $2(\lambda + 1)(\lambda + 2)$. The same expression shows that, if $k = 2(\lambda + 1)(\lambda + 2)$, then $\lambda = 1$ or 3 , giving cases (iii) or (iv) of the Theorem. If $k = (\lambda + 1)(\lambda + 2)$ then we have case (ii).

As previously noted, Hadamard designs exist for many values of λ . Also, any Hadamard 2-design is uniquely extendable. For, in forming the extension, the new point p must be added to all existing blocks; the proof of (1.12) then shows that the complements of all these blocks must be included as blocks, and these are all the blocks. Apart from these, only one design is known which satisfies the hypotheses of (1.12), namely the $3 - (22, 6, 1)$ design (case (ii) with $\lambda = 1$): this will be discussed later. It is an easy deduction from (1.12) that the projective plane of order 4 is the only twice-extendable symmetric design.

For affine planes, the situation is a little different, since the necessary condition (1.10) is always satisfied. An extension of an affine plane (that is, a $2 - (q^2 + 1, q + 1, 1)$ design) is called an inversive plane or Möbius plane of order q . The simplest example is constructed as follows: the point set is $\{\infty\} \cup \text{GF}(q^2)$, the projective line over $\text{GF}(q^2)$; blocks are all images of $\{\infty\} \cup \text{GF}(q)$ under the linear fractional group $\text{PGL}(2, q^2) = \{z \mapsto \frac{az + b}{cz + d} \mid a, b, c, d \in \text{GF}(q^2), ad - bc \neq 0\}$. Any derived design of this inversive plane is isomorphic to the Desarguesian affine plane of order q . Another description of this design is as the point set of an elliptic quadric in $\text{PG}(3, q)$, the blocks being the non-trivial plane sections. Dembowski [42], [43] has shown that any inversive plane of even order q can be represented similarly as an 'ovoid' in $\text{PG}(3, q)$

with its non-trivial plane sections. Using this and a further embedding theorem in conjunction with (1.10), Kantor [74] showed that if $AG(2, q)$ (with $q > 2$) is twice extendable, then $q = 3$ or 13 . In fact, $AG(2, 3)$ is three times extendable; the extensions are all 'embedded' in projective spaces over $GF(3)$ in a similar way, and are closely related to the extensions of $PG(2, 4)$. It is not known whether any $AG(2, 13)$ is twice extendable, or whether any non-Desarguesian affine plane is extendable.

Our next topic in this chapter concerns ovals. Let \mathcal{D} be a symmetric $2 - (v, k, \lambda)$ design. An n -arc is a set of n points of \mathcal{D} , no three of which are contained in a block. Given an n -arc S , a block B is called a secant, tangent or passant to S according as $|B \cap S| = 2, 1$ or 0 .

(1.13) Proposition. Any point of an n -arc in a symmetric $2 - (v, k, \lambda)$ design lies on $(n - 1)\lambda$ secants and $k - (n - 1)\lambda$ tangents. In particular, $n \leq 1 + k/\lambda$.

Proof. Let S be an n -arc, and $p \in S$. Count pairs (q, B) where B is a secant containing p and $q, q \in S$.

An n -arc is called an oval of type I if each point lies on a unique tangent (that is, $n = 1 + (k - 1)/\lambda$), and an oval of type II if it has no tangents (that is, $n = 1 + k/\lambda$). Note that ovals can exist only if $\lambda \mid k - 1$ or $\lambda \mid k$ respectively. //

(1.14) Proposition. If a symmetric $2 - (v, k, \lambda)$ design has an oval of type II, then $k - \lambda$ is even.

Proof. Let S be the oval, and p a point outside S . The number of secants containing p is $\frac{1}{2}n\lambda = \frac{1}{2}(k + \lambda)$. //

(1.15) Proposition. Let S be a type I oval in a symmetric $2 - (v, k, \lambda)$ design with $k - \lambda$ even. Then any point is on either one or all tangents to S .

Proof. Observe that k, λ and n are all odd, and so any point lies on at least one tangent to S . Let n_i be the number of points which

are on i tangents. Then

$$\begin{aligned}\sum n_i &= v, \\ \sum in_i &= nk, \\ \sum \binom{i}{2} n_i &= \lambda \binom{n}{2}.\end{aligned}$$

Therefore

$$\sum (i-1)(i-n)n_i = 0,$$

whence every point is on one or all the tangents. //

It follows from (1.15) that, in a projective plane of even order, all the tangents to a type I oval S pass through a point p , the knot (or nucleus) of S ; and $\{p\} \cup S$ is a type II oval.

Given a type II oval S , the passants to S and points outside S (with the reverse of the given incidence relation) form a

$$2 = ((k-2)(k-\lambda)/2\lambda, \frac{1}{2}(k-\lambda), \lambda) \text{ design.}$$

If \mathcal{D} is a 3-design which is an extension of a projective plane, p a point of \mathcal{D} , and B a block not containing p , then B is a type II oval in the projective plane \mathcal{D}_p .

Consider the $2 - (11, 5, 2)$ Paley design \mathcal{D} . Every triple of points not contained in a block is a type I oval. Hence any two points of \mathcal{D} are on two distinct blocks of \mathcal{D} and three ovals. Any three points either lie in a block or form an oval. We define a new design \mathcal{D}' as follows. Points of \mathcal{D}' are the points and blocks of \mathcal{D} . Blocks of \mathcal{D}' are sets of size 6 of the following types:

- (i) a point of \mathcal{D} and the five blocks of \mathcal{D} incident with it;
- (ii) a block of \mathcal{D} and the five points of \mathcal{D} incident with it;
- (iii) an oval of \mathcal{D} and its three tangents.

It is now easy to verify that \mathcal{D}' is a $3 - (22, 6, 1)$ design, i. e. an extension of $\text{PG}(2, 4)$ (cf. Assmus, Mezzaroba and Salwach [8]).

For a further reference on ovals see Assmus and van Lint [2].

We turn next to a generalisation of Fisher's inequality for designs with larger values of t . This was proved by Petrenjuk [93] for $t = 4$, and by Ray-Chaudhuri and Wilson [98] in general. This result is as follows.

(1.16) Theorem. Let \mathcal{D} be a $t - (v, k, \lambda)$ design, with $t = 2s$ and $t \leq k \leq v - s$. Then $b \geq \binom{v}{s}$. Equality holds if and only if the cardinality of the intersection of two blocks takes precisely s distinct values.

Proof. We shall prove the inequality $b \geq \binom{v}{s}$. Let M be the 'incidence matrix' with rows indexed by blocks and columns by s -subsets of the point set, with (B, S) entry 1 if $S \subseteq B$, 0 otherwise. It is enough to show that the rows of M span $\mathbb{R}^{\binom{v}{s}}$. Accordingly, let ρ_B be the row of M with label B , and γ_S the vector with 1 in the column with label S , 0 elsewhere. For $0 \leq i \leq s$ and a fixed s -set S , put

$$\begin{aligned} y_i &= \sum_{|B \cap S| = i} \rho_B \\ &= \sum_{j=0}^i \sum_{|S' \cap S| = j} \sum_{\substack{B \supseteq S' \\ |B \cap S| = i}} \gamma_{S'} \\ &= \sum_{j=0}^i \binom{s-j}{i-j} \lambda_{s+i-j, s-i} \left(\sum_{|S \cap S'| = j} \gamma_{S'} \right), \end{aligned}$$

where $\lambda_{m,n}$ denotes the number of blocks containing a given m -set M and disjoint from a given n -set N (where $M \cap N = \emptyset$); this number is easily seen to depend only on m and n if $m + n \leq t$. Putting

$x_j = \sum_{|S' \cap S| = j} \gamma_{S'}$, we have a system of $s + 1$ linear equations for the x 's in terms of the y 's. The coefficient matrix is triangular, with non-zero diagonal entries $\lambda_{s, s-i}$ (since $s \leq k \leq v - s$). So the equations have a unique solution. In particular, $x_s = \gamma_S$ is a linear combination of y 's, and so is in the row space of M , proving the assertion.

This theorem will be discussed further in chapters 3 and 17.

A t -design attaining the bound in (1.16) is called tight. Thus tight 2-designs are nothing but symmetric 2-designs, and are very plentiful. For $t > 2$, however, the position is different. Ito [71], Enomoto, Ito and Noda [91], and Bremner [20] have shown:

(1.17) Theorem. Up to complementation, the only tight 4 - (v, k, λ) design with $2 < k < v-2$ is the 4 - (23, 7, 1) design.

There are also nonexistence results for larger values of t ; and Bannai [10] has shown that, for given even $t \geq 10$, there are only finitely many tight t -designs.

We have touched on extensions of $PG(2, 4)$ and $AG(2, 3)$ several times in this chapter, sufficient to convince the reader of their importance in design theory. They occur also in coding and group theory. We conclude this chapter with a brief survey of some constructions of them.

The simplest constructions use the ideas of coding theory, since the two designs are connected with the two perfect Golay codes. We postpone discussion of this until chapters 13 and 17.

Witt [120] gave an indirect construction of the designs. He constructed the two 5-fold transitive Mathieu groups M_{24} and M_{12} as extensions of known permutation groups, and showed group-theoretically that they are groups of automorphisms of designs with the appropriate parameters. He also proved the uniqueness of the designs [121].

Lüneburg [85] gave a construction which is similar in spirit (in that it involves extending known structures) but combinatorial in nature. Let Π denote $PG(2, 4)$, and consider the problem of extending Π to a 5 - (24, 8, 1) design. We must add three new points p, q, r , and take as blocks all sets $\{p, q, r\} \cup L$, where L is a line of Π . For $i < 3$, a block containing i of the new points contains also $8 - i$ points of Π , forming some geometric configuration in Π . When $i = 2$, this configuration is a Type II oval (see the remark following (1.15)). There are 168 such ovals in Π , and counting arguments show that 168 blocks of this form are required. Write $S_1 \sim S_2$ (where S_1 and S_2 are ovals of Π) if $|S_1 \cap S_2|$ is even. It can be shown that this is an equivalence relation, with three equivalence classes of size 56. Choose a bijection between equivalence classes and pairs of new points, and adjoin each pair to all ovals in the corresponding class. Similar arguments deal with the cases $i = 1$ and $i = 0$, when the geometric configurations are Baer subplanes and symmetric differences of pairs of lines respectively. In this way the design can be constructed and proved unique.

A similar method can be applied to obtain the 5 - (12, 6, 1) design from $AG(2, 3)$. Alternatively, it can be located as having point set $\{p, q, r\} \cup U$, where U is a unital of $PG(2, 4)$, and as blocks all

those blocks of the $5 - (24, 8, 1)$ design which meet this set in six points.

Yet another construction is outlined in chapter 8.

2 · Strongly regular graphs

The theory of designs concerns itself with questions about subsets of a set (or relations between two sets) possessing a high degree of symmetry. By contrast, the large and amorphous area called 'graph theory' is mainly concerned with questions about 'general' relations on a set. This generality means that usually either the questions answered are too particular, or the results obtained are not powerful enough, to have useful consequences for design theory. There are some places where the two theories have interacted fruitfully; in the next five chapters, several of these areas will be considered. The unifying theme is provided by a class of graphs, the 'strongly regular graphs', introduced by Bose [16], whose definition reflects the symmetry inherent in t-designs. First, however, we shall mention an example of the kind of situation we shall not be discussing.

A graph consists of a finite set of vertices together with a set of edges, where each edge is a subset of the vertex set of cardinality 2. (In classical terms, our graphs are undirected, without loops or multiple edges.) As with designs, there is an alternative definition: a graph consists of a finite set of vertices and a set of edges, with an 'incidence' relation between vertices and edges, with the properties that any edge is incident with two vertices and any two vertices with at most one edge. Still another definition: a graph consists of a finite set of vertices together with a symmetric irreflexive binary relation (called adjacency) on the vertex set. A graph is complete if every pair of vertices is adjacent, and null if it has no edges at all. The complement of the graph Γ is the graph $\bar{\Gamma}$ whose edge set is the complement of the edge set of Γ (in the set of all 2-element subsets of the vertex set). In any graph Γ , $\Gamma(p)$ will denote the set of vertices adjacent to the vertex p . Given a subset S of the vertex set, $\Gamma|S$ denotes the graph with vertex set S whose

edges are those edges of Γ which join pairs of vertices of S .

For example, let n be a natural number, and let V be the set of all $n \times n$ latin squares with entries $\{1, \dots, n\}$. Form a graph Γ_n with vertex set V by saying that two latin squares are adjacent if and only if they are orthogonal. Now it is well-known that there exists a (projective or affine) plane of order n if and only if Γ_n contains the complete graph on $n - 1$ vertices as a subgraph. Graph theory provides us with lower bounds for the size of complete subgraphs of graphs; not surprisingly, these are far too weak to force the existence of a plane of given order except in trivial cases. This simple approach seems unlikely to produce any useful results for the theory of finite planes.

If p is a vertex of a graph Γ , the valency of p is the number of edges containing p (equivalently, the number $|\Gamma(p)|$ of vertices adjacent to p). If every vertex has the same valency, the graph is called regular, and the common valency is the valency of the graph. (Thus, a graph is a 0-design with $k = 2$; a regular graph is a 1-design. Only the complete graph is a 2-design, sometimes called the pair design.)

As in design theory, we can define the incidence matrix $M(\Gamma)$ of a graph Γ to be the matrix of the incidence relation (with rows indexed by edges and columns by vertices, with (e, p) entry 1 if $p \in e$, 0 otherwise). A more useful matrix is the adjacency matrix $A(\Gamma)$, the matrix of the adjacency relation (with rows and columns indexed by vertices, with (p_1, p_2) entry 1 if $\{p_1, p_2\}$ is an edge, 0 otherwise). Note that $M(\Gamma)^T M(\Gamma)$ is the sum of the symmetric $A(\Gamma)$ and a diagonal matrix whose (p, p) entry is the valency of p ; so $M(\Gamma)^T M(\Gamma) = A(\Gamma) + aI$ if Γ is regular with valency a . Note also that $A(\bar{\Gamma}) = J - I - A(\Gamma)$, where (as always) J denotes a matrix with every entry 1. Γ is regular if and only if $A(\Gamma)J = aJ$ for some constant a (which is then the valency of Γ).

A strongly regular graph is a graph which is regular, but not complete or null, and has the property that the number of vertices adjacent to p_1 and p_2 ($p_1 \neq p_2$) depends only on whether or not p_1 and p_2 are adjacent. Its parameters are (n, a, c, d) , where n is the number of vertices and a the valency, and the number of vertices adjacent to p_1 and p_2 is c or d according as p_1 and p_2 are adjacent or non-adjacent.

(Be warned: this notation is not standard. We use it because a standard notation does not exist; of the two main contenders, one is impossible here because it uses the symbols k and λ , and the other is a special case of notation for association schemes and so is too cumbersome. The notation used here is only temporary, to be abandoned for the design theory notation whenever a design appears.)

If Γ is a strongly regular graph and p_1 and p_2 are adjacent vertices, then $a - c - 1$ vertices are adjacent to p_1 but not to p_2 , and so $(n - a - 1) - (a - c - 1)$ are adjacent to neither p_1 nor p_2 . Similar remarks hold if p_1 and p_2 are non-adjacent. So the complement $\bar{\Gamma}$ is also strongly regular.

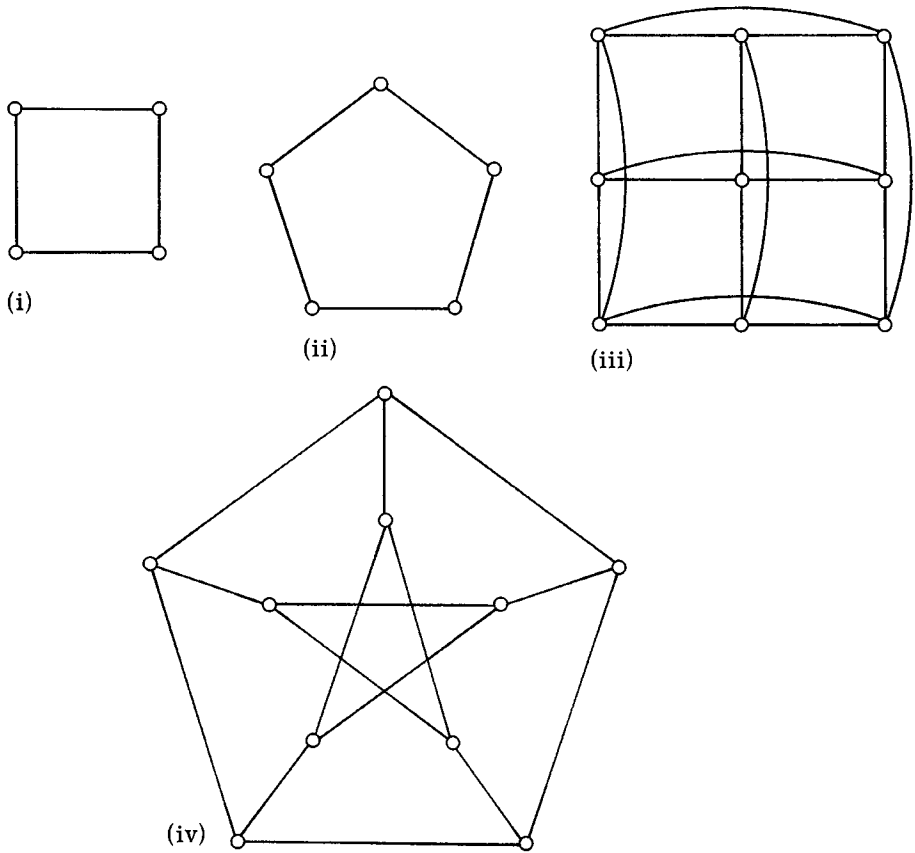


Fig. 2.1

Only a few graphs are small enough to be drawn. In drawings such as Fig. 2.1, a small circle represents a vertex, and an arc an edge, but two arcs may 'cross' without requiring a vertex at the crossing-point. Four strongly regular graphs are displayed in Fig. 2.1.

Larger graphs must be described verbally. Thus, the triangular graph $T(m)$ ($m \geq 4$) has as vertices the 2-element subsets of a set of cardinality m ; two distinct vertices are adjacent if and only if they are not disjoint. $T(m)$ is strongly regular with parameters $n = \frac{1}{2}m(m-1)$, $a = 2(m-2)$, $c = m-2$, $d = 4$. The fourth graph in Fig. 2.1, which is called the Petersen graph, is the complement of $T(5)$. The lattice graph $L_2(m)$ ($m \geq 2$) has as vertex set $S \times S$, where S is a set of cardinality m ; two distinct vertices are adjacent if and only if they have a common coordinate. $L_2(m)$ is strongly regular, with parameters $n = m^2$, $a = 2(m-1)$, $c = m-2$, $d = 2$. The first and third graphs in Fig. 2.1 are $L_2(s)$ and $L_2(3)$. The disjoint union of k complete graphs on m vertices each ($k, m > 1$) is also a strongly regular graph $\Gamma(k, m)$ with parameters $n = mk$, $a = m-1$, $c = m-2$, $d = 0$; indeed, any strongly regular graph with $d = 0$ is of this form. $\Gamma(k, 2)$ is called a ladder graph. The complement of $\Gamma(k, m)$ is called a complete k-partite graph. The first graph in Fig. 2.1 is the complete bipartite graph $\Gamma(2, 2)$. If q is a prime power with $q \equiv 1 \pmod{4}$, the Paley graph $P(q)$ has as vertex set the elements of $GF(q)$, with two vertices adjacent if and only if their difference is a nonzero square. It is strongly regular, with parameters $n = q$, $a = \frac{1}{2}(q-1)$, $c = \frac{1}{4}(q-5)$, $d = \frac{1}{4}(q-1)$, and is isomorphic with its complement. The second and third graphs of Fig. 2.1 are $P(5)$ and $P(9)$.

The Clebsch graph has as vertices all subsets of $\{1, \dots, 5\}$ of even cardinality; two vertices are adjacent whenever (as subsets) their symmetric difference has cardinality 4. In this graph, the set $\bar{\Gamma}(p)$ of vertices not adjacent to a vertex p carries the Petersen graph.

The Gewirtz graph on 56 vertices, with $a = 10$, $c = 0$, $d = 2$, can be defined by the following construction due to Sims. The vertex set is $\{\infty\} \cup \mathcal{O} \cup \mathcal{Q}$, where \mathcal{O} is the set of Sylow 3-subgroups of the alternating group A_6 , and \mathcal{Q} is the set of involutions in A_6 . Join ∞ to all vertices in \mathcal{O} ; join $P \in \mathcal{O}$ to $q \in \mathcal{Q}$ whenever $q^{-1}Pq = P$; join

$q_1, q_2 \in \mathcal{Q}$ whenever $q_1 q_2$ has order 4. Combinatorially, we may identify $P \in \mathcal{P}$ with a pair of disjoint 3-subsets of $\{1, \dots, 6\}$ (its orbits). Then typical edges of the second and third types join

$$\{\{1, 2, 3\}, \{4, 5, 6\}\} \text{ to } (12)(45),$$

and

$$(12)(34) \text{ to } (23)(56),$$

respectively.

Another construction of the Gewirtz graph uses as vertices one class of ovals in $\text{PG}(2, 4)$ (see the remarks on Lüneburg's construction in chapter 1), two ovals joined whenever they are disjoint. The fact that this graph is strongly regular will follow from (3.2).

The complete multipartite graphs and the Petersen, Clebsch and Gewirtz graphs are determined up to isomorphism by their parameters. (For the last three, see Seidel [101], Gewirtz [51].) The same holds for the triangular graphs $T(n)$ with $n \neq 8$, and lattice graphs $L_2(n)$ with $n \neq 4$; these results (due to Chang [32], Hoffman [68] and Shrikhande [107]) will be described in chapter 4. The Paley graphs are not in general determined by their parameters; counterexamples are given at the end of this chapter.

If G is a permutation group on a set V , then G has a natural component-wise action on $V \times V$. We say G has rank 3, if it is transitive on V and has just three orbits on $V \times V$, the diagonal $\{(p, p) | p \in V\}$ and two others O, O' . If the rank 3 group G has even order, it contains an involution interchanging two points, say p and q ; thus the orbit containing (p, q) is symmetric, and the other orbit is also. Form a graph Γ with vertex set V , whose edges are the unordered pairs corresponding to ordered pairs in O . G is a group of automorphisms of Γ . Since G is transitive on vertices, Γ is regular; since G is transitive on adjacent pairs and on non-adjacent pairs of vertices, Γ is strongly regular. The many known families of rank 3 groups of even order yield large numbers of strongly regular graphs, including all those already mentioned; such graphs are sometimes called rank 3 graphs.

Let A be the adjacency matrix of the strongly regular graph Γ with parameters (n, a, c, d) . The (p_1, p_2) entry of A^2 is the number

of vertices adjacent to p_1 and p_2 ; this number is a , c , or d according as p_1 and p_2 are equal, adjacent, or non-adjacent. So

$$(2.1) \quad A^2 = aI + cA + d(J - I - A).$$

Also,

$$(2.2) \quad AJ = JA = aJ.$$

Thus the matrices I , J , A span a real algebra of dimension 3 which is commutative and consists of symmetric matrices. Indeed, a strongly regular graph could be defined as a graph whose adjacency matrix satisfies (2.1) and (2.2). There is an orthogonal matrix which simultaneously diagonalises I , J and A . A has the eigenvalue a with multiplicity 1, corresponding to the eigenvalue n of J ; thus

$$(2.3) \quad a(a - c - 1) = (n - a - 1)d,$$

an equation which can also be verified by selecting a vertex p_1 and counting the number of edges $\{p_2, p_3\}$ with p_2 adjacent and p_3 non-adjacent to p_1 . Any other eigenvalue of J is zero; so the other eigenvalues ρ_1, ρ_2 of A satisfy the equation

$$\rho^2 = (a - d) + (c - d)\rho,$$

whence

$$\rho_1, \rho_2 = \frac{1}{2}[c - d \pm \sqrt{(c - d)^2 + 4(a - d)}].$$

If ρ_1 and ρ_2 have multiplicities f_1 and f_2 , then

$$n = f_1 + f_2 + 1,$$

$$0 = \text{Tr}(A) = a + f_1\rho_1 + f_2\rho_2.$$

These equations determine f_1 and f_2 (since $c = d = a$ is not possible). Indeed we find without difficulty that

$$(2.4) \quad f_1, f_2 = \frac{1}{2}\left[n - 1 \pm \frac{(n - 1)(d - c) - 2a}{\sqrt{(d - c)^2 + 4(a - d)}}\right].$$

Obviously, f_1 and f_2 are non-negative integers. This observation provides quite strong conditions on the parameters, the so-called 'rationality conditions'. They include most of the known non-existence criteria for strongly regular graphs. A few other conditions are known; some will appear later.

If Γ is a rank 3 graph, then the algebra generated by I , J , and $A(\Gamma)$ is precisely the centraliser algebra of the set of matrices in the permutation representation of the group $G = \text{Aut}(\Gamma)$, and the multiplicities of the eigenvalues of $A(\Gamma)$ are the degrees of the irreducible constituents of the permutation character of G .

We may distinguish two types of parameter sets for which f_1 and f_2 are integers.

Type I, with $(n-1)(d-c) = 2a$. Here $n = 1 + \frac{2a}{d-c} > 1 + a$, so $0 < d-c < 2$. Thus $d-c = 1$ and we find $c = d-1$, $a = 2d$, $n = 4d+1$. It can also be shown that a Bruck-Ryser like condition holds: n must be a sum of two squares of integers. The Paley graphs are of type I.

Type II, when $(d-c)^2 - 4(a-d)$ is the square of an integer u , u divides $(n-1)(d-c) - 2a$, and the quotient is congruent to $n-1 \pmod{2}$. Note that type I graphs are also of type II if, and only if, n is a square; the graph $L_2(3) \cong P(9)$ is an example of this.

Given a graph Γ with adjacency matrix A , Γ is regular if and only if the all-1 vector j is an eigenvector of A ; the corresponding eigenvalue is the valency. Since A is symmetric, j^\perp is A -invariant. Then Γ is strongly regular if and only if $A|_{j^\perp}$ has just two distinct eigenvalues. (We have already seen the 'only-if' part of this. Conversely, if $(A - \rho_1 I)(A - \rho_2 I)|_{j^\perp} = 0$, then $(A - \rho_1 I)(A - \rho_2 I) = \alpha J$ for some α , whence $A^2 \in \langle I, J, A \rangle$ and Γ is strongly regular.)

We have seen that the parameters of the strongly regular graph Γ determine the eigenvalues of A and their multiplicities. Conversely, the eigenvalues determine their multiplicities. For ρ_1 and ρ_2 are roots of the quadratic $\rho^2 = (a-d) + (c-d)\rho$; so we have $\rho_1 + \rho_2 = c-d$, $\rho_1\rho_2 = -(a-d)$, whence $c = a + \rho_1 + \rho_2 + \rho_1\rho_2$, $d = a + \rho_1\rho_2$. However, knowledge of the multiplicities alone does not in general determine the parameters. Sometimes it does give strong partial information, as the

following result, due to Wielandt [119], shows.

(2.5) Theorem. Suppose Γ is a strongly regular graph on $n = 2m$ vertices, whose eigenvalues have multiplicities $1, m - 1, m$. Then either

- (i) Γ or its complement is a ladder graph,
or (ii) Γ or its complement has parameters $n = 4s^2 + 4s + 2$,
 $a = s(2s + 1)$, $c = s^2 - 1$, $d = s^2$, for some positive integer s .

Proof. We may assume $a < m$, by replacing the graph by its complement if necessary. We have

$$a + (m - 1)\rho_1 + m\rho_2 = 0$$

$$a^2 + (m - 1)\rho_1^2 + m\rho_2^2 = 2ma$$

$$a^3 + (m - 1)\rho_1^3 + m\rho_2^3 = 2mac$$

and $|\rho_1| \leq a$, by the Perron-Frobenius theorem.

The first equation shows $a \equiv \rho_1 \pmod{m}$; so either $\rho_1 = a$ or $\rho_1 = a - m$. In the first case, $\rho_2 = -a$, $2ma^2 = 2ma$, $a = 1$, and (i) holds. In the second case put $\rho_2 = s$. We find $a = m - 1 - s$, $\rho_1 = -1 - s$; the second equation then yields $m = 2s^2 + 2s + 1$, and the value of c follows from the third equation. //

The only graph with the parameters (ii) of (2.5) with $s = 1$ is the Petersen graph. We conclude this chapter with an example, due to Delsarte and Goethals and to Turyn, which shows that these graphs exist whenever $2s + 1$ is a prime power. They are related to the so-called 'symmetric conference matrices' [40], [55].

First, let $V = V(2, q)$, where q is an odd prime power. Partition the 1-dimensional subspaces of V into two disjoint sets P and N of equal size $\frac{1}{2}(q + 1)$. Form the graph with vertex set V in which x and y are joined whenever $\langle x - y \rangle \in P$. This graph is strongly regular, with $n = q^2$, $a = \frac{1}{2}(q^2 - 1)$, $c = \frac{1}{4}(q^2 - 5)$, $d = \frac{1}{4}(q^2 - 1)$ (the same parameters as the Paley graph $P(q^2)$).

Next, choose a member of P , and select any $\frac{1}{2}(q - 1)$ of its cosets; let X be the set of $\frac{1}{2}q(q - 1)$ vertices contained in these cosets. Delete each edge $\{x, y\}$ for $x \in X$, $y \notin X$, and add new edges $\{x, y\}$ for all previously non-joined pairs of this form. Finally, add a new vertex

∞ joined to every vertex in X . The reader is invited to check that the resulting graph is strongly regular, and has the parameters of (2.5ii) with $q = 2s + 1$.

The above 'switching' construction will be considered further in chapter 7.

We conclude this chapter with an inequality connecting the parameters of a strongly regular graph, due to Delsarte, Goethals and Seidel [41].

(2.6) Theorem. Let Γ be a strongly regular graph on n vertices, having the properties that Γ and $\bar{\Gamma}$ are both connected, and that the adjacency matrix of Γ has an eigenvalue of multiplicity f ($f > 1$). Then
 $n \leq \frac{1}{2}f(f + 3)$.

Proof. The adjacency matrix $A = A(\Gamma)$ has three distinct eigenspaces, and any matrix with these eigenspaces is a linear combination of I , A , and $J - I - A$. In particular, there is such a linear combination F having the eigenvalues $0, 1$ with multiplicities $n - f, f$ respectively. Then F is positive semidefinite symmetric, and so it is the Gram matrix of inner products of a set S of vectors in \mathbb{R}^f . Since $F = \alpha I + \beta A + \gamma(J - I - A)$, any vector in S has length $\alpha^{\frac{1}{2}}$, and two vectors in S have angle $\cos^{-1}(\beta/\alpha)$ or $\cos^{-1}(\gamma/\alpha)$. We must show that such a set can have cardinality at most $\frac{1}{2}f(f + 3)$. We may normalise to assume $\alpha = 1$, i.e. S is a subset of the unit sphere Ω .

For $\underline{v} \in S$, let $f_{\underline{v}} : \Omega \rightarrow \mathbb{R}$ be the function defined by $f_{\underline{v}}(\underline{x}) = ((\underline{v}, \underline{x}) - \beta)((\underline{v}, \underline{x}) - \gamma)/(1 - \beta)(1 - \gamma)$. Now $f_{\underline{v}}$ is a polynomial function of degree 2; and the functions $f_{\underline{v}}$ ($\underline{v} \in S$) are linearly independent, since $f_{\underline{v}}(\underline{v}) = 1$, $f_{\underline{v}}(\underline{w}) = 0$ for $\underline{v}, \underline{w} \in S$, $\underline{v} \neq \underline{w}$. But the spaces of homogeneous linear and quadratic functions on Ω have dimensions f and $\frac{1}{2}f(f + 1)$ respectively; and we may ignore the constants, since $x_1^2 + \dots + x_f^2 = 1$ on Ω . Thus

$$n = |S| \leq f + \frac{1}{2}f(f + 1),$$

as claimed.

3 · Quasi-symmetric designs

Recall that a 2-design is symmetric if the cardinality of the intersection of two blocks is constant. Any 2-design has at least as many blocks as points, with equality if and only if it is symmetric.

A 2-design is called quasi-symmetric if the cardinality of the intersection of two blocks takes just two distinct values, say x and y . Thus, in a quasi-symmetric design, $b > v$. One simple class of quasi-symmetric designs is the class of 2-designs with $\lambda = 1$ which are not projective planes; here, clearly, two blocks have at most one common point, so $\{x, y\} = \{0, 1\}$. The blocks of such a design are often called 'lines'. Bose [16] studied the line graph of such a design, the graph whose vertices are the lines, with two vertices adjacent whenever their intersection is non-empty. He observed that

(3.1) **Theorem.** The line graph of a 2 - (v, k, 1) design with $b > v$ is strongly regular.

Indeed, easy counting arguments give us the parameters:

$$n = b = \frac{v(v-1)}{k(k-1)}$$

$$a = k(r-1) = \frac{k(v-k)}{k-1}$$

$$c = (r-2) + (k-1)^2 = \frac{v-2k+1}{k-1} + (k-1)^2$$

$$d = k^2.$$

The graph is not the complete graph, since $b > v$, and not the null graph, since $r > 1$. Notice that the class of strongly regular graphs obtained in this way includes the triangular graphs: they are the line graphs of the 'pair designs' with $k = 2$. It will come as no surprise to design theorists to learn that the rationality condition gives no extra information in this

case. We shall soon see the real reason for this.

(3.1) was generalised by Bose to 'partial geometries', which we discuss in the next chapter. Here we pursue a different generalisation, due to Goethals and Seidel [56]. In an arbitrary quasi-symmetric design with intersection numbers x and y ($x < y$), define the block graph to be the graph whose vertices are the blocks, with two vertices adjacent if and only if their intersection has cardinality y .

(3.2) **Theorem.** The block graph of a quasi-symmetric design is strongly regular.

Proof. We prove this by matrix methods resembling those used for Fisher's inequality (1.5). Dr. C. Norman observed that a simple counting argument will suffice to prove (3.2); but the present proof has the advantage of giving us the multiplicities. Let N be the incidence matrix of the design, and A the adjacency matrix of its block graph. We have

$$N^T N = (r - \lambda)I + \lambda J,$$

$$N N^T = kI + yA + x(J - I - A).$$

From the first equation, j is an eigenvector of $N^T N$ with eigenvalue $r - \lambda + \lambda v = rk$; and $N^T N|_{j^\perp}$ has only the one eigenvalue $r - \lambda$. Since $j N^T = kj$ (with a different j !) it follows that j is an eigenvector of $N N^T$ with eigenvalue rk , and that $N N^T|_{j^\perp}$ has eigenvalues $r - \lambda$ (with multiplicity $v - 1$) and 0 (with multiplicity $b - v$). Since $x \neq y$, A is a linear combination of I , J , and $N N^T$, and so j is an eigenvector of A , and $A|_{j^\perp}$ has just two eigenvalues. Thus the graph is strongly regular. Its parameters can be computed from the eigenvalues and their multiplicities, as described in the last section. Notice that the multiplicities have automatically turned out to be positive integers; this is why the rationality conditions are empty. However, the expressions for the parameters and eigenvalues of the block graph do give non-trivial divisibility conditions on the design parameters. //

Goethals and Seidel went on to examine some special strongly regular graphs, to see whether they could be the block graphs of quasi-symmetric designs. Suppose Γ is the block graph of \mathcal{D} , and we know Γ . Clearly we have the parameters v and b of \mathcal{D} . The other parameters of \mathcal{D} are not determined, but from expressions for the eigenvalues of Γ we have relations connecting them, and these are sufficient in some cases. In particular,

(3.3) **Proposition.** (i) If Γ is a ladder graph then \mathcal{D} is obtained from a symmetric design by counting each block twice.

