Graphs and association schemes, algebra and geometry

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE
EN INFORMATICA

EINDHOVEN UNIVERSITY OF TECHNOLOGY
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS
AND COMPUTING SCIENCE

Graphs and association schemes, algebra and geometry

by

J.J. Seidel
A. Blokhuis
H.A. Wilbrink

Notes prepared by
J.P. Boly
C.P.M. van Hoesel

AMS Subject classification 05

EUT - Report 83-WSK-02

May 1983

Contents.

Preface.

"Graphs and Association Schemes" was the subject of the Combinatorial Theory Seminar Eindhoven in the fall semester of 1982. The selection of this subject was governed both by didactical considerations and by preference and scientific involvement of the lecturers. Each week lectures were given by one of the senior members and by one of the student members. The present notes have been worked out by the students J.P. Boly and C.P.M. van Hoesel.

Chapter 1 introduces spectral methods in graph theory, concentrating on graphs with $\alpha_{max} = 2$, and on those with $\alpha_{min} = -2$. Apart from most of the line graphs, this last class contains some further interesting graphs; they are interrelated by switching. Finally Turan's theorem on cocliques is applied to a problem in coding theory. In Chapter 2 some more results on eigenvalues of matrices are derived such as interlacing theorems. These are applied in the theory of graphs (e.g. in connection with generalized quadrangles) and of designs (e.g. in connection with absolute points in a projective plane). The next chapters are dedicated to association schemes. Chapter 3 introduces the Bose-Mesner algebra and P- and Q- polynomial schemes. Examples from PG(2,4), from generalized hexagons, and from regular two-graphs are worked out. The chapter culminates in the MacWilliams transform and in Delsarte's code-clique theorem. There is an appendix on algebraic tools. Chapter 4 discusses Hollman's results on Pseudo-cyclic association schemes: (i) equal multiplicities iff equal valencies plus an extra condition; (ii) construction of a new 3-scheme on 28 vertices which, together with Mathon's scheme, is unique; (iii) construction of a new class of schemes from the action of PO(3,q) on PG(2,q), $q = 2^m$.

Chapter 5 deals with few-distance sets. The absolute and the mod p bound for spherical s-distance sets are proved. The relations between two-graphs, switching classes and equiangular lines are indicated. The possibilities for equiangular lines having $\cos \phi = 1/3$ are worked out in detail. Finally, in Chapter 6 the following theorems from combinatorial geometry are proved. (i) For large d there are at least $(1.15)^d$ points in R^d having only acute angles. (ii) There are at least $(1 + \frac{1}{2}\gamma)^d$ points in R^d having all angles smaller than $\gamma + \pi/3$ (Erdös-Füredi).

(iii) Indecomposable isosceles sets in R^d are two-distance sets.

We hope that the present notes will serve the members of the seminar and many others.

May 1983

J.J. Seidel,
A. Blokhuis,
H.A. Wilbrink.

Seminar Combinatorial Theory , fall 1982.

Subjects: Graphs and association schemes, algebra and geometry.

Members: J.J. Seidel, A. Blokhuis, H.A. Wilbrink, H. Tiersma, I.J.M. Neervoort, R. Schmitt, M. van de Ham, C.P.M. van Hoesel, J.P. Boly, J. van de Leur, F. Merkx, R. Klerx, P. Coebergh, A.J. van Zanten (T.H. Delft), P. Vroegindeweij, F.C. Bussemaker, H. van Tilborg, C. van Pul.

Lectures:

8 sept. 1982 J.J. Seidel, Graphs and their spectra.
F. Souren, The absolute bound for spherical two-distance sets.

15 sept. 1982 I.J.M. Neervoort, Graphs with $\alpha_{max} = 2$ (Perron-Frobenius).
J.J. Seidel, Graphs with $\alpha_{min} = -2$ (root-systems).

22 sept. 1982 R. Schmitt, The switching-classes of T(5), T(8), $L_2(4)$.
H.A. Wilbrink, Eigenvalue techniques.

29 sept. 1982 H. Tiersma, Generalized quadrangles.
H.A. Wilbrink, Interlacing of eigenvalues.

6 oct. 1982 J.P. Boly, Absolute points in PG(2,n).
A. Blokhuis, Sets of points with no obtuse angles.

13 oct. 1982 C.P.M. van Hoesel, Isosceles point sets in R^d.
J.J. Seidel, Association schemes.

20 oct. 1982 J. van de Leur, Generalized hexagons.
J.J. Seidel, Association schemes.

27 oct. 1982 R. Klerx, Pseudo-cyclic association schemes.
J.J. Seidel, Distribution matrix.

3 nov. 1982 P. Coebergh, The theorem of Turan about the largest coclique in a graph.
H.A. Wilbrink, Minimal idempotents.

10 nov. 1982 F. Merkx, An association scheme in PG(2,4).
A. Blokhuis, Pseudo-cyclic association schemes with three classes on 28 vertices.

17 nov. 1982 M. van de Ham, Regular two-graphs as association schemes.
H.A. Wilbrink, PSL(2,q) and PO(3,q), $q = 2^m$.

24 nov. 1982 H.A. Wilbrink, Pseudo-cyclic association schemes from PSL(2,q), $q = 2^m$.

1 dec. 1982 J.J. Seidel, One-distance sets.

8 dec. 1982 A. Blokhuis, Few-distance sets.

Chapter 1.

Graphs and their spectra.

1.1. Introduction.

In the past years much attention has been paid to the question, what properties of graphs are characterized by the spectrum of their adjacency matrix. In particular we can ask ourselves whether a graph or a class of graphs is uniquely determined by its spectrum.

This chapter deals with connected graphs, having largest eigenvalue 2 and those with smallest eigenvalue -2. Also the spectra of two classes of graphs are determined and further an equivalence relation on graphs, based on their spectrum, is given. Finally we derive a theorem about the largest coclique in a graph, with an application to coding theory. General references for this chapter are [3], [9], [11], [13], [21], [31].

1.2. Graphs with largest eigenvalue 2.

A graph (V,E), where V is the set of vertices and E the set of edges, has an adjacency matrix A defined by

$$a_{ij} = 1 \quad \text{iff} \quad (i,j) \in E \qquad (i \text{ and } j \in V)$$
$$a_{ij} = 0 \quad \text{iff} \quad (i,j) \notin E.$$

Remark. $a_{ii} = 0$ for all $i \in V$.

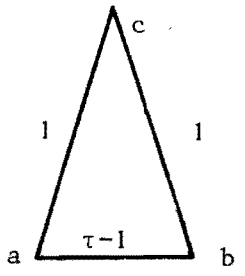
1.2.1. Example. The pentagon graph consists of five vertices with cyclic adjacencies. The adjacency matrix is

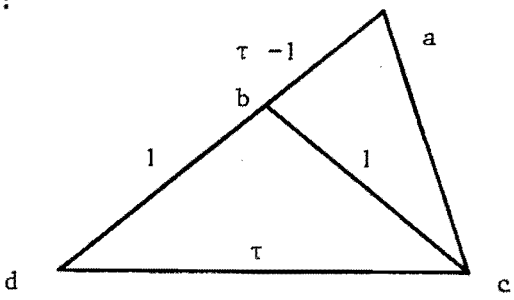
$$A_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = P_5 + P_5^T \quad \text{where} \quad P_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The eigenvalues of A_5 can be derived from those of P_5. Because $(P_5)^5 = I$, the five eigenvalues of P_5 satisfy $\alpha^5 = 1$.

This leads to $\text{spec}(P) = \{ e^{2\pi ik/5} \mid k = 1,..,5 \}$, and therefore, $\text{spec}(A) = \{ e^{-2\pi ik/5} + e^{2\pi ik/5} \} = \{ 2\cos(2\pi k/5) \}$, since $P_5^T = P_5^{-1}$. It is easy to see that $\alpha_{max} = 2$. A method to determine all eigenvalues explicitly is given below:

I





II

Let $2\cos(2\pi/5) = \tau - 1$. The triangles I and II are similar and bcd is isosceles, so bd = 1 and ad = cd = τ. Similarity of I and II leads to

$$\frac{\tau - 1}{1} = \frac{1}{\tau}, \text{ or } \tau^2 = \tau + 1, \text{ with positive solution } \tfrac{1}{2}(\sqrt{5} + 1).$$

Henceforth we will reserve the symbol τ to denote this number called the "golden ratio".

In terms of τ we have

$$\text{spec}(A) = \{ 2, \tau^{-1}, \tau^{-1}, -\tau, -\tau \}.$$

All graphs with $\alpha_{max} = 2$ can easily be found with the help of the next three theorems.

1.2.2. Theorem. (Perron-Frobenius). Let A be an irreducible, nonnegative, square matrix, then the largest eigenvalue of A is positive of multiplicity one, and it has an eigenvector with all entries positive.

Remarks.

(i) We only deal with the adjacency matrices of connected graphs. These are irreducible.

(ii) All eigenvectors belonging to $\alpha_i \neq \alpha_{max}$ have at least one negative entry, since they are orthogonal to a positive vector.

1.2.3. Lemma. If $\tilde{A} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and $\tilde{A}$ is irreducible and all its entries are nonnegative, then $\alpha_{max}(\tilde{A}) > \alpha_{max}(A)$.

Proof. From 1.2.2. we know that the eigenvector $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ of $\tilde{A}$ for $\alpha_{max}(\tilde{A})$ is positive. Therefore

$$\alpha^2_{max}(\tilde{A}) = \max \frac{\|\tilde{A}x\|^2}{\|x\|^2} = \max \frac{\|Ax_1 + Bx_2\|^2 + \|Cx_1 + Dx_2\|^2}{\|x_1\|^2 + \|x_2\|^2} >$$

$$> \max \frac{\|Ax_1 + Bx_2\|^2}{\|x_1\|^2 + \|x_2\|^2} \geq \max \frac{\|Ax_1\|^2}{\|x_1\|^2} = \alpha^2_{max}(A).$$

Since $\tilde{A}$ is irreducible, B and C are not null matrices. So inequality holds.

□

1.2.4. Definition. The complete bipartite graph $K_{i,j}$ is a graph whose vertices can be divided into two subsets X_1 and X_2 of i and j vertices, respectively, such that X_1 and X_2 form two cocliques and each vertex of X_1 is adjacent to all the vertices of X_2.

A k-claw is a complete bipartite graph $K_{1,k}$.

1.2.5. Lemma. A graph having $\alpha_{max} = 2$ does not contain k-claws with $k > 4$.

Proof. Let A be the adjacency matrix of the graph, where the first k + 1 vertices form the k-claw. Since $\alpha_{max}(A) = 2$,

$$2I - A = \left[\begin{array}{cccc|c} 2 & -1 & \cdots & -1 & \\ -1 & & & & \\ \vdots & & 0 & & B \\ & & & & \\ -1 & & & 2 & \\ \hline & B^T & & & C \end{array}\right]$$

is positive semidefinite.

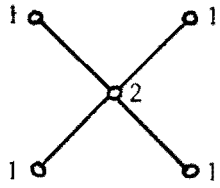
This implies that the upperleft submatrix is positive semidefinite.

Hence $$\det \left[\begin{array}{c|c} 2 & -j^T \\ \hline -j & 2I \end{array}\right] = \det \begin{bmatrix} 2 - k/2 & 0 \\ 0 & 2I \end{bmatrix} \geq 0$$

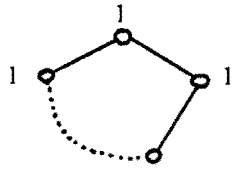
Therefore $2 - k/2 \geq 0$ and so $k \leq 4$.
For $k = 4$ we must have $B = 0$. □

Remark. If a graph has $\alpha_{max} = 2$ with eigenvector x, this eigenvector satisfies $Ax = 2x$, hence
For all i $2x_i = \Sigma\, x_j$ where the summation is over all j with j adjacent to i.

To find all graphs with $\alpha_{max} = 2$, we search systematicly for all possibilities, starting with the 4-claw.

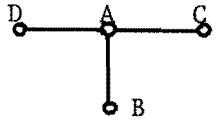
1) 

The 4-claw has $\alpha_{max} = 2$ with eigenvector $(1,1,1,1,2)^T$. This implies, by lemma 1.2.3., that all graphs having a 4-claw as a proper subgraph have $\alpha_{max} > 2$.

2) 

The graphs with only 2-claws are circular graphs. Adding edges cannot lead to other graphs with $\alpha_{max} = 2$, since these graphs have a circular graph as a subgraph or they are circular themselves.

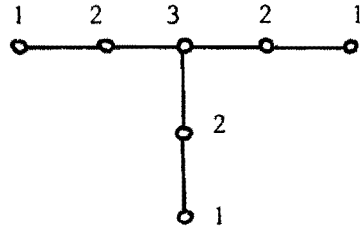
3) Now consider a 3-claw. Being a subgraph of the 4-claw a 3-claw has $\alpha_{max} < 2$. We add vertices in all possible ways until we obtain graphs with $\alpha_{max} \geq 2$. No further adding of vertices is possible, according to 1.2.3.

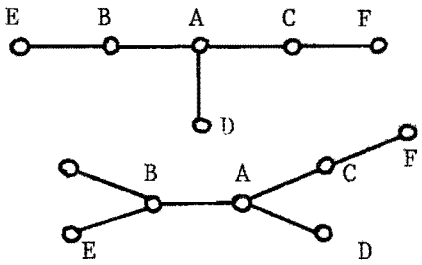


If we add a vertex to A we obtain the 4-claw again.

We distinguish three other cases:

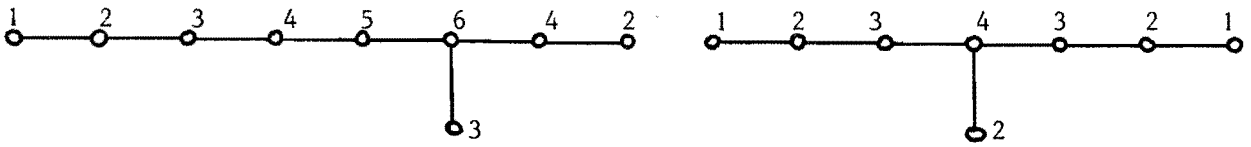
(i) Add vertices to all three vertices B, C and D. This gives the graph on the right, that has $\alpha_{max} = 2$, with eigenvector $(1,2,3,2,1,2,1)^T$.



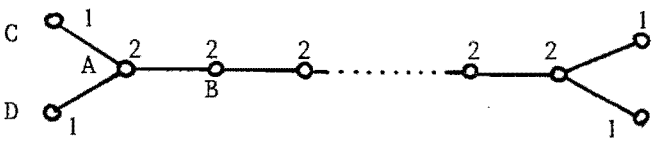


(ii) Add vertices only to B and C. This graph has still $\alpha_{max} < 2$. Adding another point to B yields a graph with $\alpha_{max} > 2$ as we will see in (iii).

The only two ways left to get a graph with $\alpha_{max} = 2$, are: adding vertices to E only (3) or one vertex to both E and F.



(iii) The last possibility is adding a vertex to B only. This can only be done as following:



Remark. We will encounter these graphs again, in relation with sets of lines in Euclidean d-spaces in section 1.5.

1.3. Line Graphs.

The incidence metrix N of a graph is a v x e matrix, where v is the number of vertices and e the number of edges of the graph.

$(N)_{ij} = 1$ iff vertex i and edge j are incident,

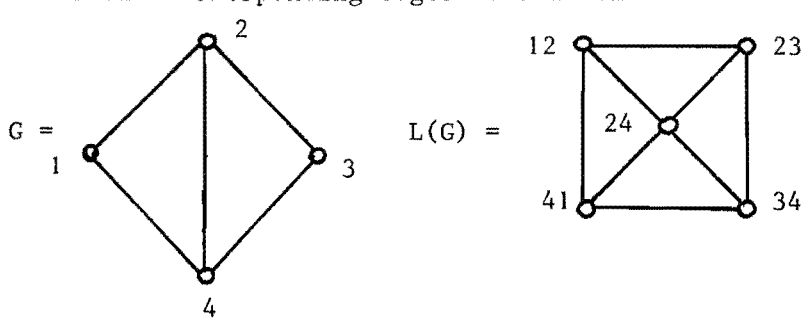
$(N)_{ij} = 0$ otherwise.

One can simply verify that

$$NN^T = D + A \quad \text{and} \quad N^TN = 2I + L,$$

where D is diagonal with d_{ii} the number of vertices adjacent to i, A is the adjacency matrix of the graph and L is the adjacency matrix of the linegraph. The vertices of the linegraph correspond with the edges of the graph. Two vertices of the linegraph are adjacent, whenever the corresponding edges have a common vertex.

Example.



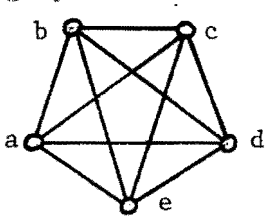
The importance of the incidence matrix lies in the fact that if we know the eigenvalues of NN^T or N^TN we can easily find the eigenvalues of L and those of A, if A is regular. This is expressed in the next theorem.