(ii) If Γ is the complement of a ladder graph then \mathcal{D} is a Hadamard 3-design.

(iii) Γ is never a lattice graph or the complement of one.

We shall prove (ii) later, using only the knowledge of b and v . A result closely related to (3.2) is

(3.4) **Proposition.** In a quasi-symmetric design (without repeated blocks),

$$b \leq \frac{1}{2}v(v-1).$$

Proof. Let $M(\epsilon_0, \epsilon_1, \epsilon_2)$ be a matrix with rows indexed by pairs of points and columns by blocks, with $(\{p_1, p_2\}, B)$ entry ϵ_i if $|\{p_1, p_2\} \cap B| = i$, for $i = 0, 1, 2$. We find that

$$\begin{aligned} M^T(0, 0, 1)M(\epsilon_0, \epsilon_1, 0) &= (y(k-y)\epsilon_1 + \binom{k-y}{2}\epsilon_0)A \\ &\quad + (x(k-x)\epsilon_1 + \binom{k-x}{2}\epsilon_0)(J - I - A). \end{aligned}$$

Suppose $b > \frac{1}{2}v(v-1)$. Then this matrix product is singular, for all choices of ϵ_0 and ϵ_1 . An eigenvector with zero eigenvalue is also an eigenvector for J and A , and is clearly not j . So if α is the corresponding eigenvalue of A , we have with $(\epsilon_0, \epsilon_1) = (0, 1)$ and $(1, 0)$ respectively,

$$\begin{aligned} y(k-y)\alpha + x(k-x)(-1-\alpha) &= 0 \\ \binom{k-y}{2}\alpha + \binom{k-x}{2}(-1-\alpha) &= 0. \end{aligned}$$

$\alpha = 0 = -1 - \alpha$ is impossible, so the determinant of these equations must be zero. But this determinant is $\frac{1}{2}(k-x)(k-y)(k-1)(x-y)$; so $k = x$ or $k = y$ or $k = 1$ or $x = y$. The first two imply that the design has repeated blocks, while the last two are impossible. //

Remark. Note how little actual information from (3.2) has been used here. We shall see a much more general result in chapter 17.

Stronger results hold in special cases. Thus

(3.5) **Proposition.** In a quasi-symmetric design \mathcal{D} with intersection numbers x and y ,

- (i) $x = 0$ implies $b \leq v(v-1)/k$;
- (ii) $x = 0, y = 1$ implies $b = v(v-1)/k(k-1)$.

Proof. We have already seen the second part. For the first suppose $x = 0$ and consider the incidence structure whose 'points' are the blocks of \mathcal{D} containing p and whose 'blocks' are the points of \mathcal{D} different from p , with incidence the dual of that in \mathcal{D} . Any two 'points' lie in $y-1$ 'blocks', and any 'block' has λ 'points', so this structure is a 2-design. Applying Fisher's inequality to it, $v-1 \geq r$, which gives the result. //

By the theorem of Petrenjuk (1.16), a 4-design satisfies $b \geq \frac{1}{2}v(v-1)$. Thus, a quasi-symmetric 4-design satisfies $b = \frac{1}{2}v(v-1)$, and is tight. In fact, we have the following result.

(3.6) **Proposition.** For a 2-design \mathcal{D} with $4 \leq k \leq v-4$, any two of the following imply the third:

- (i) \mathcal{D} is quasi-symmetric;
- (ii) \mathcal{D} is a 4-design;
- (iii) $b = \frac{1}{2}v(v-1)$.

The pair designs satisfy (i) and (ii) but not (iii) (except in a trivial sense). By (1.17), there is up to complementation a unique design satisfying (i)-(iii), namely the 4 - (23, 7, 1) design.

This 4-design provides us with several more examples of quasi-symmetric designs, and hence of strongly regular graphs. Recall the

definitions of \mathcal{D}_p , \mathcal{D}^p from chapter 1. If \mathcal{D} denotes the 4 - (23, 7, 1) design, and p and q are distinct points of \mathcal{D} , then \mathcal{D}_p , \mathcal{D}^p , \mathcal{D}_p^q and \mathcal{D}^{pq} are all quasi-symmetric. (\mathcal{D}_{pq} is in fact symmetric, being the projective plane $\text{PG}(2, 4)$.) \mathcal{D}_p achieves the bound of (3.5)(i). The blocks of \mathcal{D}_p^q (resp. \mathcal{D}^{pq}) form an equivalence class of ovals (resp. Baer subplanes) in $\text{PG}(2, 4)$, as described in Lüneburg's construction in chapter 1. The parameters of these designs and graphs are given in the following table.

Design	\mathcal{D}	\mathcal{D}_p	\mathcal{D}^p	\mathcal{D}_p^q	\mathcal{D}^{pq}
v	23	22	22	21	21
k	7	6	7	6	7
λ_1	1				
λ_3	5	1	4		
λ_2	21	5	16	4	12
λ_1	77	21	56	16	40
$\lambda_0 = n$	253	77	176	56	120
a	112	16	70	10	42
c	36	0	18	0	8
d	60	6	34	2	18
Note (1)	(2)	(3)		(4)	

Table 1

Notes: (1) These graphs are the complements of the block graphs as previously defined.

(2) This graph, together with $T(23)$, shows that the multiplicities of the eigenvalues of a strongly regular graph do not determine the parameters of the graph, even when it is known to be the block graph of a quasi-symmetric design. By contrast, (3.7) below describes a better-behaved situation.

(3) From this design, Higman and Sims [67] constructed a strongly regular graph with $n = 100$, $a = 22$, $c = 0$, $d = 6$, as follows. The vertex set is $\{\infty\} \cup \mathcal{P} \cup \mathcal{B}$, where \mathcal{P} and \mathcal{B} are the point and block sets of \mathcal{D}_p . Join ∞ to all points; join a point and a block whenever they are incident; join two blocks whenever they are disjoint. We will examine this construction in a wider context in the next chapter.

(4) This is the Gewirtz graph defined in chapter 2.

(3.7) Theorem. A quasi-symmetric design with $b = 2v - 2$ is either a Hadamard 3-design or the unique $2 - (6, 3, 2)$ design.

Proof. The eigenvalues of the block graph have multiplicities 1 , $v - 1$, $b - v = v - 2$. So (2.5) applies. Note also that $v = 2k$, $b = 4k - 2$, $r = 2k - 1$. Given a block, count the number of choices of a point in that block and another block containing that point:

$$ay + (4k - 3 - a)x = 2k(k - 1).$$

If the graph or its complement is a ladder graph, we can assume $a = n - 2$, and so

$$4(k - 1)y + x = 2k(k - 1).$$

Thus $2(k - 1)$ divides x ; since $x \leq k$ we have $x = 0$, $y = \frac{1}{2}k$. By the remarks after (2.5), \mathcal{D} is a 3-design, and so a Hadamard 3-design. Otherwise, we have $v - 1 = 2s^2 + 2s + 1$, $k = s^2 + s + 1$, $a = s(2s + 1)$, and so

$$s(2s + 1)y + (s + 1)(2s + 1)s = 2s(s + 1)(s^2 + s + 1).$$

Thus $2s + 1$ divides $2s(s + 1)(s^2 + s + 1)$, which implies $s = 1$. It is easy to show that there is a unique design with these parameters.

(3.3)(ii) is a consequence of this result. //

A result of Dembowski ([44] p. 5) asserts that a symmetric 2-design cannot be a 3-design. Suppose we consider the class of symmetric designs in which the number of blocks containing three points takes just two distinct values, say x^* and y^* . This class contains all symmetric

designs with $\lambda \leq 2$, all the projective geometries, large numbers of designs with $v = 2^{2m}$, and the complement of each of its members; so a complete determination seems difficult. But some progress can be made. Thus, for any point p , the blocks containing p and points different from p form a quasi-symmetric design \mathcal{D}^* with parameters $v^* = k$, $b^* = v - 1$, etc. From this we can show

(3.8) Proposition. A Hadamard 2-design in which any three points lie in x^* or y^* blocks is either a projective geometry over $GF(2)$ or the unique 2 - (11, 5, 2) design.

Proof. If \mathcal{D} is the complement of the given design, then \mathcal{D}^* satisfies the hypotheses of 3.7; if \mathcal{D}^* is a Hadamard 3-design for any point p it is easy to show that the original design is a projective geometry. //

Note also that if $x^* = 0$ then \mathcal{D}^* achieves the bound of (3.5)(i). Using result (1.12), we can obtain strong information about the parameters of such a design.

It can also be shown that

(3.9) Proposition. If \mathcal{D} is a symmetric design in which any 3 points lie in 0 or y^* blocks, then the same is true of the dual of \mathcal{D} .

It is not known whether this remains true when 0 is replaced by an arbitrary x^* .

4 · Partial geometries

To introduce this chapter, we prove the theorem of Chang [32] and Hoffman [68] mentioned in chapter 2. A clique in a graph is defined to be a maximal complete subgraph.

(4.1) Theorem. Let Γ be a strongly regular graph with the same parameters as $T(n)$, where $n \geq 8$. Then Γ is isomorphic to $T(n)$.

Proof. For any vertex x of Γ , $\Gamma(x)$ carries a regular graph Δ of valency $n - 2$ on $2(n - 2)$ vertices. Let $y, z \in \Gamma(x)$ be non-adjacent, and let m vertices of $\Gamma(x)$ be adjacent to y and z . Since $c = 4$, and x is adjacent to y and z , we have $m \leq 3$. There are $n - 2 - m$ vertices of $\Gamma(x)$ adjacent to y but not z , $n - 2 - m$ to z but not y , and $m - 2$ adjacent to neither; so $m \geq 2$. If $m = 3$, let w be the vertex adjacent to neither y nor z . Then every vertex of $\Gamma(x)$ adjacent to w is adjacent to y or to z , whence $n - 2 \leq 3 + 3$, contrary to assumption. So $m = 2$.

Consider the complementary graph $\bar{\Delta}$. Suppose that it contains a circuit of odd length; choose such a circuit $C = (x_0, x_1, \dots, x_k = x_0)$ with k minimal. Then there are no edges $\{x_i, x_j\}$ of $\bar{\Delta}$ with $i - j \not\equiv \pm 1 \pmod{k}$; for such an edge would divide C into two smaller circuits, one of which would have odd length. From the preceding paragraph, $k \neq 3$. Also, x_0 and x_1 are nonadjacent in Δ and have $k - 4$ common neighbours x_3, \dots, x_{k-2} there; so $k \leq 6$. We must have $k = 5$. There are $n - 5$ vertices adjacent to x_0 in $\bar{\Delta}$ (other than x_1 and x_4); these must be nonadjacent to both x_1 and x_4 . Similarly there are $n - 5$ vertices nonadjacent to x_1 and x_3 . Since x_1 is nonadjacent to $n - 4$ vertices outside C , there are at least $n - 6$ vertices outside C nonadjacent to both x_3 and x_4 . By the preceding paragraph, $n - 6 \leq 1$, a contradiction.

So $\overline{\Delta}$ contains no odd circuits, and it is bipartite. This means that Δ contains two disjoint cliques of size $n - 2$. Equivalently, any vertex in Γ lies in two 'grand cliques' of size $n - 1$, and any edge in Δ is in a unique grand clique. There are $\frac{1}{2}(n - 1)n \cdot 2/(n - 1) = n$ grand cliques, any two having at most (and hence exactly) one vertex in common. Thus the grand cliques and vertices are the points and blocks of a 2 -($n, 2, 1$) design (the pair design on n points), and Γ is its block graph; so $\Gamma \cong T(n)$. //

The theorem is in fact true under the weaker assumption $n \neq 8$. The cases $n < 8$ can be dealt with individually. For $n = 8$, there are just three exceptional graphs, discovered by Chang [33].

To study large cliques in more general strongly regular graphs, Bose [16] made the following definition.

(4.2) **Definition.** A partial geometry with parameters (r, k, t) is an incidence structure of points and lines satisfying the following conditions:

- (i) any point is incident with r lines, and any line with k points;
- (ii) two points are incident with at most one line;
- (iii) if a point p is not incident with a line L , then there are exactly t points incident with L and collinear with p .

Note that the dual of a partial geometry with parameters (r, k, t) is a partial geometry with parameters (k, r, t) .

(4.3) **Definition.** The point graph of a partial geometry has as vertices the points of the geometry, two vertices adjacent whenever they are collinear.

(4.4) **Proposition.** Let Γ be the point graph of a partial geometry with parameters (r, k, t) . Then Γ is strongly regular, with $a = r(k - 1)$, $c = (k - 2) + (r - 1)(t - 1)$, $d = rt$. //

The line graph of a partial geometry is defined dually. It is also strongly regular.

In the proof of (4.1), we showed that the points and grand cliques formed a partial geometry with parameters $(2, n - 1, 2)$. The proof of

(4. 6) below by Bose [16] uses the same idea.

(4. 5) **Definition.** A strongly regular graph is pseudo-geometric (r, k, t) if its parameters are given by $a = r(k - 1)$, $c = k - 2 + (r - 1)(t - 1)$, $d = rt$. It is geometric if it is the point graph of a partial geometry.

(4. 6) **Theorem** (Bose [16]). A pseudo-geometric graph (r, k, t) is geometric if $k > \frac{1}{2}[r(r-1) + t(r+1)(r^2 - 2r + 2)]$. //

Since a partial geometry with parameters $(n - 1, 2, 2)$ is necessarily the pair design on n points, (4.1) may be regarded as a special case of (4. 6). Another important special case is the following.

(4. 7) **Theorem** (Shrikhande [107]). A strongly regular graph with the same parameters as $L_2(n)$, for $n > 4$, is isomorphic to $L_2(n)$.

Proof. By (4. 6), such a graph is geometric. But a partial geometry $(n, 2, 1)$ is a complete bipartite graph, and so its dual $(2, n, 1)$ is necessarily an $n \times n$ square lattice. //

This theorem is true for $n \neq 4$. In the case $n = 4$, Shrikhande found that there is a unique exception. It is the graph drawn below, with opposite sides identified as shown (so it should be regarded as drawn on a torus).

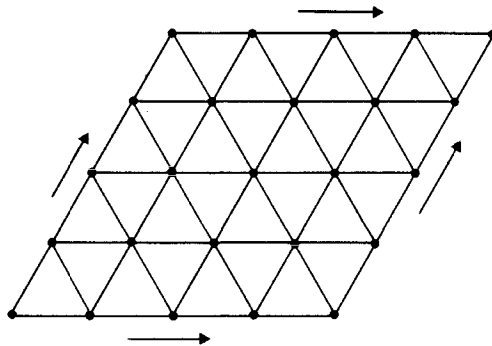


Fig. 4. 1

We will not go further into the theory of partial geometries, referring interested readers to [16] or [113]. Instead, we describe four connections with the theory of designs.

First, a triviality. A partial geometry with $t = k$ is the same thing as a $2 - (v, k, 1)$ design (with $(v - 1) = r(k - 1)$); its line graph is the block graph of the design as defined in chapter 3.

Second, we remark on two constructions of partial geometries from ovals. Let Π be a projective plane of even order n , and \underline{O} a type Π oval in Π . Then the points outside \underline{O} and secants to \underline{O} form a partial geometry with parameters $r = \frac{1}{2}(n + 2)$, $k = n - 1$, $t = \frac{1}{2}(n - 2)$. If Π is a Desarguesian, we may regard \underline{O} as a collection of 1-dimensional subspaces of the vector space $V = V(3, n)$, where n is a power of 2. Taking the elements of V as points, and the cosets of members of \underline{O} as lines, we obtain a partial geometry with $r = n + 2$, $k = n$, $t = 1$. (A partial geometry with $t = 1$ is called a generalized quadrangle.)

Third, we show how the Hall-Connor theorem can be deduced from (4.1).

(4.8) **Theorem** (Hall-Connor [61]). A quasi-residual design with $\lambda = 2$ is residual.

Proof. Let \mathcal{D} be a $2 - (v, k, 2)$ design with $v = \frac{1}{2}k(k + 1)$. We suppose $k > 6$ (the cases $k < 6$ follow from the strengthened version of (4.1) in the same way, while $k = 6$ requires separate treatment). Let B be a block of \mathcal{D} , and let n_i denote the number of blocks which intersect B in i points ($i \geq 0$). Counting as in (1.7), we find that

$$\sum n_i = \frac{1}{2}k(k + 3)$$

$$\sum i n_i = k(k + 1)$$

$$\sum i(i-1)n_i = k(k - 1).$$

$$\text{Thus } \sum (i-1)(i-2)n_i = 0,$$

whence $n_i = 0$ unless $i = 1$ or 2 . So any two blocks of \mathcal{D} meet in 1 or 2 points, and \mathcal{D} is quasi-symmetric.

Let Γ be the block graph of \mathcal{D} (where adjacency corresponds to intersection of size 1). Then Γ is strongly regular and has the same parameters as $T(k + 2)$. By (4.1), $\Gamma \cong T(k + 2)$. That is, we can label

the blocks with the 2-subsets of $X = \{1, \dots, k+2\}$ in such a way that two blocks meet in i points if and only if their labels meet in $2-i$ points for $i = 1, 2$. Now adjoin X to the point set of \mathcal{D} ; adjoin to each block its label; and let X be a new block. We obtain a symmetric design with $\lambda = 2$ whose residual (with respect to X) is \mathcal{D} . //

Using an elaboration of these ideas, Bose, Shrikhande and Singhi proved the following result.

(4.9) Theorem (Bose-Shrikhande-Singhi [19]). There is a function g defined on the natural numbers with the property that a quasi-residual design with $k > g(\lambda)$ is residual. //

Specifically, they gave

$$g(\lambda) = \begin{cases} 76 & \text{for } \lambda = 3 \\ \frac{1}{2}(\lambda - 1)(\lambda^4 - 2\lambda^2 + \lambda + 2) & \text{for } 4 \leq \lambda \leq 9 \\ \frac{1}{2}(\lambda - 1)(\lambda - 2)(M + \sqrt{M^2 + 4(\lambda - 1)}) - (\lambda - 1) & \text{for } \lambda \geq 10, \\ & \text{where } M = (\lambda - 1)(\lambda^2 - 3\lambda + 3). \end{cases}$$

Finally, a connection with Latin squares. It is known that the existence of an affine plane of order n is equivalent to that of a system of $n-1$ mutually orthogonal Latin squares of order n (see [44], p.142). The same argument shows that, more generally, the existence of a partial geometry with parameters $(r, n, r-1)$ is equivalent to that of $r-2$ orthogonal Latin squares of order n . Such a partial geometry is called a net, and its point graph is said to be of Latin square type $L_r(n)$. (This is consistent with our notation $L_2(n)$.) For example, let $V = V(2, n)$ be a 2-dimensional vector space, and S any set of 1-dimensional subspaces. Then the cosets of the members of S are the lines of a net on the point set V .

Bruck [21] proved a special case of (4.7) and used it to show that a set of 'sufficiently many' mutually orthogonal Latin squares of order n can be completed to a set of $n-1$ such squares.

We shall return to partial geometries in chapter 12.

Related classes of geometries include generalized polygons [50], semi-partial geometries [36], Moore geometries [75], and partial-geometric designs [19].

5 · Strongly regular graphs with no triangles

In a graph, a path is a sequence of vertices in which consecutive vertices are adjacent, and a circuit is a path with initial and terminal point equal. A graph is connected if any two vertices lie in a path. The function d defined by $d(p, q) = \text{length of the shortest path containing } p \text{ and } q$, is a metric in a connected graph; the diameter of the graph is the largest value assumed by d . The girth of a graph is the length of the shortest circuit which contains no repeated edges, provided such a circuit exists.

For strongly regular graphs, the connectedness, diameter and girth are simply determined by the parameters. Γ is connected with diameter 2 if $d > 0$, and is disconnected if $d = 0$. Γ has a girth provided $a > 1$; the girth is 3 if $c > 0$, 4 if $c = 0$ and $d > 1$, and 5 if $c = 0$, $d = 1$.

It is easy to see that a graph with diameter 2 and maximal valency a has at most $a^2 + 1$ vertices; and a graph with girth 5 and minimal valency a has at least $a^2 + 1$ vertices. Equality holds in either case if and only if the graph is strongly regular with $c = 0$, $d = 1$. Such a graph is called a Moore graph with diameter 2. It is worth noting that analogous bounds exist for larger values of diameter and girth, but recently Bannai and Ito [11] and Damerell [35] have shown that they are attained only by graphs consisting of a single circuit. In the diameter 2 case, however, non-trivial examples do exist.

The condition $c = 0$, $d = 1$ is so strong that the rationality condition can be expected to give useful information. Indeed it shows that $\frac{1}{2}[a^2 \pm \frac{a(a-2)}{\sqrt{4a-3}}]$ are integers. Type I occurs precisely if $a = 2$; here the pentagon is the unique graph. In type II we have $a = \frac{1}{4}(u^2 + 3)$ for some integer u which divides $\frac{1}{16}(u^2 + 3)(u^2 - 5)$; so u divides 15. $u = 1$ is not possible, so $u = 3, 5$ or 15 , $a = 3, 7$ or 57 , $n = 10, 50$ or 3250 .

This was first proved by Hoffman and Singleton [69], who went on to analyse the first two cases. If $n = 10$, $a = 3$, it is easy to see that the Petersen graph is the unique example. Hoffman and Singleton were able to show the existence and uniqueness of a graph with $n = 50$, $a = 7$. (We outline a construction and uniqueness proof in chapter 8.) The final case is too large for any complete analysis so far.

Since this case is fairly well settled, we shall exclude it and consider strongly regular graphs of girth 4. These include the complete bipartite graphs (with $c = 0$, $d = a$), which are uninteresting, so we exclude them as well and assume $c = 0$, $1 < d < a$.

(5.1) **Theorem.** Let Γ be a strongly regular graph with $c = 0$, $1 < d < a$. Let p be any vertex, and let $\mathcal{D}(\Gamma, p)$ denote the incidence structure with point set $\Gamma(p)$ and block set $\bar{\Gamma}(p)$, with a point and block incident if and only if they are adjacent in Γ . Then $\mathcal{D}(\Gamma, p)$ is a 2-design with $v = a$, $k = d$, $\lambda = k - 1$, $r = v - 1$, $b = v(v - 1)/k$, possibly having repeated blocks.

Proof. Clearly any block is incident with d points. Take two points of $\mathcal{D}(\Gamma, p)$. They are both adjacent to p , and so are not adjacent to each other, and $d - 1$ more vertices are adjacent to both, all of which must lie in $\bar{\Gamma}(p)$. The other parameters follow. //

For the remainder of this chapter, we will allow designs to have repeated blocks, and will use the design parameters v and k in place of a and d . Now we can ask: which 2-designs with $\lambda = k - 1$ are expressible as $\mathcal{D}(\Gamma, p)$ for some strongly regular graph Γ of girth 4?

The rationality conditions give us some information, though it is not as strong as in the Moore graph case. They show that

$$\frac{1}{2} \left[n - 1 \pm \frac{v(v + k - 3)}{\sqrt{(k^2 - 4k + 4v)}} \right]$$

are integers. Type I cannot occur ($d \neq c + 1$), so $k^2 - 4k + 4v$ is a square, say

$$k^2 - 4k + 4v = (k + 2s)^2$$

where s is an integer (since $k^2 - 4k + 4v \equiv k^2 \pmod{2}$), $s \geq 0$. Then

(5.2) **Proposition.** $v = (s + 1)k + s^2$, and

$$\frac{1}{2} \left[\frac{((s+1)k+s^2)((s+2)k+s^2-1)}{k} \pm \frac{((s+1)k+s^2)((s+2)k+s^2-3)}{k+2s} \right]$$

are integers.

In particular, the two terms inside the square brackets are both integers, whence k divides $s^2(s^2-1)$ and $k+2s$ divides $s(s+1)(s+2)(s+3)$. The last condition implies that $k+2s$ divides $k(k-2)(k-4)(k-6)$, so for any value of k different from 2, 4 or 6, there are only finitely many possible values of v . This was observed by Biggs [13]. For $k = 2$, 4 or 6, the rationality condition allows infinitely many values of v . For example, if $k = 2$, then $v = (s + 1)^2 + 1$, and $s + 1$ is not divisible by 4.

Having chosen a 2-design with $\lambda = k - 1$ as a potential $\mathcal{D}(\Gamma, p)$, we know all the edges of Γ except those joining distinct blocks. (Thus the problem resembles that of extending a given design.) Any block must be adjacent to $v - k$ others, and adjacent blocks must be disjoint (since the graph contains no triangles); furthermore, if two blocks are non-adjacent and have x common points, then $k - x$ blocks must be adjacent to both. Sometimes it happens that exactly $v - k$ blocks are disjoint from any given block. Then there is no choice in the construction; two blocks are adjacent if and only if they are disjoint. Two examples of this, where the resulting graph is strongly regular, are the pair design on five points, and the unique $3 - (22, 6, 1)$ design. The graphs obtained are the complement of the Clebsch graph ($n = 16$) and the Higman-Sims graph ($n = 100$) respectively. In fact, only two further examples of strongly regular graphs of girth 4 (other than complete bipartite graphs) are known. These are the graphs on 56 and 77 vertices constructed in the last chapter. The first of these is the Gewirtz graph, in which $\mathcal{D}(\Gamma, p)$ is the pair design on 10 points. In the second case, $\mathcal{D}(\Gamma, p)$ is the 4-dimensional affine symplectic geometry over $GF(2)$ (see chapter 1); two blocks are adjacent whenever they are disjoint but not parallel.

If p and q are adjacent vertices in the Higman-Sims graph Γ ,

then $\Gamma|_{\overline{\Gamma}(p)}$ and $\Gamma|_{(\overline{\Gamma}(p) \cap \overline{\Gamma}(q))}$ are the graphs on 77 and 56 vertices just described. (Similarly, if p and q are adjacent vertices in the complement of the Clebsch graph, then $\Gamma|_{\overline{\Gamma}(p)}$ is the Petersen graph, and $\Gamma|_{(\overline{\Gamma}(p) \cap \overline{\Gamma}(q))}$ is a ladder graph.) In addition, the Petersen graph can be partitioned into two pentagons, and the Higman-Sims graph into two Hoffman-Singleton graphs. (The last fact was proved by Sims [109].) We shall see later the reason for some of these facts; others, however, remain slightly mysterious.

In the situation of a strongly regular graph with girth 4, the observation that adjacent blocks are disjoint gives the following result.

(5.3) **Theorem.** Let Γ be a strongly regular graph with $a = v$, $c = 0$, $d = k$, and $1 < k < v$. Let $\mathcal{D}(\Gamma, p)$ be the 2-design of (5.1). Then

$$v \geq \frac{1}{2}[3k + 1 + (k - 1)\sqrt{4k + 1}].$$

If $v = (s + 1)k + s^2$ (as in (5.2)) then $k \leq s(s + 1)$.

Proof. By (1.7), the number of blocks disjoint from a given block is at most $\frac{v(v-1)}{k} - 1 - \frac{k(v-2)^2}{k^2 - 3k + v} = \frac{(v-k)^2(v-k-1)}{k(k^2 - 3k + v)}$; but this number is at least $v - k$. So

$$k(k^2 - 3k + v) \leq (v - k)(v - k - 1),$$

which gives the result. //

(5.3) eliminates some parameter sets satisfying the rationality condition (5.2), for example $(v, k) = (9, 4)$ or $(256, 48)$. It is worth noting that a more general result can be proved by the method. Instead of requiring that the strongly regular graph contains no triangles, it is enough to assume that it contains no configurations of shape as in Fig. 5.1.

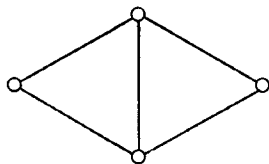


Fig. 5.1

This gives an inequality for a class of strongly regular graphs which include all those with $c \leq 1$, the point and line graphs of generalised quadrangles, and many other interesting graphs. For generalised quadrangles it gives a simple proof of an inequality due to D. G. Higman [65].

What about the case of equality? We need first a simple lemma on designs, which should be compared with (3.6).

(5.4) **Lemma.** Of the following three statements about a design \mathcal{D} with $2 < k < v - 1$,

- (i) \mathcal{D} is a 3-design,
- (ii) \mathcal{D} is a quasisymmetric 2-design with $x = 0$,
- (iii) $b = v(v - 1)/k$,

any two together imply the third, and imply also that \mathcal{D} is an extension of a symmetric 2-design (so that the conclusions of (1.12) hold).

Proof. The three statements are equivalent respectively to the following three statements about \mathcal{D}_p :

- (i) \mathcal{D}_p is a 2-design;
- (ii) the dual of \mathcal{D}_p is a 2-design;
- (iii) \mathcal{D}_p has equally many points and blocks. //

(5.5) **Theorem.** With the hypotheses of (5.3), suppose $k > 2$. Then the following are equivalent:

- (i) $\mathcal{D}(\Gamma, p)$ is a 3-design;
- (ii) $\mathcal{D}(\Gamma, p)$ is quasisymmetric;
- (iii) $\Gamma|_{\overline{\Gamma}(p)}$ is strongly regular;
- (iv) $v = \frac{1}{2}[3k + 1 + (k - 1)\sqrt{(4k + 1)}]$.

Any one of these implies that $v = s(s^2 + 3s + 1)$, $k = s(s + 1)$, and that $\Gamma|_{\overline{\Gamma}(p)}$ is the complement of the block graph of $\mathcal{D}(\Gamma, p)$.

Remark. Before proving this, we note that the condition $k \neq 2$ is essential, as the Gewirtz graph on 56 vertices shows.

Proof. By (5.4), (i) and (ii) are equivalent (since $b = v(v-1)/k$). If either holds, then (1.12) gives us rather limited possibilities for the parameters of $\mathcal{D}(\Gamma, p)$:

- (i) $v = 4y, k = 2y;$
- (ii) $v = y(y^2 + 3y + 1), k = y(y + 1);$
- (iii) $v = 112, k = 12, y = 2;$
- (iv) $v = 496, k = 40, y = 4.$

Of these, the first is excluded by (5.3), and the third and fourth fail the rationality condition (5.2). We are left with $v = y(y^2 + 3y + 1), k = y(y + 1)$, for which (iv) is easily verified.

If (iv) holds then we have equality in (5.3), and so two blocks are adjacent if and only if they are disjoint, while non-disjoint pairs of blocks have equally many common points. So (ii) and (iii) hold.

Finally, suppose (iii) holds. Then any two non-adjacent blocks are both adjacent to t further blocks, and so are adjacent to (that is, contain) $k - t$ points, for some integer t ; adjacent blocks are disjoint. Thus $\mathfrak{D}(\Gamma, p)$ is quasi-symmetric and $\Gamma|_{\bar{\Gamma}(p)}$ is the complement of its block graph. //

Remark. Much of the proof of (1.12) is concerned with establishing that, except in the Hadamard case, the number of blocks disjoint from a given block is at least $v - k$. In the situation of (5.5), this is automatically true, and the proof of (1.12) can be considerably shortened. (Indeed, the special case of (1.12) required for (5.5) was proved first.)

If Γ satisfies the hypotheses of (5.5), then $\mathfrak{D}(\Gamma, p)$ is a quasi-symmetric 3-design, and so $\mathfrak{D}(\Gamma, p)^q$ is a quasisymmetric 2-design for any point q . Thus, if p and q are adjacent vertices, $\Gamma|_{\bar{\Gamma}(p)}$ and $\Gamma|_{(\bar{\Gamma}(p) \cap \bar{\Gamma}(q))}$ are strongly regular graphs containing no triangles. The parameters of the corresponding designs are $2 - (s^2(s + 2), s^2, s^2 - 1)$ and $2 - (s(s^2 + s - 1), s(s - 1), s^2 - s - 1)$. Note also that if p and r are non-adjacent, $(\Gamma(p) \cap \bar{\Gamma}(r), \bar{\Gamma}(p) \cap \Gamma(r))$ is a symmetric 2-design with parameters $(s^2(s + 2), s(s + 1), s)$, with incidence = adjacency in Γ .

Let us exhibit one corollary of (5.5), concerning extendability of designs. (1.12) shows that the parameters of an extendable symmetric design are of one of the forms

- (i) $(4\lambda + 3, 2\lambda + 1)$ (Hadamard 2-design);
- (ii) $((\lambda + 2)(\lambda^2 + 4\lambda + 2), \lambda^2 + 3\lambda + 1, \lambda);$
- (iii) $(111, 11, 1);$

(iv) (495, 39, 3).

It is known that any Hadamard design is uniquely extendable. This is not true for the other parameter sets. Let us consider case (ii). With $\lambda = 1$, there is a unique design, namely $\text{PG}(2, 4)$, and it possesses three different (though isomorphic) extensions. With $\lambda = 2$, there are four known $2 - (56, 11, 2)$ designs, due to Gewirtz [51] (see p. 19), Hall, Lane and Wales [62], Assmus, Mezzaroba and Salwach [8] and Denniston (personal communication). Baumert and Hall (personal communication) have shown that the first of these is not extendable. The question has not to our knowledge been settled for the others. However, a weaker result is true:

(5. 6) Theorem. If a symmetric $2 - ((\lambda+2)(\lambda^2+4\lambda+2), \lambda^2+3\lambda+1, \lambda)$ design is extendable, then so is its dual.

Proof. Let \mathcal{D} be a 3-design and q a point of \mathcal{D} for which \mathcal{D}_q is isomorphic to the given symmetric design. In \mathcal{D} , exactly $v - k$ blocks are disjoint from any block, and there is a strongly regular graph Γ of girth 4 with a vertex p such that $\mathcal{D}(\Gamma, p) \cong \mathcal{D}$. Since (iv) of (5. 5) is independent of the vertex p , it follows that $\mathcal{D}(\Gamma, q)$ is also a 3-design; and it is easy to see that $\mathcal{D}(\Gamma, q)_p$ is the dual of the given symmetric design. //

The results of this section can be generalised. There is an inequality (the 'Krein bound') for arbitrary strongly regular graphs, which includes (5. 3); the case of equality is characterised by a result resembling (5. 5). These matters will be discussed in chapter 17.

If Γ is an arbitrary strongly regular graph, then $\mathcal{D}(\Gamma, p)$ is a 1-design, (provided only that $d > 0$), but it is not in general a 2-design. (The parameters are $v = a$, $b = n - a - 1$, $k = d$, $r = a - c - 1$.) Suppose $c > 0$ and $\mathcal{D}(\Gamma, p)$ is a 2-design. Then two points of $\Gamma(p)$ are adjacent to λ points of $\bar{\Gamma}(p)$, whether or not they are adjacent; so they are adjacent to $c - \lambda - 1$ or $d - \lambda - 1$ points of $\Gamma(p)$, according as they are adjacent to each other or not. Thus $\Gamma|_{\Gamma(p)}$ is strongly regular. Applying ' $a(a - c - 1) = (n - a - 1)d$ ' to it, we have $c\lambda = (a - c - 1)(d - \lambda - 1)$, whence

$$\lambda = \frac{(a - c - 1)(d - 1)}{a - 1} .$$

Thus

(5. 7) Theorem. Let Γ be strongly regular, with parameters
 (n, a, c, d) , where $c > 0$ and $d > 0$. Then $\mathfrak{D}(\Gamma, p)$ is a 2-design if
and only if $\Gamma|_{\Gamma(p)}$ is strongly regular with parameters

$$(a, c, c - d + \frac{c(d - 1)}{a - 1}, \frac{c(d - 1)}{a - 1}).$$

An example of such a graph Γ was found by Paulus and Seidel (J. J. Seidel, personal communication). Γ has parameters $(26, 10, 3, 4)$; $\Gamma|_{\Gamma(p)}$ is a Petersen graph, with parameters $(10, 3, 0, 1)$; and $\mathfrak{D}(\Gamma, p)$ is a 2 - $(10, 4, 2)$ design. Indeed, Paulus found six non-isomorphic graphs with these properties and parameters.

6 · Polarities of designs

Let Γ be a strongly regular graph in which $n = v$, $a = k$, $c = d = \lambda$. Then any two vertices are adjacent to exactly λ others. Such a graph is called a (v, k, λ) -graph (among other things). Clearly a symmetric 2 - (v, k, λ) design can be constructed from it as follows: the points and blocks are both indexed by the vertices of Γ , and a point and block are incident if and only if their labels are adjacent. This design has a further remarkable property: the correspondence between points and blocks indexed by the same vertices is a polarity with no absolute points. Not surprisingly, the existence of such a polarity is a very strong restriction on the design. The rationality condition shows that

$$\frac{1}{2}[(v-1) \pm \frac{k}{\sqrt{k-\lambda}}]$$

are integers. Putting $k - \lambda = u^2$, we see that u divides $k = \lambda + u^2$, and so u divides λ . Thus there exist only finitely many (v, k, λ) -graphs with a given value of λ . In the extremal case with $\lambda = u$ we have $k = \lambda(\lambda + 1)$, $v = \lambda^2(\lambda + 2)$. Ahrens and Szekeres [1] showed the existence of a graph with these parameters for each prime power value of λ ; indeed, their graphs are line graphs of generalised quadrangles. The smallest examples are the triangle with $\lambda = 1$, $L_2(4)$ and the Shrikhande graph (chapter 4) with $\lambda = 2$, and the point graph of the 27 lines in a general cubic surface with $\lambda = 3$.

The fact that the triangle is the only $(v, k, 1)$ graph has appeared in different guises. It is the Friendship Theorem of Erdős, Rényi and Sós [49], for which several elementary proofs (avoiding use of the rationality conditions) have recently been given. It is also the fact, due to Baer, that a polarity of a finite projective plane has absolute points. ([44] p. 152.)

A graph in which any two vertices are adjacent to λ vertices is either a (v, k, λ) graph or one of the 'windmills' of Fig. 6.1 with $\lambda = 1$.

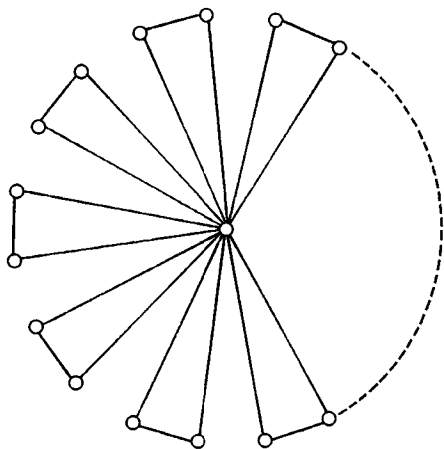


Fig. 6.1

If a symmetric $2 - (v, k, \lambda)$ design has a polarity σ with no absolute points, we can recover the (v, k, λ) graph as follows: the vertices are the points, and p and q are adjacent if $q \in p^\sigma$. (This relation is symmetric since σ is an involution, and irreflexive since σ has no absolute points; the other conditions follow from the design properties.) So the two concepts are equivalent.

Now, let Γ be a strongly regular graph in which $n = v$, $a = k - 1$, $c = \lambda - 2$, $d = \lambda$. Construct an incidence structure as follows: points and blocks are indexed by vertices, and a point and block are incident if and only if their labels are equal or adjacent. This incidence structure is a symmetric $2 - (v, k, \lambda)$ design, and the correspondence between points and blocks with the same label is again a polarity, but this time every point is absolute. (Such a polarity is called null.) Again the graph can be recovered from the design \mathcal{D} and the polarity σ . (Vertices are points of \mathcal{D} ; p and q are adjacent if $q \in p^\sigma$ but $q \neq p$.) This time the rationality condition shows that

$$\frac{1}{2}[v - 1 \pm \sqrt{\frac{v - k}{k - \lambda}}]$$

are integers. This does not give a bound for v in terms of λ .

The case $\lambda = 1$ cannot occur here, since $d = \lambda - 2$ is non-negative. This fact, clearly not peculiar to the finite case, is also a consequence of the fact that an absolute line in a projective plane carries a unique absolute point. A null polarity of a design induces a polarity of the complementary design with no point absolute; so the two cases are really the same. However, it is often convenient to separate them. Null polarities have received less attention than polarities with no absolute points. An interesting case is that with $\lambda = 2$. Here $c = \lambda - 2 = 0$, and the graphs are among those discussed in the preceding chapter, where we saw that $k = u^2 + 2$ for some integer u not divisible by 4. Examples with $u = 2$ and $u = 3$ are the Clebsch and Gewirtz graphs. Each is characterised by its parameters. Thus, $2 - (16, 6, 2)$ and $2 - (56, 11, 2)$ designs with null polarities exist and are unique. The first of these is the same one that also has polarities with no absolute points! The next result is easy to verify.

(6.1) **Theorem.** Let \mathcal{D} be a symmetric 2-design with $\lambda = 2$, and σ a null polarity of \mathcal{D} .

- (i) For any block B and any two points, $p, q \in B - \{B^\sigma\}$, p, q and B^σ 'generate' the trivial $2 - (4, 3, 2)$ design.
- (ii) σ is uniquely determined by the image of a point or block.
- (iii) Two distinct null polarities commute, and their product is a fixed-point-free involution.
- (iv) If $\sigma_1, \sigma_2, \sigma_3$ are three distinct null polarities, then $\sigma_1 \sigma_2 \sigma_3$ is a polarity with no absolute points.

It follows from a previous remark that the only non-trivial 2-design with $\lambda = 2$ admitting three distinct null polarities is the $2 - (16, 6, 2)$ design (which has 6 such polarities).

Next we give some further examples of graphs with the above properties.

Suppose H is a Hadamard matrix. We may interpret H as an incidence matrix (with, say, -1 for incidence and $+1$ for non-incidence). If H is symmetric and has a constant diagonal, we can change signs to make the first row and column consist of -1 's without affecting these properties; deleting them we obtain the incidence matrix of a Hadamard 2-design with parameters $2 - (4u^2 - 1, 2u^2 - 1, u^2 - 1)$ with a null polarity. If in addition the original H has constant row sums, then it or its negative is the incidence matrix of a 2-design with parameters $2 - (4u^2, 2u^2 \pm u, u^2 \pm u)$ with a null polarity; the sign is $+$ or $-$ according as the signs of the diagonal and the row sums agree or not. Such Hadamard matrices are quite common. Thus, one exists realising each possibility for the signs if a Hadamard matrix of order $2u$ exists. They exist for other orders, such as 36 , as well. (See [55] and [24].)

Other examples of null polarities are provided by the symplectic polarities of projective $(2m - 1)$ -space over $GF(q)$, $m \geq 2$. Also, if σ is an orthogonal polarity of projective $2m$ -space over $GF(q)$, with $m \geq 2$ and q is odd, then the absolute points and hyperplanes form a symmetric design, and σ induces a null polarity of this design. The design has the same parameters as $PG(2m - 1, q)$, but is not isomorphic with $PG(2m - 1, q)$.

Further examples when $q = 3$ arise as follows. Let Q be the quadratic form associated with σ . Since $Q(x) = Q(-x)$, Q induces a function from projective points to $GF(3)$; denote it by Q as well. If P_i is the set of points on which Q takes the value i ($i = \pm 1$), then (P_i, P_i^σ) is a symmetric design, and σ induces a polarity of it with no absolute points. The parameters of this design are

$$2 - (\tfrac{1}{2} 3^m (3^m + i), \tfrac{1}{2} 3^{m-1} (3^m - i), \tfrac{1}{2} 3^{m-1} (3^{m-1} - i)), i = \pm 1,$$

provided the sign of Q is chosen correctly.

7 · Extension of graphs

In this section we shall be considering graphs from a slightly different point of view, as incidence structures in their own right (as remarked in Chapter 2). In particular, a regular graph is a 1-design with $k = 2$, and conversely (provided we forbid repeated blocks). An interesting question is: when do such 1-designs have extensions? Since 2-designs with $k = 3$ are so common, this problem is too general, and we shall usually impose extra conditions on the extension. Extensions of designs were originally used by Witt, Hughes and Dembowski for studying transitive extensions of permutation groups, and it might be expected that extensions of regular graphs would be useful in the study of doubly transitive groups. This is indeed the case.

If we are extending a design by adding an extra point p , we know all the blocks of the extension containing p - these are obtained simply by adjoining p to all the old blocks - but it is in the blocks not containing p that possible ambiguities arise. Let us then suppose, as a first possibility, that we have a set Δ of triples, called blocks, in which the blocks not containing a point p are uniquely determined in a natural way by those containing p ; in particular let us suppose that, when we know which of $\{pqr\}$, $\{pqs\}$ and $\{prs\}$ are blocks, we can decide whether $\{qrs\}$ is a block. It is easy to see that the rule must be that, given a 4-set $\{pqrs\}$, the number of its 3-subsets which are blocks belongs to a subset S of $\{0, 1, 2, 3, 4\}$ with the property that $i, j \in S, i \neq j \Rightarrow |i - j| \geq 2$. Further analysis shows that S is a subset of one of $\{0, 2, 4\}$, $\{1, 4\}$, or $\{0, 3\}$, and that in the second or third case either Δ or its complement is the set of all triples containing a particular point, an uninteresting situation.

A set Δ of triples, with the property that an even number of the 3-subsets of any 4-set belong to Δ , was called a two-graph by G. Higman,

who first studied such sets. Two-graphs turn out to be fascinating objects, closely connected with graph theory, finite geometry, real geometry (sets of equiangular lines in Euclidean space), etc. In addition, a large number of the known finite doubly transitive groups act on two-graphs. (These include $\text{PSL}(2, q)$ for $q \equiv 1 \pmod{4}$, $\text{PSU}(3, q)$ for q odd, ${}^2G_2(q)$, $\text{Sp}(2n, 2)$ in both doubly transitive representations, $V_{2^{2n}}\text{Sp}(2n, 2)$, HS, and . 3.) Two-graphs were studied extensively by D. Taylor and J. J. Seidel, and many others contributed to the theory. For surveys, see [104], [105], [112].

Clearly a two-graph can be regarded as a map from the triples on a set into Z_2 with vanishing coboundary, that is, a 2-cocycle. Since all relevant cohomology is trivial, it is thus the coboundary of a 1-cochain, the latter being a function from pairs into Z_2 , that is, a graph; the triples of the two-graph are those carrying an odd number of edges of the graph. Two 1-cochains have the same coboundary if and only if they differ by a 1-cocycle, that is the coboundary of a 0-cochain (a function from the point set to Z_2); this means there is a partition of the point set as $X \cup Y$, and the two graphs agree within X and within Y and are complementary between these sets. In Seidel's terminology, the graphs are related by switching with respect to the partition $X \cup Y$. Thus a two-graph is equivalent to a 'switching class' of graphs. Seidel uses $(0, -, +)$ adjacency matrices for graphs (these have 0 on the diagonal, -1 for adjacency, and +1 for nonadjacency). The adjacency matrices A, A' of switching-equivalent graphs are related by $A' = DAD$, where D is a diagonal matrix with diagonal entries ± 1 . The null two-graph corresponds to the switching class of complete bipartite graphs, and the complete two-graph to that of disjoint unions of two complete graphs. These will be excluded in future.

If Δ is any set of triples on P and p is any point of P , let $\Delta(p)$ be the graph with vertex set $P - \{p\}$ and edge set $\{\{q, r\} \mid \{p, q, r\} \in \Delta\}$. It is easy to see that, if Δ is a two-graph, then the switching class corresponding to Δ contains the disjoint union of the isolated vertex p and $\Delta(p)$. (Take any graph in the class and

switch with respect to the neighbours of p .) Suppose $\Delta(p)$ is regular. $\Delta(p)$ determines Δ uniquely; when is Δ an extension of $\Delta(p)$ in the design sense, that is, when is Δ a 2-design? A two-graph which is also a 2-design is called a regular two-graph. The precise answer is:

(7.1) Theorem. A two-graph Δ is regular if and only if, for some point p , $\Delta(p)$ is strongly regular with $d = \frac{1}{2}a$. If this holds for one point, then it holds for every point.

Using this and the rationality conditions, one sees that the parameters of regular two-graphs are fairly restricted (though still general enough to include all the examples with doubly transitive automorphism groups mentioned earlier). Any strongly regular graph of Type I satisfies the condition of (7.1); if $\Delta(p)$ is the Paley graph $P(q)$ then Δ admits the doubly transitive group $\text{PSL}(2, q)$.

The construction of strongly regular graphs with the parameters of (2.5)(ii) in chapter 2 can be interpreted in terms of two-graphs. In the first step, a strongly regular graph $L_{\frac{1}{2}(q+1)}(q)$ with $d = \frac{1}{2}a$ is constructed: by (7.1), it yields a regular two-graph Δ . Next, it is shown that the switching class corresponding to Δ contains a strongly regular graph. The proof that this graph is strongly regular can be simplified by using the following result of Seidel:

(7.2) Theorem. A two-graph is regular if and only if the $(0, -, +)$ adjacency matrix of some (and hence every) graph in its switching class has just two eigenvalues.

Note that the equation $(A - \rho_1 I)(A - \rho_2 I) = 0$ is invariant under switching. Now suppose that a graph in the switching class of a regular two-graph is itself regular. Then the all-1 vector j is an eigenvector of A , and A has only two eigenvalues on j^\perp ; so the graph is in fact strongly regular. (Thus, in the above construction, it is enough to prove that the graph is regular.)

There are two possibilities for the parameters of a strongly regular graph in the switching class of a regular two-graph, depending on which of the two eigenvalues is associated with the all-1 vector j . These two possibilities may or may not occur. We give two examples.

1. A strongly regular graph on 9 vertices with $a = 4$, $c = 1$, $d = 2$ is necessarily isomorphic to $L_2(3)$. Thus, there is a unique regular two-graph with design parameters $2 - (10, 3, 4)$. Since both the Petersen graph and its complement lie in the switching class of such a two-graph, they must be equivalent under switching. (Problem: Find a switching partition.)

2. It can be shown that there is a unique strongly regular graph with parameters $(27, 10, 1, 5)$ (see [102]); so there is a unique regular two-graph with design parameters $2 - (28, 3, 10)$. The possible parameters of a strongly regular graph in its switching class are $(28, 9, 0, 4)$ and $(28, 15, 6, 10)$. The first is impossible by (5.3). The second parameter set is realised by $T(8)$ and the three exceptional Chang graphs (see chapter 4); thus, all these graphs are switching-equivalent. Indeed, the Chang graphs are most easily defined by giving switching sets of vertices in $T(8)$. The appropriate sets are

$$\begin{aligned} &\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}; \\ &\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 6\}, \{6, 7\}, \{7, 8\}, \{8, 1\}; \\ &\{1, 2\}, \{2, 3\}, \{3, 1\}, \{4, 5\}, \{5, 6\}, \{6, 7\}, \{7, 8\}, \{8, 4\}. \end{aligned}$$

Briefly, the connection with equiangular lines is as follows. Given a set of lines through a point of Euclidean space, with any two at an angle with cosine $\pm \alpha$ ($\alpha \neq 0$), the set of triples of lines for which the product of cosines is negative forms a two-graph; conversely any two-graph can be represented in this way. The 'best' known sets of equiangular lines (with most lines in space of a given dimension) often represent regular two-graphs; the theory of regular two-graphs also gives upper bounds for the number of lines. (See Lemmens and Seidel [77].)

F. Shult [108] proved the following result on transitive extensions:

(7.3) Theorem. Let Γ be a graph with a vertex-transitive automorphism group G . Suppose that, for some vertex p of Γ , there exist elements $h_1 \in \text{Aut}(\Gamma|_{\Gamma(p)})$ and $h_2 \in \text{Aut}(\Gamma|\bar{\Gamma}(p))$ such that, for $q \in \Gamma(p)$, $r \in \bar{\Gamma}(p)$, $\{q, r\} \in \Gamma \Rightarrow \{qh_1, rh_2\} \notin \Gamma$ and $\{q, r\} \notin \Gamma \Rightarrow \{qh_1, rh_2\} \in \Gamma$. Then G has a transitive extension.

Proof. If Δ is the two-graph for which $\Delta(p_0) = \Gamma$ for some vertex p_0 ; then it is easy to see that the permutation which interchanges p_0 and p and acts as h_1 on $\Gamma(p)$ and h_2 on $\bar{\Gamma}(p)$ is an automorphism of Δ . //

More generally, one could define a t -graph to be a t -cocycle over Z_2 , and a regular t -graph to be a t -graph which is also a t -design. For $t > 2$, however, examples seem to be much more limited. The only ones we know are regular 3-graphs on 8 and 12 points (the former is $AG(3, 2)$, and the latter a double extension of the Petersen graph with automorphism group M_{11} discovered by D. G. Higman) and a regular 5-graph on 12 points (the $5 - (12, 6, 1)$ design). Indeed it is trivial that any $t - (2t + 2, t + 1, 1)$ design is a regular t -graph; but only two such designs are known. Also, little machinery for studying regular t -graphs has been developed, apart from D. G. Higman's generalisation of (7.3) to t -graphs [66]. Again, one could generalise by considering cocycles over other abelian groups, but here too examples are fairly scarce and general theory is lacking.

A two-graph could be defined as a set Δ of triples such that Δ and its complement both satisfy the following condition:

(*) If $\{pqr\}, \{pqs\}, \{prs\} \in \Delta$ then $\{qrs\} \in \Delta$.

It seems that if Δ only (and not its complement) is assumed to satisfy (*), the methods used for two-graphs fail, but the structure of Δ is sufficiently restricted that some progress is possible. A useful remark is:

(7.4) **Lemma.** Let Γ be a graph on $v - 1$ vertices in which the largest complete subgraphs (cliques) have size $k - 1$, any vertex lies in λ of them, and any edge lies in at least one of them. Suppose Δ is a set of triples satisfying (*), with $\Delta(p) \cong \Gamma$ for any point p . Then there is a $2 - (v, k, \lambda)$ design D , such that Δ is the set of triples which are contained in some block of D .

The blocks are the sets S with $|S| = k$, all of whose triples belong to Δ ; these are the sets S for which $|S| - \{p\}$ is a $(k-1)$ -

clique in $\Delta(p)$ for some (and hence every) $p \in S$. Clearly two points lie in λ such blocks, and a triple is contained in a block if and only if it is in Δ . We shall say the design represents the set of triples. Note that Γ satisfies the hypothesis of (7.4) if it admits a vertex- and edge-transitive automorphism group. A few applications follow.

(7.5) Theorem. Suppose Γ is a graph, and Δ a set of triples satisfying (*) with $\Delta(p) \cong \Gamma$ for any point p .

(i) If Γ is a disjoint union of complete graphs on $k-1$ vertices, then Δ is represented by a $2-(v, k, 1)$ design, and conversely.

(ii) If Γ is a triangular graph $T(k)$, then Δ is represented by a symmetric $2-(v, k, 2)$ design satisfying the following axiom: if B is a block and $p, q, r \in B$, then the 'second blocks' through pq, qr and rp are concurrent. (Thus p, q, r generates the $2-(4, 3, 2)$ design.) The converse is also true.

(iii) If Γ is a lattice graph $L_2(m)$, then $m = 3$ and Δ is the unique regular two-graph on 10 points.

Proof. The proof of (i) is trivial. In (ii) note that for $k > 4$ the triangular graph $T(k)$ has two kinds of cliques, viz. $\{\{12\}, \{13\}, \dots, \{1k\}\}$ and $\{\{12\}, \{13\}, \{23\}\}$. The first extend to blocks, the second to point sets of $2-(4, 3, 2)$ designs. (The case $k = 4$ can be done by hand.) For (iii) we have $v = m^2 + 1$, $k = m + 1$, $\lambda = 2$; so $r = 2m$, $b = \frac{2m(m^2 + 1)}{m + 1}$, whence $m = 3$, and uniqueness is easy. //

The only known design with $k > 3$ satisfying the axiom of (7.5) (ii) is a $2-(16, 6, 2)$ design which we met in the last section; for this design, Δ is a regular two-graph! Characterising it by this axiom seems a difficult problem. We mention a weaker characterisation. Call this design \mathcal{D}_{16} for the moment.

(7.6) Theorem. If \mathcal{D} is a symmetric $2-(v, k, 2)$ design and B a block of \mathcal{D} such that any four points of B generate \mathcal{D}_{16} , then $\mathcal{D} \cong \mathcal{D}_{16}$.

This has as a consequence a result on transitive extensions, closely related to extensions of triangular graphs:

(7.7) Theorem. Let H be a permutation group of degree k inducing

a rank 3 automorphism group of $T(k)$, and G a transitive extension of this rank 3 group. Then one of the following holds:

- (i) $k = 4$, $H \cong S_4$, $G \cong \text{PSL}(2, 7)$
- (ii) $k = 5$, $H \cong A_5$, $G \cong \text{PSL}(2, 11)$
- (iii) $k = 6$, $H \cong A_6$ or S_6 , $G \cong V_{16} \cdot A_6$ or $V_{16} \cdot S_6$.

In each case G acts on a symmetric 2 - $(v, k, 2)$ design.

A similar result holds for lattice graphs:

(7.8) Theorem. Let H be a rank 3 group of automorphisms of $L_2(k)$, and G a transitive extension of H . Then $k = 3$, and $G = \text{PSL}(2, 9)$ or $\text{P}\Sigma\text{L}(2, 9)$ acts on the regular two-graph on 10 points.

See Cameron [26], [27].

8·1-factorisations of K_6

In this chapter we explore a remarkable combinatorial property of the number 6, which can be exploited to give constructions and uniqueness proofs of the projective plane of order 4, the Moore graph of valency 7, and the 5 - (12, 6, 1) Steiner system. This material is loosely based on lectures by G. Higman.

Let $A = \{a, b, c, d, e, f\}$ be a set of size 6. We regard A as the vertex set of a complete graph K_6 . A 1-factor is a set of three mutually disjoint edges (covering A), and a 1-factorisation is a partition of the set of fifteen edges of A into five 1-factors. In place of edges, 1-factors, 1-factorisations, etc. of the complete graph on A , we shall speak of edges, ..., of A .

(8.1) Proposition. There are six different 1-factorisations of A , any two isomorphic. Two disjoint 1-factors are contained in a unique 1-factorisation.

Proof. Two disjoint 1-factors together form a union of circuits of even length, hence a hexagon. A further 1-factor must include one or all of the long diagonals of the hexagon. Since there are three long diagonals, each 1-factor must include one long diagonal, and the 1-factorisation is uniquely determined (Fig. 8.1). There are 15.8 choices of two disjoint 1-factors; any 1-factorisation contains 5.4 such pairs.

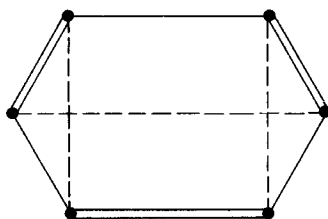


Fig. 8.1

Now consider the following structure \mathcal{D} : the points are the vertices (elements of A) and 1-factors of A ; the blocks are the edges and 1-factorisations of A . Incidence between vertices and edges, or between 1-factors and 1-factorisations, is defined by inclusion; while incidence between edges and 1-factors is reverse inclusion.

(8.2) **Proposition.** \mathcal{D} is a projective plane of order 4.

Proof. There are 21 points. $k = 5$ holds since an edge contains two vertices and is contained in three 1-factors, whereas a 1-factorisation contains five 1-factors. $\lambda = 1$ follows from a consideration of cases:

- (i) two points define a unique edge;
- (ii) given a point and a 1-factor, a unique edge of the 1-factor contains the point;
- (iii) two 1-factors either share a unique edge or lie together in a unique 1-factorisation, by (8.1). //

(8.3) **Corollary.** Any two 1-factorisations share a unique 1-factor.

Proof. Two blocks in a projective plane meet in a unique point. //

(8.4) **Corollary.** The projective plane of order 4 is unique (up to isomorphism).

Proof. Note that A is a type II oval in the plane \mathcal{D} . It can be shown that a projective plane of order 4 necessarily contains a type II oval A . Any edge of A defines a line. Given a point x outside A , the three lines on x meeting A define a 1-factor. Given a line disjoint from A , the five 1-factors defined by its points form a 1-factorisation. Thus the given plane is identified with \mathcal{D} . //

Let X be the set of 1-factorisations of A . By (8.3), 1-factors of A can be labelled with pairs of elements of X , i.e. edges of X . On edge of A lies in three 1-factors; their labels are disjoint, and so form a 1-factor of X . The five 1-factors of X corresponding in this way to the five edges through a vertex of A form a 1-factorisation. Thus we have a 'duality' between A and X : vertex \leftrightarrow 1-factorisation, edge \leftrightarrow 1-factor.

(This can also be verified by use of the dual design of \mathcal{D} .)

It is convenient to define a relation between edges of A and edges of X as follows: $ab \sim xy$ if ab is an edge in the 1-factor with label xy . This definition is self-dual (i. e. defining $xy \sim ab$ similarly, we have $xy \sim ab$ if and only if $ab \sim xy$).

We turn now to the construction of the Hoffman-Singleton graph. Suppose first that $\Gamma = M(n+1)$ is a Moore graph of valency $n+1$ and diameter 2. Let $\{\infty, 0\}$ be any edge, A the set of vertices (other than 0) joined to ∞ , and X the set of vertices (other than ∞) joined to 0. Then A and X are disjoint. Any further vertex is joined to a unique $a \in A$ and to a unique $x \in X$, and so can be labelled with the ordered pair $(a, x) \in A \times X$. It remains to describe the edges within $A \times X$. For any such edge $\{(a, x), (b, y)\}$, we must have $a \neq b$ and $x \neq y$; moreover, if (a, x) is joined to (b, y) and (c, z) , then $b \neq c$ and $y \neq z$. Thus, given $a, b \in A$, $x \in X$, there is a unique $y \in X$ such that (a, x) is joined to (b, y) . We immediately have

(i) the uniqueness of $M(3)$: for if $A = \{a, b\}$ and $X = \{x, y\}$, then $\{(a, x), (b, y)\}$ and $\{(a, y), (b, x)\}$ are edges;

(ii) the nonexistence of $M(4)$: for if $A = \{a, b, c\}$ and $X = \{x, y, z\}$, and if $\{(a, x), (b, y)\}$ is an edge, then both (a, x) and (b, y) are joined to (c, z) , yielding a triangle. (Of course, this is also a consequence of (2.4).)

Now the construction of $M(7)$ is as follows. Identify A with our original set of six vertices, and X with the set of six 1-factorisations of A . Introduce edges $\{(a, x), (b, y)\}$ whenever $ab \sim xy$. Consideration of a number of cases shows that this graph is strongly regular.

The uniqueness proof for $M(7)$ depends on the following lemma, whose proof we omit.

(8.5) Lemma. Suppose a set of ten vertices of $M(7)$ contains fourteen of the fifteen edges of $M(3)$. Then it contains the fifteenth edge also.

With the above notation, this ensures that, whenever $\{(a, x), (b, y)\}$ is an edge, as is $\{(a, y), (b, x)\}$. (Consider the ten vertices $\infty, 0, a, b, x, y, (a, x), (a, y), (b, x), (b, y)$.) Define $ab \sim xy$ if this occurs. It is straightforward to check that this relation arises from the identifica-

tion of X with the set of 1-factorisations of A as previously defined.

We turn now to the $5 - (12, 6, 1)$ design. First, a little more notation. Choose three elements $x, y, z \in X$. The three 1-factors xy, yz, zx of A are pairwise disjoint but not contained in a 1-factorisation; so the remaining six edges must form the union of two triangles. Write $abc \sim xyz$ if abc is one of these triangles. This relation is also self-dual. Now take the incidence structure with point set $A \cup X$ and blocks of the following types:

$A, X;$

$A \setminus \{a, b\} \cup \{x, y\}, X \setminus \{x, y\} \cup \{a, b\}$ whenever $ab \sim xy$;

$\{a, b, c\} \cup \{x, y, z\}$ whenever $abc \sim xyz$.

There are $132 = \binom{12}{5} / \binom{6}{5}$ blocks, and it is easily checked that any five points lie in at least one block. So we have the required design. Its uniqueness can be proved in a similar way.

It is possible to modify this construction to obtain the $5 - (24, 8, 1)$ design. Let A^* be the point set of the $5 - (12, 6, 1)$ design. The complement of any block in this design is a block. Let Ω be the set of 66 pairs of disjoint blocks, and define a graph Γ on Ω with edges $\{\{B, B'\}, \{C, C'\}\}$ whenever $|B \cap C| = 3$. (Note that two blocks of the $5 - (12, 6, 1)$ design meet in 2, 3 or 4 points.) Counting arguments show Γ is strongly regular, with the same parameters as $T(12)$. By (4.1), $\Gamma \cong T(12)$. Thus, Ω can be identified with the set of 2-element subsets of X^* , where $|X^*| = 12$. It is possible to define a $5 - (12, 6, 1)$ design on the point set X^* in such a way that a repetition of this construction leads back to A^* ; that is, we have a 'duality' between A^* and X^* . Now define a design with point set $A^* \cup X^*$, and blocks

$B \cup \{x, y\}$ where $\{B, B'\} \leftrightarrow \{x, y\}$

$Y \cup \{a, b\}$ where $\{Y, Y'\} \leftrightarrow \{a, b\}$

$\{a, b, c, d\} \cup \{x, y, z, w\}$ whenever $abcd \sim xyzw$,

for a certain relation on the quadruples of points of A^* and X^* . (The four blocks of the $5 - (12, 6, 1)$ on $\{a, b, c, d\}$ correspond to four

disjoint 2-subsets of X^* , whose complement is $\{x, y, z, w\}$.) This yields a 5 - (24, 8, 1) design.

We conclude with a group-theoretic interpretation of the duality between A and X . Any permutation of A induces naturally a permutation of the 1-factorisations of A . Thus we have an isomorphism $\theta : S_6(A) \rightarrow S_6(X)$, where $S_6(A)$ is the symmetric group on A , etc. Identifying A and X by means of any bijection, this gives an automorphism $\bar{\theta}$ of $S_6(A)$. This is not an inner automorphism, since the stabiliser of a point and the automorphism group of a 1-factorisation are not conjugate in $S_6(A)$. However, it can be shown that any subgroup of index 6 in S_6 is of one of these types, and that an automorphism preserving the conjugacy class of point stabilisers is an inner automorphism. So $|\text{Aut } S_6| = 2|S_6|$. It is known that 6 is the only cardinal number n for which S_n possesses non-inner automorphisms.

Our constructions show that S_6 is a subgroup of the automorphism groups of each of the three constructed objects; furthermore, the uniqueness proofs enable easy calculation of the orders of their full automorphism groups.

It can be shown that $ab \sim xy$ if and only if (x, y) is a cycle of the permutation $\theta(a, b)$, and that $abc \sim xyz$ if and only if (xyz) or (xzy) is a cycle of $\theta(abc)$. These facts enable some simplifications to be made in the existence and uniqueness proofs.

In similar fashion, the duality between A^* and X^* yields the existence of an outer automorphism of the Mathieu group M_{12} , the automorphism group of the (unique) 5 - (12, 6, 1) design. Since M_{24} has no outer automorphisms, the process cannot be continued!

9. Codes

In coding theory one considers a set F of q distinct symbols which is called the alphabet. In practice q is generally 2 and $F = \{0, 1\}$. In most of the theory one takes $q = p^r$ (p prime) and $F = GF(q)$.

Using the symbols of F one forms all n -tuples, i. e. F^n , and calls these n -tuples words and n the word length. If $F = GF(q)$ we shall denote the set of all words by $\mathcal{R}^{(n)}$ and interpret this as n -dimensional vector space over $GF(q)$.

In $\mathcal{R}^{(n)}$ we introduce a distance function d (called Hamming distance) which is the natural distance function to use when one is interested in the number of errors in a word that is spelled incorrectly.

(9.1) **Definition.** For $\mathbf{x} \in \mathcal{R}^{(n)}$ and $\mathbf{y} \in \mathcal{R}^{(n)}$ we denote by $d(\mathbf{x}, \mathbf{y})$ the number of coordinate places in which \mathbf{x} and \mathbf{y} differ.

The following two definitions are directly connected with d and the language of metric spaces.

(9.2) **Definition.** For $\mathbf{x} \in \mathcal{R}^{(n)}$ we define the weight $w(\mathbf{x})$ of \mathbf{x} by $w(\mathbf{x}) := d(\mathbf{x}, \mathbf{0})$.

(As usual, $\mathbf{0}$ denotes the zero-vector in $\mathcal{R}^{(n)}$.)

(9.3) **Definition.** For $\rho > 0$ and $\mathbf{x} \in \mathcal{R}^{(n)}$ we define the sphere of radius ρ with centre at \mathbf{x} by

$$S(\mathbf{x}, \rho) := \{\mathbf{y} \in \mathcal{R}^{(n)} \mid d(\mathbf{x}, \mathbf{y}) \leq \rho\}.$$

Consider a subset C of $\mathcal{R}^{(n)}$ with the property that any two distinct words of C have distance at least $2e + 1$. If we take any \mathbf{x} in C and change t coordinates, where $t \leq e$ (i. e. we make t errors), then the resulting word still resembles the original word more than any of the

others (i. e. it has a smaller distance to \mathbf{x} than to other words). Therefore, if we know C , we can correct the t errors. The purpose of coding theory is to study such e-error-correcting codes (e. g. coding, decoding, implementation). In these lectures we shall be interested in certain connections to combinatorial designs.