1.3.1. Theorem. NN^T and N^TN have the same eigenvalues, except for 0, with the same multiplicities.

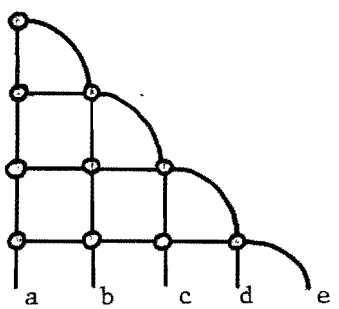
Proof. Let $\lambda \neq 0$ be an eigenvalue of NN^T of multiplicity f.
Then $NN^TU = \lambda U$ for a matrix U of rank f. Therefore
$N^TNN^TU = \lambda N^TU$.
$\text{Rank}(U) = \text{rank}(\lambda U) = \text{rank}(NN^TU) \leq \text{rank}(N^TU) \leq \text{rank}(U)$.
Hence $\text{rank}(N^TU) = f$.
Because $N^TN(N^TU) = \lambda N^TU$, we find that λ is an eigenvalue of N^TN of multiplicity f. □

Examples. The complete graph K(n) has the triangular graph T(n) as its linegraph

K(5)



T(5)



The incidence matrix N has size $n \times \binom{n}{2}$

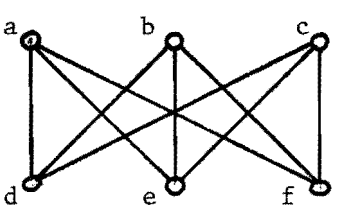
$NN^T = (n-1)I + J - I$ spec $(NN^T) = ([2n-2]^1, [n-2]^{n-1})$

spec $(N^TN) = ([2n-2]^1, [n-2]^{n-1}, [0]^{\frac{1}{2}(n-3)n})$

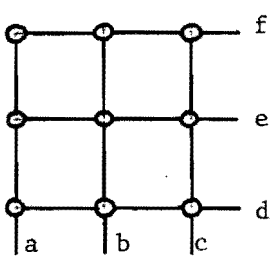
since $L = N^TN - 2I$ spec $(A(T(n))) = ([2n-4]^1, [n-4]^{n-1}, [-2]^{\frac{1}{2}(n-3)n})$

The complete bipartite graph $K_{n,n}$ has as its linegraph the lattice graph $L_2(n)$.

$K_{3,3}$



$L_2(3)$



$K_{n,n}$ has $2n \times n^2$ incidence matrix N for which holds

$$NN^T = nI + \begin{bmatrix} 0 & J \\ J & 0 \end{bmatrix} \quad \text{with} \quad \begin{aligned} \text{spec}(NN^T) &= ([n]^{2n-2}, [2n]^1, [0]) \\ \text{spec}(N^TN) &= ([n]^{2n-2}, [2n]^1, [0]^{(n-1)^2}) \\ \text{spec}(A(L_2(n))) &= ([n-2]^{2n-2}, [2n-2]^1, [-2]^{(n-1)^2}) \end{aligned}$$

We see that these linegraphs all have smallest eigenvalue -2.
The reason is that the original graphs have more edges than vertices. In that case the size of NN^T is smaller than that of N^TN which means that N^TN, being positive semidefinite has smallest eigenvalue 0. So the linegraph has smallest eigenvalue -2.

1.4. The Switching-classes of T(5), T(8), $L_2(4)$.

Apart from the (0,1) adjacency matrix A of a graph, we have the (-1,1) adjacency matrix C, where $C_{ij} = -1$ iff the vertices i and j are adjacent, and $c_{ij} = 1$ iff they are not adjacent, diag(C) = 0.
The relation between A and C is

$$C = J - I - 2A$$

For regular graphs the spectra of A and C are related as following

$$\text{spec}(C) = (\gamma_m = v-1-2\alpha_m, \gamma_i = -1-2\alpha_i)$$

where α_m is the largest eigenvalue of A and α_i are the others.

1.4.1. Examples.

T(n) has C-spectrum $\left(\frac{1}{2}(n-2)(n-7)^1, 7-2n^{n-1}, 3^{\frac{1}{2}n(n-3)}\right)$

$L_2(n)$ has C-spectrum $\left((n-1)(n-3)^1, 3-2n^{2n-2}, 3^{n^2-2n+1}\right)$

In general T(n) and $L_2(n)$ have three different eigenvalues. However for some n there are only two distinct eigenvalues.

T(n):	if $\frac{1}{2}(n-2)(n-7) = 7-2n$	then n = 5
	or $\frac{1}{2}(n-2)(n-7) = 3$	then n = 8
$L_2(n)$:	if $(n-1)(n-3) = 3$	then n = 4

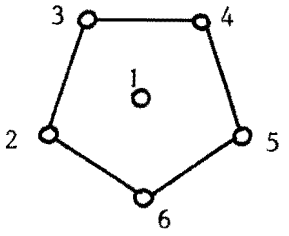
So in this case the (0,±1) adjacency matrices satisfy a quadratic equation:

T(5)	$(C - 3I)(C + 3I) = 0$	$v = 10$	$k = 6$
T(8)	$(C - 3I)(C + 9I) = 0$	$v = 28$	$k = 12$
$L_2(4)$	$(C - 3I)(C + 5I) = 0$	$v = 16$	$k = 6$

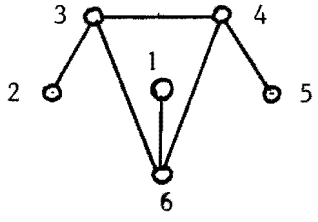
Switching.

Let x be any vertex of a graph. Switching with respect to x is defined to be the following operation: cancel all existing adjacencies to x and add all nonexisting adjacencies to x. The effect of switching with respect to x on the adjacency matrix C is that the row and column corresponding to x are multiplied by -1.

Example of switching (w.r.t. vertex 6):



$$C = \begin{bmatrix} 0 & + & + & + & + & + \\ + & 0 & - & + & + & - \\ + & - & 0 & - & + & + \\ + & + & - & 0 & - & + \\ + & + & + & - & 0 & - \\ + & - & + & + & - & 0 \end{bmatrix}$$



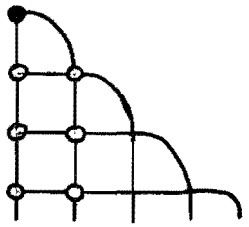
Switching with respect to any number of vertices is an equivalence relation on the set of all graphs on v vertices. For a given (-1,1) adjacency matrix C, the switching class consists of graphs with (-1,1) adjacency matrices DCD, where $D = \mathrm{diag}(\pm 1)$. It is clear that the C-spectra of switching equivalent graphs are the same.
Switching with respect to a certain subset of a graph has the same effect as switching with respect to the subset's complement. In terms of matrices this is changing D into -D.

Problem. Find all regular graphs, possibly except for an isolated vertex, in the switching-classes of T(5), T(8), $L_2(4)$.

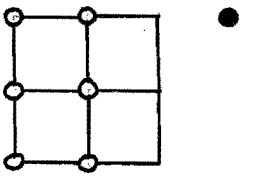
There are two ways in which one may obtain a strongly regular graph from a graph whose C-matrix has only two eigenvalues. The first one is to isolate one vertex. Then the graph on the remaining vertices is strongly regular. The second one occurs if it is possible to switch in such a way that the resulting graph is regular (it is easy to see that there are only two possible valencies). The graph will then be automatically strongly regular.

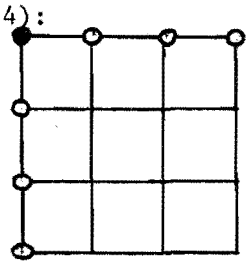
1) Isolation.

We isolate the ●-marked vertex (a "black" vertex), by switching with respect to the ○-marked vertices ("white" vertices).

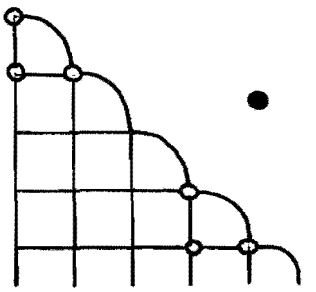
T(5): 

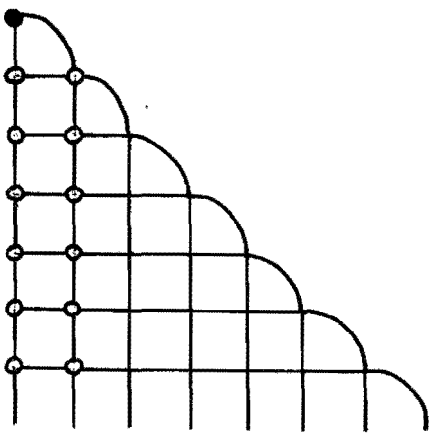
we get $L_2(3)$ and an isolated vertex.



$L_2(4)$: 

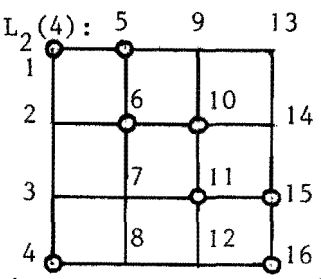
we get T(6), k = 8, and an isolated vertex.



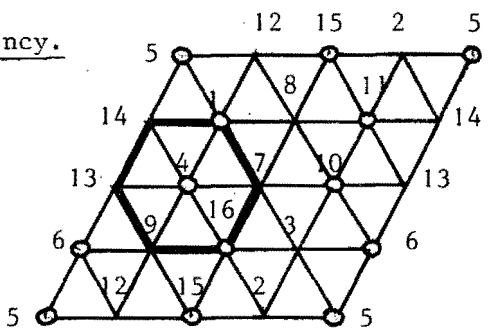
T(8): 

We get the Schläfli-graph. In this graph each vertex in the switching set is adjacent to six other switchpoints and to ten non-switchpoints. The non-switchpoints are adjacent to eight others and to eight switchpoints. So the Schläfli-graph is regular with k = 16, hence strongly regular.

2) Non-isomorphic graphs with the same valency.

$L_2(4)$: 

leads to

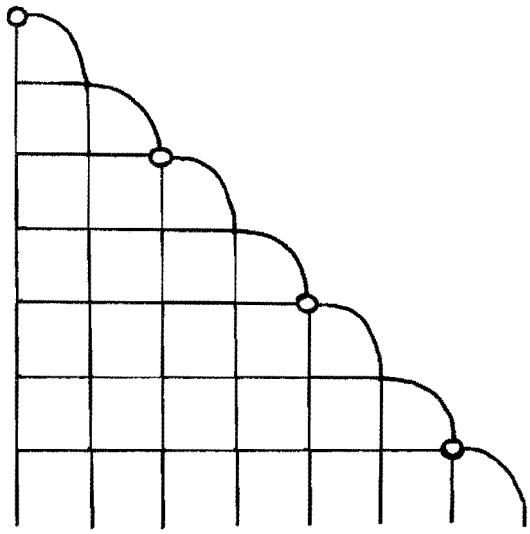


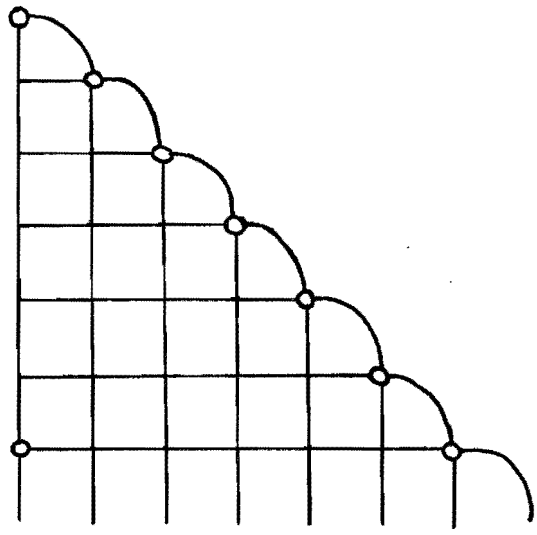
(In the second graph two vertices are adjacent iff they are adjacent in the picture, in $L_2(4)$ two vertices are adjacent iff they are on one line)

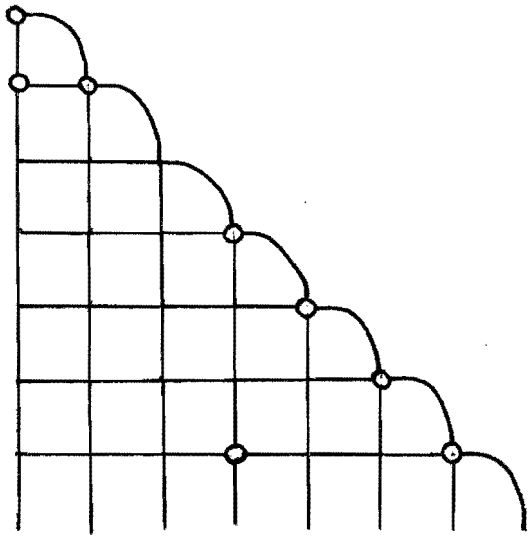
The second graph is called the Shrikhande-graph. This graph is not isomorphic to $L_2(4)$. In $L_2(4)$ each vertex is adjacent to two groups of three vertices, and in the Shrikhande-graph each vertex is adjacent to a 6-cycle.

T(8).

Switching into a non-isomorphic graph with k = 12, can only be done in three essentially different ways, leading to the following "Chang-graphs".







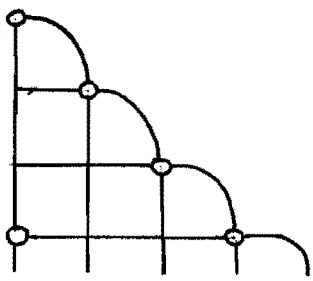
None of these graphs is isomorphic to T(8), because each point in T(8) is adjacent to a 6-clique.
T(5) has no non-isomorphic graphs with k = 6.

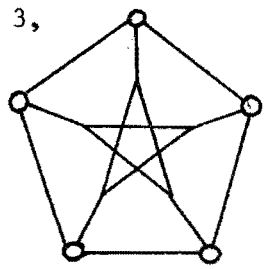
3) Graphs with a different valency k.

Regular graphs in one of the switching-classes satisfy $v-1-2k = \gamma_m$, where γ_m is an eigenvalue of the adjacency matrix C. This reduces the number of possible valencies k to two:

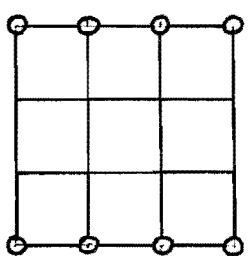
C(T(5))	has eigenvalues	3 (k = 3) and -3 (k = 6)
$C(L_2(4))$	has eigenvalues	3 (k = 6) and -5 (k =10)
C(T(8))	has eigenvalues	3 (k =12) and -9 (k =18)

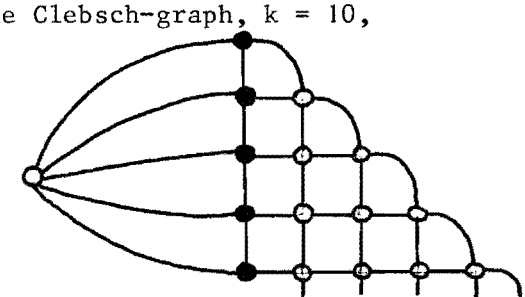
T(5): We get the Petersen-graph, k = 3,





$L_2(4)$: We get the Clebsch-graph, k = 10,





In the Clebsch-graph two ●-vertices or two ○-vertices are adjacent iff they have a line in common and a ●-vertex and a ○-vertex are adjacent iff they have no line in common.

Remark. Shrikhande has proved that the only regular graphs with v = 16 and k = 6 or k = 10 are the three graphs that we met here: $L_2(4)$, Shrikhande and the Clebsch-graph.

T(8):

Switching to a graph with k = 18 is not possible.

Proof. Let A be the (0,1) adjacency matrix of such a graph. Then its eigenvalues are k = 18, r = 4 and s = -2. (γ_m = -9, γ_i = -9 or 3) with multiplicities 1, f and g. Because the multiplicities add up to v and trace(A) = 0 we know 1 +f + g = 28 and 18 + 4f - 2g = 0. This leads to f = 6 and g = 21.

So spec(A) = $(18^1, 4^6, (-2)^{21})$ and spec(2I + A) = $(20^1, 6^6, 0^{21})$.
$\underline{j} = (1, 1, \ldots 1)^T$ is an eigenvector of A with eigenvalue k = 18.
Because $\underline{j}$ is also an eigenvector of J with eigenvalue v = 28,
we get: spec$(A + 2I - \frac{20}{28} J) = (0^1, 6^6, 0^{21})$.
Consider $A + 2I - \frac{20}{28} J$ as the Grammatrix of 28 vectors in R^6. These 28 vectors form a spherical two-distance set since

$$A + 2I - \frac{20}{28} J = \begin{bmatrix} \alpha & & \beta/\gamma \\ & \alpha & \\ & \ddots & \\ \beta/\gamma & & \alpha \end{bmatrix} \qquad \text{where} \quad \alpha = 2 - \frac{20}{28}, \quad \beta = -\frac{20}{28}, \quad \gamma = 1 - \frac{20}{28}.$$

But a spherical two-distance set in R^6 contains at most
$\frac{1}{2} \cdot 6 \cdot (6+3) = 27$ vectors. So the graph cannot exist.
(In section 5.1. we will show that a spherical two-distance set in R^d cannot contain more than $\frac{1}{2}d(d + 3)$ points). □

Remark. The graphs, we have found here are all strongly regular graphs. They have adjacency matrices C that satisfy $(C - \alpha_1 I)(C - \alpha_2 I) = 0$. Graphs with this property are examples of strong graphs, and regular graphs that are strong are strongly regular.

1.5. Graphs with smallest eigenvalue -2.

We start with some examples. We have already met the line graphs in section 1.2. Some other graphs are the cocktail party graphs on 2n vertices. These are graphs with

$$A = \begin{bmatrix} J - I & J - I \\ J - I & J - I \end{bmatrix} \qquad \text{spec}(A) = (2n-2^1, 0^n, -2^{n-1}).$$

Further the strongly regular graphs of Petersen (v = 10), Clebsch (16), Shrikhande (16), Schläfli (27), Chang (28).
If a graph has $\alpha_{min} = -2$ then

$$2I + A = \begin{bmatrix} 2 & & \\ & \ddots & 0/1 \\ 0/1 & & 2 \end{bmatrix}$$

can be considered as the Grammatrix of a set of vectors at 60 and 90 degrees in R^d.