(9. 4) **Definition.** An e-error-correcting code C is a subset of $\mathcal{R}^{(n)}$ with the property

$$\forall \mathbf{x} \in C \forall \mathbf{y} \in C [\mathbf{x} \neq \mathbf{y} \Rightarrow d(\mathbf{x}, \mathbf{y}) \geq 2e + 1],$$

i. e.

$$\forall \mathbf{x} \in C \forall \mathbf{y} \in C [\mathbf{x} \neq \mathbf{y} \Rightarrow S(\mathbf{x}, e) \cap S(\mathbf{y}, e) = \emptyset].$$

A special type of code which is not too important in practice but of great interest to combinatorialists and group theorists (because of interesting automorphism groups) is a perfect code:

(9. 5) **Definition.** An e-error-correcting code C in $\mathcal{R}^{(n)}$ is called perfect if

$$\bigcup_{\mathbf{x} \in C} S(\mathbf{x}, e) = \mathcal{R}^{(n)}.$$

One of the more interesting types of codes is the linear code:

(9. 6) **Definition.** A k -dimensional linear subspace C of $\mathcal{R}^{(n)}$ is called a linear code or (n, k) -code over $\text{GF}(q)$.

The error-correcting capacity of a code is determined by the minimum distance between all pairs of distinct code words. For an arbitrary code consisting of K code words there are $\binom{K}{2}$ comparisons to make to find this minimum distance. For linear codes we have the following advantage:

(9. 7) **Theorem.** In a linear code the minimum distance is equal to the minimal weight among all non-zero code words.

Proof. If $\mathbf{x} \in C$, $\mathbf{y} \in C$, then $\mathbf{x} - \mathbf{y} \in C$ and $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} - \mathbf{y}, \mathbf{0}) = w(\mathbf{x} - \mathbf{y})$. //

We shall now look at two ways of describing a linear code C . The first is given by a generator matrix G which has as its rows a set of basis vectors of the linear subspace C . Since the property we are most interested in is possible error-correction and this property is not changed if in all code words we interchange two symbols (e. g. the first and second letter of each code word) we shall call two codes equivalent if one can be obtained by applying a fixed permutation of symbols to the words of the other code. With this in mind we see that for every linear code there is an equivalent code which has a generator matrix of the form

$$(9.8) \quad G = (I_k \ P)$$

where I_k is the k by k identity matrix and P is a k by $n - k$ matrix. We call this the standard form of G . If one is not interested in linearity one can extend the concept of equivalence by also allowing a permutation of the symbols of the alphabet. A code C is called systematic if there is a k -subset of the coordinate places such that to each possible k -tuple of entries in these positions there corresponds exactly one code word. Note that by (7.8) an (n, k) -code is systematic.

We now come to the second description of a linear code C .

(9.9) **Definition.** If C is a linear code of dimension k then

$$C^\perp := \{ \mathbf{x} \in \mathcal{R}^{(n)} \mid \forall \mathbf{y} \in C [(\mathbf{x}, \mathbf{y}) = 0] \},$$

(where (\mathbf{x}, \mathbf{y}) denotes the normal inner product) is called the dual code of C .

The code C^\perp is an $(n, n-k)$ -code. If H is a generator matrix for C^\perp then H is called a parity check matrix for C . In general a parity check for the code C is a vector \mathbf{x} which is orthogonal to all code words of C and we shall call any matrix H a parity check matrix if the rows of H generate the subspace C^\perp . Therefore a code C is defined by such a parity check matrix H as follows:

$$(9.10) \quad C = \{ \mathbf{x} \in \mathcal{R}^{(n)} \mid \mathbf{x}H^T = 0 \}.$$

Remark. The reader is warned that often two codes, C , C^* are called duals if C^* is equivalent to C^\perp . This often leads to confusion but it also has certain advantages.

Let us consider an important example of linear codes. Consider the lines through the origin in $AG(m, q)$ and along each of these choose a vector \mathbf{x}_i ($i = 1, 2, \dots, n := (q^m - 1)/(q - 1)$). Form the matrix H (m rows, n columns) with the \mathbf{x}_i as column vectors. Since no two columns of H are linearly dependent we see that H is a parity check matrix of a code C in which every non-zero code word \mathbf{x} has $w(\mathbf{x}) \geq 3$ (by (9.10)). Clearly, this code has dimension $n - m$. It is called the $(n, n-m)$ -Hamming code over $GF(q)$. The previous remark shows that this is a single-error-correcting code.

(9.11) **Theorem.** Hamming codes are perfect codes.

Proof. Let C be a $(n, n-m)$ -Hamming code over $GF(q)$. Then $n = (q^m - 1)/(q - 1)$. If $\mathbf{x} \in C$ then $|S(\mathbf{x}, 1)| = 1 + n(q - 1) = q^m$. Since $|C| = q^{n-m}$ and C is single-error-correcting we find that $|\cup_{\mathbf{x} \in C} S(\mathbf{x}, 1)| = q^n$, i. e. C is perfect. //

Let C be an (n, k) -code. To every word (c_1, c_2, \dots, c_n) of C we add an extra letter c_0 (say in front) such that $c_0 + c_1 + \dots + c_n = 0$. This is called an overall parity check. In this way we obtain a new linear code \bar{C} which is called the extended code corresponding to C . If H is a parity check matrix for C then

$$\bar{H} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & & & & \\ 0 & & & & \\ \vdots & & & & \\ 0 & & H & & \end{pmatrix}$$

is a parity check matrix for \bar{C} . Of course if the all-one vector (which we denote by $\mathbf{1}$) is a parity check vector for H , then the extension is trivial because $c_0 = 0$ for all words of C . However, if C is a binary code with an odd minimum distance d , then obviously the minimum distance of \bar{C} is $d + 1$.

For our first connection to the theory of designs we consider as an example the extended (8, 4)-binary-Hamming code. We have seen above that

$$\bar{H} := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

is a parity check matrix for this code. It is easily seen that the code is equivalent to a code with generator $G = (I_4 \ J_4 - I_4)$. If we make a list of the 16 words of this code we find 0, 1 and 14 words of weight 4. Now, since two words of weight 4 have distance ≥ 4 , they have at most two 1's in common. It follows that no word of weight 3 is a 'subword' of more than one code word. There are $\binom{8}{3} = 56$ words of weight 3 and each code word of weight 4 has four subwords of weight 3. We have therefore proved:

(9.12) **Theorem.** The 14 words of weight 4 in the extended (8, 4)-binary Hamming code form a 3-design with parameters $v = 8, k = 4, \lambda = 1$.

We leave it as an exercise for the reader to check that this design is the extension of $PG(2, 2)$, i. e. $AG(3, 2)$.

Besides as an example, the discussion above has served a second purpose, namely to show that it can be useful to know how many words of some fixed weight i are contained in a code C . A simple way to describe such information is given in the following definition.

(9.13) **Definition.** Let C be a code of length n and let A_i ($i = 0, 1, \dots, n$) denote the number of code words of weight i . Then

$$A(\xi, \eta) := \sum_{i=0}^n A_i \xi^i \eta^{n-i}$$

is called the weight enumerator of C .

The weight enumerators of a code C and its dual C^\perp are related. The relation is due to F. J. MacWilliams.

(9.14) **Theorem.** Let $A(\xi, \eta)$ be the weight enumerator of an (n, k) -code over $GF(q)$ and let $A^\perp(\xi, \eta)$ be the weight enumerator of the dual code. Then

$$A^\perp(\xi, \eta) = q^{-k} A(\eta - \xi, \eta + (q - 1)\xi).$$

The proof of this theorem depends on the following lemma. (We write \mathcal{R} instead of $\mathcal{R}^{(n)}$.)

(9.15) **Lemma.** Let χ be a non-trivial character on the group $(GF(q), +)$ and for any $\mathbf{v} \in \mathcal{R}$ define $\chi_{\mathbf{v}} : \mathcal{R} \rightarrow \mathbf{C}^\times$ by

$$\chi_{\mathbf{v}}(\mathbf{u}) := \chi((\mathbf{u}, \mathbf{v})).$$

If A is a vector space over \mathbf{C} , $f : \mathcal{R} \rightarrow A$, and if $g : \mathcal{R} \rightarrow A$ is defined by

$$g(\mathbf{u}) := \sum_{\mathbf{v} \in \mathcal{R}} f(\mathbf{v}) \chi_{\mathbf{v}}(\mathbf{u}),$$

then for any linear subspace $V \subset \mathcal{R}$ and the dual subspace V^\perp we have

$$\sum_{\mathbf{u} \in V} g(\mathbf{u}) = |V| \sum_{\mathbf{v} \in V^\perp} f(\mathbf{v}).$$

$$\begin{aligned} \text{Proof. } \sum_{\mathbf{u} \in V} g(\mathbf{u}) &= \sum_{\mathbf{u} \in V} \sum_{\mathbf{v} \in \mathcal{R}} f(\mathbf{v}) \chi_{\mathbf{v}}(\mathbf{u}) = \\ &= \sum_{\mathbf{v} \in \mathcal{R}} f(\mathbf{v}) \sum_{\mathbf{u} \in V} \chi((\mathbf{u}, \mathbf{v})) = \\ &= |V| \sum_{\mathbf{v} \in V^\perp} f(\mathbf{v}) + \sum_{\mathbf{v} \notin V^\perp} f(\mathbf{v}) \sum_{\mathbf{u} \in V} \chi((\mathbf{u}, \mathbf{v})). \end{aligned}$$

In the inner sum of the second term (\mathbf{u}, \mathbf{v}) takes on every value in $GF(q)$ the same number of times and since $\sum_{\alpha \in GF(q)} \chi(\alpha) = 0$ for every non-trivial character, this proves the lemma. //

Proof of (9.14). In Lemma (9.15) let A be the space of all polynomials in 2 variables ξ, η with coefficients in \mathbf{C} and let $f(\mathbf{v}) := \xi^{w(\mathbf{v})} \eta^{n-w(\mathbf{v})}$. If $a \in GF(q)$ write $w(a) := 1$ if $a \neq 0$, $w(0) := 0$.

Then we have

$$\begin{aligned}
 g(\mathbf{u}) &= \sum_{v_1 \in \text{GF}(q)} \dots \sum_{v_n \in \text{GF}(q)} \xi^{w(v_1) + \dots + w(v_n)} \eta^{(1-w(v_1)) + \dots + (1-w(v_n))} \chi(u_1 v_1 + \dots + u_n v_n) = \\
 &= \prod_{i=1}^n \left\{ \sum_{v \in \text{GF}(q)} \xi^{w(v)} \eta^{1-w(v)} \chi(u_i v) \right\}.
 \end{aligned}$$

Since the inner sum is $\eta + (q - 1)\xi$ if $u_i = 0$ and $\eta + \xi \left(\sum_{\alpha \in \text{GF}(q) \setminus \{0\}} \chi(\alpha) \right) = \eta - \xi$ if $u_i \neq 0$, we find

$$g(\mathbf{u}) = (\eta + (q - 1)\xi)^{n-w(\mathbf{u})} (\eta - \xi)^{w(\mathbf{u})}.$$

Now by the result of Lemma (9.15) we have (taking $V = C$):

$$\begin{aligned}
 \sum_{\mathbf{v} \in C^\perp} f(\mathbf{v}) &= A^\perp(\xi, \eta) = q^{-k} \sum_{\mathbf{u} \in C} g(\mathbf{u}) \\
 &= q^{-k} A(\eta - \xi, \eta + (q - 1)\xi). \quad //
 \end{aligned}$$

In Chapter 13 we shall show how this equation played a role in recent investigations on the existence of a projective plane of order 10.

For the sake of completeness we mention that generalisations of Theorem (9.14) to nonlinear codes are known (cf. [39], [87]).

We give one example of a nonlinear code constructed by using design theory. It is not difficult to show that a binary code of length 10 with minimum distance 5 can have at most 12 code words. To construct a code meeting this bound we take the rows of the incidence matrix of the 2 - (11, 5, 2) Paley design and add the all-one word $\underline{1}$ to this set. These twelve binary words then clearly have mutual distance 6. By deleting a fixed coordinate we obtain a code with the required properties.

The reader interested in nonlinear codes is referred to [86].

10 · Cyclic codes

Many of the most interesting known codes are cyclic. We define these as follows

(10.1) **Definition.** An (n, k) -code C over $\text{GF}(q)$ is called cyclic if

$$\forall (c_0, c_1, \dots, c_{n-1}) \in C [(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C].$$

From now on we make the restriction $(n, q) = 1$. Let R be the ring of all polynomials with coefficients in $\text{GF}(q)$ and let S be the ideal generated by $x^n - 1$. Clearly the residue class ring $R \bmod S$ (considered as an additive group) is isomorphic to $\mathcal{R}^{(n)}$. An isomorphism is given by $(a_0, a_1, \dots, a_{n-1}) \leftrightarrow a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ since it is obvious that the polynomials of degree $< n$ form a set of representatives for $R \bmod S$. From now on we do not distinguish between words and polynomials of degree $< n \pmod{x^n - 1}$. Note that multiplication by x in $R \bmod S$ amounts to the cyclic shift $(a_0, a_1, \dots, a_{n-1}) \mapsto (a_{n-1}, a_0, a_1, \dots, a_{n-2})$. From this it follows that a cyclic code C corresponds to an ideal (which we also denote by C) in $R \bmod S$. Every ideal in $R \bmod S$ (i.e. every cyclic code in $\mathcal{R}^{(n)}$) is generated by a polynomial $g(x)$ which divides $x^n - 1$. We shall call $g(x)$ the generator (-polynomial) of the cyclic code.

Let $g(x) = g_0 + g_1x + \dots + g_{n-d}x^{n-d}$ be the generator of a cyclic code C and let $h(x) := (x^n - 1)/g(x) = h_0 + h_1x + \dots + h_dx^d$. The words $g(x), xg(x), \dots, x^{d-1}g(x)$ form a basis of the code C , i.e.

$$(10.2) \quad G := \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_{n-d} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-d} & g_{n-d} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & g_0 & \dots & \dots & \dots & g_{n-d} \end{bmatrix}$$

is a generator matrix for C . Since $g(x)h(x) = 0$ in the ring $R \bmod S$ we see that

$$(10.3) \quad H := \begin{bmatrix} 0 & 0 & \dots & 0 & h_d & h_{d-1} & \dots & h_1 & h_0 \\ \cdot & & & & h_d & & & h_0 & 0 \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ 0 & & & & & & & & \cdot \\ h_d & \dots & \dots & \dots & h_0 & 0 & \dots & 0 \end{bmatrix}$$

is a parity check matrix for C . This gives a translation into the terminology of Chapter 9. We call $h(x)$ the check polynomial of the cyclic code C . Note that the dimension of the cyclic code is equal to the degree of the check polynomial. The code generated by $h(x)$ is the dual code of C , but with the symbols in reversed order (see remark following 9.10).

Very often cyclic codes are described, not by giving the generator $g(x)$, but by prescribing certain zeros of all code words (in a suitable extension field of $GF(q)$). Clearly this is an equivalent description because the requirement that all code words are multiples of $g(x)$ means that they are 0 in the zeros of $g(x)$. To show how simple this description can be we give an example.

Let $q = 2$, $n = 2^m - 1$ and let α be a primitive element of $(GF(2^m))$. Let $m_1(x) = (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{2^{m-1}})$ be the minimal polynomial of α . We wish to consider the cyclic code generated by $m_1(x)$. Every element of $GF(2^m)$ can be expressed uniquely as $\sum_{i=0}^{m-1} \epsilon_i \alpha^i$ where $\epsilon_i \in GF(2)$. The non-zero elements of $GF(2^m)$ are the powers α^j ($j = 0, 1, \dots, 2^m - 2$). Construct a matrix H for which the j -th column is $(\epsilon_0, \epsilon_1, \dots, \epsilon_{m-1})^T$ if $\alpha^j = \sum_{i=0}^{m-1} \epsilon_i \alpha^i$ ($j = 0, 1, \dots, 2^m - 2$). If $a := (a_0, a_1, \dots, a_{n-1})$, $a(x) := a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$, then the vector aH^T corresponds to the field element $a(\alpha)$. Therefore $aH^T = 0$ means the same thing as $m_1(x) | a(x)$. Since the columns of H are a permutation of the binary representations of $1, 2, \dots, 2^{m-1}$ we have proved:

(10.4) Theorem. The binary cyclic code of length $n = 2^m - 1$ for which the generator is the minimal polynomial of a primitive element of $\text{GF}(2^m)$ is equivalent to the $(n, n-m)$ binary Hamming code.

Example. Take $q = 2$, $n = 7$, $g(x) = 1 + x + x^3$. In this case the cyclic code C generated by $g(x)$ has dimension 4. It is equivalent to the $(7, 4)$ Hamming code which corresponds to our example following (9.11). We remark that the 7 cyclic shifts of the first row of (10.2) for this example form the incidence matrix of $\text{PG}(2, 2)$. The code consists of these 7 words, 0, and the 8 words obtained by interchanging 0 and 1. This example is connected to an interesting question linking design theory with coding theory. Suppose a Steiner triple system S (like e.g. $\text{PG}(2, 2)$ in our example) is given. Is there a linear code C over some field $\text{GF}(q)$ such that for every code word of weight 3 its nonzero positions form a block of S and all blocks of S are of this form (cf. [4])?

One easily sees that the binary Hamming codes as defined in chapter 9 have the property that the words of weight 3 represent a Steiner triple system on $2^m - 1$ points (as we saw above for $m = 3$). In fact if a Steiner triple system on n points corresponds to the set of words of weight 3 of a binary linear code C , then $n = 2^m - 1$ and C is the Hamming code and the Steiner system is $\text{PG}(m - 1, 2)$.

For the Steiner triple systems on 9 resp. 13 points the problem has been solved (cf. [48]). Let $q \equiv 1 \pmod{3}$ and let α be a primitive cube root of 1 in $\text{GF}(q)$. Define

$$H = \begin{pmatrix} 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 \\ -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then H is the parity check matrix of a $(9, 6)$ linear code over $\text{GF}(q)$ such that the nonzero positions of code words of weight 3 represent $\text{AG}(2, 3)$. We refer to [48] for a proof that the two nonisomorphic Steiner triple systems on 13 points do not arise from linear codes in this way.

In our derivation of Theorem (10.4) we have demonstrated that the requirement that all the code words have α as a zero corresponds to prescribing the parity check matrix $H := (1 \ \alpha \ \alpha^2 \ \dots \ \alpha^{n-1})$, where

we have to interpret α^j as $(\epsilon_0 \epsilon_1 \dots \epsilon_{m-1})^T$ if $\alpha^j = \sum_{i=0}^{n-1} \epsilon_i \alpha^i$.

A second useful example is obtained by replacing $m_1(x)$ by $(x+1)m_1(x)$. Clearly the new code is a subcode of the Hamming code. The requirement that 1 is a zero of all the code words means that they all have even weight, i. e. we now have the $(n, n-m-1)$ -code consisting of all the words of even weight in the $(n, n-m)$ Hamming code. In terms of parity check matrices we can say that the all-one row has been added as a parity check.

We now introduce a very important class of codes known as BCH-codes. They were discovered by R. C. Bose, D. K. Ray-Chaudhuri and A. Hocquenghem. Let β be a primitive n -th root of unity in $GF(q^m)$.

(10.5) Definition. The cyclic code in $\mathcal{R}^{(n)}$ consisting of all the words which have $\beta, \beta^2, \dots, \beta^{d-1}$ as zeros is called the BCH-code of designed distance d . If β is a primitive element of $GF(q^m)$ ($n = q^m - 1$), the code is called primitive.

The generator $g(x)$ of the code defined in (10.5) is the product of the minimal polynomials $m_i(x)$ of β^i where $i = 1, 2, \dots, d-1$, with the restriction that no factor is taken more than once.

The terminology 'designed distance' is based on the following theorem:

(10.6) **Theorem.** The minimum distance of a BCH-code of designed distance d is at least d .

Proof. We use the abbreviated notation introduced above and define the $m(d-1)$ by n matrix H over $GF(q)$ by

$$H := \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \\ 1 & \beta^2 & \beta^4 & \dots & \beta^{2n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \beta^{d-1} & \beta^{2(d-1)} & \dots & \beta^{(n-1)(d-1)} \end{pmatrix}$$

A word c is in the BCH-code iff $cH^T = 0$. If c had weight $< d$, then there would be $d-1$ columns of H which are linearly dependent over $GF(q)$. The determinant of the submatrix of H obtained by taking the

columns headed by $\xi_1 := \beta^{i_1}, \xi_2 := \beta^{i_2}, \dots, \xi_{d-1} := \beta^{i_{d-1}}$ is

$$\begin{vmatrix} \xi_1 & \xi_2 & \dots & \xi_{d-1} \\ \xi_1^2 & \xi_2^2 & \dots & \xi_{d-1}^2 \\ \dots & \dots & \dots & \dots \\ \xi_1^{d-1} & \xi_2^{d-1} & \dots & \xi_{d-1}^{d-1} \end{vmatrix} = \xi_1 \xi_2 \dots \xi_{d-1} \prod_{i > j} (\xi_i - \xi_j) \neq 0.$$

This shows that all code words $\mathbf{c} \neq 0$ indeed have weight $\geq d$.

Remark. If in (10.5) we also require 1 to be a zero of all the code words then the code has minimum distance at least $d + 1$. The proof is the same as above.

Let us now take a look at BCH-codes from the point of view of the group theorist. We consider a primitive BCH-code of length $n = q^m - 1$ over $\text{GF}(q)$ with prescribed zeros $\alpha, \alpha^2, \dots, \alpha^{d-1}$ (where α is a primitive element in $\text{GF}(q^m)$). We now denote the positions of the symbols in the code words by X_i ($i = 0, 1, \dots, n-1$) where $X_i := \alpha^i$. We extend the code by adding an overall parity check. We denote the additional position by X_∞ and make the conventions $1^\infty := 1, (\alpha^i)^\infty := 0$ for $i \not\equiv 0 \pmod{n}$. We represent the code words as $c_0 + c_1 x + \dots + c_{n-1} x^{n-1} + c_\infty x^\infty$. We shall now show that the extended code is invariant under the permutations of the affine permutation group on $\text{GF}(q^m)$ applied to the positions of the code. This group, which is denoted by $\text{AGL}(1, q^m)$, consists of the permutations

$$P_{u,v}(X) := uX + v \quad (u \in \text{GF}(q^m), v \in \text{GF}(q^m), u \neq 0).$$

It is a doubly transitive group. We first observe that $P_{\alpha,0}$ is the cyclic shift on the positions X_0, X_1, \dots, X_{n-1} and that it leaves X_∞ invariant. Therefore $P_{\alpha,0}$ transforms every extended cyclic code into itself. Now let $(c_0, c_1, \dots, c_\infty)$ be any code word in the extended BCH-code and apply $P_{u,v}$ to the positions to obtain $(c'_0, c'_1, \dots, c'_\infty)$. Then for $k = 0, 1, \dots, d-1$ we have

$$\begin{aligned}\sum_i c_i' \alpha^{ik} &= \sum_i c_i (u\alpha^i + v)^k = \sum_i c_i \sum_{l=0}^k \binom{k}{l} u^l \alpha^{il} v^{k-l} = \\ &= \sum_{l=0}^k \binom{k}{l} u^l v^{k-l} \cdot \sum_i c_i (\alpha^l)^i = 0\end{aligned}$$

because the inner sum is 0 for $l = 0, 1, \dots, d-1$. Therefore the permuted word is also in the extended code. We have proved:

(10.7) **Theorem.** Every extended primitive BCH-code of length $n+1 = q^m$ over $\text{GF}(q)$ is invariant under the affine permutation group on $\text{GF}(q^m)$.

As an application consider a primitive binary BCH-code C of length n . Let $\sum_{i=0}^n a_i \xi^i \eta^{n-i}$ be the weight enumerator of C and let $\sum_{i=0}^{n+1} A_i \xi^i \eta^{n+1-i}$ be the weight enumerator of \bar{C} . We have $A_{2i} = a_{2i-1} + a_{2i}$ and $A_{2i-1} = 0$. In \bar{C} there are a_{2i-1} words of weight $2i$ with a 1 in position X_∞ . The total weight of the code words of weight $2i$ in \bar{C} is $2iA_{2i}$. Since the extended code is invariant under a transitive permutation group the weight is equally divided among all the positions, i. e. $(n+1)a_{2i-1} = 2iA_{2i}$. A consequence is:

(10.8) **Theorem.** The minimum weight of a primitive binary BCH-code is odd.

Remark. Notice that the result of Theorem (10.8) holds for any binary code for which the extended code is invariant under a transitive permutation group.

11. Threshold decoding

There are several codes which allow a very simple error correction procedure of which the simplest example is majority decoding. We consider a linear code C .

(11.1) **Definition.** An orthogonal check set of order r on a position i of C is a set of r words of C^\perp , say $\mathbf{y}^{(1)}, \mathbf{y}^{(2)}, \dots, \mathbf{y}^{(r)}$, such that

- (i) $y_i^{(\nu)} = 1$ ($\nu = 1, 2, \dots, r$),
- (ii) if $j \neq i$ then $y_j^{(\nu)} \neq 0$ for at most one value of ν .

To show how decoding works let $i = 1$ and let \mathbf{a} be a word with $t \leq [\frac{1}{2}r]$ errors. Take an orthogonal check set $\mathbf{y}^{(1)}, \dots, \mathbf{y}^{(r)}$ on position 1. Then

$$(\mathbf{a}, \mathbf{y}^{(\nu)}) \neq 0 \text{ for } \begin{cases} \leq t \text{ values of } \nu \text{ if the symbol } a_1 \text{ is correct,} \\ \geq r - (t-1) \text{ values of } \nu \text{ if } a_1 \text{ is in error.} \end{cases}$$

Since $r - (t - 1) > t$, the majority of the values of $(\mathbf{a}, \mathbf{y}^{(\nu)})$ (zero or not zero) decides whether a_1 is correct or not. In the case of $\text{GF}(2)$ the error can immediately be corrected. The procedure is applied to every position of a code. Here we see one advantage of cyclic codes because the procedure has to be applied to one fixed position only, followed by a cyclic shift of the received word etc.

It is not difficult to generalise (11.1). Suppose that in (ii) we replace 'at most one' by 'at most λ '. Then, if there are $t \leq [\frac{r + \lambda - 1}{2\lambda}]$ errors in \mathbf{a} , we can use the set of parity checks, now called a λ -check set of order r , to correct position i . In the same way as above it is easily checked that if the number of parity checks which do not yield 0 exceeds the threshold $r - \lambda(t - 1) - \frac{1}{2}$ then position i is in error.

Of course the reader has seen the connection to combinatorial designs. Let A be the incidence matrix of a BIBD with parameters

(b, v, r, k, λ). We consider the rows of A as basis vectors of a linear code C^\perp over $GF(q)$. Then the dual C has the rows of C^\perp as parity checks and for every position i of C we can find a λ -check set of order r on position i (by the definition of BIBD). Here we encounter a problem in coding theory which has been solved for a few cases only, namely the problem of determining the dimension of C in the situation described above. This amounts to finding the rank of A over $GF(q)$ (cf. [47], [63]). If this rank is v , then C consists of 0 only which is hardly interesting! We shall return to this problem in chapter 13. We consider one example now with $q = 2$. Let A be the incidence matrix of $PG(2, 2)$,

$$A := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

In the example following (10.4) we learned that the first 4 rows of A generate the cyclic code C^\perp over $GF(2)$ which has $g(x) = 1 + x + x^3$ as generator polynomial. This implies that C , in reversed order, is generated by $(1 + x)(1 + x^2 + x^3)$. From our second example in Chapter 10 we know that the code C consists of the words of even weight in the (7, 4) Hamming code. For every position of this (cyclic!) code there are 3 rows of A which form an orthogonal check set of order 3 on that position (correcting 1 error). Of course, there is a much simpler error correction procedure for Hamming codes but this example serves as an introduction to the discussion of codes generated by projective planes.

A further generalisation should be mentioned here. Instead of using a number of parity checks to check one position we can use the same procedure to determine whether a certain subset of the positions of a word contains an error. Once this has been decided it may be possible to use other parity checks (in the same fashion) to localise the error. This is called multistep majority decoding (see Chapter 12).

We refer the reader who is interested in learning more about the topic of this chapter to Goethals [54] and Massey [90]. (Also see chapter 13.)

12 · Finite geometries and codes

The first class of codes connected to finite geometries which we shall discuss was first treated by D. F. Muller and I. S. Reed. To be able to introduce them we first need a lot of notation. We consider $AG(m, 2)$. The standard basis vectors will be called u_1, \dots, u_m (considered as column vectors). We make a list of all the points of $AG(m, 2)$ as columns of a matrix F (m rows, $n := 2^m$ columns). The order of the columns is given as follows: column j is the binary representation of the integer j ($j = 0, 1, \dots, 2^m - 1$).

If $j = \sum_{i=1}^m \xi_{ij} 2^{i-1}$ (a notation we use throughout this section), then the j -th column of F is $x_j := \sum_{i=1}^m \xi_{ij} u_i$. We need the following definition:

(12.1) Definition. $A_i := \{x_j \in AG(m, 2) \mid \xi_{ij} = 1\}$.

Note that A_i is an $(m-1)$ -dimensional affine subspace (an $(m-1)$ -flat).

(12.2) Definition. For $i = 1, 2, \dots, m$

$v_i := i$ of F , i.e. the characteristic function of A_i ;

and $v_0 := 1$, the characteristic function of $AG(m, 2)$.

(Here the rows of F are considered as words in $\mathcal{O}^{(n)}$.)

(12.3) Definition. If $a = (a_0, a_1, \dots, a_{n-1})$ and $b = (b_0, b_1, \dots, b_{n-1})$ then

$$ab := (a_0 b_0, a_1 b_1, \dots, a_{n-1} b_{n-1}).$$

Note that by (12.1), (12.2), and (12.3) the product $v_{i_1} v_{i_2} \dots v_{i_k}$ is the characteristic function of $A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}$. If the indices i_1, \dots, i_k are distinct this is an $(m-k)$ -dimensional affine subspace of

AG(m, 2). Therefore we have

$$(12.4) \text{ Theorem. } w(\mathbf{v}_1 \mathbf{v}_2 \dots \mathbf{v}_k) = 2^{m-k}.$$

(12.5) **Definition.** If $S \subset \{1, 2, \dots, m\}$ then the subset $C(S)$ of $\{0, 1, \dots, 2^m - 1\}$ is defined by

$$C(S) := \{j = \sum_{i=1}^m \xi_{ij} 2^{i-1} \mid i \notin S \Rightarrow \xi_{ij} = 0\}.$$

The standard basis vector $\mathbf{e}_j = (0, 0, \dots, 0, 1, 0, 0, \dots, 0) \in \mathbb{R}^{(n)}$, (the 1 is in position j), is the characteristic function of $\{\mathbf{x}_j\}$. We have

$$(12.6) \quad \mathbf{e}_j = \prod_{i=1}^m \{\mathbf{v}_i + (1 + \xi_{ij})\mathbf{v}_0\}.$$

Therefore each of the 2^m basisvectors of $\mathbb{R}^{(n)}$ can be written as a polynomial of degree $\leq m$ in $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m$. Therefore $\mathbb{R}^{(n)}$ is generated by the set $\{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{v}_1 \mathbf{v}_2, \dots, \mathbf{v}_1 \mathbf{v}_2 \dots \mathbf{v}_m\}$.

This set contains $1 + \binom{m}{1} + \dots + \binom{m}{m} = 2^m$ vectors, i. e. it is a basis of $\mathbb{R}^{(n)}$, i. e. we have proved:

(12.7) **Theorem.** The vectors $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_m, \mathbf{v}_1 \mathbf{v}_2, \dots, \mathbf{v}_1 \mathbf{v}_2 \dots \mathbf{v}_m$ form a basis of $\mathbb{R}^{(n)}$.

Example. $m = 4, n = 16$. Then

$$\begin{aligned} \mathbf{v}_0 &= (1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1) \\ \mathbf{v}_1 &= (0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1) \\ \mathbf{v}_2 &= (0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1) \\ \mathbf{v}_3 &= (0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1) \\ \mathbf{v}_4 &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1) \\ \mathbf{v}_1 \mathbf{v}_2 &= (0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1) \\ \mathbf{v}_1 \mathbf{v}_3 &= (0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1) \\ \mathbf{v}_1 \mathbf{v}_4 &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1) \\ \mathbf{v}_2 \mathbf{v}_3 &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1) \\ \mathbf{v}_2 \mathbf{v}_4 &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1) \\ \mathbf{v}_3 \mathbf{v}_4 &= (0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1) \end{aligned}$$

$$\begin{aligned}
\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1) \\
\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_4 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1) \\
\mathbf{v}_1 \mathbf{v}_3 \mathbf{v}_4 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1) \\
\mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_4 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1) \\
\mathbf{v}_1 \mathbf{v}_2 \mathbf{v}_3 \mathbf{v}_4 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1)
\end{aligned}$$

(12.8) **Definition.** The linear subspace of $\mathcal{R}^{(n)}$ which has as basis $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_m$ and all products $\mathbf{v}_{i_1} \dots \mathbf{v}_{i_k}$ with $k \leq r$ is called the r -th order Reed-Muller code (RM-code) of length $n = 2^m$. The 0-th order RM code has \mathbf{v}_0 as a basis. It is a repetition code of length 2^m .

Many authors prefer the following description of RM codes. Consider all polynomials of degree $\leq r$ in m variables x_1, x_2, \dots, x_m which can take values in $\text{GF}(2)$. Consider a fixed order of the points in $\text{AG}(m, 2)$. The sequence of values of a polynomial in these points is a code word of length 2^m in the RM code of order r .

Let $\mathbf{a} = \mathbf{v}_{i_1} \dots \mathbf{v}_{i_k}$ be a basis vector of the r -th order RM code and let $\mathbf{b} = \mathbf{v}_{j_1} \dots \mathbf{v}_{j_l}$ be a basis vector of the $(m-r-l)$ -st order RM code. Then \mathbf{ab} is a basis vector of the $(m-l)$ -st order RM code and by (12.4) it therefore has even weight. This implies that $(\mathbf{a}, \mathbf{b}) = 0$. The dimension of the r -th order RM code is $1 + \binom{m}{1} + \dots + \binom{m}{r}$. Since the dimension of the $(m-r-l)$ -st order RM code is $1 + \binom{m}{1} + \dots + \binom{m}{m-r-l} = \binom{m}{r+1} + \dots + \binom{m}{m}$ we have proved:

(12.9) **Theorem.** The dual of the r -th order RM code of length 2^m is the $(m-r-l)$ -st order RM code of length 2^m .

(12.10) **Corollary.** The $(m-2)$ -nd order RM code of length $n = 2^m$ is the $(n, n-m-1)$ extended Hamming code.

The following theorem establishes a connection with the previous paragraph.

(12.11) **Theorem.** Let C be the $(m-l)$ -th order RM code of length 2^m . Then the characteristic function of any l -dimensional affine subspace of $\text{AG}(m, 2)$ is a codeword of C .

Proof. Let A be an l -flat in $AG(m, 2)$ and let $f \in \mathbb{R}^{(n)}$ be the characteristic function of A . Suppose $f = \sum_{j=0}^{n-1} f_j e_j$. Then

$$(12.12) f = \sum_{k=0}^m \sum_{(i_1, i_2, \dots, i_k)} \left\{ \sum_{j \in C(i_1, i_2, \dots, i_k)} f_j \right\} v_{i_1} v_{i_2} \dots v_{i_k}$$

because by (12.6) $v_{i_1} \dots v_{i_k}$ occurs in the expansion of e_j only if $\xi_{ij} = 0$ for all $i \notin \{i_1, i_2, \dots, i_k\}$. Now $\sum_{j \in C(i_1, \dots, i_k)} f_j$ is the number of points of

A which are also in the k -dimensional linear subspace $L := \{x_j \in AG(m, 2) \mid j \in C(i_1, \dots, i_k)\}$. If $k > m-l$ then $L \cap A$ is empty or an affine subspace of dimension > 0 . In both cases $L \cap A$ has an even number of points, i.e.

$\sum_{j \in C(i_1, i_2, \dots, i_k)} f_j = 0$ if $k > m-l$. This proves that f is in the $(m-l)$ -th order RM code. //

Now we combine theorems (12.9) and (12.11). Let C be the t -th order RM code of length 2^m . We now know that every $(t+1)$ -flat in $AG(m, 2)$ provides us with a parity check equation. These $(t+1)$ -flats form a BIBD with parameters:

$$v = 2^m, \quad b = 2^{m-t-1} \frac{(2^{m-1}-1)(2^{m-2}-1) \dots (2^{m-t}-1)}{(2^{t+1}-1)(2^t-1) \dots (2-1)}, \quad k = 2^{t+1},$$

$$r = \frac{(2^{m-1}-1)(2^{m-2}-1) \dots (2^{m-t}-1)}{(2^{t+1}-1)(2^t-1) \dots (2-1)}, \quad \lambda = \frac{(2^{m-1}-1) \dots (2^{m-t}-1)}{(2^t-1) \dots (2-1)}.$$

Consider any t -flat T in $AG(m, 2)$. There are $2^{m-t} - 1$ distinct $(t+1)$ -flats containing T . Every point outside T is in exactly one of these $(t+1)$ flats. By the procedure described in Chapter 11 we can let a majority vote provide a parity check on the positions of T if there are less than 2^{m-t-1} errors. By induction one sees that in $t+1$ steps of majority decoding up to $2^{m-t-1} - 1$ errors can be corrected. Since the minimum weight in the t -th order RM code is even we have, using (12.4),

(12.13) **Theorem.** The minimum weight in the t -th order RM code of length 2^m is 2^{m-t} .

Remark. We leave it as an exercise for the reader to show that Theorem (12.13) can be proved directly by induction on m and t .

Now we take another look at groups. By definition every code word in the r -th order RM code of length 2^m is a sum of characteristic functions of affine subspaces of dimension $\geq m - r$. By Theorem (12.11) a sum of characteristic functions of affine subspaces of dimension $\geq m - r$ is a code word in the r -th order RM code. It follows that every permutation of $AG(m, 2)$ which also permutes the affine subspaces leaves all RM codes invariant. This is $AGL(m, 2)$, the group of affine transformations of $AG(m, 2)$, a triply transitive group of order $2^m \prod_{i=0}^{m-1} (2^m - 2^i)$.

(12.14) **Theorem.** Every RM code of length 2^m is invariant under all affine transformations (acting on the positions interpreted as points in $AG(m, 2)$).

Since the original definition of RM codes is more combinatorial we have chosen this way to present them here. For the sake of completeness we must mention that it was discovered later that RM codes are extended cyclic codes! To give the cyclic definition we introduce the notation $w(j)$ for the weight of the binary representation of j (interpreted as vector over $GF(2)$).

(12.15) **Theorem.** Let α be a primitive element in $GF(2^m)$. Let $g(x) := \prod^*(x - \alpha^j)$ where \prod^* is the product over all integers j in $(0, 2^m - 2]$ with $w(j) < m - r$. If C is the cyclic code of length $2^m - 1$ generated by $g(x)$, then \overline{C} is equivalent to the r -th order RM code.

We do not prove this theorem here. The proof is not difficult. The reader interested in a proof is referred to [79]. We remark that (12.13) can easily be derived from (10.6) and (12.15). The advantage of the definition (12.15) is that it can be generalised to other fields $GF(q)$.

Remark. One can show that RM codes are equivalent to extended cyclic codes by considering $AG(m, 2)$ as the field $GF(2^m)$ and then looking at the mapping $x \mapsto \alpha x$ where α is a primitive element of

$GF(2^m)$. The result follows from the fact that this is a linear mapping of order $2^m - 1$ and from Theorem (12.14). (Readers familiar with the proof of Singer's theorem will see the connection.)

The RM codes treated in this paragraph are examples of a larger class of codes known as Euclidean Geometry Codes (cf. [54]).

Closely related to these codes are the Projective Geometry Codes. We shall give only one example.

(12.16) Definition. Let p be a prime, $q = p^\alpha$, and let A be the incidence matrix of points and hyperplanes of $PG(m, q)$. The rows of A generate a code C^\perp over the alphabet $GF(p)$. The dual code C is called a projective geometry code.

It can be shown (cf. e. g. [54]) that C^\perp has dimension $1 + \binom{m+p-1}{p-1} \alpha$. An example connected to the topic of our next chapter is the case $p = \alpha = m = 2$. In this case A is the incidence matrix of $PG(2, 4)$. The code C^\perp has dimension 10. By straightforward calculation one can show that C^\perp has exactly 21 words of weight 5. This implies that a code word of C^\perp has weight 5 if and only if it is a line of $PG(2, 4)$. In other words: A can be retrieved from its linear span! Once again we have an example of a linear code for which the vectors of minimum weight ($\neq 0$) form a 2-design.

To conclude this paragraph we give one more example linking RM-codes to a familiar part of combinatorial theory.

Consider the 1^{st} -order RM code of length 2^m . By (12.9) and (12.10) this is the dual of the extended Hamming code. Also by (12.9) this code is self-orthogonal, i. e. $(a, b) = 0$ for every pair of code words. The code has dimension $m + 1$. For each code word a in this code $1 + a$ is also a code word. From each such pair we choose one word and with these we form a matrix (2^m rows, 2^m columns). If we replace 0's by -1's in this matrix the result is a Hadamard matrix!

We now consider so-called equidistant codes. These are codes with the property that any two distinct code words have the same distance d . The code treated at the end of chapter 9 is an example with $d = 6$. We treat only the binary case. If d is odd the code clearly can have

only two words. If $d = 2k$ and the code has m words of length n (where n is sufficiently large) then it is not difficult to show that $n \leq k^2 + k + 2$ or that the code is trivial. Here, a code is called trivial if the m by n matrix with the code words as rows has the property that every column has at least $m - 1$ equal entries (cf. [46]). Now, let A be the incidence matrix of $PG(2, k)$. To A we add $k - 1$ columns of ones and then we add a row of zeros. The resulting matrix has as its rows the code words of an equidistant code with $k^2 + k + 2$ words with mutual distance $d = 2k$. It is much more difficult to show that the converse is true, namely that if an equidistant code with $k^2 + k + 2$ words and mutual distance $2k$ exists, then a $PG(2, k)$ exists (cf. [81]). We remark that it has been shown that in the case that $k = 6$, i. e. $d = 12$, the maximal number of words is 32 (cf. [58]).

We now discuss a connection between coding theory and partial geometries (cf. chapter 4). At present only one partial geometry with $t = 2$ and $\min\{n, k\} > 3$ is known. It has parameters $r = k = 6$. The easiest way to describe the corresponding strongly regular graph is to take as its 81 vertices the code words of the $(5, 4)$ linear code C over $GF(3)$ defined by $c \in C \iff (c, 1) = 0$ and to join two vertices by an edge iff their Hamming distance is 2 or 5. It is not difficult to check that this graph is indeed strongly regular with parameters $(81, 30, 9, 12)$, eigenvalues 3 and -6 with multiplicities 50 and 30. To construct the partial geometry one has to pick certain 6-cliques and take these to be the lines. We do this as follows. Define $c_0 = 0$, $c_1 = (1, 2, 2, 2, 2)$, $c_2 = (2, 1, 2, 2, 2)$, $c_3 = (2, 2, 1, 2, 2)$, $c_4 = (2, 2, 2, 1, 2)$, $c_5 = (2, 2, 2, 2, 1)$. These six code words of C form a clique in the graph. We take $S := \{c_0, c_1, c_2, c_3, c_4, c_5\}$ as a line and define the remaining lines by translation, i. e. $c + S$, where $c \in C$. The essential observation in the proof that we now have a partial geometry is the fact that $\sum_{i=1}^5 c_i = 0$ is the only nontrivial linear relation involving c_1 to c_5 . Therefore all differences $c_i - c_j$ ($i \neq j$) are different. Two points x and y are collinear if there is a c and i and j such that $x = c + c_i$, $y = c + c_j$, i. e. $x - y = c_i - c_j$. It follows that two points are on at most

one line, each line has 6 points and each point is on 6 lines. By a simple counting argument we see that for a nonincident point-line pair (x, L) the average number of lines through x and meeting L is 2. It is now sufficient to take $x \notin S$ and to show that there are two points in S collinear with x . We saw above that x is collinear with c_k if $x = c_k + c_i - c_j$. If $k \neq i$ then we see that x is also collinear with c_i . If $k = i$ then $x = -c_i - c_j$ and x is collinear with c_j . There are 15 combinations $c_k + c_i - c_j$ with $k = i \neq j$ and there are 60 such combinations with i, j , and k all different. By the observation made above these 75 linear combinations are all different! Since there are 75 points $x \notin S$ the proof is complete.

For more information on this partial geometry and connections to association schemes we refer to [84].

13 · Self-orthogonal codes, designs and projective planes

The (8, 4)-extended binary Hamming code discussed in Chapter 9 coincides with its dual. This is an example of the class of r -th order RM codes of length 2^{2r+1} (see (12.10)) which are self-dual by Theorem (12.9). We now give an example of such a code over $GF(3)$.

Let S_5 be the circulant with first row $(0 \ 1 \ -1 \ -1 \ 1)$. Define G by

$$(13.1) \quad G := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & & & & & & & & & & \\ 0 & & I_5 & & & & S_5 & & & & \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \\ 0 & & & & & & & & & & \end{pmatrix},$$

and H by

$$H := \begin{pmatrix} 1 & & & & & & & & & & \\ 1 & & & & & & & & & & \\ 1 & & S_5 & & & & I_5 & & & & \\ 1 & & & & & & & & & & \\ 1 & & & & & & & & & & \end{pmatrix}.$$

Then $GH^T = 0$. Clearly the rows of G are independent and hence G is the generator matrix of an (11, 6) code C over $GF(3)$ and H is a parity check matrix for C . We remark that

$$(13.2) \quad GG^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & & & & & \\ 0 & & -J_5 & & & \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & & & \end{pmatrix}.$$

This implies that if $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5, a_6)$ then

$$\mathbf{a} G G^T \mathbf{a}^T = - \left(\sum_{i=2}^6 a_i \right)^2 \neq 1,$$

i. e. all words in C have weight $\not\equiv 1 \pmod{3}$. Clearly no code word can have weight 2 and in fact it is immediately clear that a linear combination of 2 rows of G produces a word of weight 5 or 6. This implies that a linear combination of 3 rows has weight > 3 , and since this weight cannot be 4 it must also be at least 5. Trivially a linear combination of more than 3 rows of G has weight ≥ 4 and hence ≥ 5 . This implies that the minimum weight and minimum distance are 5, i. e. the code is 2-error-correcting. Since the number of words is 3^6 and the volume of an $S(x, 2)$ is $1 + 2\binom{11}{1} + 4\binom{11}{2} = 3^5$, the code is perfect! This code is known as the ternary Golay code. The weight enumerator is easily found to be

$$(13.3) \quad \eta^{11} + 132\xi^5\eta^6 + 132\xi^6\eta^5 + 330\xi^8\eta^3 + 110\xi^9\eta^2 + 24\xi^{11}.$$

Now consider the extended code \bar{C} , a $(12, 6)$ -code over $GF(3)$. It has a generator matrix \bar{G} obtained from G in (13.1) by adding a column $(0 \ -1 \ -1 \ -1 \ -1 \ -1)^T$. By (13.2) we then have $\bar{G}\bar{G}^T = 0$, i. e. the code C is self-dual. From (13.3) we find the weight enumerator to be

$$(13.4) \quad \eta^{12} + 264\xi^6\eta^6 + 440\xi^9\eta^3 + 24\xi^{12}.$$

Remark. If we had started with \bar{C} instead of C , the proof would have been even more simple (cf. Chapter 15).

Consider two code words \mathbf{a} and \mathbf{b} in \bar{C} , both with weight 6. Let there be k positions where \mathbf{a} and \mathbf{b} both have non-zero coordinates. Then either $\mathbf{a} + \mathbf{b}$ or $\mathbf{a} - \mathbf{b}$ has weight $\leq 12 - k - \lfloor \frac{k+1}{2} \rfloor$. This implies that either $\mathbf{a} = \pm \mathbf{b}$ or $k \leq 4$. We say that a subset D of $\{1, 2, \dots, 12\}$ supports a code word \mathbf{a} in C if the non-zero coordinates occur in the positions of D . We now have the following theorem.

(13.5) **Theorem.** Let \mathcal{D} be the collection of 6-subsets of the set $S := \{1, 2, \dots, 12\}$ which support code words of weight 6 in C . Then \mathcal{D} is a 5-design with parameters $(12, 6, 1)$, i. e. a Steiner system.

Proof. We have seen above that two code words a and b are supported by sets which intersect in at most 4 points unless $a = \pm b$. Therefore (13.4) implies that there are $\frac{1}{2} \times 264 \times 6 = 792$ distinct 5-subsets of S contained in sets of the collection \mathcal{D} . Since S has $\binom{12}{5} = 792$ 5-subsets the proof is complete. //

Of course this is a well-known 5-design (cf. chapter 1). We mention it here because it motivated a search for 5-designs of this type. In chapter 15 we return to this question. The result of Theorem (13.5) is a special case of Theorem (14.13).

Our next topic is another remarkable perfect code which will give us a second construction of the Steiner system $5 - (24, 8, 1)$ (cf. chapter 1). Consider the $(8, 4)$ extended Hamming code \overline{C} as defined in the example following Theorem (10.4). Let C' be the code obtained from C by reversing the order of the symbols. One easily checks that $\overline{C} \cap C' = \{0, 1\}$. We now construct a binary linear code G_{24} of length 24 by taking as code words linear combinations of vectors $(a, 0, a)$, $(0, b, b)$, (x, x, x) , where $a \in \overline{C}$, $b \in C$, $x \in C'$. The following observations are obvious:

- (i) G_{24} is a linear code of dimension 12,
- (ii) any two basis vectors are orthogonal, i. e. G_{24} is a self-dual code,
- (iii) all basis vectors have weight divisible by 4 and therefore it follows from (ii) that this holds for all code words in G_{24} ,
- (iv) if in some code word (p, q, r) one of p, q, r is 0 then (p, q, r) is a linear combination of basis vectors with $x = 0$ or 1. Therefore the weight of this code word is the sum of the weights of two nonzero words of \overline{C} , i. e. 8, or one of p, q, r is 1 and the weight is again 8.

By combining (i) to (iv) we see that G_{24} has minimum distance 8. If we shorten G_{24} by deleting one coordinate we obtain a binary $(23, 12)$ -code with minimum distance 7. In the same way as we did above for the ternary Golay code we find that this code is perfect. This famous code is known as the binary Golay code (and G_{24} is the corresponding extended code).

Let us now look at the words of weight 8 in G_{24} . Since the Golay code is perfect its weight enumerator can be determined (the reader should check this!) and one finds that G_{24} has 759 words of weight 8. Since no two of these words have 1's in the same five positions they cover $759 \binom{8}{5} = \binom{24}{5}$ different five tuples. Hence these code words represent the blocks of a 5 - (24, 8, 1).

It was shown by Goethals (cf. [53]) that the code G_{24} can be decoded by a variation of the method discussed in chapter 11. Since G_{24} is self-dual any word is also a parity check. Consider a fixed position and take as parity checks all words of weight 8 in G_{24} with a 1 in this position. These 253 words represent on the remaining 23 positions the blocks of the derived design 4 - (23, 7, 1). Suppose that a received word has at most 4 errors. We now compute the 253 parity checks. Assume that there are 3 errors, one of which is in the fixed position. The other two errors occur together in 21 of the parity checks (cf. (1.1)) and both do not occur in 120 of the parity checks. It follows that exactly 141 of the parity checks fail. Arguing in the same way for the other cases we find the following table.

Number of errors	Number of parity checks that fail	
	fixed position in error	fixed position correct
1	253	77
2	176	112
3	141	125
4	128	128

Therefore the number of parity checks which fail tells us the number of errors and also whether the fixed position is correct or not except in the case of four errors which can be detected but not corrected. If there are more than four errors in the received word we also find one of the numbers in the table and the procedure fails.

The last topic in this chapter concerns self-dual codes associated with projective planes and related questions.

We shall show that a projective plane generates a self-dual code. A first example of a code generated by a plane was given in chapter 11.

Let A be the incidence matrix of $PG(2, n)$. We consider the subspace C of $\mathcal{R}^{(n^2+n+1)}$ over $GF(2)$ which is generated by the rows of A . If n is odd it is easy to see what the code C is. If we take the sum of the rows of A which have a 1 in a fixed position the result is a row with a 0 in that position and 1's elsewhere. These vectors generate the subspace of $\mathcal{R}^{(n^2+n+1)}$ consisting of all words of even weight and this is C (because C obviously has no words of odd weight). The case of even n is more difficult.

(13.6) Theorem. If $n \equiv 2 \pmod{4}$ then the rows of the incidence matrix A of $PG(2, n)$ generate a code C with dimension $\frac{1}{2}(n^2 + n + 2)$.

Proof. (i) Since n is even the code \overline{C} is self-orthogonal, i.e. $\overline{C} \subset (\overline{C})^\perp$. Therefore $\dim C \leq \frac{1}{2}(n^2 + n + 2)$.

(ii) Let $\dim C = r$ and let $k := n^2 + n + 1 - r = \dim C^\perp$. Let H be a parity check matrix of rank k for C and assume the coordinate places have been permuted in such a way that H has the form $(I_k \ P)$.

Define $N := \begin{pmatrix} I_k & P \\ 0 & I_r \end{pmatrix}$. Interpret A and N as rational matrices. Then $\det AN^T = \det A = (n+1)n^{\frac{1}{2}(n^2+n)}$. Since all entries in the first k columns of AN^T are even we find that $2^k \mid \det A$. It then follows that $r \geq \frac{1}{2}(n^2 + n + 2)$.

From (i) and (ii) the theorem follows. //

Remark. Theorem (13.6) can also be proved using the invariant factors of A . The method which has the advantage that it generalises to other characteristics will be illustrated in the proof of Theorem (13.12).

From (13.6) we immediately have:

(13.7) Theorem. If $n \equiv 2 \pmod{4}$ then the rows of the incidence matrix A of $PG(2, n)$ generate a code C , for which \overline{C} is self-dual.

We continue with a few other properties of the plane $PG(2, n)$, where $n \equiv 2 \pmod{4}$, interpreted in coding terms.

(13.8) Theorem. The code C of Theorem (13.6) has minimum weight $n + 1$ and every vector of minimum weight is a line in $PG(2, n)$.

Proof. Let $v \neq 0$ be a code word with $w(v) = d$. Since every line has a 1 as overall parity check we see that:

- (i) if d is odd then v meets every line at least once and
- (ii) if d is even then every line through a fixed point of v meets v in a second point.

In case (ii) we immediately have $d > n + 1$. In case (i) we find $(n + 1)d \geq n^2 + n + 1$, i. e. $d \geq n + 1$. If $w(v) = n + 1$ then there is a line l of $PG(2, n)$ which meets v in at least 3 points. If there is a point of l not on v , then every line $\neq l$ through this point meets v by (i). This would yield $d \geq n + 3$. //

In chapter 1 we gave the definition of type II oval.

(13.9) Theorem. The vectors of weight $n + 2$ in C are precisely the type II ovals of $PG(2, n)$.

Proof. (i) Let $v \in C$ and $w(v) = n + 2$. Every line meets v in an even number of points. Let l be a line and suppose v and l have $2a$ points in common. Each of the n lines $\neq l$ through one of these $2a$ points meets v at least once more. Therefore $2a + n \leq n + 2$, i. e. $a = 0$ or $a = 1$.

(ii) Let V be a type II oval. Let S be the set of $\frac{1}{2}(n+1)(n+2)$ distinct lines of $PG(2, n)$ through the pairs of points of v . Each point not in v is on $\frac{1}{2}(n+2)$ of these lines; each point of v is on $n + 1$ lines of S . Since $n \equiv 2 \pmod{4}$ it follows that v is the sum of the lines of S , i. e. $v \in C$. //

(Also see [4].)

Remark. We leave it as an interesting exercise for the reader to check that Theorem (13.9) also holds for the dual of the code generated by $PG(2, 4)$ which was treated at the end of chapter 12.

For a self-dual (n, k) code C over $GF(q)$ we find from Theorem (9.14) the following relation for the weight enumerator $A(\xi, \eta)$:

$$(13.10) A(\xi, \eta) = q^{-k} A(\eta - \xi, \eta + (q-1)\xi),$$

where $k = \frac{1}{2}n$. This means that the polynomial is invariant under the linear transformation with matrix $q^{-\frac{1}{2}} \begin{pmatrix} -1 & q-1 \\ 1 & 1 \end{pmatrix}$. If $q = 2$, all code words of C have even weight, i. e. $A(\xi, \eta)$ is invariant under the transformation $\xi \rightarrow -\xi$. The 2 transformations generate the dihedral group D_8 . It was shown by A. M. Gleason (cf. [12], [52], [89]), that the ring of polynomials in ξ and η which are invariant under this group is the free ring generated by $\xi^2 + \eta^2$ and $\xi^2 \eta^2 (\xi^2 - \eta^2)^2$.

Let us now consider a possible plane of order 10. From (13.6), (13.7) and (13.8) we know that the incidence matrix of this plane generates a code C for which \bar{C} is a $(112, 56)$ -self-dual code and that the weight enumerator $A(\xi, \eta)$ of C has coefficients $A_0 = 1, A_1 = A_2 = \dots = A_{10} = 0, A_{11} = 111$. Since all the generators of \bar{C} have weight 12 and any two words of \bar{C} have an even number of 1's in common we see that all weights in \bar{C} are divisible by 4. Therefore $A_{13} = A_{14} = 0$. By substituting this in (13.10) or by using Gleason's results one sees that $A(\xi, \eta)$ is uniquely determined if we know A_{12}, A_{15} and A_{16} . Recently F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson (cf. [88]) investigated the code words of weight 15 in C . It was assumed that the incidence matrix of the plane led to a code for which $A_{15} \neq 0$. Arguments of the same type as the ones we used in proving Theorems (13.8) and (13.9) severely restricted the possibilities. In fact it was found that the plane had to contain a particular configuration of 15 lines. A computer search showed that starting from such a configuration the plane could not be completed. Therefore we now know that if a plane of order 10 exists, then

$$(13.11) A_{15} = 0.$$

It was pointed out by A. Bruen and J. C. Fisher (cf. [22]) that this same result also follows from a computer result of R. H. F. Denniston concerning 6-arcs which are not contained in 7-arcs

(applied to the dual plane).

Remark. In this way (1.11) has been proved again.

The result (13.11) uniquely determines the weight enumerator of the code \overline{C} if we assume that the plane of order 10 is extendable, i. e. that example (iv) is possible.

Further references: [100], [8].

We now generalise Theorem (13.6). We replace the usual inner product on $\mathcal{R}^{(N+1)}$, where $N = n^2 + n + 1$, by the Minkowski inner product

$$\langle x, y \rangle := x_1 y_1 + x_2 y_2 + \dots + x_N y_N - x_{N+1} y_{N+1}.$$

(13.12) **Theorem.** Let A be the incidence matrix of a projective plane π of order n , and C the code generated by the rows of A over $\text{GF}(p)$ with a parity check adjoined. Then, if $p \nmid n$, C is self-dual relative to the Minkowski inner product.

Proof. Since $p \nmid n$ we can take the parity check -1. The rows of $(A - j)$ are orthogonal, so $C \subseteq C^\perp$. The dimension of C is equal to the p -rank $\text{rk}_p(A)$ of A (i. e. its rank regarded as a matrix over $\text{GF}(p)$). We now appeal to the theory of invariant factors, or Smith normal form (cf. Cohn [34] p. 279). There are integral matrices P and Q , invertible over \mathbb{Z} (i. e. having determinants ± 1), such that $PAQ = D$, where D is a diagonal matrix $\text{diag}(d_1, d_2, \dots, d_N)$ with $d_i \in \mathbb{Z}$, satisfying $d_i \mid d_{i+1}$ for $1 \leq i \leq N-1$. Now $\text{rk}_p(A) = \text{rk}_p(D)$ is the number of invariant factors d_i which are not divisible by p . We have

$$(\det A)^2 = \det AA^T = \det(nI + J) = (n+1)^2 n^{N-1},$$

so $\pm \det A = \det D = d_1 d_2 \dots d_N$ is exactly divisible by $p^{\frac{1}{2}(N-1)}$. Thus at most $\frac{1}{2}(N-1)$ of the invariant factors are divisible by p , i. e. $\dim C \geq \frac{1}{2}(N+1)$. Since we already know that $C \subseteq C^\perp$ we must have $C = C^\perp$. //

This construction has been generalised by Lander [76], who

showed the following.

(13.13) Theorem. Let π be a projective plane of order n with incidence matrix A . Let $N = n^2 + n + 1$, and let p be a prime such that $p^s \parallel n$ ($s > 0$). Then there is a sequence

$$\{0\} = C_{-1} \subseteq C_0 \subseteq \dots \subseteq C_s = \mathcal{R}^{(N+1)}$$

of codes of length $N + 1$ over $\text{GF}(p)$, with the following properties:

- (i) each code C_i is invariant under all automorphisms of π ;
- (ii) C_0 is the extended code generated by the rows of A ;
- (iii) for $-1 \leq i \leq s$, $C_i^\perp = C_{s-1-i}$ (relative to the Minkowski inner product);
- (iv) $\dim C_i$ is equal to the number of invariant factors of A not divisible by p^{i+1} for $i < s$;
- (v) for $0 \leq i \leq s-1$, C_i has minimum weight $n + 2$, and the words of weight $n + 2$ in C_0 correspond to lines or (possibly if $p = 2$) ovals in π .

Remarks. (i) If s is odd, we see from (iii) that $C_{\frac{1}{2}(s-1)}$ is a self-dual code associated with π .

(ii) Lander has also calculated the dimensions of the codes C_i in the case where π is Desarguesian, generalising the known result that $\dim C_0 = 1 + \binom{p+1}{2}^s$ in this case (cf. [54]).

Theorem (13.8) led to a different attempt to find a $\text{PG}(2, 10)$, involving ovals in two ways. Let A be the incidence matrix of any block design $2 - (56, 11, 2)$, (four of which are known, cf. Chapter 5). Then the rows of $G := (I_{56} \ A)$ clearly generate a $(112, 56)$ binary self-dual code C . We discuss only the case where the $2 - (56, 11, 2)$ design corresponds to the Gewirtz graph. In that case A is symmetric and therefore $(A \ I_{56})$ is also a generator matrix for C . It follows that in order to show that C has minimum weight 12 it is sufficient to consider the sum of $i \leq 6$ rows of G . Let x_j ($1 \leq j \leq 56$) be the number of ones in the i chosen rows and the j -th column of A . Then we have $\sum x_j = 11i$, $\sum \binom{x_j}{2} = 2\binom{i}{2}$. Therefore $\sum x_j(x_j - 2) = 2i^2 - 13i$, i.e. at least $13i - 2i^2$ columns have exactly one 1, which shows that the weight of the sum of the

i rows is at least $2i(7-i)$. Now this is 12 if and only if $i = 1$ (a row of G) or $i = 6$. Furthermore, if the sum of 6 rows of G is 12 then $x_j = 0$ for 20 values of j , $x_j = 1$ for 6 values of j , $x_j = 2$ for the remaining 30 columns of A . So, the 6 rows of A have the property that no point is in more than two of them, i.e. they correspond to the tangents of an oval in $2 - (56, 11, 2)$. If we are lucky then the $(112, 56)$ -code corresponds to $PG(2, 10)$. Then, we can reconstruct the plane, using Theorem (13.8), by considering the ovals of $2 - (56, 11, 2)$ through a fixed point. The other designs with the same parameters can be treated in a similar fashion. None of the known designs have produced the desired result! (Also see [8], [9], [123].)

The methods of this chapter were used recently to give a characterisation of the biplane of order 2 (cf. [2]).

(13.14) Theorem. Let \mathcal{D} be a symmetric $2 - (v, k, \lambda)$ -design with $k \equiv 0 \pmod{4}$, $\lambda \equiv 2 \pmod{4}$, $\lambda \nmid k$. Suppose \mathcal{D} has ovals and that these ovals also form a design $2 - (v, K, \Lambda)$. Then \mathcal{D} is the unique $2 - (7, 4, 2)$.

Proof. First we observe that the design formed by the type II ovals has $K = (k + \lambda)/\lambda$. Let A be the incidence matrix of \mathcal{D} and let C be the binary code generated by the rows of A . Clearly $C \subset C^\perp$. Since v is odd we have $\dim C \leq \frac{1}{2}(v-1)$. We proceed as in the proof of Theorem (13.12). Let d_1, d_2, \dots, d_v be the invariant factors of A . Then $d_1 \mid d_{i+1}$ ($1 \leq i \leq v-1$), $d_1 d_2 \dots d_v = \det A = k(k-\lambda)^{\frac{1}{2}(v-1)}$, and $d_1 d_2 \dots d_{v-1}$ is the g.c.d. of the minors of order $v-1$ of A . If we add all the rows of A we find a row with all entries k . It follows that $d_1 \dots d_{v-1}$ is a divisor of $(k-\lambda)^{\frac{1}{2}(v-1)}$. Therefore at least $\frac{1}{2}(v-1)$ of the invariant factors are odd and hence the rank of A over $GF(2)$ is at least $\frac{1}{2}(v-1)$. Since $1 \in C^\perp$ but $1 \notin C$ (all code words of C have even weight) we have proved that $\dim C = \frac{1}{2}(v-1)$ and C^\perp is the direct sum of C and 1 .

Now consider a vector of weight $d > 0$ in C^\perp . The same argument as in Theorem (13.9) shows that $d \geq (k + \lambda)/\lambda$, i.e. the ovals are vectors of minimum weight in C^\perp . Now, using the fact that the ovals also form

a design we can repeat the argument again and show that the minimum weight of C is k (which is achieved by the blocks of \mathcal{D}). Since the minimum weight of C^\perp is less than k we see that each oval has the form $1 + c$, where $c \in C$. It follows that the sum of two ovals is in C . If these two ovals meet in a points we must have $2(\frac{k + \lambda}{\lambda} - a) \geq k$. Because we know that all words in C have weight divisible by 4 we find $a = 1$ as only possibility (and hence $\lambda = 2$). This means that the design formed by the ovals of \mathcal{D} is a projective plane of order $\frac{1}{2}k$ on $v = 1 + \frac{1}{2}.k(k - 1)$ points, i. e. $k = 4$. //

14 · Quadratic residue codes

Before we can start with the actual topic of this chapter we must prove a theorem on cyclic codes (cf. Chapter 10). We use the symbol π_j to denote the permutation of $\{0, 1, \dots, n-1\}$ given by $\pi_j(k) := jk \pmod{n}$ and also to denote the automorphism of $\mathcal{R}^{(n)}$ given by $\pi_j(x^k) := x^{jk} \pmod{x^n - 1}$, where we use the identification of vectors in $\mathcal{R}^{(n)}$ and polynomials $\pmod{x^n - 1}$. We consider binary cyclic codes of length n , where n is odd.

(14.1) **Theorem.** For every ideal V in $\mathcal{R}^{(n)}$ there is a unique polynomial $c(x) \in V$, called the idempotent of V , with the following properties:

- (i) $c(x) = c^2(x)$,
- (ii) $c(x)$ generates V ,
- (iii) $\forall f(x) \in V [c(x)f(x) = f(x)]$, i. e. $c(x)$ is a unit for V ,
- (iv) if $(j, n) = 1$ then $\pi_j(c(x))$ is the idempotent of $\pi_j V$.

Proof. (i) Let $g(x)$ be the generator of V and let $g(x)h(x) = x^n - 1$ (in $\text{GF}(2)[x]$). Since $x^n - 1$ has no multiple zeros we have $(g(x), h(x)) = 1$. Therefore there are polynomials $p_1(x)$ and $p_2(x)$ such that

$$(14.2) \quad p_1(x)g(x) + p_2(x)h(x) = 1 \quad (\text{in } \text{GF}(2)[x]).$$

We multiply both sides of this equation by $c(x)$, where $c(x) := p_1(x)g(x)$. We find

$$c^2(x) + p_1(x)p_2(x)g(x)h(x) = c(x).$$

Since in $\mathcal{R}^{(n)}$ we have $g(x)h(x) = 0$, we have proved (i).

(ii) The monic polynomial of lowest degree in the ideal generated by $c(x)$ is $(c(x), x^n - 1) = (p_1(x)g(x), g(x)h(x)) = g(x)$.

(iii) By (ii) every $f(x) \in V$ is a multiple of $c(x)$. Let $f(x) = c(x)f_1(x)$. Then $c(x)f(x) = c^2(x)f_1(x) = c(x)f_1(x) = f(x)$, i. e. $c(x)$ is a unit in V .

(iv) Since π_j is an automorphism of $\mathcal{R}^{(n)}$ the polynomial $\pi_j(c(x))$ is an idempotent and also a unit in $\pi_j V$.