Since each vector spans a line, through the origin, we have a set of lines at 60 and 90 degrees in R^d. Conversely suppose we have a set of 1 lines at 60 and 90 degrees. We can take two vectors along each line, of length $\sqrt{2}$. Their Grammatrix G has entries $\{ \pm 2, \pm 1, 0 \}$, and it is positive semidefinite. If we rearrange G we get

$$G = \begin{bmatrix} 2 & 0/-1 & & \\ 0/-1 & 2 & 0/1/-1/2 & \\ & & \ddots & 2 \\ & 0/1/-1/-2 & 2 & 0/1 \\ & & 0/1 & 2 \end{bmatrix}$$

The upperleft submatrix is $2I - B$, where B is a (0,1) matrix with $\alpha_{max} \leq 2$. The lowerright submatrix is $2I + A$, where A is a (0,1) adjacency matrix having $\alpha_{max} \geq -2$. Such a set of lines can be completed in the following sense. If it contains two lines, 1 and m at 60^o, a third line, in the plane of 1 and m, can be added at 60^o with 1 and m, and at 60^o and 90^o with all other lines. A collection to which no more lines like these can be added is called star-closed.

1.5.1. Theorem. The irreducible sets of lines at 60^o and 90^o which are star-closed, are the root systems:

$$A_n, D_n, E_6, E_7, E_8.$$

(Irreducible sets of lines are collections that cannot be divided in two or more orthogonal subsets.)

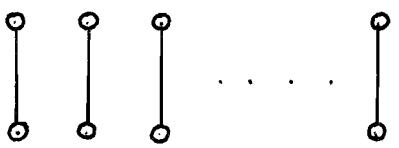
Let $\underline{e}_1, \ldots \ldots \underline{e}_n$ be the orthonormal basis in R^n. The root-systems A_n, D_n, E_n $(n = 6,7,8)$ are described as following:

$$D_n := \{< \pm \underline{e}_i \pm \underline{e}_j > \mid i \neq j \in \{1,2, \ldots n\}\}, |D_n| = n(n-1).$$

$$A_n := \{< \underline{e}_i - \underline{e}_j > \mid i \neq j \in \{1,2, \ldots n+1\}\}, |A_n| = \tfrac{1}{2}n(n+1).$$

For example the cocktail party graphs consist of a subset of D_n:

$\{<\underline{e}_1 \pm \underline{e}_i> \mid i = 2, \ldots \ldots n+1\}$ where two "vertices" are adjacent iff they have only $\underline{e}_1$ incommon, hence it is the complement of the graph



(n times)

The friendship graph $\{\langle \underline{e}_1 \pm \underline{e}_i \rangle \mid i = 1,2, \ldots 8\} \cup \{\underline{e}_9 + \underline{e}_{10}\}$.

For the graph $G = (\{\underline{e}_1, \ldots \underline{e}_n\}, E)$, its linegraph is described by $\{\langle \underline{e}_i + \underline{e}_j \rangle \mid (i,j) \in E\}$ where two elements are adjacent iff they have $\underline{e}_i$ or $\underline{e}_j$ in common.

$L(K_6) = \{\langle \underline{e}_i + \underline{e}_j \rangle \mid i \neq j \quad i,j = 1,2, \ldots 6\}$.

$L(K_{3,3}) = \{\langle \underline{e}_i - \underline{e}_j \rangle \mid i = 1,2,3, \quad j = 4,5,6\}$.

$E_8 := D_8 \cup \{\frac{1}{2}(\varepsilon_1 \underline{e}_1 + \ldots \varepsilon_8 \underline{e}_8) \mid \varepsilon_i = \pm 1, \prod_{i=1}^{8} \varepsilon_i = 1\}$.

E_8 contains 56 + 64 = 120 lines. If we take one vector along each line we find a Grammatrix 2I + C. Since rank(2I + C) = 8 and 2I + C is p.s.d. the following holds:

$$\text{spec}(C) = ((-2)^{112}, \lambda_1, \ldots \lambda_8).$$

We have trace $C = 0 = 112(-2) + \sum_1^8 \lambda_i$, $\sum_1^8 \lambda_i = 224 = 8 \cdot 28$.

trace $C^2 = 120(120-1-63) = \sum \lambda_i^2 + 112 \cdot 4$, $\sum_1^8 \lambda_i^2 = 8 \cdot 28^2$.

So with help of the inequality of Cauchy-Schwarz $\lambda_1 = \ldots = \lambda_8 = 28$.

This results in

$$(C + 2I)(C - 28I) = 0.$$

Furthermore graphs in E_8 have ≤ 36 vertices, valency ≤ 28 and regular graphs have ≤ 28 vertices with valency ≤ 16.

Example: the Schläfli-graph is

$\{\langle \underline{e}_i + \underline{e}_j \rangle \mid i,j = 1,2, \ldots 6, i \neq j\} \cup$

$\cup \{\frac{1}{2}(\sum_{k=1}^{8} \underline{e}_k - \underline{e}_i - \underline{e}_j) \mid i = 1,2, \ldots 6, \quad j = 7,8\}$.

E_7 is the set of lines orthogonal to a single line in E_8. It has 63 lines.

E_6 is the line set orthogonal to a star in E_8. It contains 36 lines.

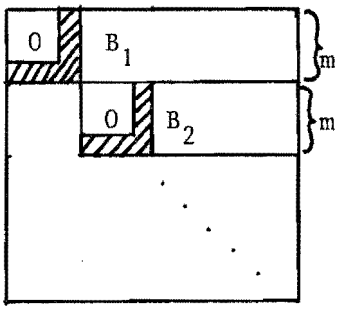
We refer to [9] to further details and proofs.

1.6. The theorem of Turan about the largest coclique in a graph; an application to coding theory.

1.6.1. Theorem. (Turan, [34]). In a graph on v vertices and with e edges, the size of the largest coclique is at least M, where

$$M = \min \{ m \in N \mid e \geq [\tfrac{v}{m}] \cdot v - \binom{[\frac{v}{m}]+1}{2} \cdot m \}$$

Proof. Assume that for some $m \in N$ the graph does not contain a coclique of more than m vertices. Let $q := [v/m]$. So $v = q \cdot m + r$, where $0 \leq r < m$. Divide the graph in a subgraph on m vertices, that contains the largest coclique, and a subgraph on $(q-1)m+r$ vertices. Repeat thisproces on the latter graph $q - 1$ times. Now each column in B_i contains at least one 1, since the corresponding coclique is maximal (see diagram). So



$$e \geq (v-m) + (v-2m) + \ldots\ldots\ldots (v - qm) =$$

$$= qv - \binom{q+1}{2}m.$$

□

1.6.2. Theorem. In a graph on v vertices and with e edges, the size M of the largest coclique is at least $v^2/(v + 2e)$ (*)

Proof. Consider the graphs in which the largest coclique contains at most m vertices. Fix $0 \leq r < m$. For these graphs on $qm + r$ vertices we prove that

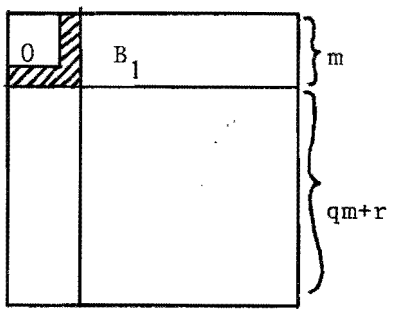
$$e \geq v(v-m)/2m \quad . \qquad (**)$$

Note that (*) $\Longleftrightarrow$ (**).

We use induction to q. For $q = 0$ (**) is trivial, because in that case $v < m$ holds, which means $v(v-m)/2m < 0$.

Assume (**) holds for q. Divide the graph on $v' = (q+1)m + r$ once as in 1.6.1. We immediately see $e' \geq v + v(v-m)/2m = v(v+m)/2m = (v'-m)v'/2m$.

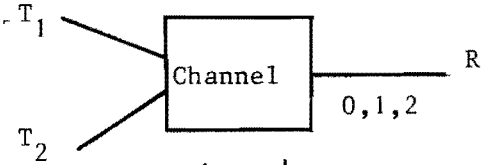
This can be done for any r, $0 \leq r < m$. □



Remark. The graph with $A = \left[\begin{array}{c|c} I_r \otimes (J - I)_{q+1} & O \\ \hline O & I_{m-r} \otimes (J - I)_q \end{array}\right]$

is an example for which in theorem 1.5.1. equality holds, for $|\text{maxcoclique}| = m$ and $e = qv - \binom{q+1}{2}m$.
For theorem 1.6.2. such a graph cannot be found for all v and m.

Application. (For more details see [12]).
Consider two transmitters that transmit simultaneously along a single channel. We are interested in block-codes such that the receiver can read the information that each transmitter has sent. So we want codes



T_1	T_2	R
0	0	0
0	1	1
1	0	1
1	1	2

$C \subset \{0,1\}^n$, $D \subset \{0,1\}^n$, with the property that for all $\underline{c}$, $\underline{c}' \in C$ and for all $\underline{d}$, $\underline{d}' \in D$ the following holds:

$$\underline{c} + \underline{d} = \underline{c}' + \underline{d}' \quad \text{iff} \quad \underline{c} = \underline{c}', \ \underline{d} = \underline{d}' \qquad (*)$$

(here "+" is addition in Z).

Example. $C = \{00,11\}$, $D = \{01,10,11\}$.

Now choose C, and let all its words have length n.

1.6.3. Lemma. If (*) holds and $\underline{c}$, $\underline{c}' \in C$, $\underline{c} \neq \underline{c}'$ and if $\underline{u} \in \{0,1\}^n$ with $u_i = 1 \longrightarrow c_i = c_i'$, then either $\underline{c} \oplus \underline{u}$ or $\underline{c}' \oplus \underline{u}$ in D, but not both. ($\oplus$ is addition mod 2).

Proof. We can easily verify that $\underline{c} + (\underline{c}' \oplus \underline{u}) = \underline{c}' + (\underline{c} \oplus \underline{u})$.

□

1.6.4. Lemma. If not both d and d' are allowed in D, then there are $\underline{c}$, $\underline{c}' \in C$ and there is a $\underline{u}$ for which holds:

$$\text{if } u_i = 1 \text{ then } c_i = c_i' ,$$

such that

$$\underline{d} = \underline{c}' \oplus \underline{u} \quad \text{and} \quad \underline{d}' = \underline{c} \oplus \underline{u} .$$

Proof. Let $\underline{c}$, $\underline{c}' \in C$ and $\underline{c} + \underline{d} = \underline{c}' + \underline{d}'$.

Without loss of generality we have

$$\underline{c} = 0.\ldots.0\ 0.\ldots.0\ 1.\ldots.1\ 1.\ldots.1$$
$$\underline{d} = 0.\ldots.0\ 1.\ldots.1\ 0.\ldots.0\ 1.\ldots.1$$
$$\underline{c} + \underline{d} = 0.\ldots.0\ 1.\ldots.1\ 1.\ldots.1\ 2.\ldots.2$$

and
$$\underline{c}' = 0.\ldots.0\ 0..0\ 1..1\ 0..0\ 1..1\ 1.\ldots.1$$
$$\underline{d}' = 0.\ldots.0\ 1..1\ 0..0\ 1..1\ 0..0\ 1.\ldots.1$$

define
$$\underline{u} := 0.\ldots.0\ 1..1\ 0..0\ 0..0\ 1..1\ 1.\ldots.1$$

□

1.6.5. Corollary. Define the graph $G_C = (V_C, E_C)$ where $V_C = \{0,1\}^n$ (the vertices), and $E_C :=$

$$\bigcup_{\underline{c}\in C} \bigcup_{\underline{c}'\in C\setminus\{\underline{c}\}} \bigcup_{\underline{u}\,|\,u_i=1 \Rightarrow c_i=c_i'} \{\{\underline{c} \oplus \underline{u},\ \underline{c}' \oplus \underline{u}\}\}$$

(the edges). Now, a code D for which (*) holds is a coclique in G_C and a coclique in G_C is a suitable code D.

1.6.6. Theorem. Fix code C again, with $C \subset \{0,1\}^n$. Let

$A_i := \frac{1}{|C|}\{(\underline{c}, \underline{c}') \in C^2 \mid d_h(\underline{c},\underline{c}') = i\}$. d_h is the Hamming distance between two vectors, that is the number of coördinates with $|c_i - c_i'| \neq 0$.

The maximum cardinality for D such that (*) holds is at least

$$2^n \Big/ (1 + |C| \cdot \sum_{i=1}^{n} a_i \cdot 2^{-i})$$

Proof. We know: $|V_C| = 2^n$.

Furthermore

$$|E_C| \leq \tfrac{1}{2} \sum_{\underline{c}\in C} \sum_{\underline{c}'\in C} \sum_{\underline{u}|\ldots} 1 = \sum_{\underline{c}\in C} \sum_{\underline{c}'\in C} 2^{n-d_h(\underline{c},\underline{c}')-1} =$$

$$= \sum_{i=1}^{n} 2^{n-i-1} \sum_{(c,c')\in C^2 \mid d_h(c,c')=i} 1 =$$

$$= 2^{n-1} \sum_{i=1}^{n} |C|\, a_i \cdot 2^{-i}.$$

Apply 1.6.1. and 1.6.5. Then we get: the maximum cardinality of a coclique is at least $2^n \Big/ (1 + |C| \cdot \sum_{i=1}^{n} a_i\, 2^{-i})$.

□

Chapter 2.

Eigenvalue techniques in graph and design theory.

2.1. Introduction.

In this chapter we shall derive some results about eigenvalues of matrices. We will also apply these results to graph theory (e.g. generalized quadrangles) and design theory (e.g. projective planes). the matrices considered will be real and square of size n. If $\lambda \in spec(A)$, then the span of the eigenvectors of A for λ is called $E_\lambda(A)$. Suppose A has n (not necessarily distinct) real eigenvalues; Then we shall denote these eigenvalues by

$$\lambda_1(A) \geq \lambda_2(A) \geq \ldots \geq \lambda_n(A).$$

General references for this chapter are [13], [21].

2.2. Some basic theorems.

2.2.1. Theorem. Let A be a symmetric matrix.

(i) If $\lambda \in spec(A)$, then $\lambda \in R$.

(ii) If $\lambda_1, \lambda_2 \in spec(A)$, $\lambda_1 \neq \lambda_2$, $x_1 \in E_{\lambda_1}(A)$, $x_2 \in E_{\lambda_2}(A)$, then $< x_1, x_2 > = 0$.

(iii) There exists an orthonormal basis of eigenvectors of A. (in other words: there exists an orthogonal matrix S with $S^TAS = diag(\lambda_1, \ldots, \lambda_n)$, where $\lambda_1 \geq \ldots \geq \lambda_n$ are the eigenvalues of A.)

Proof. (i) Let x be an eigenvector of A for λ. Then $\lambda \bar{x}^T x = \bar{x}^T A x = x^T \bar{A} \bar{x} = \overline{\bar{x}^T A x} = \overline{\lambda \bar{x}^T x} = \bar{\lambda} x^T \bar{x} = \bar{\lambda} \bar{x}^T x$. Therefore $\lambda \in R$.

(ii) $\lambda_1 < x_1, x_2 > = < Ax_1, x_2 > = < x_1, Ax_2 > = \lambda_2 < x_1, x_2 >$.

$\lambda_1 \neq \lambda_2$, hence $< x_1, x_2 > = 0$.

(iii) This we prove by induction on n, the size of A.

If n = 0, there is nothing to prove. Suppose n > 0. A has at least one eigenvalue λ_1. Let $x_1 \in E_{\lambda_1}(A)$, $< x_1, x_1 > = 1$. If S_1 is the matrix with first column x_1 and as other columns an orthonormal basis of $< x_1 >^\perp$, then S_1 is orthogonal and

$$S_1^T A S_1 = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A^{(2)} & \\ 0 & & & \end{bmatrix}, \text{ where } A^{(2)} \text{ is symmetric of size } n-1.$$

By the induction hypothesis, there exists an orthogonal matrix S_2 with

$$S_2^T A^{(2)} S_2 = \begin{bmatrix} \lambda_2 & & \\ & \ddots & 0 \\ & 0 & \lambda_n \end{bmatrix}$$

If $S = S_1 \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & S_2 & \\ 0 & & & \end{bmatrix}$, then S is orthogonal, and

$$S^T A S = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}$$

□

2.2.2. Theorem. (Rayley's principle)

Let A be a symmetric matrix of size n, and assume that A has eigenvalues $\lambda_1(A) \geq \dots \geq \lambda_n(A)$.

Let $u_1, \dots, u_n$ be an orthonormal basis of eigenvectors of A, $u_i \in E_{\lambda_i(A)}(A)$, $i = 1, \dots, n$. Then:

(i) $\lambda_i(A) \leq \dfrac{u^T A u}{u^T u}$, for $u \in < u_1, \dots, u_i >$, $u \neq 0$, $0 < i \leq n$;

equality holds iff u is an eigenvector of A for $\lambda_i(A)$.

(ii) $\lambda_{i+1} \geq \dfrac{u^T A u}{u^T u}$, for $u \in < u_1, \dots, u_i >^{\perp} = < u_{i+1}, \dots, u_n >$,

$u \neq 0$, $0 \leq i < n$;

equality holds iff u is an eigenvector of A for $\lambda_{i+1}(A)$.

Proof. $u = \Sigma_{j=1}^{i} a_j u_j$. Then,

$$\frac{u^T A u}{u^T u} = \frac{\Sigma\, a_j^2 \lambda_j}{\Sigma\, a_j^2} \geq \frac{\lambda_i \Sigma\, a_j^2}{\Sigma\, a_j^2} = \lambda_i .$$

Equality holds iff $\Sigma_{j=1}^{i} (\lambda_j - \lambda_i)\alpha_j^2 = 0$, i.e. iff $\lambda_j > \lambda_i \Rightarrow \alpha_j = 0$, i.e. iff $u \in E_{\lambda_i(A)}(A)$.

((ii) can be seen replacing A by -A).

□

2.2.3. Corollary. $\lambda_1 = \max_u \frac{u^T A u}{u^T u}$, $\lambda_n = \min_u \frac{u^T A u}{u^T u}$.

2.2.4. Theorem. If $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix}$ is a symmetric matrix of size n, A_{11} symmetric of size m, then

$$\lambda_1(A) \geq \lambda_1(A_{11}) \geq \lambda_m(A_{11}) \geq \lambda_n(A).$$

Proof.

$$\lambda_1(A) = \max_u \frac{u^T A u}{u^T u} \geq \max_{u=\begin{pmatrix} u_1 \\ 0 \end{pmatrix}} \frac{u^T A u}{u^T u} = \max_{u_1} \frac{u_1^T A_{11} u_1}{u_1^T u_1} = \lambda_1(A_{11}).$$

($\lambda_n(A) \leq \lambda_m(A_{11})$ can be proved in the same way by applying the above to $-A$ and $-A_{11}$).

□

2.2.5. Corollary. Let S_1 be a n x m matrix such that $S_1^T S_1 = I_m$. Let A be a symmetric matrix of size n. Define $B := S_1^T A S_1$. Then

$$\lambda_1(A) \geq \lambda_1(B) \geq \lambda_m(B) \geq \lambda_n(A).$$

Proof. (Note that B is also symmetric). Let $S_2 := (x_1, \ldots, x_{n-m})$, where $x_1, \ldots, x_{n-m}$ is an orthonormal basis of $\langle S_1 \rangle^{\perp}$ ($\langle S_1 \rangle$ being the span of the columns of S_1). Then $(S_1 \mid S_2)$ satisfies $S^T S = I$ and S is square; hence $S^T = S^{-1}$. Also

$$S^T A S = \begin{bmatrix} B & S_1^T A S_2 \\ S_2^T A S_1 & S_2^T A S_2 \end{bmatrix}$$

$S^T A S$ has the same spectrum as A. Therefore, theorem (2.2.4.) yields

$$\lambda_1(A) \geq \lambda_1(B) \geq \lambda_m(B) \geq \lambda_n(A).$$

□

2.2.6. Corollary. Let A be a symmetric matrix partitioned as follows

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix} ,$$

such that A_{ii} is square for i = 1,2, ... m , of size n_i. Let b_{ij} be the average row sum of A_{ij}, for i,j = 1, . . . m. Define the m x m matrix $B := (b_{ij})$.

Then

$$\lambda_1(A) \geq \lambda_1(B) \geq \lambda_m(B) \geq \lambda_n(A).$$

Proof. Define

$$\tilde{S}_1^T := \begin{bmatrix} 1 \ldots 1 & 0 \ldots 0 & \cdot & \cdot & 0 \ldots 0 \\ 0 \ldots 0 & 1 \ldots 1 & \cdot & \cdot & 0 \ldots 0 \\ 0 \ldots 0 & 0 \ldots 0 & \cdot & \cdot & 0 \ldots 0 \\ \cdot \quad\quad \cdot & \cdot \quad\quad \cdot & \cdot & \cdot & \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot & \cdot \quad\quad \cdot & \cdot & \cdot & \cdot \quad\quad \cdot \\ \underbrace{0 \ldots 0}_{n_1} & \underbrace{0 \ldots 0}_{n_2} & \cdot & \cdot & \underbrace{1 \ldots 1}_{n_m} \end{bmatrix}$$

$D := \operatorname{diag}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_m})$ and $S_1 := \tilde{S}_1 D^{-1}$.
Then $S_1^T S_1 = D^{-1}\tilde{S}_1^T\tilde{S}_1 D^{-1} = D^{-1}\operatorname{diag}(n_1, \ldots, n_m)D^{-1} = I_m$, and $\tilde{S}_1^T\tilde{S}_1 = D^2$.
It is clear now that $(\tilde{S}_1^T A \tilde{S}_1)_{ij}$ equals the sum of the entries of A_{ij}.
Hence

$$B = D^{-2}\tilde{S}_1^T A \tilde{S}_1 \quad , \quad \text{and therefore} \quad DBD^{-1} = S_1^T A S_1 .$$

B has the same eigenvalues as DBD^{-1}. Hence corollary 2.2.5. yields

$$\lambda_1(A) \geq \lambda_1(B) \geq \lambda_m(B) \geq \lambda_n(A).$$

□

Using corollary 2.2.6 the following theorem in the graph theory can easily be proved:

2.2.7. Theorem. Let G be a regular graph on n vertices of degree k, containing a coclique of size c. Then

$$c(k - \lambda_n(A)) \leq -n\lambda_n(A),$$

where $\lambda_n(A)$ is the smallest eigenvalue of the adjacency matrix A of G.

Proof. We can write A as

$$A = \begin{bmatrix} 0_{cxc} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix}$$

The average row sum matrix of A, corresponding to this partition, is

$$B = \begin{bmatrix} 0 & k \\ \frac{ck}{n-c} & \frac{(n-2c)k}{n-c} \end{bmatrix}$$

with eigenvalues $\lambda_1(B) = k$ and $\lambda_2(B) = -\frac{kc}{n-c}$.

Corollary 2.2.6 yields

$$-\frac{kc}{n-c} \geq \lambda_n(A).$$

hence, $c(k - \lambda_n(A)) \leq -n\lambda_n(A)$.

□

In the following paragraph we shall give more applications of the results obtained sofar.

2.3. Generalized Quadrangles.

2.3.1. Definition. A generalized quadrangle of order (s,t) is an incidence structure with points and lines such that:

(i) each line has $s + 1$ points,

(ii) each point is on $t + 1$ lines,

(iii) two distinct lines meet in at most one point,

(iv) for any nonincident point - line pair x,l there is a unique line through x that meets l.

We can easily see that the number of points in a generalized quadrangle of order (s,t) is $(s + 1)(st + 1)$.

The point graph of a generalized quadrangle Q is the graph, whose vertices are the points of Q, two points being adjacent, whenever they are on a line of Q.

This graph is strongly regular with parameters

$$v = (s + 1)(st + 1), \qquad k = s(t + 1),$$
$$\lambda = s - 1, \qquad \mu = t + 1,$$

The complement of this graph has parameters

$$v = (s + 1)(st + 1), \qquad k = s^2t,$$
$$\lambda = s^2t - st - s + t, \qquad \mu = s^2t - st.$$

An account of the theory of generalized quadrangles can be found in [23], [34].

2.3.2. Lemma. The smallest eigenvalue of the complement G of the point graph of a generalized quadrangle of order (s,t) is $-s$.

Proof. Let A be the adjacency matrix of the graph G. Because G is strongly regular, the following holds:

$$AJ = kJ \quad \text{and} \quad A^2 = kI + \lambda A + \mu(J - I - A).$$

Hence, A and J can be diagonalized simultaneously, and therefore $\rho^2 + (\mu - k) + (\mu - \lambda)\rho = 0$ for the eigenvalues $\rho \neq k$ of A.

This yields $-s$ as the smallest eigenvalue of A.

□

2.3.3. Theorem. Let Q denote a generalized quadrangle of order (s,t), $s > 1$. Then $t \leq s^2$.

Proof. Let G be a regular graph on n points of degree k, and assume that G contains two disjoint cliques of size 1 and m, respectively, such that no two points in different cliques are adjacent.
If A is the adjacency matrix of G, then we can write

$$A = \begin{bmatrix} J - I & 0 & A_{13} \\ 0 & J - I & A_{23} \\ A_{13}^T & A_{23}^T & A_{33} \end{bmatrix} .$$

The average row sum matrix of A is in this case

$$B = \begin{bmatrix} 1 - 1 & 0 & k - 1 + 1 \\ 0 & m - 1 & k - m + 1 \\ \frac{1(k-1+1)}{n-1-m} & \frac{m(k-m+1)}{n-1-m} & k - \frac{1(k-1+1) + m(k-m+1)}{n-1-m} \end{bmatrix}$$

It is easy to see that $\lambda_1(B) = k$.
Call $\alpha := \text{trace}(B) - k = \frac{(1+m)(n-k+1) - 2(n-m1)}{n - 1 - m} = \lambda_2(B) + \lambda_3(B)$.

and

$$\beta := \det B \cdot k^{-1} = \frac{(n-2k)1m - (n-k)(1+m) + n}{n - 1 - m} = \lambda_2(B) \cdot \lambda_3(B)$$

Hence, $\lambda_2(B)$, $\lambda_3(B)$ are the roots of the equation $x^2 - \alpha x + \beta = 0$.
If we apply this on the complement of the point graph of Q with $n = (1 + s)(1 + st)$, $k = s^2t$ and smallest eigenvalue $-s$, we find with corollary 2.2.6 that $(-s)^2 - \alpha(-s) + \beta \geq 0$.
This yields $s = 1$ or $(1-1)(m-1) \leq s^2$.
Clearly, in a generalized quadrangle (s,t) the induced subgraph on the configuration of two nonadjacent points x,y together with the $t + 1$ points that are adjacent to both x and y is a $K_{2,t+1}$ graph (see chapter 1); so we can apply the above with $1 = 2$ and $m = t + 1$.
Then we find that if $s > 1$, then $t \leq s^2$.

□

2.3.4. Theorem. Assume that a generalized quadrangle Q of order (s,t) contains a subquadrangle Q_1 of order (s_1,t_1).
Then $s = s_1$ or $s_1t_1 \leq s$.

Proof. The parameters of the complement of the point graph of Q are

$$v = (s+1)(st+1) \quad , \quad \lambda = s^2t - st - s + t \quad ,$$
$$k = s^2t \quad , \quad \mu = s^2t - st.$$

The parameters of the complement of the point graph of Q_1 are

$$v_1 = (s_1+1)(s_1t_1+1) \quad , \quad \lambda_1 = s_1^2t_1 - s_1t_1 - s_1 + t_1 \quad ,$$
$$k_1 = s_1^2t_1 \quad , \quad \mu_1 = s_1^2t_1 - s_1t_1 \quad .$$

We can partition the adjacency matrix of the complement of the point graph of Q in such a way that we get the following average row sum matrix

$$B = \begin{bmatrix} k_1 & k - k_1 \\ v_1(k-k_1) & \dfrac{k - v_1(k-k_1)}{v-v_1} \end{bmatrix}$$

It is easy to see that $\lambda_1(B) = k$. Furthermore,

$$\lambda_1(B) + \lambda_2(B) = \text{trace}(B) = k_1 + k - \frac{v_1(k-k_1)}{v-v_1} .$$

Hence $\lambda_2(B) = k_1 - \dfrac{v_1}{v-v_1}(k-k_1)$.

Corollary 2.2.6. yields $\lambda_2(B) \geq \lambda_v(A)$.

$\lambda_v(A) = -s$, and therefore $k_1 - \dfrac{v_1}{v-v_1}(k-k_1) \geq -s$.

This leads to $(s-s_1)(s^2t+s-ss_1t_1t-s_1t_1) \geq 0$.
Then $s = s_1$ or, because $s \geq s_1$, $s^2t + s - ss_1t_1t - s_1t_1 \geq 0$
Therefore

$$s = s_1 \quad \text{or} \quad s_1t_1 \leq s.$$

□

2.4. Interlacing of eigenvalues.

We now introduce a useful property of eigenvalues.

2.4.1. Definition. Suppose A and B are square real matrices of size n and m $(m \leq n)$, respectively, having only real eigenvalues. If $\lambda_i(A) \geq \lambda_i(B) \geq \lambda_{n-m+i}(A)$, for all $i = 1, \ldots, m$, then we say that the eigenvalues of B interlace the eigenvalues of A.

2.4.2. Theorem. Let

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix}$$

be a symmetric matrix of size n, A_{11} square of size m.

Then the eigenvalues of A_{11} interlace those of A.

Proof. Let $\tilde{v}_1, \ldots, \tilde{v}_m$ be a orthonormal basis of eigenvectors of A_{11}, and define $v_i^T := (\tilde{v}_i^T \mid (\underbrace{0 \ldots 0}_{n-m}))$, for all $i = 1, \ldots, m$.

Let $u_1, \ldots, u_n$ be an orthonormal basis of eigenvectors of A. For $i = 1, \ldots, m$, select a $u \in (\langle u_i, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_m \rangle) \setminus \{0\}$.
(This is possible because $\dim(\langle u_i, \ldots, u_n \rangle) = n - i + 1$, and $\dim(\langle v_1, \ldots, v_i \rangle) = i$, and therefore $\dim(\langle u_i, \ldots, u_n \rangle \cap \langle v_1, \ldots, v_i \rangle) \geq 1$).
Then u has the following structure: $u = (\tilde{u} \mid \underbrace{0 \ldots 0}_{n-m})$, and therefore we find with theorem 2.2.2. that

$$\lambda_i(A) \geq \frac{u^T A u}{u^T u} = \frac{\tilde{u}^T A_{11} \tilde{u}}{\tilde{u}^T \tilde{u}} \geq \lambda_i(A_{11}). \qquad (\tilde{u} \in \langle \tilde{v}_1, \ldots, \tilde{v}_m \rangle).$$

If we do the same with -A and $-A_{11}$ we find:
$-\lambda_i(A_{11}) = \lambda_{m-i+1}(-A_{11}) \leq \lambda_{m-i+1}(-A) = -\lambda_{n-m+i}(A)$.
Hence, $\lambda_i(A) \geq \lambda_i(A_{11}) \geq \lambda_{n-m+i}(A)$, for all $i = 1, \ldots, m$.

□

2.4.3. Corollary. Let S_1 be a n x m matrix such that $S_1^T S_1 = I_m$.
Let A be a symmetric matrix of size n and define

$$B := S_1^T A S_1.$$

Then, the eigenvalues of B interlace the eigenvalues of A.

Proof. Define S_2 and S as in the proof of corollary 2.2.5., and use theorem 2.4.2.

□

2.4.4. Corollary. Let A be a symmetric matrix partitioned as follows:

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix},$$

and let B be the average row sum matrix of A.
Then the eigenvalues of B interlace those of A.

Proof. Define $\tilde{S}_1$, D and S_1 as in corollary 2.2.6.; then

$$DBD^{-1} = S_1^T A S_1.$$

With corollary 2.4.3. we find that the eigenvalues of B interlace the eigenvalues of A.

□

The following shows an application to graph theory:

2.4.5. Theorem. (Cvetković bound).

Let G be a graph on n vertices with a coclique of size c. Then c doesn't exceed the number of nonnegative (or nonpositive) eigenvalues of the adjacency matrix A of G.

Proof. A can be partitioned as follows:

$$A = \begin{bmatrix} 0_{cxc} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix}$$

Then with theorem 2.4.2. we find that

$$\lambda_c(A) \geq \lambda_c(0) = 0 \text{ and } \lambda_{n-c+1}(A) \leq \lambda_1(0) = 0.$$

Hence, c cannot exceed the number of nonegative (or nonpositive) eigenvalues of A.

□

2.5. Block designs.

2.5.1. Definition. A block design (balanced incomplete block design) with parameters $(v,k;b,r,\lambda)$ is a set X of v elements and a collection of b-subsets of X, called blocks, such that,

1) each block has cardinality k,
2) each element of X occurs in exactly r blocks,
3) each pair of distinct elements of X occurs in exactly λ blocks.

In other words, a block design is a $2-(v,k,\lambda)$ design.
A block design is called symmetric if v = b.

We want to apply the results obtained in the preceeding paragraphs to block designs. But, because the incidence matrix of a block design is usualy nonsymmetric, we need the following theorem:

2.5.2. Theorem. Let M^T and N be real $m_1 \times m_2$ matrices. Put

$$A = \begin{bmatrix} 0 & N \\ M & 0 \end{bmatrix} ;$$

then the following are equivalent:

(i) $\lambda \neq 0$ is an eigenvalue of A of multiplicity f;

(ii) $-\lambda \neq 0$ is an eigenvalue of A of multiplicity f;

(iii) $\lambda^2 \neq 0$ is an eigenvalue of MN of multiplicity f;

(iv) $\lambda^2 \neq 0$ is an eigenvalue of NM of multiplicity f.

Proof. (i)$\Longleftrightarrow$(ii).

Let $AU = \lambda U$, for some matrix U of rank f. Write $U = \begin{bmatrix} U_1 \\ U_2 \end{bmatrix}$ and define $\tilde{U} = \begin{bmatrix} U_1 \\ -U_2 \end{bmatrix}$, where U_i has m_i rows for $i = 1,2$. Then $NU_2 = \lambda U_1$ and $MU_1 = \lambda U_2$. This implies $A\tilde{U} = -\lambda\tilde{U}$. Since rank U = rank $\tilde{U}$, the first equivalence is proved.

(iii)$\Longleftrightarrow$(iv).

Let $MNU' = \lambda^2 U'$, for some matrix U' of rank f, $\lambda^2 \neq 0$. Then $NM(NU') = \lambda^2 U'$, and rank NU' = rank U', since,

rank U' = rank $\lambda^2 U'$ = rank MNU' $\leq$ rank NU' $\leq$ rank U'.

This proves the second equivalence.

(i)$\Longleftrightarrow$(iii).