Since the unit is unique we have proved (iv). //

(14.3) **Example.** We consider an example in detail. Let $n = 2^m - 1$. Let $m_1(x)$ be the minimal polynomial of a primitive element α of $GF(2^m)$. Then by Theorem (10.4) $m_1(x)$ generates the Hamming code which we now denote by H_m . Let $x^n - 1 = m(x)h(x)$ in $GF(2)[x]$. We know that $h(x)$ generates the dual H_m^* of H_m (cf. Chapter 10). This code H_m^* has dimension m and hence it consists of 0 and the n cyclic shifts of the word $h(x)$. It follows that there is an exponent s such that $f(x) := x^s h(x)$ is the idempotent of H_m^* and hence (14.2) now has the form

$$p_1(x)m_1(x) + x^s h(x) = 1.$$

Clearly, the polynomial $1 + f(x)$ is the idempotent of H_m . We leave it to the reader to check that $f(x)$ has weight 2^{m-1} . E. g. if $m = 4$, $n = 15$ and $m_1(x) = x^4 + x + 1$ then

$$(x^8 + x^2 + 1)m_1(x) + x(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) = 1,$$

and

$$xh(x) = f(x) = (x + x^2 + x^4 + x^8) + (x^3 + x^6 + x^9 + x^{12}).$$

We shall need example (14.3) and proposition (14.4) below in Chapter 16.

By Theorem (14.1) (ii) we have

(14.4) **Proposition.** For every polynomial $q(x)$ the word $q(x)\{1 + f(x)\}$ is in H_m .

In the description of quadratic residue codes we shall use the following notation.

(14.5) **Notation.** (i) n is an odd prime,

(ii) α is a primitive n -th root of unity in an extension field of

$GF(q)$ (α suitably chosen later on),

(iii) R_0 denotes the set of quadratic residues mod n , R_1 denotes the set of nonzero elements of $GF(n) \setminus R_0$,

(iv) $g_0(x) := \prod_{r \in R_0} (x - \alpha^r)$, $g_1(x) := \prod_{r \in R_1} (x - \alpha^r)$ (note that $x^n - 1 = (x - 1)g_0(x)g_1(x)$).

We assume that $q^{(n-1)/2} \equiv 1 \pmod{n}$, i. e. q is a quadratic residue mod n .

The nonzero elements of $GF(n)$ are powers of a primitive element $a \in GF(n)$. Clearly a^e is a quadratic residue if $e \equiv 0 \pmod{2}$ and a non-residue if $e \equiv 1 \pmod{2}$. Since q is a quadratic residue the set R_0 is closed under multiplication by $q \pmod{n}$.

(14.6) **Definition.** The cyclic codes of length n over $GF(q)$ with generators $g_0(x)$ and $(x - 1)g_0(x)$ are both called quadratic residue codes (QR codes). The extended quadratic residue code of length $n + 1$ is obtained by annexing an overall parity check to the code with generator $g_0(x)$.

(Cf. remark following (14.10).)

In the binary case the code with generator $(x - 1)g_0(x)$ consists of the words of even weight in the code with generator $g_0(x)$. If G is a generator matrix for the first of these codes, then $\begin{pmatrix} 1 & 1 \\ G & 1 \end{pmatrix}$ is a generator matrix for the second code and the generator matrix for the extended

code is $\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & & & & \\ \vdots & G & & & \\ 0 & & & & \end{pmatrix}$ (cf. Chapter 9). Note that in the binary case the

condition that q is a quadratic residue mod n is satisfied if

$n \equiv \pm 1 \pmod{8}$. If $j \in R_1$ then the permutation π_j maps R_0 into R_1 and vice versa. It is easily seen that if we replace R_0 by R_1 in (14.6) we obtain equivalent codes in the sense of Chapter 9 (cf. [79] Theorem 3.2.2). If $n \equiv -1 \pmod{4}$ then $-1 \in R_1$ and therefore the transformation $x \mapsto x^{-1}$ maps a code word of the code with generator $g_0(x)$ into a code word of the code with generator $g_1(x)$.

(14.7) **Theorem.** If $c = c(x) = \sum_{i=0}^{n-1} c_i x^i$ is a code word of the QR code with generator $g_0(x)$, if $\sum_{i=0}^{n-1} c_i \neq 0$, and if $w(c) = d$ is the weight of this code word, then

- (i) $d^2 \geq n$,
- (ii) if $n \equiv -1 \pmod{4}$ then $d^2 - d + 1 \geq n$,
- (iii) if $n \equiv -1 \pmod{8}$ and $q = 2$ then $d \equiv 3 \pmod{4}$.

Proof. (i) Since $\sum_{i=0}^{n-1} c_i \neq 0$ the polynomial $c(x)$ is not divisible by $x - 1$. By a suitable permutation π_j we can transform $c(x)$ into a polynomial $\hat{c}(x)$ which is divisible by $g_1(x)$ and of course again not divisible by $x - 1$. This implies that $c(x)\hat{c}(x) = 1 + x + x^2 + \dots + x^{n-1}$. The number of nonzero coefficients of the left-hand side is at most d^2 . This proves (i).

(ii) Now π_j can be chosen such that $\hat{c}(x) = c(x^{-1})$ and then $c(x)\hat{c}(x)$ has at most $d^2 - d + 1$ nonzero coefficients.

(iii) Let $c(x) = \sum_{i=1}^d x^{e_i}$, $\hat{c}(x) = \sum_{i=1}^d x^{-e_i}$. If $e_i - e_j = e_k - e_l$, then $e_j - e_i = e_l - e_k$. Hence, if any terms cancel, then four at a time, i. e. $n = d^2 - d + 1 - 4a$ for some $a \geq 0$. This proves (iii). //

Now, again consider binary QR codes. We define

$$(14.8) \quad \theta(x) := \sum_{r \in R_0} x^r.$$

Clearly $\theta(x)$ is an idempotent in $\mathcal{R}^{(n)}$ (2 is a quadratic residue mod n). Hence $\{\theta(\alpha)\}^2 = \theta(\alpha)$, i. e. $\theta(\alpha) \in \text{GF}(2)$. In the same way we have $\theta(\alpha^i) = \theta(\alpha)$ if $i \in R_0$ and $\theta(\alpha^i) + \theta(\alpha) = 1$ if $i \in R_1$. We now choose α in such a way that $\theta(\alpha) = 0$. Then $\theta(\alpha^i) = 0$ if $i \in R_0$, $\theta(\alpha^i) = 1$ if $i \in R_1$ and finally $\theta(\alpha^0) = \frac{n-1}{2}$. This proves:

(14.9) **Theorem.** If α in (14.5) (ii) is suitably chosen then the polynomial $\theta(x)$ of (14.8) is the idempotent of the QR code with generator $(x-1)g_0(x)$ if $n \equiv 1 \pmod{8}$ and of the QR code with generator $g_0(x)$ if $n \equiv -1 \pmod{8}$.

Let C be the circulant with the code word θ as its first row. Define:

$$c := \begin{cases} 0 & \text{if } n \equiv 1 \pmod{8}, \\ 1 & \text{if } n \equiv -1 \pmod{8}, \end{cases}$$

and

$$G := \begin{pmatrix} 1 & 1 \\ c^T & C \end{pmatrix}.$$

It now follows from (14.9) that the rows of G (which are not independent!) generate the extended binary QR code of length $n + 1$.

Let us number the coordinate places of the code words in the extended binary QR code using the coordinates of the projective line, i. e. $\infty, 0, 1, \dots, n-1$. The position of the overall parity check is ∞ . We make the usual conventions about arithmetic operations: $\pm 0^{-1} = \infty$, $\pm \infty^{-1} = 0$, $\infty + a = \infty$ for $a \in \text{GF}(n)$. We now consider the permutations of $\text{PSL}(2, n)$ acting on the positions and show that the extended QR code remains invariant. The group is generated by the transformations $Sx := x + 1$ and $Tx := -x^{-1}$. Since S leaves ∞ invariant and it is a cyclic shift on the other positions it leaves the code invariant. It is a simple exercise to show that T maps the rows of G into linear combinations of at most 3 rows of G (cf. [79] p. 83). To most readers this is probably a familiar property of G (compare with automorphism groups of certain Hadamard matrices). We have shown:

(14.10) Theorem. The automorphism group of the extended binary QR code of length $n + 1$ contains $\text{PSL}(2, n)$.

Remark. Gleason and Prange (for a discussion cf. [3]) slightly altered the definition of extended code for the non-binary case. They require that the coordinate in the extended position is multiplied by a factor in such a way that the resulting code is self-orthogonal ($n \equiv -1 \pmod{4}$) or orthogonal to the other QR code, if extended ($n \equiv 1 \pmod{4}$). They show that (14.10) is also true for the q -ary codes.

Again, we consider an extended binary QR code. By (14.10) this code is invariant under a doubly transitive group. By the remark following (10.8) we see that the binary QR code has odd minimum weight. This allows us to apply Theorem (14.7). Thus we find:

(14.11) Theorem. The minimum weight of the binary QR code of length n with generator $g_0(x)$ is an odd number d for which

- (i) $d^2 > n$ if $n \equiv 1 \pmod{8}$,
- (ii) $d^2 - d + 1 \geq n$ if $n \equiv -1 \pmod{8}$.

Remark. The reader familiar with the theory of difference sets and designs should have no difficulty checking that the proof of (14.7) (ii) and (iii) implies that, if equality holds in (14.11) (ii), then there exists a projective plane of order $d - 1$.

A more combinatorial form of the square root bound (which is the name by which (14.11) is known) was recently found by Assmus, Mattson, and Sachar (cf. [100]). It states that if C is an $(n, \frac{n+1}{2})$ cyclic code with minimum weight d and $C^\perp \subseteq C$, and if the subsets of the positions, which support code words of minimum weight, form a 2-design, then $d^2 - d + 1 \geq n$ with equality if and only if the design is a projective plane of order $d - 1$.

We consider a very important example of QR codes.

(14.12) Example. Over $GF(2)$ we have

$$\begin{aligned} x^{23} - 1 &= (x-1)(x^{11} + x^9 + x^7 + x^6 + x^5 + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) = \\ &= (x-1)g_0(x)g_1(x). \end{aligned}$$

The binary QR code C of length 23 with generator $g_0(x)$ is a $(23, 12)$ -code. By (14.11) the minimum distance d of this code satisfies $d(d-1) \geq 22$. Since d is odd we have $d \geq 7$. In this case the volume of $S(\mathbf{x}, 3)$ is 2^{11} , i. e. $\sum_{\mathbf{x} \in C} S(\mathbf{x}, e) = 2^{23}$ or in other words: the code is perfect! Since it is known that the Golay code is unique we have found this code again (cf. chapter 13). The present representation shows that the code is cyclic.

The automorphism group of the extended binary Golay code is M_{24} , i. e. a much larger group than the one guaranteed by Theorem (14.10).

In $n \equiv -1 \pmod{4}$ then the extended binary QR code \bar{C} of length $n+1$ is self-dual. This follows from the remark preceeding (14.7) and (10.3) etc. using the form we found above for the generator matrix of \bar{C} . It can also be seen from the matrix G , defined after (14.9).

We now come to one of the most important theorems of this course. The theorem, which shows that many codes can be used to yield t -designs, is due to E. F. Assmus, Jr., and H. F. Mattson, Jr. (cf. [3]).

(14.13) **Theorem.** Let A be an (n, k) -code over $GF(q)$ and let A^\perp be the $(n, n - k)$ dual code. Let the minimum weights of these codes be d and e . Let t be an integer less than d . Let v_0 be the largest integer satisfying $v_0 - \lfloor \frac{v_0 + q - 2}{q - 1} \rfloor < d$, and w_0 the largest integer satisfying $w_0 - \lfloor \frac{w_0 + q - 2}{q - 1} \rfloor < e$, where, if $q = 2$, we take $v_0 = w_0 = n$. Suppose the number of non-0 weights of A^\perp which are less than or equal to $n - t$ itself less than or equal to $d - t$. Then, for each weight v with $d \leq v \leq v_0$, the subsets of $S := \{1, 2, \dots, n\}$ which support code words of weight d in A form a t -design. Furthermore, for each weight w with $e \leq w \leq \min\{n - t, w_0\}$, the subsets of S which support code words of weight w in A^\perp form a t -design.

Proof. In the proof we shall use the following notation. For A^\perp we write B . If T is a fixed t -subset of S and C is any code then we denote by C' the code obtained by deleting the coordinates in T from the code words of C . We denote by C_0 the subcode of C which consists of the words of C which have zeros at all the positions of T . The proof is in 6 steps.

(i) By definition of v_0 two words of A with weight $\leq v_0$ which have the same support must be scalar multiples of each other (because there exists a linear combination of these two words with weight $< d$). An analogous statement holds for B .

(ii) We shall use the following property of t -designs. Let (S, \mathcal{D}) be a t -design and let T be a t -subset of S . Denote by α_i the number of blocks D of \mathcal{D} with $|D \cap T| = i$. Then by (1.1) we have

$$\sum_{i=0}^t \binom{t}{i} \alpha_i = \binom{t}{j} \lambda_j \quad (j = 0, 1, \dots, t).$$

By solving these equations we find that α_i does not depend on the choice of the set T . The statement for $i = 0$ implies that the complements of the blocks of \mathcal{D} also form a t -design.

(iii) Consider any $d - 1$ columns of the generator matrix of A and delete these. From the definition of d it follows that the resulting matrix still has rank k .

(iv) Consider any t -subset T of S . By (iii) A' is an $(n-t, k)$ -code. Clearly $(B'_0)' \subset (A')^\perp$. The dimension of B'_0 is at least $n - k - t$. Hence $B'_0 = (A')^\perp$. Let $0 < v_1 < v_2 < \dots < v_r \leq n - t$ (where $r \leq d - t$) be the possible nonzero weights less than or equal to $n - t$ in the code B . Then these are also the only possible nonzero weights for B'_0 . Since the minimum weight of A' is at least $d - t$ we know $d - t$ coefficients of the weight enumerator of A' . This is equal to the number of coefficients of the weight enumerator of B'_0 which we do not know yet. The MacWilliams relations, i. e. Theorem (9.14), yield a system of linearly independent equations which we can solve in principle. The important observation, however, is that the solution, i. e. the weight enumerator of B'_0 , does not depend on the choice of T . Since $A' = (B'_0)^\perp$ the same holds for A' , again by Theorem (9.14).

(v) We first prove the second assertion of the theorem. Let $w \leq \min\{n - t, w_0\}$. Let \mathcal{E} be the collection of w -subsets of S which support words of weight w in B . Consider the set \mathcal{E}' of complements of sets in \mathcal{E} . For any t -subset T of S we find from (i) that the number of sets of \mathcal{E}' containing T is $\frac{1}{q-1}$ times the number of words of weight w in B'_0 . By (iv) this number does not depend on T . Hence \mathcal{E}' is a t -design. By (ii) \mathcal{E} is also a t -design.

(vi) To prove the first assertion of the theorem we start with $v = d$. Let \mathcal{D} be the collection of v -subsets of S which support words of weight v in A . In the same way as in (v) we see that the number of sets in \mathcal{D} containing a given t -subset T of S is $\frac{1}{q-1}$ times the number of words of weight $d - t$ in A' . By (iv) this number does not depend on T . We now proceed by induction. Let $d \leq v \leq v_0$ and assume that the assertion of the theorem is true for all v' with $d \leq v' < v$. Let \mathcal{D} be as before. The number of subsets of \mathcal{D} containing a given t -subset T of S is $\frac{1}{q-1}$ times the number of words of weight $v - t$ in A' corresponding to words of weight v in A . By (iv) the total number of words of weight $v - t$ in A' does not depend on T . By the induction hypothesis and (ii) the number of words of weight $v - t$ in A' corresponding to

words of weight $< v$ in A is also independent of T . Hence \mathcal{D} is a t -design. //

We shall look at several examples of this theorem.

(14.14)Example. Take $n = 8$, $k = 4$, $q = 2$ and let $A = A^\perp$ be the extended (8, 4)-Hamming code. Then $d = e = 4$. Take $t = 3$. The condition of (14.13) is satisfied. Taking $v = 4$, we find the result of Theorem (9.12).

(14.15)Example. Take $n = 12$, $k = 6$, $q = 3$ and let $A = A^\perp$ be the extended ternary Golay code. Then $d = e = 6$ (cf. (13.14)). By (13.4) the condition of (14.13) is satisfied for $t = 5$. We now find the result of Theorem (13.5).

(14.16)Example. Let A be a $(12l, 6l)$ -self-dual code over $GF(3)$. Suppose $d > 3l$. Take $t = 5$. Since all weights in A are divisible by 3 the condition of the theorem is satisfied. Taking $v = d$ we find that the supports of the minimum weight words of A form a 5-design.

(14.17)Example. Take $n = 24$, $k = 12$, $q = 2$ and let $A = A^\perp$ be the extended binary Golay code G_{24} (cf. chapter 13, (14.12)) we have already proved that 0, 8, 12, 16, and 24 are the only weights which occur. Therefore the existence of the 5 - (24, 8, 1) Steiner system also follows from Theorem (14.13).

(14.18)Example. Let $n = 47$. Consider the binary QR code of length 47. By (14.11) the minimum distance d is at least 9. Then (14.7) (iii) implies that the minimum distance is at least 11. Since $|S(x, 6)| > 2^{23}$ the code cannot be 6-error-correcting. Hence the minimum distance is 11. Therefore the extended code \bar{C} has minimum distance $d = 12$ and again it is self-dual. One can compute the weight enumerator of this code using Theorem (9.14). The only occurring weights are 0, 12, 16, 20, 24, 28, 32, 36 and 48. Hence (14.13) applies with $t = 5$. We can take $v = 12, 16, 20$ or 24. This yields 4 different 5-designs. If we take $v = 28, 32, 36$ we find the complementary designs.

These examples explain the interest (from the point of view of

design theorists) in determining the minimum weight of quadratic residue codes. Very little is known in this area. A survey for $n \leq 59$ can be found in [5]. See also [86].

It would be beyond the scope of this course to go into a method of treating QR codes which looks very promising. This is the idea of contractions of self-orthogonal codes. The idea is to use an element of the automorphism group of a self-orthogonal code to map the code into a code of smaller length which is still self-orthogonal. This method was used successfully by Assmus and Mattson to determine the minimum weight of the $(60, 30)$ extended QR code over $\text{GF}(3)$ (cf. [6]). The minimum weight turned out to be 18. This means that the condition of (14.13) is satisfied if $t = 5$. Hence this QR code yields 5-designs on 30 points.

We give one more example of (14.13) which will turn up again later.

(14.19) Example. Consider a $(2^{2l-1} - 1, 2^{2l-1} - 1 - 2l)$ -2-error-correcting primitive binary BCH-code C (cf. (10.5)). Using Theorem (9.14) one can show that in C^\perp the only weights which occur are 2^{2l-2} , $2^{2l-2} \pm 2^{l-1}$. Now take $n = 2^{2l-1}$, $k = 2^{2l-1} - 1 - 2l$, $q = 2$ and let A be \overline{C} . In A^\perp only 3 weights occur. Hence if we take $t = 3$ the condition of (14.13) is satisfied. It follows that for each v the subsets which support code words of weight v form a 3-design.

Several authors have generalized the idea of QR codes (cf. [31], [37], [118]). An elementary presentation of the theory is given in [83]. We shall only sketch the ideas and show a connection with certain well known designs. In the generalization the length of the codes is $q = p^m$ ($m > 1$). We shall take $m = 2$. As alphabet we may use any finite field F . Let G be the additive group of $\text{GF}(q)$. We identify the positions of the code with elements of G and represent a code word as

$$(14.20) c = \sum_{g \in G} c_g x^g, \quad (c_g \in F),$$

which is to be considered as a formal expression. Note that this corresponds to the representation of cyclic codes in the case that $m = 1$, where $G = \{0, 1, \dots, p-1\}$.

The group algebra \mathbf{FG} consists of all expressions of the form (14.20) with the following rules for addition and multiplication.

$$(14.21) \quad \begin{aligned} \sum a_g x^g \oplus \sum b_g x^g &:= \sum (a_g + b_g) x^g, \\ \sum a_g x^g * \sum b_g x^g &:= \sum \left(\sum_{g_1 + g_2 = g} a_{g_1} b_{g_2} \right) x^g \end{aligned}$$

where the summations are over all g in G . Then $(\mathbf{FG}, \oplus, *)$ is a ring.

Let ξ be a primitive p -th root of unity in some extension field $\hat{\mathbf{F}}$ of \mathbf{F} . Let α be a primitive element of $\mathbf{GF}(q)$. Every element $g \in G$ can be represented as $g = i_0 + i_1 \alpha$ with i_0 and i_1 in $\mathbf{GF}(p)$. We now define the character $\psi_1 : G \rightarrow \hat{\mathbf{F}}$ by

$$(14.22) \quad \psi_1(g) := \xi^{i_0}$$

and for each $h \in G$ we define the character ψ_h by

$$(14.23) \quad \psi_h(g) := \psi_1(gh).$$

Finally the characters are extended to \mathbf{FG} linearly by defining

$$(14.24) \quad \psi_f \left(\sum_{g \in G} a_g x^g \right) := \sum_{g \in G} a_g \psi_f(g).$$

The reader who is familiar with character theory will see that we now have all the characters of G and that $h \leftrightarrow \psi_h$ establishes an isomorphism between G and the group of characters. Since the proofs of all the facts to be stated below depend heavily on calculations with characters we leave out these proofs (which are straightforward and which can be found in [83]). For the definition of the generalized codes we denote by U (resp. V) the set of nonzero squares (resp. non-squares) in G .

(14.25) Definition. The generalized quadratic residue code (GQR code) of length q over \mathbf{F} consists of all $c = \sum c_g x^g$ such that $\psi_u(c) = 0$ for all $u \in U$.

We denote this code by A^+ and define B^+ by replacing U by V . The codes A and B are subcodes defined by the additional requirement $\psi_0(c) = 0$. From the independence of the characters one sees that A^+ has

dimension $\frac{1}{2}(q+1)$.

The reader should now convince himself that if $m=1$ Definition (14.25) is the same as (14.6)!

In [83] it is shown that the idea of idempotent (cf. (14.1)) can be generalized. In the same way as was mentioned in the remark following (14.10) one can extend A^+ and B^+ to A_∞ resp. B_∞ by adding an extra symbol to the code words such that the extended codes are dual codes. One can show that these codes are both invariant under $\text{PSL}(2, q)$. It then follows that Theorem (14.7) also generalizes. In fact, in this case one can show that if $K = \text{GF}(p)$ then the word $c = \sum_{g \in K} x^g$ is in A^+ . Therefore we actually know that the minimum weight is equal to p . So we have a complete generalization of the theory of QR codes.

Subsequently, a fairly difficult proof shows that the only words of minimum weight in A_∞ are the words in the orbit of $(\sum_{g \in K} x^g, 1)$ under $\text{PSL}(2, q)$, and multiples of these words. It then follows that the union of the supports of code words of minimal weight in A_∞ and B_∞ are the images of $\text{GF}(p) \cup \{\infty\}$ under the action of $\text{PGL}(2, p^2)$ on the projective line of order p^2 (represented by $G \cup \{\infty\}$). So these words form the Möbius plane $3 - (p^2+1, p+1, 1)$, (cf. chapter 1). Once again we find a design from the words of minimal weight in a code (and its dual). The codes discussed above were first constructed (for $F = \text{GF}(2)$) by Delsarte (cf. [37]) starting from the designs. The connection to QR codes did not appear in that approach.

Further references for this chapter: [89], [110].

15 · Symmetry codes over GF(3)

In this section we treat a sequence of codes which have a number of properties in common with QR codes, e. g. they also lead to new 5-designs. The results are due to V. Pless ([94], [95]).

(15.1) **Definition.** A C-matrix of order m is a matrix C with entries ± 1 (outside the diagonal) and 0 (on the diagonal) such that $CC^T = (m-1)I_m$.

A lot is known about these matrices. The first construction is the well known Paley construction (cf. Paley graphs in chapter 2).

Let q be a power of an odd prime and let χ be the quadratic character on $GF(q)$. We number the rows and columns of a matrix of order $q+1$ using the coordinates of the projective line of order q , i. e. ∞ and the elements of $GF(q)$. Define C_{q+1} by

$$\begin{aligned} c_{\infty, \infty} &:= 0, \quad c_{\infty, a} = 1, \quad c_{a, \infty} = \chi(-1), \\ c_{a, b} &:= \chi(b - a) \quad (a, b \in GF(q)). \end{aligned}$$

Then C_{q+1} is a C-matrix of order $q+1$ (cf. [60]). We note that $C_{q+1}C_{q+1}^T = -I_{q+1}$ over $GF(3)$ if $q \equiv -1 \pmod{3}$ and that C_{q+1} is symmetric if $q \equiv 1 \pmod{4}$, skew-symmetric if $q \equiv -1 \pmod{4}$.

(15.2) **Definition.** Let $q \equiv -1 \pmod{6}$. We define a symmetry code of dimension $q+1$ as a $(2q+2, q+1)$ -code Sym_{2q+2} over $GF(3)$ with generator

$$G_{2q+2} := (I_{q+1} \ C_{q+1}),$$

where C_{q+1} is a C-matrix of order $q+1$. If q is a power of an odd prime then we take for C_{q+1} the Paley matrix defined above.

We prove a number of properties of these codes:

(15.3) **Proposition.** A Sym_{2q+2} is self-dual (and hence all weights are divisible by 3).

Proof. This follows from $C_{q+1} C_{q+1}^T = -I_{q+1}$ over $\text{GF}(3)$. //

(15.4) **Proposition.** If C_{q+1} is a Paley matrix then

$G_{2q+2}^* := ((-1)^{(q+1)/2} C_{q+1} I_{q+1})$ is also a generator matrix for Sym_{2q+2} .

Proof. Since $C_{q+1}^T = (-1)^{\frac{q-1}{2}} C_{q+1}$ we find $G_{2q+2} G_{2q+2}^{*T} = 0$, Sym_{2q+2} is self-dual, and G_{2q+2}^* has rank $q+1$. //

(15.5) **Proposition.** The linear transformation of $\mathcal{R}^{(2q+2)}$ with matrix

$\begin{pmatrix} 0 & I_{q+1} \\ (-1)^{(q+1)/2} I_{q+1} & 0 \end{pmatrix}$ leaves Sym_{2q+2} invariant.

Proof. This follows from (15.4). //

(15.6) **Example.** Take $q = 5$. We find

$$G_{12} := \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ I_6 & 1 & 1 & 0 & 1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix},$$

i. e. Sym_{12} is the extended ternary Golay code (cf. [3, 1]).

Remark. In the case of the binary Golay code it is also possible to find a generator matrix of the form of (15.2) (cf. [79] p. 101).

In describing code words in a symmetry code we shall denote by $w_l(x)$, $w_r(x)$ respectively, the contribution to the weight of x due to the first $q+1$, respectively the last $q+1$ coordinates.

(15.7) **Lemma.** We have for every code word x in a symmetry code:

- (i) if $w_l(x) = 1$ then $w_r(x) = q$,
- (ii) if $w_l(x) = 2$ then $w_r(x) = (q+3)/2$,
- (iii) if $w_l(x) = 3$ then $w_r(x) \geq [3(q-3)/4]$.

Proof. Consider three rows of the generator matrix. Since multiplication of a column by -1 does not alter weights we may assume that \mathbf{x} in (i), (ii), (iii) is the sum of 1, 2 or 3 rows of the following array:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & \dots & 0 & 0 & + & + & \overbrace{+ \dots +}^a & \overbrace{+ \dots +}^b & \overbrace{+ \dots +}^c & \overbrace{+ \dots +}^d \\ 0 & 1 & 0 & 0 & \dots & 0 & x_{21} & 0 & x_{23} & + \dots + & + \dots + & - \dots - & - \dots - \\ 0 & 0 & 1 & 0 & \dots & 0 & x_{31} & x_{32} & 0 & + \dots + & - \dots - & + \dots + & - \dots - \end{array} \right]$$

At the right, a, b, c, and d denote the number of columns of the 4 different types.

By the definition of C-matrix we have (over \mathbf{R}):

$$\begin{aligned} a + b + c + d &= q - 2, \\ a + b - c - d &= -x_{23}, \\ a - b + c - d &= -x_{32}, \\ a - b - c + d &= -x_{21}x_{31}. \end{aligned}$$

Now (i) is obvious. To prove (ii) we add the first two rows and find

$$w_{\mathbf{r}}(\mathbf{x}) = 2 + \frac{1}{2}(1 + x_{23}) + a + b = \frac{1}{2}(q + 3). \text{ Now add all three rows. Then } w_{\mathbf{r}}(\mathbf{x}) \geq b + c + d = \frac{1}{4}\{3(q - 2) + x_{23} + x_{32} + x_{21}x_{31}\} \geq \frac{3}{4}(q - 3). //$$

(15.8) **Lemma.** Let w_1 and w_2 be integers. Then in a symmetry code:

- (i) There is a code word \mathbf{x} with $w_{\mathbf{l}}(\mathbf{x}) = w_1$, $w_{\mathbf{r}}(\mathbf{x}) = w_2$ iff there is a code word \mathbf{y} with $w_{\mathbf{l}}(\mathbf{y}) = w_2$, $w_{\mathbf{r}}(\mathbf{y}) = w_1$,
- (ii) For all code words \mathbf{x} we have $w_{\mathbf{r}}(\mathbf{x}) > 0$.

Proof. (i) This follows from (15.4); (ii) C_{q+1} is non-singular. //

(15.9) **Example.** Let $q = 17$. We consider Sym_{36} . By (15.7) a code word \mathbf{x} with $w_{\mathbf{l}}(\mathbf{x}) \leq 3$ has weight ≥ 12 . By (15.3) all weights are divisible by 3. By (15.8) the existence of a code word with weight < 12 implies the existence of a code word \mathbf{x} with $w_{\mathbf{l}}(\mathbf{x}) = 4$, $w_{\mathbf{r}}(\mathbf{x}) = 5$.

Since C_{18} is a bordered circulant there are not very many different possibilities for such an \mathbf{x} . It is easily checked by hand that no such \mathbf{x} exists. The reader should try this as an exercise. First he should add one more line to the array in the proof of Lemma (15.7). There are a few

cases to be distinguished. One should keep in mind that C-matrices are defined over \mathbf{R} and that the remaining rows should be orthogonal to the ones we have. The original work was done by computer but it is possible to do it by hand in half an hour and thus show that Sym_{36} has minimum weight 12. Now we apply Theorem (14.13). Here $n = 36$, $k = 18$, $q = 3$, $d = e = 12$, $v_0 = w_0 = 23$. So we can take $v = 12, 15, 18$ or 21 . If $t = 5$ the condition of the theorem is satisfied. We find 5-designs on 36 points with blocks of size 12, 15, 18, or 21. These are new and so are the complementary designs with one possible exception. It is not known whether the design with block size 18 is self complementary.

In [95] the examples $q = 5$, $q = 11$, $q = 17$, $q = 23$ and $q = 29$ are treated. Of course $q = 5$ yields the well-known Steiner system $5 - (12, 6, 1)$ as shown in (13.5). The other designs are new. To show this, one has to study the transformations which leave such codes invariant. Let $G(q)$ denote the group of monomial transformations which leave Sym_{2q+2} invariant, and let $\bar{G}(q)$ be the group of permutations induced by $G(q)$.

(15.10) Lemma. If A and B are monomial transformations of order $q + 1$ such that $A^{-1}C_{q+1}B = C_{q+1}$ then $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in G(q)$.

Proof. Code words in Sym_{2q+2} have the form $a^T (I_{q+1} C_{q+1})$. Now $a^T (I_{q+1} C_{q+1}) \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = a^T A (I_{q+1} A^{-1} C_{q+1} B)$ which is a code word. //

Let q be a power of an odd prime. We have defined C_{q+1} by numbering rows and columns with coordinates of the projective line. We order these in the same way as for cyclic codes. We now define monomial transformations in the same way as was done (in chapter 14) in the binary case for QR codes. S is the permutation $x \mapsto x + 1$. We consider C_{q+1} and S as linear transformations of the space $\mathcal{R}^{(q+1)}$ over $\text{GF}(3)$. We have for the standard basis vectors e_∞, e_a ($a \in \text{GF}(q)$):

$$e_\infty C_{q+1} = \sum_{a \in \text{GF}(q)} e_a,$$

$$e_a C_{q+1} = \chi(-1)e_\infty + \sum_{b \in \text{GF}(q)} \chi(b - a)e_b.$$

It follows that

$$e_\infty C_{q+1} S = e_\infty S C_{q+1}$$

and

$$\begin{aligned}
e_a C_{q+1} S &= \chi(-1) e_\infty + \sum_{b \in \text{GF}(q)} \chi(b - a) e_{b+1} \\
&= \chi(-1) e_\infty + \sum_{b \in \text{GF}(q)} \chi(b - a - 1) e_b = e_a^S C_{q+1},
\end{aligned}$$

i. e.

$$(15.11) S^{-1} C_{q+1} S = C_{q+1}.$$

In the same way the permutation $P(b^2)$ defined by $x \mapsto b^2 x$ ($b \neq 0$) can be shown to satisfy

$$(15.12) P(b^2)^{-1} C_{q+1} P(b^2) = C_{q+1}.$$

The permutation $Tx := x^{-1}$ which was used for QR codes is now replaced by a monomial transformation which behaves in the same way as T when considered as a permutation only. We denote it by T^* . Define

$$e_\infty T^* := (-1)^{(q-1)/2} e_0, \quad e_0 T^* := e_\infty, \quad e_a T^* := \chi(a) e_{-1/a} \quad (a \neq 0, \infty).$$

Once again it is straightforward to check that

$$(15.13) T^{*-1} C_{q+1} T^* = C_{q+1}.$$

From (15.11), (15.12), (15.13) we see that the permutations S , $P(b^2)$, and the monomial transformation T^* generate a group R^* . It is easily seen that $R^*/\{I, -I\}$ is isomorphic to $\text{PSL}(2, q)$. We combine this knowledge with Lemma (15.10) to find:

(15.14) **Theorem.** $\overline{G}(q)$ contains a subgroup isomorphic to $\text{PSL}(2, q)$.

Remark. In [95] it is shown that $\overline{G}(q)$ contains a subgroup isomorphic to $\text{PGL}(2, q) \times \mathbb{Z}_2$. It is known that $\overline{G}(5)$ is M_{12} . For other values of q it is not known what the group $G(q)$ is.

(15.15) **Example.** One of the applications of our Theorem (14.13) in [3] uses the (24, 12) extended quadratic residue code over $\text{GF}(3)$. Since the minimum weight of this code is 9 one finds a 5-design with parameters (24, 9, 6). In [3] it is also shown that $\text{PSL}(2, 23)$ is the automorphism group of this design. If we consider the prime $q = 11$ and construct the

corresponding symmetry code Sym_{2^4} we can apply Theorem (14.13) again. This also yields a 5-design. The two designs have the same parameters. By Theorem (15.14) these are not equivalent 5-designs since $\text{PSL}(2, 11)$ is not contained in $\text{PSL}(2, 23)$. For more details and further information we refer the reader to [94] and [95]. The method of attack in [95] is another example of contraction which we briefly mentioned at the end of Chapter 14. In many cases Sym_{2^q+2} can be contracted to the ternary Golay code.

16 · Nearly perfect binary codes and uniformly packed codes

The two 5-designs connected with the Golay codes have very interesting automorphism groups. It is easy to see that the collection of $(2e + 1)$ -subsets of $\{1, 2, \dots, n\}$ which support code words of weight $2e + 1$ in a binary perfect e -error-correcting code of word length n form an $(e + 1)$ -design with parameters $(n, 2e + 1, 1)$, i. e. a Steiner system (cf. [79] (5.2.6)). This design can be extended to an $(e + 2)$ -design. These two statements explain the interest of both group- and design-theorists in perfect codes. However, it has been shown that for $e > 1$ the Golay codes are the only nontrivial perfect codes if the size of the alphabet is a power of a prime (cf. [80], [114]).

We now present some of the theory of binary nearly perfect codes due to J. -M. Goethals and S. L. Snover (cf. [57]). These codes are a special case of the class of uniformly packed codes, introduced by N. V. Semakov, V. A. Zinovjev and G. V. Zaitzev (cf. [106]). These codes also lead to t -designs. Necessary conditions for the existence of such codes are very similar to those for perfect codes. The theory of uniformly packed codes was developed by J. -M. Goethals and H. C. A. van Tilborg. For a survey of most of what is known about these codes we refer to [115]. Later in this chapter we shall describe some of the connections between uniformly packed codes, so-called two-weight codes and strongly regular graphs.

First, we shall be concerned with the subclass of nearly perfect codes. We restrict ourselves to binary codes.

Let $C \subset \mathcal{R}^{(n)}$ be a code with minimum distance $d = 2t + 1$. For all $v \in C$ we define

$$\begin{aligned}
 (16.1) \quad (i) \quad & T(v) := S(v, t + 1) \setminus S(v, t), \\
 (ii) \quad & T_{\alpha}(v) := \{x \in T(v) \mid \exists_{u \in C} [x \in S(u, t)]\}, \\
 (iii) \quad & T_{\beta}(v) := T(v) \setminus T_{\alpha}(v).
 \end{aligned}$$

(Note that in (ii) the code word u is uniquely determined by x .)

(16.2) **Lemma.** For each $v \in C$ we have

$$(i) \quad |T_\alpha(v)| \leq \binom{n}{t} \left\lfloor \frac{n-t}{t+1} \right\rfloor,$$

$$(ii) \quad |T_\beta(v)| \geq \binom{n}{t+1} - \binom{n}{t} \left\lfloor \frac{n-t}{t+1} \right\rfloor.$$

Proof. If $x \in T_\alpha(v)$ and $u \in C$ is such that $x \in S(u, t)$, then $d(v, u) \leq 2t+1$, i. e. $d(v, u) = 2t+1$. But then

$$|T_\alpha(v) \cap S(u, t)| = \binom{2t+1}{t+1}.$$

Let $N_{2t+1}(v) := \{u \in C \mid d(v, u) = 2t+1\}$. Then $|T_\alpha(v)| = \binom{2t+1}{t+1} |N_{2t+1}(v)|$. To estimate $|N_{2t+1}(v)|$ observe that for two code words in $N_{2t+1}(v)$ there are at most t coordinate places where they both differ from v . For each t -subset of the coordinate places this yields at most $\left\lfloor \frac{n-t}{t+1} \right\rfloor$ elements of $N_{2t+1}(v)$. Hence

$$|N_{2t+1}(v)| \leq \left\lfloor \frac{n-t}{t+1} \right\rfloor \binom{n}{t} / \binom{2t+1}{t+1}. \text{ This proves (i). Then (ii) is obvious. //}$$

The following estimate is a specialised version of the Johnson bound (cf. [72]).

(16.3) **Theorem.** If $C \subset \mathcal{R}^{(n)}$ is a code with minimum distance $d = 2t+1$ then

$$|C| \left\{ \sum_{i=0}^t \binom{n}{i} + \frac{1}{\lfloor n/(t+1) \rfloor} \binom{n}{t} \left(\frac{n-t}{t+1} - \left\lfloor \frac{n-t}{t+1} \right\rfloor \right) \right\} \leq 2^n.$$

Proof. By the definition of $T_\beta(v)$ we see that all the $S(v, t)$ where $v \in C$ and $\bigcup_{v \in C} T_\beta(v)$ are pairwise disjoint sets. Since code words have distance at least $2t+1$, a given $x \in \mathcal{R}^{(n)}$ can be contained in at most $\lfloor n/(t+1) \rfloor$ distinct sets $T_\beta(v)$, $v \in C$. Therefore by (16.2) (ii) we have

$$\left| \bigcup_{v \in C} T_\beta(v) \right| \geq \frac{|C|}{\lfloor n/(t+1) \rfloor} \left\{ \binom{n}{t+1} - \binom{n}{t} \left\lfloor \frac{n-t}{t+1} \right\rfloor \right\}.$$

The proof is complete since $|\mathcal{R}^{(n)}| = 2^n$ and $|S(v, t)| = \sum_{i=0}^t \binom{n}{i}$.

(16.4) **Definition.** Binary codes for which equality holds in the inequality of (16.3) are called nearly perfect.

Remark. If $(t+1) \mid (n+1)$ then a nearly perfect code with these parameters is perfect. This divisibility condition is a well-known necessary condition for the existence of binary perfect codes (cf. [79] (5.2.8)).

(16.5) **Definition.** An e -error-correcting code C of length n over $GF(q)$ is called uniformly packed with parameters α and β iff for every word $x \in \mathcal{R}^{(n)}$

- (i) if x has distance e to C then x has distance $e+1$ to exactly α code words,
 - (ii) if x has distance $> e$ to C then x has distance $e+1$ to exactly β code words,
- where $\alpha < (n-e)(q-1)/(e+1)$.

We shall show that nearly perfect codes are uniformly packed. In the following C denotes a nearly perfect binary code in $\mathcal{R}^{(n)}$ with minimum distance $d = 2t+1$.

(16.6) **Theorem.** (i) If $x \in \mathcal{R}^{(n)}$ and if $\forall_{v \in C} [d(v, x) > t]$ then $d(v, x) = t+1$ for exactly $\lfloor n/(t+1) \rfloor$ code words v .

(ii) If $x \in \mathcal{R}^{(n)}$, $u \in C$ and $d(u, x) = t$ then $d(v, x) = t+1$ for exactly $\lfloor (n-t)/(t+1) \rfloor$ other code words v .

Proof. Equality in (16.3) implies equality in (16.2) (i) and (ii) and in the estimates for $|N_{2t+1}(v)|$ and $\sum_{v \in C} T_\beta(v)$. The last of these implies (i), the first implies (ii). //

(16.7) **Theorem.** If $v \in C$ then the collection \mathcal{D}_1 of d -subsets of $\{1, 2, \dots, n\}$ which support the words $u - v$, where $u \in N_d(v)$, is a t -design with parameters $(n, d, \lambda = \lfloor (n-t)/(t+1) \rfloor)$.

Proof. Let A be a t -subset of the coordinate places and let a be the word with 1's in the positions of A . By Theorem (16.6) (ii) there are $\lfloor (n-t)/(t+1) \rfloor$ code words u in $N_d(v)$ such that $d(u, v+a)=t+1$, i.e. such that A is contained in the set of coordinate places, where $u - v$ has coordinate 1. //

(16.8) **Theorem.** If $v \in C$ then the collection \mathcal{D}_2 of $(t+1)$ -subsets of $\{1, 2, \dots, n\}$ which support the words $u - v$, where $u \in T_\beta(v)$, is a t -design with $\lambda = (n - t) - (t + 1)[(n - t)/(t + 1)]$.

Proof. $T_\beta(v)$ consists of the vectors u such that $d(u, v) = t + 1$ and $d(u, w) > t$ for all $w \in N_d(v)$. Hence \mathcal{D}_2 contains all the $(t + 1)$ -subsets of $\{1, 2, \dots, n\}$ which are not contained in a subset belonging to the design \mathcal{D}_1 . The $(t + 1)$ -subsets of the blocks of \mathcal{D}_1 form a t -design. Apparently \mathcal{D}_2 is the t -design formed by all the other $(t + 1)$ -subsets of $\{1, 2, \dots, n\}$. //

(16.9) **Theorem.** The design \mathcal{D}_1 can be extended to a $(t + 1)$ -design with parameters $(n + 1, d + 1, \lambda = [(n - t)/(t + 1)])$.

Proof. Consider \bar{C} and delete the k -th coordinate of each word (k fixed). The resulting code C_k again has word length n , minimum distance d and $|C_k| = |C|$. Hence C_k is nearly perfect. Since this is true for every k it follows from Theorem (16.7) that the collection of $(d + 1)$ -subsets of $\{1, 2, \dots, n, n + 1\}$ which support the words $u - v$, where $u \in \bar{C}$, $v \in \bar{C}$, $u \in N_{d+1}(v)$, form a $(t + 1)$ -design with the same λ as in Theorem (16.7).

By now, the more pessimistic design-theorists begin to wonder whether there are any nearly perfect codes!

(16.10) **Example.** Consider the parity check matrix of a binary Hamming code (cf. Chapter 9) and delete any column. We obtain the parity check matrix of a linear code with $d = 3$, $n = 2^m - 2$ and dimension $2^m - 2 - m$. We have equality in (16.3), i. e. this code is nearly perfect, but not perfect.

The Preparata Codes (cf. [96]). We now introduce a sequence of codes which are of great combinatorial interest. We need quite a lot of preparation. Let $m \geq 3$. Let H_m be the cyclic Hamming code of word length $n = 2^m - 1$ as described in (14.3). The word 1 considered as a polynomial in $GF(2)[x] \pmod{x^n - 1}$ is $u(x) := (x^n - 1)/(x - 1)$. Let B_m be the cyclic code with generator $(x - 1)m_1(x)m_3(x)$. This BCH-code is a subcode of H_m and by the remark following Theorem (10.6) we see that this code has minimum distance at least 6.

We define the code C_m by

$$(16.11) C_m := \{(m(x), i, m(x) + (m(1) + i)u(x) + s(x)) \mid m(x) \in H_m, i \in \{0, 1\}, s(x) \in B_m\}.$$

This is obviously a linear code with word length $2n + 1$ and dimension equal to $\dim H_m + 1 + \dim B_m = 2n - 3m$.

We now prove:

(16.12) **Lemma.** C_m has minimum distance ≥ 5 .

Proof. Since the code is linear we can consider weights.

(i) Let $m(x) = 0$, $i = 0$, $s(x) \neq 0$. Then $w(s(x)) \geq 6$ because $s(x) \in B_m$.

(ii) Let $m(x) = 0$, $i = 1$. Then $u(x) + s(x) \neq 0$, $u(\alpha) + s(\alpha) = u(\alpha^3) + s(\alpha^3) = 0$ and therefore $w(u(x) + s(x)) \geq 5$ by Theorem (10.6).

(iii) $m(x) \neq 0$. Since $m(x) + (m(1) + i)u(x) + s(x) \in H_m$ we are finished unless $m(x) + (m(1) + i)u(x) + s(x) = 0$. In that case we find by substituting $x = \alpha^3$ that $m(\alpha^3) = 0$, i. e. $w(m(x)) \geq 5$. //

Now consider $S(0, 1)$ in polynomial form, i. e.

$$S(0, 1) = \{0, 1, x, x^2, \dots, x^{n-1}\} \subset GF(2)[x] \pmod{x^n - 1}.$$

In $\mathcal{R}^{(2n+1)}$ we consider the set of vectors

$$(16.13) \hat{S} := \{(q(x), 0, q(x)f(x)) \mid q(x) \in S(0, 1)\},$$

where $f(x)$ is the idempotent of H_m^* defined in (14.3).

(16.14) **Definition.** The Preparata code K_m is the union of cosets of C_m given by $C_m + \hat{S}$.

It is obvious that no 2 elements of \hat{S} are in the same coset. Hence $|K_m| = (n + 1)|C_m|$.

(16.15) **Theorem.** For odd m the Preparata code K_m is a nearly perfect code with minimum distance 5.

Proof. (i) Since K_m is nonlinear we must now consider any two words of K_m and determine the weight of their sum. By Lemma (16.12) it is sufficient to consider words from different cosets. Such a

sum has the form

$$(16.16) \quad (m(x), i, m(x) + (m(1) + i)u(x) + s(x)) + (q_1(x) + q_2(x), 0, (q_1(x) + q_2(x))f(x)).$$

Since H_m is perfect there is a unique element $x^S \in S(0, 1)$ such that

$$m'(x) := q_1(x) + q_2(x) + x^S \in H_m.$$

Observe that $m'(x) = 0$ if $q_1(x) = 0$ or $q_2(x) = 0$. We define

$$m''(x) := x^S(1 + f(x)) + m'(x) + m'(1)u(x).$$

We remark that $m''(x) \in H_m$ (cf. (14.3)). Since all polynomials are considered mod $x^n - 1$ we have $m'(x)f(x) = 0$. We replace $m(x) + m'(x)$ by $m(x)$ and rewrite (16.16) as

$$(16.17) \quad (m(x), i, m(x) + (m(1) + i)u(x) + s(x)) + (x^S, 0, x^S) + (0, 0, m''(x)).$$

(ii) From (16.17) we find that the weight W which we wish to determine is

$$(16.18) \quad W = w(m(x) + x^S) + i + w(m(x) + (m(1) + i)u(x) + s(x) + x^S + m''(x)).$$

(ii) If $m'(x) \neq 0$, then $m'(x)$ has the form $x^S + x^j + x^k$, and by definition $m'(\alpha) = 0$. It follows that $m'(\alpha^3) = \alpha^{3S}(\alpha^h + \alpha^{2h})$, where $h = j - s \neq 0$. If, on the other hand, $m'(x) = 0$ then $m'(\alpha^3)$ can also be written as $\alpha^{3S}(\alpha^h + \alpha^{2h})$, where $h = 0$.

(iv) Since m is odd the equation $\alpha^{3h} = 1$ has $h = 0$ as its only solution ($\alpha^h \in \text{GF}(2^m)$). It follows that $1 + \alpha^h + \alpha^{2h} \neq 0$ for all h . Therefore $m''(\alpha^3) = \alpha^{3S} + m'(\alpha^3) = \alpha^{3S}(1 + \alpha^h + \alpha^{2h}) \neq 0$.

(v) Let $\phi(x)$ be any word with $\phi(1) = 0$, $\phi(\alpha) = \alpha^S$, $\phi(\alpha^3) = \alpha^{3S}(\alpha^h + \alpha^{2h})$ for some h . Then $\phi(x)$ has weight at least 4.

To prove this, first observe that $\phi(x)$ clearly is not 0 and that it has even weight. If $\phi(x)$ has weight 2 this would imply that there are two elements x_1 and x_2 in $\text{GF}(2^m)$ such that $x_1 + x_2 = \alpha^S$ and $x_1^3 + x_2^3 = \alpha^{3S}(\alpha^h + \alpha^{2h})$. From this we find that $\alpha^{-S}x_1 + \alpha^h$ and $\alpha^{-S}x_2 + \alpha^h$ are the solutions of the equation $1 + \xi + \xi^2 = 0$. We showed above that this equation has no solutions in $\text{GF}(2^m)$ if m is odd.

(vi) Let $s(x) \in B_m$. Define $s'(x) := m''(x) + x^S + s(x)$. Then in (v) we can take $\phi(x) = s'(x)$. We find

$$(16.19) \quad w(s'(x)) \geq 4.$$

In the remaining part of the proof we consider 5 different possible forms of (16.17).

(vii) Let $m(1) = 0$, $i = 1$. By (16.18) we have

$$W \geq 1 + w(s''(x)),$$

where $s''(x) := u(x) + s(x) + m''(x)$. Since $s''(1) = s''(\alpha) = 0$ and $s''(\alpha^3) \neq 0$ by (iv), we find $w(s''(x)) \geq 4$ from Theorem (10.6).

(viii) Let $m(1) = 0$, $i = 0$, $m(x) \neq 0$. Then by Theorem (10.6) we have $w(m(x)) \geq 4$. Then (16.18) yields

$$W \geq w(m(x)) + w(m(x) + m''(x) + s(x)) - 2 \geq 4 + 3 - 2 = 5,$$

once again using Theorem (10.6) and the fact that $m(1) + m''(1) + s(1) = 1$ and $m(\alpha) + m''(\alpha) + s(\alpha) = 0$.

(ix) Let $m(x) = 0$, $i = 0$. Then we find from (16.18) and (16.19)

$$W \geq 1 + w(s'(x)) \geq 5.$$

(x) Let $m(1) = 1$, $i = 0$. Let $\phi(x) := m(x) + u(x) + s'(x)$. Then $\phi(x) \neq 0$. From (16.18) we find

$$W \geq w(m(x) + x^S) + w(\phi(x)).$$

By Theorem (10.6) $w(m(x) + x^S) \geq 4$ unless $m(x)$ is a trinomial. In that case $\phi(x)$ satisfies the conditions of (v) and hence $w(\phi(x)) \geq 4$. So in both cases $W \geq 5$.

(xi) Let $m(1) = 1$, $i = 1$. From (16.18) we find

$$W \geq w(m(x) + x^S) + 1 + w(m(x) + s'(x)).$$

In the same way as in (x) we are finished unless $m(x)$ is a trinomial, say $m(x) = x^S + x^C + x^D$. In that case $m(1) + s'(1) = 1$, and then $W < 5$ would imply that $s'(x) = x^S + x^C + x^D + x^E$, i. e. $m(x) + m''(x) + s(x) = x^S + x^E \notin H_m$, a contradiction.

The steps (vii) to (xi) prove that K_m has minimum distance 5.

(xii) We have already seen that $|K_m| = 2^m 2^{2n-3m} = 2^{2n-2m}$.

The word length is $2n + 1$ and $d = 2t + 1 = 5$. If m is odd we have

$$|K_m| \{1 + \binom{2n+1}{1} + \binom{2n+1}{2} + \frac{3}{2n+1} (\binom{2n+1}{2} \binom{2n-1}{3} - [\frac{2n-1}{3}])\} = 2^{2n+1},$$

i. e. equality holds in (16.3). //

(16.20) Example. Let $m = 2k - 1$. Consider the extended Preparata code \bar{K}_m which has word length 4^k . By Theorem (16.9) the words of weight 6 in this code form a 3-design with parameters $(4^k, 6, \frac{4^k-4}{3})$. As an exercise the reader should work out the example $k = 2$ using the example following (10.4) and example (14.3). In this case B_m consists of 0 only and C_m has minimum distance 7. Because the definition is cyclic one only has to consider the coset of C_m given by taking $q(x) = 1$ in (16.13). This coset then has 6 words of weight 5 and 10 words of weight 6. In the extended code \bar{K}_m these words yield 16 words of weight 6 forming a 2-design corresponding to a Hadamard matrix of order 16. The 112 blocks of the 3-design mentioned above are obtained by simultaneous cyclic shifts on the positions 0 to 6 and 8 to 14 (we assume that the overall parity check is in position 15). The blocks of this design can be considered as 112 words of weight 6 and length 16 with mutual distances at least 6. It can be shown that such a code cannot have more than 112 words and 112 can be attained only by the blocks of a 3-design.

It was shown by K. Lindström [78] and H. C. A. van Tilborg [115] that the codes treated in (16.10) and (16.15) are the only nearly perfect codes. In fact in [115] it is shown that for $e \geq 4$ there does not exist a nontrivial uniformly packed code. For smaller values of e there are many interesting examples (such as G_{24}). We first give an example of a uniformly packed code.

(16.21) Example. Let C be the 2-error-correcting binary BCH-code of example (14.19). The supports of the code words of weight 6 in the extended code \bar{C} form a 3-design. We see that this implies that every word of weight 2 or 3 is at distance 2 or 3 from 0 and λ code words of C (where λ is the parameter of the 3-design). Therefore C is a uni-

formly packed code with $\alpha = \lambda$, $\beta = \lambda + 1$.

The following theorem which follows from the general theory of uniformly packed codes makes it easier to decide whether a code is uniformly packed than using the definition. For a proof of the theorem we refer to [115].

(16.22) Theorem. Let C be an e -error-correcting linear code. Then C is uniformly packed (resp. perfect) iff the number of nonzero weights in the dual code C^\perp is $e + 1$ (resp. e).

If $e = 1$ in Theorem (16.22) then C^\perp has only two nonzero weights. Such a code is called a two-weight code.

(16.23) Example. Let H be the parity check matrix of the Hamming code of length $(q^m - 1)/(q - 1)$ over $GF(q)$. The columns of H represent the points of $PG(m-1, q)$. Let the columns be numbered in such a way that the first $(q^k - 1)/(q - 1)$ columns represent a subspace $S = PG(k-1, q)$. Let $c = (c_1, c_2, \dots, c_m)$. The equation $c_1 x_1 + c_2 x_2 + \dots + c_m x_m = 0$ represents a hyperplane in $PG(m-1, q)$ which either contains S or meets S in $(q^{k-1} - 1)/(q - 1)$ points. It follows that a linear combination of the rows of H has $(q^k - 1)/(q - 1)$ zeros or $(q^{k-1} - 1)/(q - 1)$ zeros in the positions corresponding to S . Now we leave out the columns corresponding to S and generate a code with the rows of the remaining matrix. This code has dimension m and the code words have weight q^{m-1} or $q^{m-1} - q^{k-1}$. By Theorem (16.22) this code is the dual of a uniformly packed code.

The following two theorems, due to Delsarte [38], show how two-weight codes are related to certain strongly regular graphs. If the columns of the generator matrix of a linear code C are pairwise linearly independent (i.e. C^\perp has minimum weight ≥ 3) the code C is called projective.

(16.24) Theorem. Let C be a two-weight projective code with weights w_1, w_2 ($w_1 < w_2$). Define the graph $\Gamma(C)$ by taking the code words as vertices and joining x and y by an edge iff $d(x, y) = w_1$. Then $\Gamma(C)$ is a strongly regular graph.

Proof. Let C be an (n, k) -code over $GF(q)$ with weights W_1, W_2 and let there be b_i words of weight W_i ($i = 1, 2$). Consider the matrix $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ in which the rows of A_i are all the code words of weight W_i ($i = 1, 2$). Then every column of A has $q^k - q^{k-1}$ nonzero entries. Therefore $b_1 + b_2 = q^k - 1$ and $b_1 W_1 + b_2 W_2 = n(q^k - q^{k-1})$. So we can calculate b_1 and b_2 . Take any column of A . Let it have r_1 zeros in A_1 and r_2 zeros in A_2 . The vectors with a zero in this column form a two-weight subcode of C and we can therefore calculate r_1 and r_2 in the same way as we calculated b_1 and b_2 . Hence r_1 and r_2 are constants. Now consider A_1 . Every column of A_1 has r_1 zeros. Therefore we know the sum of the distances of the rows of A_1 to the first row of A_1 . If there are s_i words of weight w_i with distance W_i to the first row of A_1 then $s_1 + s_2 = b_1 - 1$ and $s_1 w_1 + s_2 w_2$ is the sum determined above. So, we can determine s_i . We have proved that if $\{x, y\}$ is an edge in $\Gamma(C)$, then there is a constant number of vertices z joined to x and to y . The calculation in the case that $\{x, y\}$ is not an edge is similar. //

The next theorem is the converse of Theorem (16.24).

(16.25) Theorem. Let Γ be a strongly regular graph on $n = p^k$ vertices, p prime, with integral eigenvalues a, ρ_1, ρ_2 . Let the elementary abelian p -group G_n be a regular group of automorphisms of Γ . Then there is a two-weight code C over $GF(p)$ such that $\Gamma = \Gamma(C)$.

For a proof we refer to [38]. In the proof it is shown that the eigenvalues, the word length N of C , and the weights W_1, W_2 of C are related by

$$(16.26) (\rho_1 - \rho_2)(p - 1)N = -a - \rho_2(p^k - 1)$$

$$(16.27) (\rho_1 - \rho_2)W_i = (-\rho_2 + \frac{(-1)^i - 1}{2})p^{k-1}, \quad (i = 1, 2).$$

This theorem allows us to provide connections between several of the topics treated so far. As an example we consider the partial geometry treated in chapter 12 which has parameters $r = k = 6, t = 2$. This geometry was associated with a strongly regular graph Γ with

parameters 81, 30, 9, 12 and $\rho_1 = 3, \rho_2 = -6$. The graph Γ was defined from a (5, 4)-code over $\text{GF}(3)$ in such a way that translating over a code word is obviously an automorphism. So Γ admits the elementary abelian group of order 81 as a group of automorphisms. Therefore Theorem (16.25) states that Γ is associated with a two-weight code of dimension 4 over $\text{GF}(3)$ which has word length $N = 25$ and weights 15 and 18. By Theorem (16.22) the dual of this code is uniformly packed.

We have been rather sketchy in our treatment of uniformly packed codes and two-weight codes. However, we trust that it has been enough to convince the reader that this is a rewarding area for further study. A better understanding of this area is found in the theory of association schemes which we introduce in the next chapter.

17 · Association schemes

After a short account of the theory of association schemes, this final chapter contains an outline of part of the thesis of P. Delsarte, in which many of the concepts of classical coding theory and design theory are generalised to classes of association schemes. For proofs, we refer the reader to [39].

Association schemes were introduced by Bose and Shimamoto [18] as a generalisation of strongly regular graphs. An association scheme consists of a set X together with a partition of the set of 2-element subsets of X into n classes $\Gamma_1, \dots, \Gamma_n$, satisfying the conditions

(i) given $p \in X$, the number n_i of $q \in X$ with $\{p, q\} \in \Gamma_i$ depends only on i ;

(ii) given $p, q \in X$ with $\{p, q\} \in \Gamma_k$, the number a_{ijk} of $r \in X$ with $\{p, r\} \in \Gamma_i$, $\{q, r\} \in \Gamma_j$ depends only on i, j , and k .

It is convenient to take a set of n 'colours' c_1, \dots, c_n , and colour an edge of the complete graph on X with colour c_i if it belongs to Γ_i ; so Γ_i is the c_i -coloured subgraph. The first condition asserts that each graph Γ_i is regular; the second, that the number of triangles with given colouring on a given base depends only on the colouring and not on the base. A complementary pair of strongly regular graphs forms an association scheme with two classes, and conversely.

Two important classes of association schemes are those which Delsarte calls the Hamming and Johnson schemes; they generalise the square lattice and triangular graphs respectively. In the Hamming scheme $H(n, q)$, X is the set of ordered n -tuples of elements from a set of cardinality q (in practice often taken to be a finite field, though this is not significant here), and Γ_i is the set of pairs of n -tuples which agree in $n - i$ coordinate places, where $1 \leq i \leq n$. In the Johnson scheme $J(v, k)$, with $k \leq \frac{1}{2}v$, X is the set of k -subsets of a v -set, and Γ_i the set of

pairs of k -subsets whose intersection is a $(k - i)$ -subset, where $1 \leq i \leq k = n$. The Hamming schemes provide a setting for classical error-correcting coding theory, and the Johnson schemes may be regarded as a setting for design theory. We shall see that these schemes have properties which are not typical of association schemes in general. Note that $H(v, 2)$ can be identified with the set of all subsets of a v -set, and so 'contains' all the Johnson schemes $J(v, k)$.

If G is a transitive permutation group on a set X with the property that any two points are interchanged by an element of G , then the orbits of G on the set of 2-subsets of X form an association scheme on X . (The condition on G can be weakened; it is enough that the permutation character of G is 'multiplicity-free'. Still weaker conditions suffice, but these are not easy to state.) D. G. Higman [64] has defined and studied a more general combinatorial object, which he calls a 'coherent configuration', which 'describes' the action of an arbitrary permutation group in the same way. (The main difference is that unordered pairs are replaced by ordered pairs.)

An association scheme is called metric if Γ_i is the set of pairs of points at distance i in the graph Γ_1 , for $1 \leq i \leq n$. (Γ_1 is then called a metrically regular, or perfectly regular, graph.) A strongly regular graph is metrically regular, but for $n > 2$ metric schemes seem to be fairly rare among association schemes in general. However, the Hamming and Johnson schemes are easily seen to be metric. (In the scheme $J(2k + 1, k)$, the graph Γ_k is also metrically regular.) A scheme is metric if and only if $a_{ijk} = 0$ unless $|i - j| \leq k \leq i + j$ (this is just the 'triangle inequality'), and $a_{i-1, i+1} \neq 0$ for $1 \leq i \leq n - 1$.

To simplify formulae, we extend the range of definition of subscripts to include 0, and define $n_0 = 1$, $a_{ij0} = \delta_{ij} n_i$, $a_{i0k} = a_{0ik} = \delta_{ik}$. (This can be interpreted to mean that Γ_0 is the graph in which every vertex is joined to itself and nothing else!) Now the parameters satisfy a number of identities, for example

$$\begin{aligned}
 (17.1) \quad & a_{ijk} = a_{jik}, \\
 & n_k a_{ijk} = n_i a_{kji}, \\
 & \sum_{j=0}^n a_{ijk} = n_i, \\
 & \sum_{t=0}^n a_{lit} a_{tjm} = \sum_{k=0}^n a_{lkm} a_{ijk}.
 \end{aligned}$$

(The last equation comes from counting in two ways, as indicated in Fig. 17.1, paths with colour sequence c_l, c_i, c_j joining x to y , where $\{x, y\} \in \Gamma_m$.)

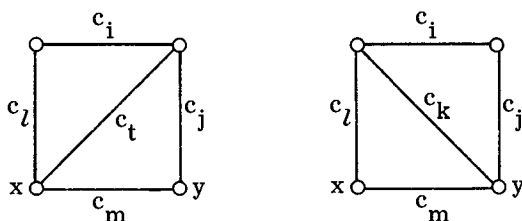


Fig. 17.1

Let A_i be the adjacency matrix of Γ_i , and $A_0 = I$. Then

$$(17.2) \quad A_i A_j = \sum_{k=0}^n a_{ijk} A_k,$$

so the commuting symmetric matrices A_0, \dots, A_n span an $(n+1)$ -dimensional real algebra called the Bose-Mesner algebra [17] or centraliser algebra [64] of the scheme. (The second name derives from the fact that if the scheme comes from a permutation group in the manner previously described, then this algebra is just the set of matrices commuting with all the permutation matrices representing the group.) Note that, if the scheme is metric, then A_1 generates the centraliser algebra.

The relations (17.1) have interpretations in terms of the structure of this algebra; in particular, the first and fourth assert that $A_i A_j = A_j A_i$ and $(A_l A_i) A_j = A_l (A_i A_j)$ respectively.

As for strongly regular graphs, eigenvalues of the matrices A_i

and their multiplicities are important. For convenience we speak of (irreducible) representations or characters of the Bose-Mesner algebra; one of these is simply the function associating with each matrix in the algebra its eigenvalue on a common eigenvector. (Note that the matrices can be simultaneously diagonalised.) The irreducible representations and their multiplicities are determined by, and determine, the parameters a_{ijk} ; thus there are 'rationality conditions' for arbitrary schemes. We sketch the process.

Define intersection matrices M_i , $0 \leq i \leq n$, by $(M_i)_{lm} = a_{lim}$. Then

$$\begin{aligned}(M_i M_j)_{lm} &= \sum_{t=0}^n a_{lit} a_{tjm} \\ &= \sum_{k=0}^n a_{lkm} a_{ijk} \\ &= \left(\sum_{k=0}^n a_{ijk} M_k \right)_{lm},\end{aligned}$$

so $M_i M_j = \sum_{k=0}^n a_{ijk} M_k$, and the map $A_i \mapsto M_i$ induces an algebra isomorphism. So the irreducible representations can be found by simultaneously diagonalising the M_i . (These matrices are usually much smaller than the A_i , and depend only on the parameters a_{ijk} and not on the particular scheme considered.)

Let ρ_0, \dots, ρ_n be the irreducible representations; we can assume that $\rho_0(A_i) = n_i$ for $0 \leq i \leq n$ (so ρ_0 corresponds to the all-1 eigenvector). Suppose μ_m is the multiplicity of ρ_m . Then $\mu_0 = 1$ and

$$|X| \delta_{i0} = \text{Trace}(A_i) = \sum_{m=0}^n \mu_m \rho_m(A_i)$$

is a system of linear equations for the multiplicities μ_m .

Conversely, suppose the ρ_m and μ_m are known. The valencies n_i are determined as $\rho_0(A_i)$, or alternatively are given by

$$|X| n_i \delta_{ij} = \text{Trace}(A_i A_j) = \sum_{m=0}^n \mu_m \rho_m(A_i) \rho_m(A_j).$$

Counting triangles with edges coloured c_i, c_j, c_k , we determine a_{ijk} :

$$|X|n_k a_{ijk} = \text{Trace}(A_i A_j A_k) = \sum_{m=0}^n \mu_m \rho_m(A_i) \rho_m(A_j) \rho_m(A_k).$$

If the scheme is metric, the process is simplified. First, A_1 generates the Bose-Mesner algebra, so we only have to diagonalise the intersection matrix M_1 . Second, this matrix is tridiagonal, so it is easier to diagonalise, and its eigenvalues are distinct. Almost all applications of the rationality conditions for association schemes have been to metric schemes; the theorem of Bannai and Ito [11] and Damerell [35] on Moore graphs is a good example.

Let P be the $(n+1) \times (n+1)$ matrix with (i, k) entry $\rho_i(A_k)$, that is, the 'character table' of the Bose-Mesner algebra; let Q be the matrix defined by $PQ = QP = |X|I$. From the second-last paragraph, we see that Q can also be defined as $\Delta_n^{-1} P^T \Delta_\mu$, where $n = (n_0, \dots, n_n)$, $\mu = (\mu_0, \dots, \mu_n)$, and for any vector u , Δ_u is the diagonal matrix with diagonal entries the components of u .

An error-correcting code is simply a subset Y of the point set X of a Hamming scheme; one is concerned with the distance (in the graph Γ_1) between two members of Y , or between a member of Y and a member of X . To formalise this, Delsarte defines, for any subset Y of the point set X of any scheme, its inner distribution $a = (a_0, \dots, a_n)$, by

$$a_i = |Y|^{-1} |\tilde{\Gamma}_i \cap Y^2|,$$

where $\tilde{\Gamma}_0 = \{(x, x) | x \in X\}$ and $\tilde{\Gamma}_i = \{(x, y) | \{x, y\} \in \Gamma_i\}$ for $i > 0$; and the distribution matrix B of Y , the $|X| \times (n+1)$ matrix whose (x, i) entry is $B_{x,i} = |\Gamma_i(x) \cap Y|$, $x \in X$, $0 \leq i \leq n$. Thus $a_0 = 1$ and a_1 is the average valency of $\Gamma_1|_Y$. Y is said to be a regular subset if every graph $\Gamma_i|_Y$ is regular (with valency a_i). If Y is a regular subset, then the rows of B corresponding to points of Y are equal to a , and conversely.

Which $(n+1)$ -tuples can be inner distributions of subsets? Clearly the entries must be non-negative rational numbers, with $a_0 = 1$ and

$\sum_{i=0}^n a_i = |Y|$ an integer. Delsarte proves a deeper necessary condition.

$$(17.2) \quad B^T B = (|Y|/|X|) P^T \Delta_{aQ} P.$$

It follows that aQ has all its components non-negative.