Because $A^2 = \begin{bmatrix} NM & 0 \\ 0 & MN \end{bmatrix}$, it follows that (i)$\Longrightarrow$(iii).

If $MNU' = \lambda^2 U'$, U' of rank f, then

$A\begin{bmatrix} NU' \\ \lambda U' \end{bmatrix} = \begin{bmatrix} \lambda NU' \\ \lambda^2 U' \end{bmatrix} = \lambda \begin{bmatrix} NU' \\ \lambda U' \end{bmatrix}$, and $\begin{bmatrix} NU' \\ \lambda U' \end{bmatrix}$ has also rank f. Hence (iii)$\Longrightarrow$(i). □

2.5.3. Theorem. Let N be the incidence matrix of size v x b of a block design with parameters $(v,k;b,r,\lambda)$ ($r = \frac{v-1}{k-1}\lambda$).

Assume that

$$N = \begin{bmatrix} N_1 & N_2 \\ N_3 & N_4 \end{bmatrix}, \text{ where } N_1 \text{ is a } v_1 \times b_1 \text{ matrix.}$$

Let r_1 be the average row sum of N_1, and $k_1 = \frac{v_1 r_1}{b_1}$ the average column sum of N_1. Then,

$$(vr_1 - b_1k)(bk_1 - v_1r) \leq (r - \lambda)(v - v_1)(b - b_1).$$

Proof. Consider the symmetric matrix $A = \begin{bmatrix} 0 & N \\ N^T & 0 \end{bmatrix}$.

Because $NN^T = (r - \lambda)I + \lambda J$, we find that the eigenvalues of NN^T are kr, of multiplicity 1, and $(r - \lambda)$ of multiplicity $v - 1$. With theorem 2.5.2. we see that the eigenvalues of A are $(rk)^{\frac{1}{2}}$ and $-(rk)^{\frac{1}{2}}$, each of multiplicity 1, $(r - \lambda)^{\frac{1}{2}}$ and $-(r - \lambda)^{\frac{1}{2}}$, each of multiplicity $v - 1$, and 0 of multiplicity $b - v$. If we write

$$A = \begin{bmatrix} 0 & 0 & N_1 & N_2 \\ 0 & 0 & N_3 & N_4 \\ N_1^T & N_3^T & 0 & 0 \\ N_2^T & N_4^T & 0 & 0 \end{bmatrix}$$, then the average row sum matrix of A is:

$$B = \begin{bmatrix} 0 & 0 & r_1 & r-r_1 \\ 0 & 0 & x & r-x \\ k_1 & k-k_1 & 0 & 0 \\ y & k-y & 0 & 0 \end{bmatrix}$$, where $x = \frac{b_1(k - k_1)}{v - v_1}$ and $y = \frac{v_1(r - r_1)}{b - b_1}$.

It is easy to see that $\lambda_1(B) = -\lambda_4(B) = (rk)^{\frac{1}{2}}$, and with $\det(B) = rk(r_1 - x)(k_1 - y)$ and $\text{trace}(B) = 0$, we also find that

$$\lambda_2(B) = -\lambda_3(B) = ((r_1 - x)(k_1 - y))^{\frac{1}{2}}.$$

Corollary 2.4.4. yields $\lambda_2(B) \leq \lambda_2(A)$, and therefore

$$(r_1 - x)(k_1 - y) \leq r - \lambda \text{ . Hence}$$

$$(vr_1 - b_1k)(bk_1 - v_1r) \leq (r - \lambda)(v - v_1)(b - b_1).$$

□

2.5.4. Corollary. If a block occurs s times in a block design, then

$$b/v \geq s \text{ .}$$

Proof. In this case we can write for the incidence matrix of the block design:

$$N = \begin{bmatrix} J_{kxs} & N_2 \\ 0 & N_4 \end{bmatrix},$$

then, if we use theorem 2.5.3. with $v_1 = k_1 = k$ and $b_1 = r_1 = s$, then we find that $b/v \geq s$

□

2.5.5. Corollary. A subplane of a projective plane of order n has order

$$m \leq \sqrt{n}.$$

Proof. A projective plane of order n is a symmetric $2\text{-}(n^2+n+1, n+1, 1)$ design, with $r = n + 1$ and $b = n^2 + n + 1$. Theorem 2.5.3. with $b_1 = v_1 = m^2 + m + 1$ and $k_1 = r_1 = m + 1$ yields $m \leq \sqrt{n}$. (equality holds for Baer subplanes.)

□

2.5.6. Corollary. If f is the number of fixed points of an automorfism of a symmetric $2\text{-}(v,k,\lambda)$ design, then

$$f \leq k + \sqrt{n}, \text{ where } n = k - \lambda .$$

Proof. (Note that # fixed points = # fixed blocks.)
Let N_1 be the incidence matrix of the nonfixed points and the nonfixed blocks. A nonfixed block cannot contain more than λ fixed points (for, if B is a nonfixed block and B' its image, then the points in $B \setminus B'$ are nonfixed). Therefore we can use theorem 2.5.3. with $v_1 = b_1 = v - f$, $k_1 = r_1 \geq k - \lambda = n$. This yields $f \leq k + \sqrt{n}$.

□

2.6. Tight interlacing of eigenvalues.

2.6.1. Definition. Suppose A and B are square matrices of size n and m, respectively ($m \leq n$), having only real eigenvalues, and assume that the eigenvalues of B interlace the eigenvalues of A.
(Hence $\lambda_i(A) \geq \lambda_i(B) \geq \lambda_{n-m+i}(A)$, $i = 1,\ldots,m$)
If there exists an integer k, $0 \leq k \leq m$ such that

$$\lambda_i(A) = \lambda_i(B), \quad i = 1,\ldots,k$$
$$\lambda_{n-m+i}(A) = \lambda_i(B), \quad i = k+1,..,m.$$

Then the interlacing is called tight.

2.6.2. Theorem. Suppose $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix}$ is a symmetric matrix of size n, A_{11} square of size m. We know that the eigenvalues of A_{11} interlace those of A(theorem 2.4.2.).
If the interlacing is tight, then $A_{12} = 0$.

Proof. Let 1 be an integer with $\lambda_i(A) = \lambda_i(A_{11})$, for i = 1,..., 1, and let $\tilde{v}_1,\ldots,\tilde{v}_m$ be an orthonormal basis of eigenvectors of A_{11}. We shall first prove the following by induction on 1:

(x) $v_1 = \begin{pmatrix} \tilde{v}_1 \\ 0 \end{pmatrix}, \ldots v_1 = \begin{pmatrix} \tilde{v}_1 \\ 0 \end{pmatrix}$ are orthonormal eigenvectors of A for the eigenvalues $\lambda_1(A_{11}),\ldots,\lambda_1(A_{11})$.

If 1 = 0, then there is nothing to prove. Suppose 1 > 0. We have

$$\lambda_1(A) = \lambda_1(A_{11}) = \tilde{v}_1^T A_{11} \tilde{v}_1 = v_1^T A v_1.$$

Because $v_1 \in \langle v_1,\ldots,v_{1-1} \rangle^{\perp}$, and by the induction hypothesis $v_1,\ldots,v_{1-1}$ are orthonormal eigenvectors of A for the eigenvalues $\lambda_1(A),\ldots,\lambda_{1-1}(A)$, we find with theorem 2.2.2.(ii) that $v_1 \in E_{\lambda_1(A)}(A)$. This proves (x).

If the interlacing is tight, then there exists an interger $0 \leq k \leq m$ with $\lambda_i(A) = \lambda_i(A_{11})$ for i = 1,...,k, $\lambda_{n-m+i}(A) = \lambda_i(A_{11})$ for i=k+1,..,m. If we apply (x) to A_{11} and A with 1 = k and to $-A_{11}$ and -A with 1 = m - k, we find that if $\tilde{v}_1,\ldots,\tilde{v}_m$ is an orthonormal basis of eigenvectors of A_{11}, then $v_1 = \begin{pmatrix} \tilde{v}_1 \\ 0 \end{pmatrix}, \ldots, v_m = \begin{pmatrix} \tilde{v}_m \\ 0 \end{pmatrix}$ are orthonormal eigenvectors of A.

If $V = (v_1,\ldots,v_m)$ and $\tilde{V} = (\tilde{v}_1,\ldots,\tilde{v}_m)$, then $V = \begin{pmatrix} \tilde{V} \\ 0 \end{pmatrix}$ and AV = VD, where D is a diagonal matrix. Therefore $A_{12}^T \tilde{V} = 0$, and because $\tilde{V}$ is nonsingular we find that $A_{12} = 0$

□

2.6.3. Corollary. Let S_1 be a nxm matrix such that $S_1^T S_1 = I_m$. Let A be symmetric of size n. Define $B = S_1^T A S_1$. We know that the eigenvalues of B and A interlace (corollary 2.4.3.). If the interlacing is tight, then $S_1 B = A S_1$.

Proof. Define S_2 as in the proof of corollary 2.2.5.. Then $I = (S_1, S_2)(S_1, S_2)^T = S_1 S_1^T + S_2 S_2^T$, and with theorem 2.6.2. we see that $S_2^T A S_1 = 0$ (see also the proof of corollary 2.2.5.). Therefore

$$0 = S_2 S_2^T A S_1 = (I - S_1 S_1^T) A S_1 = A S_1 - S_1 B.$$

Hence, $A S_1 = S_1 B$.

□

2.6.4. Corollary. Let B be the average row sum matrix of

$$A = \begin{bmatrix} A_{11} \cdots A_{1m} \\ \vdots \quad\quad \vdots \\ A_{m1} \cdots A_{mm} \end{bmatrix}, \quad A \text{ symmetric of size } n.$$

We know that the eigenvalues of B interlace those of A (corollary 2.4.4.). If the interlacing is tight, then A_{ij}, $i,j = 1,\ldots,m$ has constant row and column sums.

Proof. Use the proof of corollary 2.2.6. (define S_1, $\tilde{S}_1$, D the same way). Then $DBD^{-1} = S_1^T A S_1$. If the interlacing of B and A is tight, then the interlacing of DBD^{-1} and A is also tight. With corollary 2.6.3. we obtain $AS_1 = S_1 DBD^{-1}$. This yields $A\tilde{S}_1 = \tilde{S}_1 B$.
Hence, the average row (and column) sums of the A_{ij} are constant.

□

We now apply tight interlacing to graph and design theory:
1) In theorem 2.2.7. we see that the interlacing of the eigenvalues of B and A (see the proof of theorem 2.2.7.) is tight when the graph contains a coclique of size $(-n\lambda_n(A))/(k - \lambda_n(A))$. In that case,

$$A = \begin{bmatrix} 0_{cxc} & A_{12} \\ A_{12}^T & A_{22} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & k \\ \lambda_n(A) & k+\lambda_n(A) \end{bmatrix} .$$

A_{12}^T has constant row and column sums, viz. $-\lambda_n(A)$ (corollary 2.6.4.). Hence every vertex not in the coclique is adjacent to $-\lambda_n(A)$ vertices of the coclique.
If the considered graph is strongly regular (with n,k,λ,μ), then we can construct a $2-((-n\lambda_n(A))/(k-\lambda_n(A)),\ -\lambda_n(A),\ \mu\ )$ design as follows:

- the points are the vertices of the coclique; $v = (-n\lambda_n(A))/(k-\lambda_n(A))$;
- let x be a vertex not in the coclique. Then all the vertices of the coclique adjacent to x define a block. With what is stated above we see that each block contains $-\lambda_n(A)$ points. Furthermore, we can easily see that each pair of distinct points occurs in μ blocks.

2) In theorem 2.5.3. we see that if equality holds, then

$$(r_1 - x)(k_1 - y) = r - \lambda.$$ (see the proof of the theorem).

Hence,

$\lambda_1(B) = \lambda_1(A)$, $\lambda_2(B) = \lambda_2(A)$, $\lambda_3(B) = \lambda_{n-1}(A)$, $\lambda_4(B) = \lambda_n(A)$,

and this means that the interlacing is tight.

3) Consider a block design with a block that occurs s times(see corollary 2.5.4.). If b = vs, then equality holds in theorem 2.5.3. and with 2) and corollary 2.6.4. we find that the column sums of N_2 are constant, viz. $k\frac{r-s}{b-s}$. We claim that the points of the repeated block and the blocks of the original block design, the repeated block excluded, constitute a $2\text{-}(k, k\frac{r-s}{b-s}, \lambda-s)$ design, for: the number of points is k;

each block has $k\frac{r-s}{b-s}$ points (viz. the row sums of N_2); a pair of distinct points occurs in $\lambda - s$ blocks.

The next and final paragraph of this chapter is an example of interlacing in projective geometry.

2.7. Absolute points in PG(2,n).

Consider the projective plane of order n, denoted by PG(2,n).

A polarity π of PG(2,n) is a permutation of order 2 of the points and lines of PG(2,n) such that:

i) p^π is a line for every point p,

ii) l^π is a point for every line l,

iii) $p \in l \Longleftrightarrow l^\pi \in p$, for all points p and lines l.

Points p of PG(2,n) with $p \in p^\pi$ are called absolute points. We denote their number with a. Lines l in PG(2,n) with $l^\pi \in l$ are called absolute lines. It is easy to see that their number equals a.

2.7.1. Theorem. $a \geq 1$, and if n is not a square, then $a = n + 1$.

Proof. We can write the incidence matrix of PG(2,n) as follows:

$$N = \begin{array}{c} \\ P_1 \\ \vdots \\ P_{n^2+n+1} \end{array} \begin{array}{c} P_1^\pi \ldots\ldots P_{n^2+n+1}^\pi \\ \boxed{} \end{array}$$

N is symmetric, for: $P_i \in P_j \Longleftrightarrow P_j \in P_i$.

Therefore $N^2 = NN^T = nI + J$. This leads to the following eigenvalues for N:

$n + 1$, of multiplicity 1; $n^{\frac{1}{2}}$, of multiplicity α; $-(n)^{\frac{1}{2}}$, of multiplicity β, α and β being integers with $\alpha + \beta = n^2 + n$. Then

$a = \text{trace}(N) = n + 1 + (\alpha - \beta)n^{\frac{1}{2}} \geq 0 \quad (n \geq 1)$.

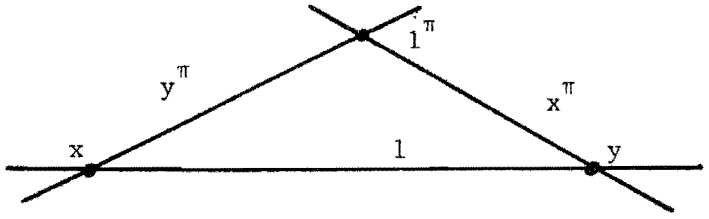
If $a = 0$, then $n^{\frac{1}{2}}$ is an integer and $n^{\frac{1}{2}} \mid (n + 1)$. But this is not possible. Hence $a \geq 1$.

If n is not a square, then $n^{\frac{1}{2}}$ is not an integer and therefore $\alpha = \beta$. This yields $a = n + 1$.

□

2.7.2. Lemma. A nonabsolute line has an even number of nonabsolute points.

Proof.



Consider a nonabsolute line l and let x be a nonabsolute point on l. $l^\pi \notin l$, $x \notin x^\pi$ and $x \in l$. Hence $l^\pi \in x^\pi$ and x^π meets l in a point $y \neq x$. y is also nonabsolute, because: $y \in l$ and $y \in x^\pi$, and therefore $x \in y^\pi$ and $l^\pi \in y^\pi$, and this yields $y \notin y^\pi$ (y is nonabsolute) and y^π meets l in x. This way, the set of the nonabsolute points on l is partitioned in pairs. Hence l has an even number of nonabsolute points.

□

2.7.3. Theorem. Assume that n is odd.
Then $a \geq n + 1$, and if $a = n + 1$, then the set of the absolute points is an oval in PG(2,n).

Proof. Consider an absolute point x ($a \geq 1$). $n + 1$ distinct lines meet in x and exactly one of these is absolute, viz. x^π (if $x \in y^\pi$, y absolute, then $y \in x^\pi$ and thus $x,y \in x^\pi$ and $x,y \in y^\pi$. This yields $x = y$). In other words, n nonabsolute lines meet in x. Each of these nonabsolute lines contains $n + 1$ (an even number) of points, and an even number of these points is nonabsolute (lemma 2.7.2.). In other words, on each nonabsolute line through x there is, x excluded, an odd number of absolute points, so at least one. Hence $a \geq n + 1$ (x is absolute).

If $a = n + 1$, then then the above yields that a nonabsolute line has at most 2 absolute points. An absolute line has exactly one absolute point. Hence, the set of the absolute points is an oval. □

2.7.4. Theorem. Assume that n is even.
Then $a \geq n + 1$, and if $a = n + 1$, then the absolute points lie on a line.

Proof. Consider a nonabsolute point x (if this is not possible, then there is nothing to prove).
$n + 1$ lines meet in x, and on each line there is an odd number of points (viz. $n + 1$). An absolute line contains exactly one absolute point.
A nonabsolute line contains an even number of nonabsolute points, hence an odd number of absolute points, so at least one.
This means that every line through x has at least one absolute point.
x is nonabsolute; hence $a \geq n + 1$.
If $a = n + 1$, then the above yields that a line, that has a nonabsolute point, has exactly one absolute point. But this means that the line through 2 absolute points only has absolute points.
Hence, the $n + 1$ absolute points lie on a line. □

2.7.5. Theorem. Assume that $n = m^2$.
Then $a \leq m^3 + 1$, and if $a = m^3 + 1$, then the absolute points and the nonabsolute lines constitute a $2\text{-}(m^3+1, m+1, 1)$ design (a unital).

Proof. Consider the incidence matrix of PG(2,n) as in theorem 2.7.1., partitioned as follows:

$$N = \begin{bmatrix} I_{a \times a} & N_{12} \\ N_{12}^T & N_{22} \end{bmatrix}$$

$I_{a \times a}$ being the (sub-)incidence matrix of the absolute points and lines. The average row sum matrix of N is:

$$B = \begin{bmatrix} 1 & m^2 \\ \dfrac{m^2 a}{m^4+m^2+1-a} & m^2+1-\dfrac{m^2 a}{m^4+m^2+1-a} \end{bmatrix}$$

The eigenvalues of N are m^2+1 (multiplicity 1), m (multiplicity α), $-m$ (multiplicity β) (see 2.7.1.).

$\alpha + \beta = m^4 + m^2$, $m^2 + 1 + (\alpha - \beta)m = a$.

Because $a \leq m^4+m^2+1$, we find $\beta \geq 0$.
Hence, $\lambda_1(N) = m^2+1$, $\lambda_{m^4+m^2+1}(N) = -m$.

We can easily see that the eigenvalues of B are

$$\lambda_1(B) = m^2+1 \quad , \quad \lambda_2(B) = 1 - \frac{am^2}{m^4+m^2+1-a}$$

Corollary 2.4.4. says that the eigenvalues of B interlace those of N. This yields

$$\lambda_2(B) = 1 - \frac{am^2}{m^4+m^2+1-a} \geq \lambda_{m^4+m^2+1}(N) = -m.$$

This leads to $a \leq m^3+1$.
If $a = m^3+1$, then $\lambda_1(B) = \lambda_1(N)$ and $\lambda_2(B) = \lambda_{m^4+m^2+1}(N)$.

Hence, the interlacing is tight.
Therefore, the column sums of N_{12} are constant and equal to m+1. (corollary 2.6.4.).
This means that a nonabsolute line has m+1 absolute points. Furthermore, the line through 2 absolute points is nonabsolute.
Hence, the absolute points and teh nonabsolute lines constitute a $2-(m^3+1, m+1, 1)$ design.

□

(See also [18] p. 63-65)

Chapter 3.

Association schemes.

3.1. Introduction.

Association schemes first appeared in statistics. They were introduced in combinatorial theory by Bose and Smimamoto as a generalization of strongly regular graphs.

The theory of association schemes has proved to be useful in the study of permutation groups and graphs. Ph. Delsarte applied association schemes in coding theory and combinatorics.

This chapter contains an outline of part of the work of Delsarte.

We begin with the Bose-Mesner algebra of an association scheme in section 3.2. together with some examples. The relations between its two bases are described in section 3.3., as well as the important P- and Q-polynomial schemes.

To motivate the study of association schemes we continue with three applications. These are a theorem about generalized hexagons, an association scheme in PG(2,4) and regular two-graphs as association schemes. Section 3.7. uses the setting of A-modules. In 3.8. we introduce the distribution matrix $D(\underline{x},\underline{y})$. It leads directly to the Mac-Williams transform and it provides the link to the linear programming method.

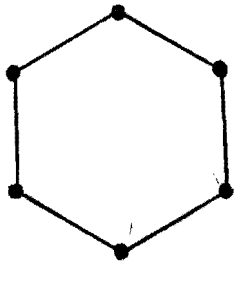
Section 3.9. contains a proof of the code-clique theorem and its dual concerning designs.

Two appendices are added in which theorems, used in this chapter about minimal idempotents and the A-module, are proved.

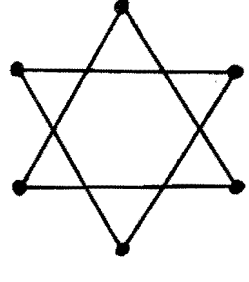
General references for this chapter are [8], [15].

3.2. Bose-Mesner algebra.

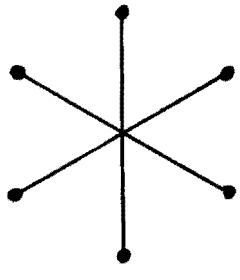
Consider the regular hexagon. On its six vertices three graphs can be defined as stated in the pictures



I



II



III

Their adjacency matrices are respectively

$$A_1 = P^1 + P^5 \ , \ A_2 = P^2 + P^4 \ , \ A_3 = P^3 \quad \text{where } P = \begin{bmatrix} 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \\ 1&0&0&0&0&0 \end{bmatrix}$$

Since the three graphs together form a complete graph we have

$$A_1 + A_2 + A_3 = J - I$$

Relations between the A_i for $i = 1,2,3$ are

$$A_1^2 = 2I + A_2 \ , \quad A_2^2 = 2I + A_2 \ , \quad A_3^2 = I$$

$$A_1A_2 = A_1 + 2A_3 \ , \quad A_1A_3 = A_2 \ , \quad A_2A_3 = A_1$$

This expresses that the vector space $\langle I, A_1, A_2, A_3 \rangle_R$ is an algebra over R.

This example can be generalized in the following way:

3.2.1. Definition. An association scheme

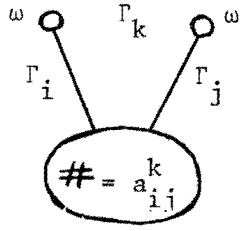
$$(\Omega, \{I, \Gamma_1, \ldots \Gamma_s\})$$

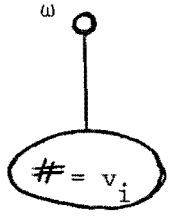
consists of a set Ω together with a partition of the set of 2-element subsets of X into s relations $\Gamma_1, \ldots \Gamma_s$, satisfying the following conditions:

(i) For each $\omega \in \Omega$, the number v_i of $q \in X$ with $\{\omega, q\} \in \Gamma_i$ depends only on i;

(ii) For each pair ω, ω' with $\{\omega, \omega'\} \in \Gamma_k$ the number a_{ij}^k of $q \in X$ with $\{\omega, q\} \in \Gamma_i$ and $\{\omega', q\} \in \Gamma_j$ depends only on i,j and k.

In other words, if we take the complete graph of X, we colour all edges with the"colours" Γ_i, for $i = 1,2,\ldots s$. Then 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 points.





$v_i := a_{ii}^0$

The a_{ij}^k are called the intersection numbers.

It is clear that the following relations hold

1) $\sum_{i=0}^{s} v_i = n$ since all vertices have some relation to ω.

2) $\sum_{i=0}^{s} a_{ij}^k = v_j$ for each k, since the vertices that have relation Γ_i to ω' have also some relation to ω

3) $a_{ij}^k = a_{ji}^k$.

We now translate the defining conditions above in terms of the (0,1) adjacency matrices A_i of the colours Γ_i. Since the graph on Ω is complete, we have

$$A_1 + A_2 + \ldots + A_s = J - I.$$

Condition (i) translates into

$$A_i J = v_i J.$$

By analysis of the matrix product it is seen that condition (ii) translates into

$$A_i A_j = \sum_{k=0}^{s} a_{ij}^k A_k.$$

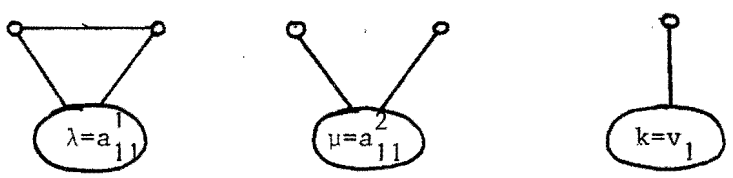
These formulae imply that the R-vector space

$$\mathcal{A} = \langle I = A_0, A_1, \ldots, A_s \rangle_R$$

is an algebra with respect to matrix multiplication. This so called Bose-Mesner algebra of the association scheme is commutative. This follows from 3) and

$$A_i A_j = \sum_{k=0}^{s} a_{ij}^k A_k = \sum_{k=0}^{s} a_{ij}^k A_k^T = \left(\sum_{k=0}^{s} a_{ij}^k A_k\right)^T = (A_i A_j)^T = A_j^T A_i^T = A_j A_i.$$

3.2.2. Example. An association scheme with two colours (s = 2) consists of a strongly regular graph Γ and its complement. The numbers k, λ, μ are defined by:



In terms of the adjacency matrices A of Γ and B of the complement of Γ this reads

$$AJ = kJ \quad , \quad A^2 = kI + \lambda A + \mu B \quad , \quad J - I = A + B.$$

3.2.3. Example. In a distance regular graph any pair of vertices x, y with distance k has a constant number of vertices z such that dist(x,z) = i and dist(y,z) = j. This number a_{ij}^k does not depend on the choice of x and y. The adjacency matrix A_i of the relation Γ_i (distance i in the graph) is a polynomial in A_1 of degree i , for i = 1,...,s. The relations I, Γ_1, . . . Γ_s constitute an association scheme.

The regular hexagon provides an example of a distance regular graph and

$$A_1 = A_1 \quad , \quad A_2 = A_1^2 - 2I \quad , \quad ,A_3 = \tfrac{1}{2}A_1^3 - 1\tfrac{1}{2}\, A_1 \ .$$

3.2.4. Example. A permutation group G on a finite set Ω is called generously transitive if

$$\forall_{\alpha,\beta \in \Omega} \exists_{g \in G} [\alpha^g = \beta \ , \ \beta^g = \alpha]$$

The orbits on Ω^2 of such a group constitute an association scheme.

For instance, the symmetric group S_4 on four symbols contains the subgroup

$$\{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \ ,$$

called the Klein-group. This group is generously transitive on $\Omega := \{1, 2, 3, 4\}$. The orbits in Ω^2 are,

Γ_0	Γ_1	Γ_2	Γ_3
(1,1)	(1,2)	(1,3)	(1,4)
(2,2)	(2,1)	(3,1)	(4,1)
(3,3)	(3,4)	(2,4)	(2,3)
(4,4)	(4,3)	(4,2)	(3,2)

3.2.5. Example. The Hamming scheme H(v,2) is defined as follows. The set Ω consists of the vectors of the vector space F_2^v. Two vectors are in the relation Γ_i whenever their Hamming distance, the number of coördinates in which they differ, equals i. This defines an association scheme with the parameters

$$n = 2^v \quad , \quad v_i = \binom{v}{i} \quad ,$$

$$a_{ij}^k = \begin{cases} \binom{k}{\frac{1}{2}(i-j+k)} \cdot \binom{v-k}{\frac{1}{2}(i+j-k)} & , \text{ if } i+j+k \text{ is even} \\ 0 & , \text{ if } i+j+k \text{ is odd.} \end{cases}$$

Indeed, let ω and ω' have Hamming distance k. Without loss of

generality we can take $\omega = (0, 0, .., 0)$ and $\omega' = (\underbrace{1, .., 1}_{k}, \underbrace{0, \ldots 0}_{v-k})$

The number of vectors to be counted are those that have distance i to ω and j to ω'. So x contains i ones. Let a be the number of ones at the first k coördinates of x and b the number of ones at the last v-k coördinates.

$$\omega' = (1, \ldots\ldots 1, 0, \ldots\ldots 0)$$
$$x = (\underbrace{1, \ldots 1}_{a}, \underbrace{0, \ldots 0}_{k-a}, \underbrace{1, \ldots 1}_{b}, \underbrace{0, \ldots 0}_{v-k-b})$$

Now it is clear that $\mathrm{dist}(\omega', x) = k-a+b = j$ and $a+b = i$.
So $a = \frac{1}{2}(k+i-j)$ and $b = \frac{1}{2}(i+j-k)$.
The number of possible x is $\binom{k}{a}\binom{v-k}{b} = \binom{k}{\frac{1}{2}(i-j+k)} \cdot \binom{v-k}{\frac{1}{2}(i+j-k)}$

if i+j+k is even, and 0 otherwise.

3.2.6. Example. The Johnson scheme J(v,k) is defined as follows. The set Ω consists of the k-subsets of a v-set. Two k-subsets are in the relation Γ_i whenever their intersection has k - i elements. This defines an association scheme with the parameters

$$n = \binom{v}{k} \quad , \quad v_i = \binom{k}{i}\binom{v-k}{i} \quad .$$

J(v,k) may be viewed as the set of all words of weight k in H(v,2). In this terminology the notion of a t-(v,k,λ) design may be defined as following. A subset $X \subset J(v,k)$ is a t-(v,k,λ) design over the v-set if for each $\underline{z} \in J(v,t)$ the number of blocks $\underline{x} \in X$ having distance k-t to $\underline{z}$ is a constant, independent of $\underline{z}$, called λ.

3.3. Bases for the Bose-Mesner algebra.

The Bose-Mesner algebra of an association scheme

$$A = \langle A_0 = I, A_1, \ldots A_s \rangle_R$$

consists of commuting, hence simultaneously diagonalizable symmetric matrices.

Therefore A also has a basis of s+1 orthogonal minimal idempotents (see appendix):

$$A = \langle E_0 = \frac{1}{n}J,\ E_1,\ \ldots\ .E_s \rangle_R \quad .$$

3.3.1. Example. For s = 2, for a strongly regular graph with spec(A) = (k^1, r^f, s^g) we have the idempotents

$$E_0 = \frac{1}{n}J \qquad \text{, of rank 1 ,}$$

$$E_1 = \frac{1}{r-s}\left(A - sI + \frac{k-s}{n}J\right) \qquad \text{, of rank f ,}$$

$$E_2 = \frac{1}{r-s}\left(rI - A + \frac{k-r}{n}J\right) \qquad \text{, of rank g .}$$

By definition, the algebra A is closed with respect to matrix multiplication. Since the A_i are (0,1) matrices, the algebra A is also closed with respect to Schur multiplication, that is, the entrywise multiplication of matrices

$$A \circ B = C \quad \text{with} \quad c_{ij} = a_{ij}b_{ij}.$$

Hence

$$E_iE_j = \delta_{ij}E_i \quad , \quad A_i \circ A_j = \delta_{ij}A_i$$

$$A_iA_j = \sum_{k=0}^{s} a_{ij}^k A_k \quad , \quad E_i \circ E_j = \sum_{k=0}^{s} b_{ij}^k E_k$$

The coëfficients b_{ij}^k are nonnegative, since $E_i \circ E_j$ is a principle submatrix of $E_i \otimes E_j$, the Kronecker product, hence positive semi-definite. Since the eigenvalues of $E_i \otimes E_j$ are the numbers $\lambda(E_i)\cdot\lambda(E_j)$ with $\lambda(E_i)$ and $\lambda(E_j)$ eigenvalues of E_i and E_j respectively, and $\lambda(E_i) \in \{0,1\}$, since $E_i^2 = E_i$. An explicite expression for b_{ij}^k is obtained by use of

$$\sum \text{entries } M \circ N = \text{trace } MN^T \ ;$$

$$\sum \text{entries}(E_i \circ E_j \circ E_k) = \text{trace}(E_i \circ E_j)E_k = b_{ij}^k \text{ trace}(E_k) =$$

$$= b_{ij}^k \cdot \mu_k,$$

where μ_k is the multiplicity of the eigenvalue 1 of E_k.

Expressing one basis into the other we define the coefficients p_{ik} and q_{ki} by

$$A_k = \sum_{i=0}^{s} p_{ik} E_i \quad , \qquad E_i = \frac{1}{n} \sum_{k=0}^{s} q_{ki} A_k \quad .$$

By multiplication the formulae

$$A_k E_i = p_{ik} E_i \quad , \qquad E_i \circ A_k = \frac{1}{n} q_{ki} A_k \quad .$$

are obtained. We define the diagonal matrices

$$\Delta_v = \mathrm{diag}(v_k) \quad , \quad \text{for the valencies } v_k = p_{0k}$$

$$\Delta_\mu = \mathrm{diag}(\mu_i) \quad , \quad \text{for the multiplicities } \mu_i = q_{0i}$$

viz. $\mu_i = \mathrm{trace}(E_i) = \mathrm{trace}(E_i \circ I) = \mathrm{trace}(\frac{1}{n} q_{0i} I) = q_{0i}$.

The character table $P := [p_{ik}]$, and its inverse Q (from $PQ = nI = QP$), satisfy the following theorem .

3.3.2. Theorem. $\Delta_\mu \cdot P = Q^T \cdot \Delta_v$.

Proof. $(\Delta_\mu P)_{ik} = \mu_i p_{ik} = p_{ik}\, \mathrm{tr}(E_i) = \mathrm{tr}(A_k E_i) = \sum \mathrm{entries}(E_i \circ A_k) =$

$$= \frac{1}{n} q_{ki} \sum \mathrm{entries}(A_k) = q_{ki} v_k = (Q^T \cdot \Delta_v)_{ik}.$$

□

3.3.3. Corollary. $P^T \Delta_\mu \cdot P = n \Delta_v \quad , \qquad \sum_{z=0}^{s} \mu_z p_{zk} p_{zl} = n v_k \delta_{kl}$.

If p_{zi} is a polynomial in p_{z1} of degree i, for i = 1,..,s then the corollary implies that the p_{zi} constitute a family of polynomials, orthogonal with respect to the weight function μ_z. This corresponds to a P-polynomial association scheme.

Observing that

$$A_i A_j = \sum_{k=0}^{s} a_{ij}^k A_k \quad , \qquad A_k E_z = p_{zk} E_z \quad ,$$

imply

$$p_{zi} p_{zj} = \sum_{k=0}^{s} a_{ij}^k p_{zk} \quad .$$

We give the following equivalent definitions for an association scheme $(\Omega, <I, \Gamma_1, \Gamma_2, \ldots .\Gamma_s>)$ to be P-polynomial:

3.3.4. (i) p_{zi} is a polynomial in p_{z1} of degree i, for i = 1,...,s ;

(ii) $a_{i,1}^{i+1} \neq 0$ for i = 1,...,s-1 and
$a_{ij}^{k} \neq 0$ only if $|i - j| \leq k \leq i + j$;

(iii) Γ_i is the (distance i) relation in the graph (Ω,Γ_1) for i = 1,2....,s.