This fact is applied by Delsarte to find bounds on the sizes of subsets whose inner distributions satisfy various conditions, using the techniques of linear programming.

Clearly, for any choice of $n+1$ distinct real numbers z_0, \dots, z_n , we can find polynomials Φ_0, \dots, Φ_n , each of degree at most n , such that $P_{ik} = \Phi_k(z_i)$ for $0 \leq i, k \leq n$. Delsarte calls a scheme P-polynomial if there is a choice of z_0, \dots, z_n with $z_0 = 0$ for which Φ_k has degree k , for $0 \leq k \leq n$. Q-polynomial schemes are defined similarly, with Q replacing P in the definition. Polynomial schemes appear to be fairly rare among association schemes in general, and neither of the P-polynomial and Q-polynomial conditions implies the other; but, remarkably, the important Hamming and Johnson schemes are both P- and Q-polynomial. (For the Hamming schemes, $P = Q$, $z_i = i$; for the Johnson schemes, $z_i = i(v+1-i)$ for the P-polynomials, and $z_i = i$ for the Q-polynomials. The actual polynomials are, apart from trivial modifications, the Krawtchouk and Eberlein polynomials respectively for the two schemes.) Note that the P-polynomial condition depends on the ordering of the graphs Γ_i , while the Q-polynomial condition depends on that of the representations ρ_i .

The P-polynomial condition has a simple combinatorial interpretation:

(17.3) **Theorem.** An association scheme is P-polynomial if and only if it is metric.

Proof. If a scheme is metric, then there are polynomials Φ_0, \dots, Φ_n , such that $\deg \Phi_k = k$ and $A_k = \Phi_k(A_1)$ for $0 \leq k \leq n$. (This is clear for $k = 0, 1$, and follows by induction from the relation

$$A_k A_1 = a_{k1k-1} A_{k-1} + a_{k1k} A_k + a_{k1k+1} A_{k+1}$$

with the condition $a_{klk+1} \neq 0$.) Applying the character ρ_i yields

$$P_{ik} = \rho_i(A_k) = \Phi_k(\rho_i(A_1)).$$

The converse can be proved by reversing the argument.

Suppose we have a P-polynomial (= metric) scheme on X . For any subset Y of X , define the minimal distance of Y to be the index of the first non-zero component of its inner distribution a after a_0 , and the external distance r of Y to be the number of non-zero components of aQ excluding $(aQ)_0$. The minimal distance is obviously the smallest distance between two distinct points of Y . The name 'external distance' is justified by the fact that any point of X lies at distance at most r from a point of Y , though r may not be the smallest such integer. Now we have the following result:

(17.4) Theorem. Let Y be a subset of X with minimal distance d and external distance r ; put $e = \lfloor \frac{1}{2}(d - 1) \rfloor$. Then

$$\sum_{i=0}^e n_i \leq |X|/|Y| \leq \sum_{i=0}^r n_i.$$

(In particular, $e \leq r$.) If one of these bounds is attained, then so is the other.

Proof. For any integer c , the 'sphere of radius c ' centred on a point x (the set of points at distance at most c from x) contains $\sum_{i=0}^c n_i$ points. The spheres of radius e centred on points of Y are pairwise disjoint, while those of radius r cover X . The result follows. It is also possible to give a purely algebraic proof, based on the P-polynomial concept and the linear programming method mentioned earlier. //

A subset achieving the bound of (17.4) is called a perfect e -code; it is simply a subset Y of X with the property that any point of X is at distance at most e from a unique point of Y . Its minimal distance is $2e + 1$ (rather than $2e + 2$). The repetition, Hamming, and Golay codes provide examples in the Hamming schemes. A pair of disjoint $(2e + 1)$ -sets forms a perfect e -code in the Johnson scheme $J(4e + 2)$, $(2e + 1)$. Apart from these, very few examples are known. In the

Johnson scheme $J(2k+1, k)$ with the alternative metric defined by the graph Γ_k , it can be shown that a perfect 1-code is a $(k-1) - (2k+1, k, 1)$ design, and conversely. Examples are known with $k=3$ and $k=5$. For other perfect 1-codes in metric schemes, see [15], [30].

The theorem of Lloyd on classical perfect codes has been generalised to arbitrary metric schemes, independently by Delsarte [39] and Biggs [14].

(17.5) Theorem. If a perfect e-code Y exists, then the zeros of the sum polynomial $\Psi_e(z)$ are contained in the set $\{z_1, \dots, z_n\}$, and the inner distribution of Y is determined by e and the parameters of the scheme.

Notice that $\Psi_e(z)$ depends only on e and the parameters of the scheme. Also, $\{z_1, \dots, z_n\}$ is the set of roots of $\Psi_n(z)$; so the first part of the theorem can be expressed in the form ' $\Psi_e(z)$ divides $\Psi_n(z)$ in $R[z]$ '. This should be compared with the 'sphere-packing condition', which asserts that $\Psi_e(0)$ (the size of a sphere of radius e) divides $\Psi_n(0) = |X|$ in Z .

Other concepts from coding theory (such as uniformly packed codes), as well as theorems about such codes, can also be generalised to metric schemes. However, concepts of design theory arise more naturally in Q-polynomial schemes. There is an analogy, or 'formal duality', between certain pairs of concepts, which is useful in suggesting results about Q-polynomial schemes, for which there is no simple equivalent of the 'metric' condition for P-polynomial schemes (17.3).

Given an association scheme, let E_0, \dots, E_n be the minimal idempotents of the Bose-Mesner algebra \mathcal{A} . Thus, E_i is the matrix in \mathcal{A} with eigenvalue 1 on the i-th eigenspace and 0 on the others. By definition of P, we have

$$A_k = \sum_{i=0}^n P_{ik} E_i,$$

whence

$$E_i = |X|^{-1} \sum_{k=0}^n Q_{ki} A_k.$$

We have $E_i E_j = \delta_{ij} E_i$.

There is a second operation defined on \mathcal{G} , that of Hadamard (or pointwise) product: $(a_{ij}) \circ (b_{ij}) = (a_{ij} b_{ij})$. Since each A_i is a zero-one matrix, the defining properties ensure that $A_i \circ A_j = \delta_{ij} A_i$, whence A_0, \dots, A_n are the minimal idempotents with respect to this multiplication. Since \mathcal{G} is closed under Hadamard product, we have

$$E_i \circ E_j = \sum_{k=0}^n b_{ijk} E_k$$

for some real numbers b_{ijk} , given by

$$|X|^2 \mu_k b_{ijk} = \sum_{m=0}^n n_m Q_{mi} Q_{mj} Q_{mk}.$$

They are known as the Krein parameters, because the following result (the Krein bound) was proved, using a theorem of M. G. Krein, by L. L. Scott [101].

(17.6) Theorem. $0 \leq b_{ijk} \leq 1$.

Proof. The Hadamard product $E_i \circ E_j$ is a principal submatrix of the Kronecher product $E_i \otimes E_j$, and so its eigenvalues b_{ijk} are bounded above and below by those of $E_i \otimes E_j$, which is idempotent. //

For strongly regular graphs, the Krein bound takes the following form.

(17.7) Proposition. Let Γ be a strongly regular graph whose adjacency matrix has eigenvalues a, ρ_1, ρ_2 . Suppose that Γ and its complement are connected. Then

$$\begin{aligned} (\rho_1 + 1)(a + \rho_1 + 2\rho_1\rho_2) &\leq (a + \rho_1)(\rho_2 + 1)^2, \text{ and} \\ (\rho_2 + 1)(a + \rho_2 + 2\rho_2\rho_1) &\leq (a + \rho_2)(\rho_1 + 1)^2. \end{aligned}$$

Remark. (5.3) is a consequence of this result, as noted at the end of chapter 5.

The vanishing of Krein parameters also has combinatorial significance; see [28], [29]. For example, if equality holds in either bound of (17.7), then the subconstituents $\Gamma|_{\Gamma(p)}$ and $\Gamma|\overline{\Gamma}(p)$ are both strongly

regular, for any vertex p . Conversely, if $\Gamma|\bar{\Gamma}(p)$ and $\Gamma|\bar{\Gamma}(p)$ are strongly regular for some vertex p , then equality holds in (17. 7), provided certain parameter sets are excluded.

The Krein parameters b_{ijk} are formally dual to the intersection numbers a_{ijk} . For example, an association scheme is Q-polynomial if and only if $b_{ijk} = 0$ unless $|i - j| \leq k \leq i + j$ while $b_{i \ i+1} \neq 0$ for $1 \leq i \leq n-1$. In the same sense, the theories of metric and Q-polynomial schemes are formally dual. We proceed to the analogues of (17. 4) and (17. 5).

In a Q-polynomial scheme on X , define the maximum strength t of a subset Y of X to be one less than the index of the first non-zero component of aQ after $(aQ)_0$, and the degree s of Y to be the number of non-zero components of a excluding a_0 , where a is the inner distribution of Y . Thus we have the duality $t \leftrightarrow d - 1$, $s \leftrightarrow r$. The degree is the number of colours occurring in the restriction of the scheme to Y . The meaning of the maximum strength is not obvious, and must be discovered in each individual case. We now have the result

(17. 8) Theorem. Let Y be a subset of X with maximal strength t and degree s ; put $e = \frac{1}{2}t$. Then

$$\sum_{i=0}^e \mu_i \leq |Y| \leq \sum_{i=0}^s \mu_i.$$

(In particular, $e \leq s$.) If one of these bounds is attained, then so is the other.

The simple combinatorial proof of (17. 4) does not apply here, but the algebraic proof can easily be dualised.

A subset attaining these bounds is called a tight $2e$ -design, for reasons which will become clear. Its maximal strength is $2e$ (and not $(2e + 1)$).

(17. 9) Theorem. If a tight $2e$ -design Y exists, then the zeros of the sum polynomial $\Psi_e(z)$ are contained in the set $\{z_1, \dots, z_n\}$, and the inner distribution of Y is determined by e and the parameters of the scheme.

We mention another result, which dualises a lesser-known result for metric schemes.

(17.10) Theorem. With the hypotheses of (17.8), suppose $t \geq 2s - 2$. Then the restriction of the given scheme to Y is an association scheme, which is Q -polynomial with multiplicities μ_0, \dots, μ_{s-1} , and

$$|Y| = \sum_{i=0}^{s-1} \mu_i.$$

The importance of results (17.8)-(17.10) to us depends on the following fact:

(17.11) Theorem. The maximum strength t of a subset Y of the Johnson scheme $J(v, k)$ is the largest integer t for which Y is a t -design.

Let us then interpret the results in the context of t -designs. For this, we need the fact that the multiplicities in $J(v, k)$ are given by $\mu_i = \binom{v}{i} - \binom{v}{i-1}$, $0 \leq i \leq k$. This can be proved directly, by an argument involving embedding the Bose-Mesner algebra of $J(v, k-1)$ in that of $J(v, k)$, or by an argument based on the character theory of the symmetric group. The degree of a design is the number of values taken by the size of the intersection of two distinct blocks. Thus, remembering that we are considering only designs with $k \leq \frac{1}{2}v$ having no repeated blocks, we have

(17.8)' Theorem. (i) A t -design has at least $\binom{v}{e}$ blocks, where $e = \lfloor \frac{1}{2}t \rfloor$; equality holds if and only if its degree is e .

(ii) A 0 -design of degree s has at most $\binom{v}{s}$ blocks; equality holds if and only if it is a $2s$ -design.

Of course, the first part of this result is the theorem (1.16) of Ray-Chaudhuri and Wilson. The second part improves (3.6).

(17.10)' Theorem. In a $(2s-2)$ -design of degree s , the s relations on the blocks determined by cardinality of intersection form an association scheme.

This generalises the construction of strongly regular graphs from quasi-symmetric designs in chapter 3; the multiplicities of the eigen-

values given by (17.10) agree with those found there.

(17.10)' is 'best possible'. For consider the design of points and planes in $AG(4, 2)$. This is a $3 - (16, 4, 1)$ design, and has degree 3 (since two blocks have at most two common points); but the number of blocks disjoint from a given pair of disjoint blocks depends on whether the given blocks are parallel or not. Examples of 4-designs with degree 3 are the $5 - (24, 8, 1)$, $4 - (23, 8, 4)$ (residual of the first) and $4 - (11, 5, 1)$ designs.

Maximum strength has a well-known interpretation in Hamming schemes as well. The maximum strength of a subset is simply its maximum strength as an orthogonal array, as defined by Rao [97], who proved the first part of (17.8) in this case. (An orthogonal array of strength t is a subset Y of the point set of $H(n, q)$ with the property that, given any t coordinate places, every t -tuple occurs equally often in those places in a member of Y .) The analogue of (1.17), the determination of tight 4-designs in Hamming schemes, was given by Noda [92].

A final word on duality. For certain schemes, notably the additive schemes (those admitting a transitive Abelian automorphism group A), it is possible to define dual schemes, for which the P and Q matrices are the Q and P matrices respectively of the original schemes. An additive scheme can be regarded as a Schur-ring on A , and this duality agrees with the concept defined by Tamaschke [111]. The point sets of the scheme and its dual are identified with A and its dual A' (the group of characters of A). To a subgroup Y of A corresponds a subgroup Y' of A' (the set of characters whose restriction to Y is trivial). The inner distributions a and a' are related by

$$|Y|a' = aQ, \quad |Y'|a = a'P.$$

Thus duality interchanges the parameters $d - 1$ and t and the parameters r and s , where they are defined. The Hamming schemes are additive, and in fact are isomorphic to their duals; for them, the relation $|Y|a' = aQ$ expresses the MacWilliams identities (9.14).

References

- [1] R. W. Ahrens and G. Szekeres. On a combinatorial generalization of 27 lines associated with a cubic surface, J. Austral. Math. Soc., 10 (1969), 485-92.
- [2] E. F. Assmus, Jr. and J. H. van Lint. Ovals in projective designs, J. Combinatorial Theory, (A) 27 (1979), 307-24.
- [3] E. F. Assmus, Jr. and H. F. Mattson, Jr. New 5-designs, J. Combinatorial Theory, 6 (1969), 122-51.
- [4] E. F. Assmus, Jr. and H. F. Mattson, Jr. Algebraic theory of codes II, Report AFCRL-0013, Appl. Research Lab. of Sylvania Electronic Systems, Bedford, Mass. (1971).
- [5] E. F. Assmus, Jr. and H. F. Mattson, Jr. On weights in quadratic residue codes, Discr. Math. 3 (1972), 1-20.
- [6] E. F. Assmus, Jr. and H. F. Mattson, Jr. Contractions of self-orthogonal codes, Discr. Math. 3 (1972), 21-32.
- [7] E. F. Assmus, Jr., H. F. Mattson, Jr. and Marcia Guza. Self-orthogonal Steiner systems and projective planes, Math. Z., 138 (1974), 89-96.
- [8] E. F. Assmus, Jr., J. A. Mezzaroba and C. J. Salwach. Planes and biplanes, Higher Combinatorics (M. Aigner, ed.), D. Reidel, Dordrecht (1977), 205-12.
- [9] E. F. Assmus, Jr. and H. E. Sachar. Ovals from the point of view of coding theory, Higher Combinatorics (M. Aigner, ed.), D. Reidel, Dordrecht (1977), 213-16.
- [10] E. Bannai. On tight designs, Quart. J. Math. (Oxford), 28 (1977), 433-48.
- [11] E. Bannai and T. Ito. On finite Moore graphs, J. Fac. Sci. Univ. Tokyo, 20 (1973), 191-208.

- [12] E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane. Gleason's theorem on self-dual codes, IEEE Trans. Inf. Theory IT-18 (1972), 409-14.
- [13] N. L. Biggs. Finite groups of automorphisms, L. M. S. Lecture Notes, 6, C. U. P. (1971).
- [14] N. L. Biggs. Perfect codes in graphs, J. Combinatorial Theory (B) 15 (1973), 289-96.
- [15] N. L. Biggs. Perfect codes and distance-transitive graphs, Combinatorics (T. P. McDonough and V. C. Mavron, eds.), L. M. S. Lecture Notes 13, C. U. P. (1974), 1-8.
- [16] R. C. Bose. Strongly regular graphs, partial geometries, and partially balanced designs, Pacific J. Math., 13 (1963), 389-419.
- [17] R. C. Bose and D. M. Mesner. On linear associative algebras corresponding to association schemes of partially balanced designs, Ann. Math. Statist., 30 (1959), 21-38.
- [18] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block design with two associate classes, J. Amer. Statist. Assoc., 47 (1952), 151-84.
- [19] R. C. Bose, S. S. Shrikhande and N. M. Singhi. Edge-regular multigraphs and partial geometric designs, Teorie Combinatorie (Tomo I), Accad. Naz. Lincei, Rome (1977).
- [20] A. Bremner. A diophantine equation arising from tight 4-designs, Osaka J. Math., 167 (1979), 353-6.
- [21] R. H. Bruck. Finite sets II: uniqueness and embedding, Pacific J. Math., 13 (1963), 421-57.
- [22] A. Bruen and J. C. Fisher. Blocking sets, k-arcs and nets of order ten, Advances in Mathematics, 10 (1973), 317-20.
- [23] F. Buekenhout. Une caractérisation des espaces affines basée sur la notion de droite, Math. Z., 111 (1969), 367-71.
- [24] F. C. Bussemaker and J. J. Seidel. Symmetric Hadamard matrices of order 36, Ann. N.Y. Acad. Sci., 175 (1970), 66-79.
- [25] P. J. Cameron. Extending symmetric designs, J. Combinatorial Theory (A), 14 (1973), 215-20.
- [26] P. J. Cameron. Biplanes, Math. Z., 131 (1973), 85-101.
- [27] P. J. Cameron. On doubly transitive permutation groups of degree prime squared plus one, J. Austral. Math. Soc. (A),

26 (1978), 317-18.

- [28] P. J. Cameron, J.-M. Goethals and J. J. Seidel. The Krein condition, spherical designs, Norton algebras and permutation groups, Proc. Kon. Nederl. Akad. Wetensch. (A), 81 (1978) (Indag. Math., 40 (1978)), 196-206.
- [29] P. J. Cameron, J.-M. Goethals and J. J. Seidel. Strongly regular graphs having strongly regular subconstituents, J. Algebra, 55 (1978), 257-80.
- [30] P. J. Cameron, J. A. Thas and S. E. Payne. Polarities of generalized hexagons and perfect codes, Geometriae Dedicata, 5 (1976), 525-8.
- [31] P. Camion. Global quadratic abelian codes, in Information Theory (CISM Courses and Lectures no. 219), G. Longo (ed.), Springer-Verlag, Vienna (1975).
- [32] Chang Li-Chien. The uniqueness and non-uniqueness of the triangular association schemes, Sci. Record Peking Math. (New Ser.) 3 (1959), 604-13.
- [33] Chang Li-Chien. Association schemes of partially balanced designs with parameters $v = 28$, $n_1 = 12$, $n_2 = 15$, and $p_{11}^2 = 4$, Sci. Record Peking Math. (New Ser.) 4 (1960), 12-18.
- [34] P. M. Cohn. Algebra (vol. 1), Wiley, London (1974).
- [35] R. M. Damerell. On Moore graphs, Proc. Camb. Phil. Soc., 74 (1973), 227-36.
- [36] I. Debroey and J. A. Thas. On semipartial geometries, J. Combinatorial Theory (A), 25 (1978), 242-50.
- [37] P. Delsarte. Majority logic decodable codes derived from finite inversive planes, Inform. Control, 18 (1971), 319-25.
- [38] P. Delsarte. Weights of linear codes and strongly regular normed spaces, Discrete Math., 3 (1972), 47-64.
- [39] P. Delsarte. An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements 1973, no. 10.
- [40] P. Delsarte, J.-M. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal, II, Canad. J. Math., 23 (1971), 816-32.

- [41] P. Delsarte, J. -M. Goethals and J. J. Seidel. Spherical codes and designs, Geometriae Dedicata, 6 (1977), 363-88.
- [42] P. Dembowski. Inversive planes of even order, Bull. Amer. Math. Soc., 69 (1963), 850-4.
- [43] P. Dembowski. Möbiusebenen Gerader Ordnung, Math. Ann., 157 (1964), 179-205.
- [44] P. Dembowski. Finite geometries, Springer-Verlag, Berlin-Heidelberg-New York (1968).
- [45] R. H. F. Denniston. Some new 5-designs, Bull. London Math. Soc., 8 (1976), 263-7.
- [46] M. Deza. Une propriété extrême des plans projectifs finis dans une classe de codes équidistants, Discr. Math., 6 (1973), 353-8.
- [47] J. Doyen, X. Hubaut and M. Vandensaval. Ranks of incidence matrices of Steiner triple systems, Math. Z. (to appear).
- [48] L. M. H. F. Driessen, G. H. M. Frederix, and J. H. van Lint. Linear codes supported by Steiner triple systems, Ars Combinatoria, 1 (1976), 33-42.
- [49] P. Erdős, A. Rényi and V. Sós. On a problem in graph theory, Studies Math. Hungar., 1 (1966), 215-35.
- [50] W. Feit and G. Higman. The nonexistence of certain generalized polygons, J. Algebra, 1 (1964), 434-46.
- [51] A. Gewirtz. Graphs of maximal even girth, Canad. J. Math., 21 (1969), 915-34.
- [52] A. M. Gleason. Weight polynomials of self-dual codes and the MacWilliams identities, Actes congrès Intern. Math. 1978, vol. 3, 211-5.
- [53] J. M. Goethals. On the Golay perfect binary code, J. Combinatorial Theory (A), 11 (1971), 178-86.
- [54] J. -M. Goethals. Some combinatorial aspects of coding theory, Chapter 17 in A survey of combinatorial theory (J. N. Srivastava et al., eds), North-Holland Publishing Company, Amsterdam (1973).
- [55] J. -M. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal, Canad. J. Math., 19 (1967), 1001-10.

- [56] J. -M. Goethals and J. J. Seidel. Strongly regular graphs derived from combinatorial designs, Canad. J. Math., 22 (1970), 597-614.
- [57] J. -M. Goethals and S. L. Snover. Nearly perfect binary codes, Discr. Math., 2 (1972), 65-88.
- [58] J. I. Hall, A. J. E. M. Janssen, A. W. J. Kolen and J. H. van Lint. Equidistant codes with distance 12, Discrete Math. 17 (1977), 71-83.
- [59] M. Hall, Jr. Automorphisms of Steiner triple systems, IBM J. Res. Develop., 4 (1960), 460-72.
- [60] M. Hall, Jr. Combinatorial theory, Blaisdell, Waltham, Mass. (1967).
- [61] M. Hall, Jr. and W. S. Connor. An embedding theorem for balanced incomplete block designs, Canad. J. Math., 6 (1953), 35-41.
- [62] M. Hall, Jr., R. Lane and D. Wales. Designs derived from permutation groups, J. Combinatorial Theory, 8 (1970), 12-22.
- [63] N. Hamada. On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes, Hiroshima Math. J., 3 (1973), 153-226.
- [64] D. G. Higman. Combinatorial considerations about permutation groups, Mathematical Institute, Oxford (1971).
- [65] D. G. Higman. Partial geometries, generalized quadrangles, and strongly regular graphs, Atti del convegno geometria combinatoria e sue applicazioni, Perugia (1971).
- [66] D. G. Higman. Remark on Shult's graph extension theorem, Finite groups '72 (ed. T. Gagen, M. P. Hale, Jr. and F. F. Shult), North-Holland Publishing Company, Amsterdam (1973).
- [67] D. G. Higman and C. C. Sims. A simple group of order 44,352,000, Math. Z., 105 (1968), 110-13.
- [68] A. J. Hoffman. On the uniqueness of the triangular association scheme, Ann. Math. Statist., 31 (1960), 492-7.
- [69] A. J. Hoffman and R. R. Singleton. On Moore graphs of diameters 2 and 3, IBM J. Res. Develop., 4 (1960), 497-504.
- [70] D. R. Hughes. On t-designs and groups, Amer. J. Math., 87 (1965), 761-78.

- [71] N. Ito. Tight 4-designs, Osaka J. Math., 12 (1975), 493-522.
- [72] S. M. Johnson. A new upper bound for error-correcting codes, IEEE Trans. Inform. Theory IT-8 (1962), 203-7.
- [73] W. Johnson. On the Mathieu groups M_{22} , M_{23} , M_{24} and the associated Steiner systems, Math. Z., 125 (1972), 193-214.
- [74] W. M. Kantor. Dimension and embedding theorems for geometric lattices, J. Combinatorial Theory (A), 17 (1974), 173-95.
- [75] W. M. Kantor. Moore geometries and rank 3 groups having $\mu=1$, Quart. J. Math. (Oxford), 28 (1977), 309-28.
- [76] F. S. Lander. To appear.
- [77] P. W. Lemmens and J. J. Seidel. Equiangular lines, J. Algebra, 24 (1973), 494-512.
- [78] K. Lindström. The nonexistence of unknown nearly perfect binary codes, Ann. Univ. Turku, Ser. AI, 169 (1975).
- [79] J. H. van Lint. Coding theory, Lecture Notes in Math. 201, Springer-Verlag, Berlin (1971).
- [80] J. H. van Lint. Recent results on perfect codes and related topics, in Combinatorics part 1 (M. Hall and J. H. van Lint editors), Mathematical Centre Tracts 55 (1974), 158-78.
- [81] J. H. van Lint. Equidistant point sets, Combinatorics (T. P. McDonough and V. C. Mavron, eds), LMS Lecture Notes 13, C. U. P. (1969), 169-76.
- [82] J. H. van Lint. Non-embeddable quasi-residual designs, Proc. Kon. Nederl. Akad. Wetensch. (A), 81 (1978), 269-75.
- [83] J. H. van Lint and F. J. MacWilliams. Generalized quadratic residue codes, IEEE Trans. Inform. Theory, 24 (1978), 730-7.
- [84] J. H. van Lint and A. Schrijver. Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields, to appear in Combinatorica.
- [85] H. Lüneburg. Transitive Erweiterungen endlicher Permutationsgruppen, Lecture Notes in Mathematics 84, Springer-Verlag, Berlin-Heidelberg-New York (1969).
- [86] F. J. MacWilliams and N. J. A. Sloane. The theory of error-correcting codes, North-Holland, Amsterdam (1977).

- [87] F. J. MacWilliams, N. J. A. Sloane and J. -M. Goethals. The MacWilliams identities for nonlinear codes, Bell System Tech. J., 51 (1972), 803-19.
- [88] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson. On the existence of a projective plane of order 10, J. Combinatorial Theory, 14 (1973), 66-78.
- [89] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes, Information and control, 22 (1973), 188-200.
- [90] J. L. Massey. Threshold decoding, M.I.T. Press, Cambridge, Mass. (1963).
- [91] H. Enomoto, N. Ito and R. Noda. Tight 4-designs, Osaka J. Math. 16 (1979), 39-43.
- [92] R. Noda. On orthogonal arrays of strength 4 achieving Rao's bound, J. London Math. Soc. (2), 19 (1979), to appear.
- [93] A. Ja. Petrenjuk. Math. Zametski, 4 (1968), 417-25.
- [94] V. Pless. Symmetry codes over $GF(3)$ and new 5-designs, J. Combinatorial Theory, 12 (1972), 119-42.
- [95] V. Pless. Symmetry codes and their invariant subcodes, J. Combinatorial Theory ser A, 18 (1975), 116-25.
- [96] F. P. Preparata. A class of optimum nonlinear double-error-correcting codes, Inform. Control, 13 (1968), 378-400.
- [97] C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays, J. Roy. Statist. Soc., 9 (1947), 128-39.
- [98] D. K. Ray-Chaudhuri and R. M. Wilson. On t-designs, Osaka J. Math., 12 (1975), 737-44.
- [99] H. J. Ryser. Combinatorial mathematics, Wiley, New York (1965).
- [100] H. Sachar. Error-correcting codes associated with projective planes, Ph.D. Thesis, Lehigh University, Bethlehem, Pa. (1973).
- [101] L. L. Scott. Some properties of character products, J. Algebra, 45 (1977), 259-65.
- [102] J. J. Seidel. Strongly regular graphs with $(-1, 1, 0)$ adjacency matrix having eigenvalue 3, Linear Alg. Appl., 1 (1968), 281-98.
- [103] J. J. Seidel. Strongly regular graphs, Recent progress in combinatorics (ed. W. T. Tutte) Acad. Press (1969), 185-97.

- [104] J. J. Seidel. A survey of two-graphs, Proc. Int. Coll. Theorie Combinatorie, Acc. Naz. Lincei, Roma (1973).
- [105] J. J. Seidel and D. E. Taylor. Two-graphs, a second survey, Algebraic methods in graph theory, Szeged (1978).
- [106] N. V. Semakov, V. A. Zinovjev, G. V. Zaitzef. Uniformly packed codes, Probl. Peredaci Inform., 7 (1971), 38-50 (Russian); translation in Problems of Information Transmission, 7 (1971), 30-9.
- [107] S. S. Shrikhande. The uniqueness of the L_2 association scheme, Ann. Math. Statist., 30 (1959), 781-98.
- [108] E. F. Shult. The graph extension theorem, Proc. Amer. Math. Soc., 33 (1972), 278-84.
- [109] C. C. Sims. On the isomorphism of two groups of orders 44, 350,000, Theory of finite groups (ed. R. Brauer and C. H. Sah); Benjamin, New York (1969).
- [110] N. J. A. Sloane. Is there a $(72, 36, d = 16)$ self-dual code? IEEE Trans. on Information Theory IT-19, (1973), 251.
- [111] O. Tamaschke. Zur Theorie der Permutationsgruppen mit Regulärer Untergruppe I und II, Math. Z., 80 (1963), 328-52 and 443-65.
- [112] D. F. Taylor. Regular 2-graphs, Proc. London Math. Soc., 35 (1977), 257-74.
- [113] J. A. Thas. Combinatorics of partial geometries and generalized quadrangles, Higher Combinatorics (M. Aigner, ed.), D. Reidel, Dordrecht, (1977), 183-99.
- [114] A. Tietäväinen. On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math., 24 (1973), 88-96.
- [115] H. C. A. van Tilborg. Uniformly packed codes, Thesis, Technological University Eindhoven (1976).
- [116] J. A. Todd. A representation of the Mathieu group M_{24} as a collineation group, Ann. di Mat. Pura ed Appl. (ser. 4) 71 (1966), 199-238.
- [117] O. Veblen and J. W. Young. Projective geometry, Ginn and Co., Boston (1916).

- [118] H. N. Ward. Quadratic residue codes and symplectic groups, J. Algebra, 29 (1974), 150-71.
- [119] H. Wielandt. Finite permutation groups, Acad. Press, New York-London (1964).
- [120] E. Witt. Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Seminar Hamburg 12 (1938), 256-64.
- [121] E. Witt. Über Steinersche Systeme, Abh. Math. Seminar Hamburg 12 (1938), 265-75.
- [122] E. F. Assmus, Jr. and C. J. Salwach. The $(16, 6, 2)$ designs, Internat. J. Math. and Math. Sci., 2 (1979), 261-81.
- [123] C. J. Salwach and J. A. Mezzaroba. The four known biplanes with $k = 11$, Internat. J. Math. and Math. Soc., 2 (1979), 251-60.

Index

- adjacency matrix 17
- affine geometry 7
 - permutation group, $AGL(1, q)$ 72
 - plane 7
 - symplectic geometry 8
- alphabet 61
- arc 11, 89
- Assmus-Mattson theorem 101
- association scheme 124
 - additive 135
 - dual 135
 - metric 125
 - polynomial 129
- block design 2
- Bose-Mesner algebra 126
- Bruck-Ryser-Chowla theorem 4
- centraliser algebra 22, 126
- check polynomial 69
- circuit 37
- C-matrix 107
- cocycle 50
- code
 - BCH 71
 - binary Golay 86, 100, 108
 - cyclic 68
 - dual 63
 - equidistant 81
 - equivalent 63
 - Euclidean geometry 81
 - extended 64
 - generalised quadratic residue 105
 - Hamming 69, 78
 - linear 62
 - nearly perfect 113, 115
 - perfect 62, 85, 86, 100, 130
 - Preparata 116
 - primitive BCH 71
 - projective 121
 - projective geometry 81
 - quadratic residue 97
 - Reed-Muller (RM) 78
 - self-dual 84
 - self-orthogonal 81, 84
 - symmetry 107
 - systematic 63
 - ternary Golay 85, 108
 - two-weight 113, 121
 - uniformly packed 113, 115
- complement (of a graph) 16
- degree 133
- Desarguesian 7
- design
 - derived 8
 - Hadamard 5
 - pair 17

design

- Paley 5, 67
- quasi-residual 8, 35
- quasi-symmetric 25
- residual 8
- symmetric 3
- t- 1
- tight 13, 133

diameter 37

distance 61, 130

- designed 71
- external 130
- minimal 130

distribution matrix 128

error 61

error-correcting code 62

Euclidean geometry 7

extension

- of a code 64
- of a design 8, 51
- of a permutation group 52, 55
- of a symmetric design 9, 41

1-factor 56

finite geometry 76

Fisher's inequality 3

generalised quadrangle 35

generator matrix 63

- polynomial 68

girth 37

graph 16

- block 26
- Clebsch 19
- complete 16

graph

- complete k-partite 19
- connected 37
- geometric 34
- Gewirtz 19, 39, 92
- Higman-Sims 30
- Hoffman-Singleton 38, 58
- ladder 19
- Latin square 36
- lattice, $L_2(n)$ 19, 34, 54
- line 25, 33
- Moore 37, 58
- null 16
- Paley 19
- Petersen 19, 52
- point 33
- pseudo-geometric 34
- rank-3 20
- regular 17
- Shrikhande 34
- strongly regular 17, 25, 33, 37, 45, 51, 121
- triangular, $T(n)$ 19, 32, 59

group algebra 105

Hadamard design 5

- matrix 5

Hamming distance 61

- scheme 124

hyperplane 6

idempotent 95, 131

incidence matrix 2, 17

inner distribution 128

inversive plane 10

- Johnson bound 114
 - scheme 124
- Krein bound 132
- Latin square 16, 36
- linear fractional group, $\text{PGL}(2, q)$
 - 10, 106
- majority decoding 74
- Mathieu groups 14, 60
- Möbius plane 10, 106
- multiplicities 21, 23, 127
- net 36
- null polarity 46
- orthogonal check set 74
- oval 11, 89, 93
- parity check 63
 - matrix 63
 - overall 64
- partial geometry 33, 82
- path 37
- passant 11
- polarity 3, 45
- projective geometry 6
 - plane 6, 88
- rationality condition 21
- regular 17, 51, 128
- secant 11
- sphere 61
- square root bound 100
- standard form 63
- Steiner system 1, 70, 85, 131
 - strength 133, 135
 - switching 24, 50
 - tangent 11
 - threshold decoding 74
 - two-graph 49
 - valency 17
 - weight 61
 - enumerator 65
 - word 61
 - length 61