3.3.5. Corollary. $Q^T \Delta_v Q = n \Delta_\mu$, $\sum_{z=0}^{s} v_z q_{zk} q_{z1} = n\mu_k \delta_{k1}$.

If q_{zi} is a polynomial in q_{z1} of degree i, then the corollary implies that the q_{zi} constitute a family of polynomials, orthogonal with respect to the weight function v_z. This corresponds to a Q-polynomial association scheme.

Observing that

$$E_i \circ E_j = \sum_{k=0}^{s} b_{ij}^{k} E_k \quad , \quad E_i \circ A_z = \frac{1}{n} q_{zi} A_z \ .$$

imply

$$q_{zi} q_{zj} = \sum_{k=0}^{s} b_{ij}^{k} q_{zk} \ .$$

We give the following equivalent definitions for an association scheme $(\Omega, \{I, \Gamma_1, \Gamma_2, \ldots. \Gamma_s\})$ to be Q-polynomial:

3.3.6. (i) q_{zi} is a polynomial in q_{z1} of degree i, for i = 1,...,s;

(ii) $b_{i,1}^{i+1} \neq 0$ for i = 1,...,s-1 and
$b_{ij}^{k} \neq 0$ only if $|i - j| \leq k \leq i + j$.

For Q-polynomial schemes no combinatorial interpretation is known which would be the analogue of the condition (iii) above.
The preceding is illustrated in a few examples. More details and further examples may be foundin the references.

3.3.7. Example. The Hamming scheme H(v,2) has

$$v_i = \mu_i = \binom{v}{i}$$

It is both P- and Q-polynomial, with the same family of orthogonal polynomials; viz. the Krawtchouk polynomials.

3.3.8. Example. The Johnson scheme J(v,k) has

$$v_i = \binom{k}{i}\binom{v-k}{i} \quad , \quad \mu_i = \binom{v}{i} - \binom{v}{i-1} \ .$$

It is Q-polynomial with Hahn polynomials, and P-polynomial with dual Hahn polynomials. The underlying group is the symmetric group on v letters.

3.3.9. Example. Let Ω denote the set of the k-subspaces of the vector space $V(v,F_q)$. Two k-subspaces are in the relation Γ_i whenever their intersection has dimension k-i. The resulting association scheme is P- and Q-polynomial, with q-Hahn polynomials, under the group $GL(v,F_q)$.

3.3.10. Example. Polynomial schemes are provided by the action of the symplectic, the orthogonal, and the unitary group, respectively, on the set of the maximal totally isotropic subspaces (of dimension k, say), two such subspaces being in the relation Γ_i whenever their intersection has dimension k-i.

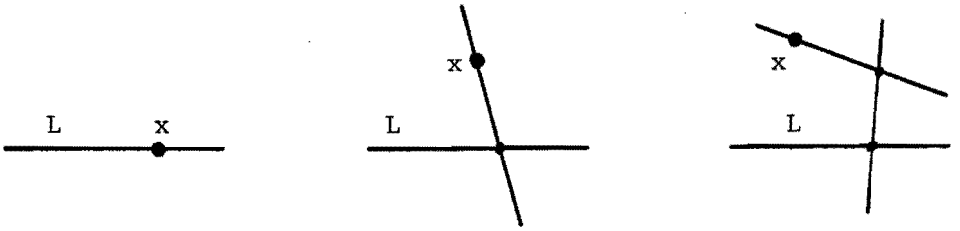
3.3.11. Example. Polynomial schemes are provided by the $2^{m(2m-1)}$ alternating bilinear forms on $V(2m,F_2)$, two forms being in the relation Γ_i whenever their sum has rank 2i.

3.4. An inequality for generalized hexagons.

3.4.1. Definition. A generalized hexagon H of order (s,t) is an incidence structure with points and lines, such that

(i) each line has s+1 points,
(ii) each point is on t+1 lines,
(iii) two distinct points are on at most one line,
(iv) for any non-incident point-line pair x,L there is a unique path of length ≤ 2, between x and L.

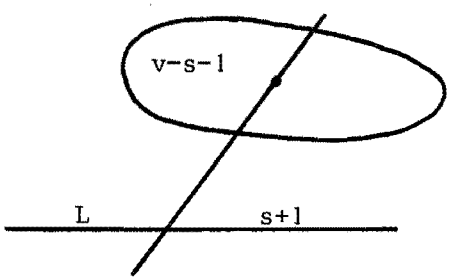
From the definition it is immediately clear that the only possible situations fo a point x and a line L are:



3.4.2. Theorem. The number of points v, of a generalized hexagon H of order (s,t) equals

$$(s+1)(s^2t^2+st+1) .$$

Proof. Take a line L with its s+1 points x_i for i = 1,....,s+1.



Through each x_i there are t lines distinct from L, with each s points different from x_i. The total number of points at distance 1 to L therefore is (s+1)st. Analogously we find st distinct points at distance 2 from L for any of the points at distance 1. So there are (s+1)stst points at distance 2 to L. Due to property (iv) of the generalized hexagons these are all distinct and we have now found all points. Hence the total number is

$$(s+1) + (s+1)st + (s+1)s^2t^2 = (s+1)(s^2t^2+st+1).$$

□

We define an association scheme on the points of H as follows. Two points are in relation Γ_i for i = 0,1,2.3, if their distance equals i. The adjacency matrix of Γ_i is A_i. By use of the definition of H one can find the intersection numbers a_{ij}^k by straightforward counting. The amount of work in computing these numbers can be reduced by use of the equalities

$$\sum_{i=0}^{3} a_{ij}^k = v_j \quad , \qquad \sum_{j=0}^{3} v_j = v = (s+1)(s^2t^2+st+1) .$$

The a_{ij}^k can be found in the following table which shows at once that the association scheme is distance regular.

k	a_{11}^k	a_{12}^k	a_{22}^k	a_{13}^k	a_{23}^k	a_{33}^k
0	s(t+1)	0	$s^2t(t+1)$	0	0	s^3t^2
1	s	st	st(s-1)	0	s^2t^2	$s^2t^2(s-1)$
2	1	s-1	$s(t^2+t-1)$	st	st(s-1)(t+1)	$st(s^2t-st-s+t)$
3	0	t+1	$(s-1)(t+1)^2$	(s-1)(t+1)	$(t+1)(s^2t-st-s+t)$	$t(s-1)(s^2t-s+t)+1$

(see [20], p. 53)

3.4.3. Theorem. For a generalized hexagon of order (s,t) the following holds:

$$t \leq s^3 \quad \text{or} \quad s = 1.$$

Proof. Let $A := A_2 - (s-1)A_1$, then we find with the help of

$A_1 + A_2 + A_3 + I = J$ and $AJ = kJ$ $\quad (k=s(t+1)(st-s+1))$:

$$(A + (s^2-s+1)I)(A - (t+1)(s+t-1)I) = s(t+1)(st-s+1)J$$

So $\quad spec(A) = ([s(t+1)(st-s+1)]^1, [-(s^2-s+1)]^m, [(t+1)(s+t-1)]^n).$

$$spec(A + (s^2-s+1)I) = ([s(t+1)(st-s+1) + (s^2-s+1)]^1, 0^m, \lambda^n)$$

where $\lambda = (t+1)(s+t-1) + (s^2-s+1)$.

But trace $(A + (s^2-s+1)I) = (s^2-s+1)v = k + n\lambda$

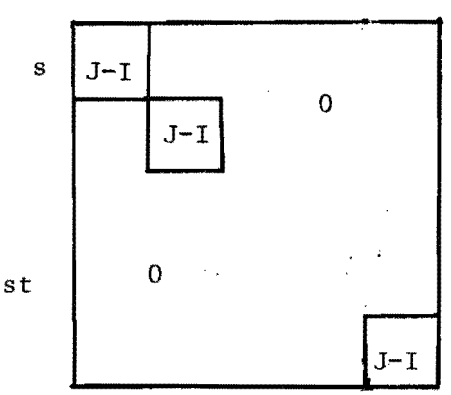
This yields

$$n = s^3 \frac{(s^2t^2+st+1)}{(s^2+st+t^2)}$$

and rank $(A + (s^2-s+1)I) = 1 + n$.

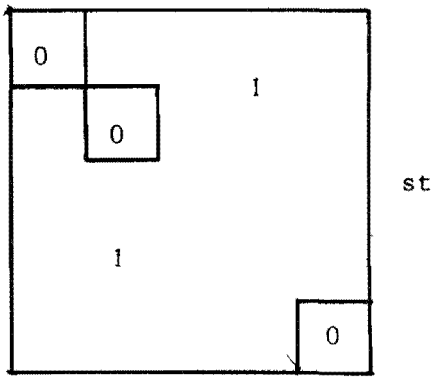
Now take a line L and consider all points x for which dist(x,L) = 1. We divide these points in s+1 classes (each point on L coincides with one class). Each class is divided again in t blocks (the lines) that consist of s points. We define B_1 to be the adjacency matrix of Γ_1 (distance 1), if only the points in a class are considered.

$B_1 =$



Analogously B_2 is the adjacency matrix of Γ_2, if only the points in one class are considered.

$B_2 =$



So $B_1 = I_t \otimes J_s - I_{st}$, $B_2 = J_{st} - I_t \otimes J_s$.

Define $B := B_2 - (s-1)B_1 + (s^2-s+1)I_{st} = s^2 I_{st} - sI_t \otimes J_s$.

$$\text{spec}(B) = ([s^2+st-s^2]^1, [s^2]^m, 0^n).$$

$$\text{trace}(B) = st(s^2-s+1) = st + s^2 m.$$

This yields $m = st - t$ and $\text{rank}(B) = (st-t+1)$.

$A' := I_{s+1} \otimes B$, $\text{rank}(A') = (s+1)(st-t+1)$.

Since A' is a principle submatrix of A the following holds :

$$\text{rank}(A') \leq \text{rank}(A),$$

$$\text{So } (s+1)(st-t+1) \leq 1 + s^3 \frac{(s^2t^2+st+1)}{s^2+st+t^2}$$

which leads to $t^2(s^2-1)(t-s^3) \leq 0$. □

Remark. If we define the points as "lines" and the lines as "points" we get an incidence structure that is again a generalized hexagon, of order (t,s), as can be simply verified. But this means that 3.4.3. holds in this case too,

$$s \leq t^3 \quad \text{or} \quad t = 1.$$

3.5. An association scheme in PG(2,4).

(In this paragraph $< , >_F$ denotes the standard inner product in a vectorspace over the field F).

Consider the projective plane PG(2,4). It has 21 points, which we denote by $p_1,\ldots,p_{21}$, and 21 lines, which we denote by $l_1,\ldots,l_{21}$. Furthermore, each point is on 5 lines and each line has 5 points.

For $i = 1,\ldots,21$ we define the vector $\underline{l}_i \in V(21, GF(2))$ by

$$(\underline{l}_i)_j = 1 \quad \text{if } p_j \in l_i$$
$$(\underline{l}_i)_j = 0 \quad \text{if } p_j \notin l_i \qquad\qquad j = 1,\ldots,21.$$

$\underline{l}_i$ is the characteristic vector of the line l_i.

Consider the code C generated by $\underline{l}_1,\ldots,\underline{l}_{21}$ over GF(2).

C is a binary linear code of length 21. We recall the following definition:

3.5.1. Definition. Let X be a linear code of length n and dimension k over the field F.

The dual code $X^\perp$ of X is defined as follows:

$$X^\perp := \{\underline{y} \in V(n,F) \mid \forall_{\underline{x}\in X} [<\underline{x},\underline{y}>_F = 0]\}.$$

It is easy to see that $X^\perp$ is a linear code of length n and dimension n-k.

3.5.2. Theorem. The dimension of C is at most 11.

Proof. The extended code $\overline{C}$ of C consists of the vectors

$$\overline{\underline{c}} = (c_1,\ldots,c_{22}), \quad \text{where } \underline{c} = (c_1,\ldots c_{21}) \in C$$

and

$$\sum_{i=1}^{22} c_i = 0 \qquad \text{(in GF(2))}.$$

Clearly, $\overline{C}$ is a linear code, and has the same dimension as C.

Also $\overline{C}$ is generated by $\overline{l}_1,\ldots,\overline{l}_{21}$,

and

$$<\overline{l}_i,\overline{l}_j>_{F_2} = 0, \qquad i,j = 1,2,\ldots,21.$$

Let $\overline{\underline{c}}_1 \in \overline{C}$ and $\overline{\underline{c}}_2 \in \overline{C}$. Then, we can write

$$\overline{\underline{c}}_1 = \sum_{i=1}^{21} c_{1i}\overline{\underline{l}}_i, \quad \overline{\underline{c}}_2 = \sum_{j=1}^{21} c_{2j}\overline{\underline{l}}_j \qquad c_{1i},c_{2j} \in \{0,1\}.$$

Hence

$$\langle \bar{c}_1, \bar{c}_2 \rangle_{F_2} = \sum_{i=1}^{21} \sum_{j=1}^{21} c_{1i} c_{2j} \langle \bar{l}_i, \bar{l}_j \rangle_{F_2} = 0.$$

This yields $\bar{C} \subset (\bar{C})^{\perp}$.

Therefore, if k is the dimension of $\bar{C}$, then $k \leq 22-k$ ($\bar{C}$ has length 22). Hence $k \leq 11$, and so

$$\dim(C) = \dim(\bar{C}) \leq 11. \qquad \square$$

3.5.3. Lemma. Let $\underline{x}$ be a word of C of even weight $w(\underline{x})$. Then $w(\underline{x}) = 0 \bmod 4$.

Proof. We can easily see that a word of even weight of C is generated by an even number of lines. Inother words, the words of C of even weight are generated by

$$\underline{b}_1 := \underline{l}_1 + \underline{l}_2 \ , \ \underline{b}_2 := \underline{l}_1 + \underline{l}_3 \ , \ \ldots \ , \ \underline{b}_{20} := \underline{l}_1 + \underline{l}_{21}$$

The following holds:

$$\langle \underline{b}_i, \underline{b}_i \rangle_R = w(\underline{b}_i) = 8 \ , \quad i = 1,2,\ldots,20$$

$$\langle \underline{b}_i + \underline{b}_j, \underline{b}_i + \underline{b}_j \rangle_R = w(\underline{b}_i + \underline{b}_j) = w(\underline{l}_{i+1} + \underline{l}_{j+1}) = 0 \bmod 8$$

$$i,j = 1,2,\ldots,20.$$

Because $\langle \underline{b}_i + \underline{b}_j, \underline{b}_i + \underline{b}_j \rangle_R = \langle \underline{b}_i, \underline{b}_i \rangle_R + \langle \underline{b}_j, \underline{b}_j \rangle_R + 2\langle \underline{b}_i, \underline{b}_j \rangle_R$

we get $\langle \underline{b}_i, \underline{b}_j \rangle_R = 0 \bmod 4 \qquad i,j = 1,2,\ldots,10.$

Now let $\underline{d} \in C$ have even weight. Then we can write

$$\underline{d} = \sum_{i=1}^{20} d_i \underline{b}_i \ , \quad d_i \in \{0,1\}, \text{ and therefore}$$

$$w(\underline{d}) = \langle \underline{d}, \underline{d} \rangle_R = \sum_{i=1}^{20} \sum_{j=1}^{20} d_i d_j \langle \underline{b}_i, \underline{b}_j \rangle_R = 0 \bmod 4.$$

$\square$

3.5.4. Theorem. The dimension of C is at most 10.

Proof. A hyperoval H in PG(2,4) consists of 6 points, such that each line of PG(2,4) has 0 or 2 points of H. Let $\underline{h}$ be the characteristic vector of H. Then $\underline{h}$ has weight 6, and with lemma 3.5.3. this yields $\underline{h} \notin C$.

Also $\quad \langle \overline{\underline{h}}, \overline{\underline{l}}_i \rangle_{F_2} = 0 \qquad i = 1,2,..,21.$

for $|H \cap l_i| = 0$ or 2, and $(\overline{\underline{h}})_{22} = 0$.

Let $\overline{\underline{c}} \in \overline{C}$ then $\overline{\underline{c}} = \sum_{i=1}^{21} c_i \overline{\underline{l}}_i$ and

$$\langle \overline{\underline{c}}, \overline{\underline{h}} \rangle_{F_2} = \sum_{i=1}^{21} c_i \langle \overline{\underline{l}}_i, \overline{\underline{h}} \rangle_{F_2} = 0.$$

Hence $\overline{\underline{h}} \in (\overline{C})$ and $\overline{\underline{h}} \notin \overline{C}$ ($\underline{h} \notin C$). This yields

$\dim(\overline{C}) < \dim((\overline{C})^{\perp})$, and therefore

$$\dim(C) = \dim(\overline{C}) \leq 10 \qquad \text{(see also theorem 3.5.2.)}$$

□

3.5.5. Theorem. The dimension of C is 10 and C has the following weight distribution :

weight	0	5	8	9	12	13	16	21
words	1	21	210	280	280	210	21	1

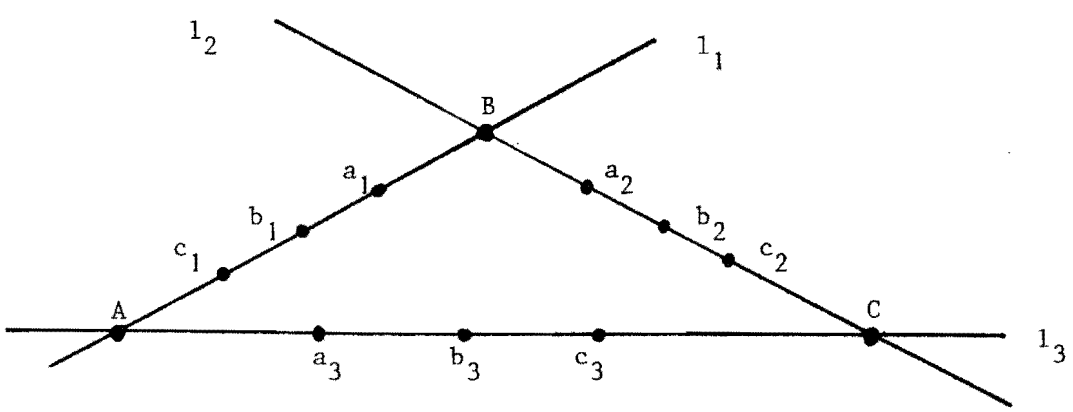
Proof. We prove this theorem by simply counting:

1) $\underline{0} \in C$, hence there is one word of weight 0.

2) a line in PG(2,4) is a word of weight 5 in C. Hence the number of words of weight $5 \geq 21$.

3) A pair of lines in PG(2,4) is a word of weight 8 in C. Hence the number of words of weight $8 \geq \binom{21}{2} = 210$.

4) A triple of lines in PG(2,4) that don't go through the same point is a word of weight 9:



There are $\frac{21 \cdot 20 \cdot 16}{3!} = 1120$ of such triples in PG(2,4). We will now show that for every triple there are 3 other (distinct) triples that lead to the codeword produced by that triple. Consider the triple above. Select a point a_2 on l_2 not on l_1, l_3 (there are 3 possibilities) and let a_3 be the intersection point of the lines $a_1 \vec{\cup} a_2$ and l_3. Let $c_2 := (b_1 \cup a_3) \cap l_2$ and let b_2 be the third point on l_2 that is not on l_1 or l_3. Then the lines $b_1 \cup b_2$ and l_3 meet in a point $b_3 \neq a_3$. Call c_3 the third point on l_3 that is not on l_1 or l_2. Then it is easy to see that $c_3 = (c_1 \cup c_2) \cap l_3$.

Now assume that the lines $(a_1 \cup a_2 \cup a_3)$, $(b_1 \cup b_2 \cup b_3)$ and $(c_1 \cup c_2 \cup c_3)$ meet in one point x. Then there are at least 6 distinct lines that meet in x, viz.

$(a_1 \cup a_2 \cup a_3)$, $(b_1 \cup b_2 \cup b_3)$, $(c_1 \cup c_2 \cup c_3)$, $(x \cup A)$, $(x \cup B)$ and $(x \cup C)$.

But this is in contradiction with the fact that only 5 lines meet in x. Hence $(a_1 \cup a_2 \cup a_3)$, $(b_1 \cup b_2 \cup b_3)$ and $(c_1 \cup c_2 \cup c_3)$ form a triangle in PG(2,4) that leads to the same codeword as the original triangle. There are in total 4 triangles that lead to that word (there are 3 choices for a_2); hence

$$\# \text{ words of weight } 9 \geq \frac{1120}{4} = 280.$$

5) $(1,1,\ldots,1) \in C$ for $(1,\ldots,1) = \sum_{i=1}^{21} l_i$

(each point is on 5 lines).

Therefore the complement of every codeword is in the code. This yields a lower bound on the number of words of weight 12, 13, 16 and 21. We see that $|C| \geq 1024$. Theorem 3.5.4. says that $|C| \leq 1024$. Hence $|C| = 1024$ and therefore, C has dimension 10 and weight distribution as above. □

Consider the code D that consists of the words in C of even weight. Clearly, D is a linear code and has dimension 9 ($|D| = 512$). Define the following relations on D:

let $\underline{\omega},\underline{\omega}' \in D$

$\{\underline{\omega}, \underline{\omega}'\} \in \Gamma_1 :\Longleftrightarrow$ the Hamming distance $d_h(\underline{\omega}, \underline{\omega}') \in D$ between $\underline{\omega}$ and $\underline{\omega}'$ is 16.

$\{\underline{\omega}, \underline{\omega}'\} \in \Gamma_2 :\Longleftrightarrow d_h(\underline{\omega}, \underline{\omega}') = 8.$

$\{\underline{\omega}, \underline{\omega}'\} \in \Gamma_3 :\Longleftrightarrow d_h(\underline{\omega}, \underline{\omega}') = 12.$

Without proof we state the following theorem:

3.5.6. Theorem. $(D, \{id, \Gamma_1, \Gamma_2, \Gamma_3\})$ is a 3-class Q-polynomial association scheme.

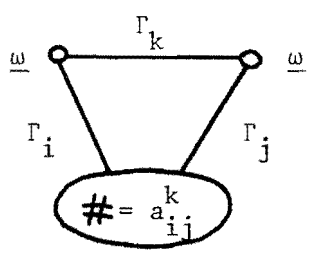
We will now determine the character table P. Let A_1, A_2, A_3 be the (512 x 512)-matrices corresponding with Γ_1, Γ_2, Γ_3, respectively, and $A_0 := I_{512}$.
With the relations $A_0E_i = p_{i0}E_i$ $i = 0,1,2,3$ and $A_kE_0 = p_{0k}E_0$ $k = 0,1,2,3$ it is easy to see that $p_{i0} = 1$, $i = 0,1,2,3$ and $p_{01} = v_1 = 21$, $p_{02} = v_2 = 210$, $p_{03} = v_3 = 280$.

Furthermore we have the following relations:

$$(*) \quad p_{zi}p_{zj} = \sum_{k=0}^{3} a_{ij}^k p_{zk} \qquad z,i,j = 0,1,2,3$$

$$(**) \quad A_i A_j = \sum_{k=0}^{3} a_{ij}^k A_k \qquad i,j = 0,1,2,3$$

To solve the equations of (*), we have to determine the a_{ij}^k's.
The combinatorial interpretation of the a_{ij}^k's (see 3.2.) is



Without loss of generality we can take $\underline{\omega} = \underline{0}$.
Then:

1) Clearly, $a_{11}^0 = v_1 = 21$, and $a_{11}^1 = 0$ for, it is not possible to find 2 vectors in V(21,GF(2)) of weight 16 and Hamming distance 16.

2) Let $\underline{\omega}'$ have weight 8, $\underline{x}$ have weight 16 and assume that $d_h(\underline{\omega}', \underline{x}) = 16$ then $\langle \underline{\omega}', \underline{x} \rangle = 4$.
The complement of $\underline{x}$ is a line $\underline{1}$ in PG(2,4) and $\langle \underline{\omega}', \underline{1} \rangle = 4$.
$\underline{\omega}'$ is a pair of lines in PG(2,4), hence $\underline{1}$ is one of those lines, and therefore there are 2 $\underline{x}$'s with the above properties. This yields $a_{11}^2 = 2$.

3) $a_{11}^3 = 0$ for it is not possible to find 2 vectors of weight 12 and 16, respectively, with Hamming distance 16.

4) $a_{12}^0 = 0$ (trivial).

5) It is easy to see that the following equality holds:

$$v_1 a_{12}^2 = v_2 a_{11}^2.$$

Hence $a_{12}^1 = \frac{210 \cdot 2}{21} = 20$.

Similar techniques can be used to determine the other $a_{ij}^k = a_{ji}^k$.
With this and the equatinns (*), we find

$$P = \begin{bmatrix} 1 & 21 & 210 & 280 \\ 1 & -11 & 50 & -40 \\ 1 & 5 & 2 & -8 \\ 1 & -3 & -6 & 8 \end{bmatrix}$$

(Note that $p_{z2} = \frac{1}{2}(p_{z1}^2 - 21)$ (the scheme is P-polynomial)).

With $PQ = nI$ we find that $Q = P$.
Also, because $\Delta_v = \mathrm{diag}(p_{0k})$, $\Delta_\mu = \mathrm{diag}(q_{oi})$ we find

$$\Delta_v = \Delta_\mu = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 21 & 0 & 0 \\ 0 & 0 & 210 & 0 \\ 0 & 0 & 0 & 280 \end{bmatrix}$$

Hence the scheme is self-dual and P- and Q-polynomial.

3.6. Regular Two-graphs as Association schemes.

Let A and B denote symmetric (0,1) matrices such that
$A + B = J - I$ and $A - B$ has only two distinct eigenvalues.

Consider the 2n x 2n matrices

$$A_0 = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}, \quad A_1 = \begin{bmatrix} A & B \\ B & A \end{bmatrix}, \quad A_2 = \begin{bmatrix} B & A \\ A & B \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

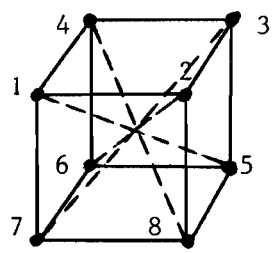
We claim that A_0, A_1, A_2, A_3 determine a 3-class association scheme. Before proving this, we consider the following examples:

3.6.1. Example. n = 4, and

$$A - B = \begin{bmatrix} 0 & 1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 0 \end{bmatrix}$$

Clearly, $A + B = J - I$. Also $(A - B)^2 + 3I - 2(A - B) = 0$, and therefore $(A - B + 3I)(A - B - I) = 0$. Hence $(A - B)$ has 2 eigenvalues viz. -3 and +1.

Consider the 8 vertices of a cube in R^3.



A_1, A_2, A_3 correspond to the relations Γ_1, Γ_2, Γ_3, respectively, where:

Γ_1: two vertices are in relation Γ_1 iff they are connected by a —— line.

Γ_2: two vertices are in relation Γ_2 iff they are not connected by a —— or a – – – line.

Γ_3: two vertices are in relation Γ_3 iff they are connected by a – – – line.

3.6.2. Example. n = 6, and

$$A - B = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}$$

Clearly, $A + B = J - I$ and $(A - B)^2 = 5I$. Hence, $A - B$ has eigenvalues $\sqrt{5}$ and $-\sqrt{5}$. The relations corresponding to A_1, A_2, A_3 are similar to those given in example 3.6.1., but on a icosahedron instead of a cube.

We return to the general case stated above. Then

$$(A + B)^2 = (J - I)^2 = (n-2)J + I = (n-2)(A + B) + (n-1)I \qquad (*)$$

Also $A - B$ has two eigenvalues, say ρ and σ.
Then $(A - B - \rho I)(A - B - \sigma I) = 0$, and this yields

$$(A - B)^2 = (\rho + \sigma)(A - B) - \rho\sigma I. \qquad (**)$$

It is easy to see that $(A + B)^2$ and $(A - B)^2$ have the same diagonal.
Therefore $(*)$ and $(**)$ yield

$$n - 1 = -\rho\sigma.$$

With this we can write

$$A^2 + B^2 + AB + BA = -(\rho+\sigma+1)(A + B) - \rho\sigma I \ , \quad \text{and}$$
$$A^2 + B^2 - AB - BA = (\rho+\sigma)(A - B) - \rho\sigma I \ .$$

Hence,

$$(***) \begin{cases} 2(A^2 + B^2) = -2\rho I - (1-\rho)(1-\sigma)A - (1+\rho)(1+\sigma)B \\ 2(AB + BA) = \quad - (1-\rho)(1-\sigma)B + (1+\rho)(1+\sigma)A \end{cases}$$

Now we can prove the following theorem:

3.6.3. Theorem. The matrices A_0, A_1, A_2, A_3 defined as above determine a 3-class association scheme.

Proof.

1) Clearly, $A_0 + A_1 + A_2 + A_3 = \begin{bmatrix} J & J \\ J & J \end{bmatrix}$

2) We have to prove :

$$A_i A_j = \sum_{k=0}^{3} a_{ij}^k A_k \ , \text{ for certain } a_{ij}^k \in R \ , \quad i,j = 0,1,2,3.$$

For $i = 0$ and $i = 3$ it is trivial. Furthermore

$$A_1^2 = A_2^2 = \begin{bmatrix} A^2 + B^2 & AB + BA \\ AB + BA & A^2 + B^2 \end{bmatrix} \qquad \text{and}$$

$$A_1 A_2 = \begin{bmatrix} AB + BA & A^2 + B^2 \\ A^2 + B^2 & AB + BA \end{bmatrix}$$

With (***) we see that

$$A_1^2 = A_2^2 = -\rho\sigma A_0 - \tfrac{1}{2}(1-\rho)(1-\sigma)A_1 - \tfrac{1}{2}(1+\rho)(1+\sigma)A_2 \qquad \text{and}$$
$$A_1A_2 \quad = -\rho\sigma A_3 - \tfrac{1}{2}(1-\rho)(1-\sigma)A_2 - \tfrac{1}{2}(1+\rho)(1+\sigma)A_1 .$$

Because $a_{ij}^k = a_{ji}^k$ $\quad i,j,k = 0,1,2,3$, we have proved the theorem. □

We are interested in the charactertable P of the association scheme. Let μ and ν be the multiplicities of the eigenvalues ρ and σ of A - B. (for μ,ν,ρ,σ the following holds:
$\mu + \nu = n$ and $\operatorname{trace}(A - B) = 0 = \rho\mu + \sigma\nu$). Let x and y be eigenvectors of A - B for ρ and σ, respectively. Then it is easy to see that

$$A_0\begin{pmatrix} x \\ -x \end{pmatrix} = \begin{pmatrix} x \\ -x \end{pmatrix}, \; A_1\begin{pmatrix} x \\ -x \end{pmatrix} = \rho\begin{pmatrix} x \\ -x \end{pmatrix}, \; A_2\begin{pmatrix} x \\ -x \end{pmatrix} = -\rho\begin{pmatrix} x \\ -x \end{pmatrix}, \; A_3\begin{pmatrix} x \\ -x \end{pmatrix} = -\begin{pmatrix} x \\ -x \end{pmatrix}$$

$$A_0\begin{pmatrix} y \\ -y \end{pmatrix} = \begin{pmatrix} y \\ -y \end{pmatrix}, \; A_1\begin{pmatrix} y \\ -y \end{pmatrix} = \sigma\begin{pmatrix} y \\ -y \end{pmatrix}, \; A_2\begin{pmatrix} y \\ -y \end{pmatrix} = -\sigma\begin{pmatrix} y \\ -y \end{pmatrix}, \; A_3\begin{pmatrix} y \\ -y \end{pmatrix} = -\begin{pmatrix} y \\ -y \end{pmatrix}$$

Hence this way we have found $\mu + \nu = n$ simultaneous orthogonal eigenvectors of A_0, A_1, A_2, A_3. Also because $(A + B)j = (J - I)j = (n-1)j$ we see that

$$A_0\begin{pmatrix} j \\ j \end{pmatrix} = \begin{pmatrix} j \\ j \end{pmatrix}, \; A_1\begin{pmatrix} j \\ j \end{pmatrix} = (n-1)\begin{pmatrix} j \\ j \end{pmatrix}, \; A_2\begin{pmatrix} j \\ j \end{pmatrix} = (n-1)\begin{pmatrix} j \\ j \end{pmatrix}, \; A_3\begin{pmatrix} j \\ j \end{pmatrix} = \begin{pmatrix} j \\ j \end{pmatrix}.$$

Hence j is also a simultaneous eigenvector of A_0, A_1, A_2, A_3.
Let z be a vector with $z^T j = 0$. (we can choose n-1 of these vectors that are orthogonal). Then

$$A_0\begin{pmatrix} z \\ z \end{pmatrix} = \begin{pmatrix} z \\ z \end{pmatrix}, \; A_1\begin{pmatrix} z \\ z \end{pmatrix} = -\begin{pmatrix} z \\ z \end{pmatrix}, \; A_2\begin{pmatrix} z \\ z \end{pmatrix} = -\begin{pmatrix} z \\ z \end{pmatrix}, \; A_3\begin{pmatrix} z \\ z \end{pmatrix} = \begin{pmatrix} z \\ z \end{pmatrix} .$$

We now have $\mu+\nu+1+n-1 = 2n$, simultaneous orthogonal eigenvectors of A_0, A_1, A_2, A_3, and they determine the 4 simultaneous eigenspaces of A_0, A_1, A_2, A_3. Then,

$$P = \begin{bmatrix} 1 & n-1 & n-1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & \rho & -\rho & -1 \\ 1 & \sigma & -\sigma & -1 \end{bmatrix} .$$

Also $\Delta_\nu = \operatorname{diag}(1,n-1,n-1,1)$ and $\Delta_\nu = \operatorname{diag}(1,n-1,\mu,\nu)$.

The matrix A - B can be considered as the (-1,1) adjacency matrix of a graph. Clearly, graphs that are switching equivalent with this graph lead to the same association scheme, for the (-1,1) adjacency matrices of graphs that are switching equivalent have the same eigenvalues and multiplicities for further details see chapter 5.5.: "Two-graphs".

3.7. The A-module V.

We now return to the theory of the association schemes.
For the set Ω of cardinality n, let V denote the vector space of dimension n which consists of all formal real combinations

$$x = \sum_{\omega\in\Omega} x(\omega)\omega \quad , \quad x(\omega) \in R.$$

The space V is provided with the inner product

$$\langle x,y\rangle = \sum_{\omega\in\Omega} x(\omega)\ y(\omega)$$

Consider the basis $\{ \omega \mid \omega\in\Omega\}$ of V. Let $\underline{x}(\omega)$ be the vector representing $x(\omega)\omega$ w.r.t. this basis. Then the matrices of the Bose-Mesner algebra A of an association scheme on Ω act on V following

$$A_k\underline{x}(\omega) = \sum_{\{\omega,\omega'\}\in\Gamma_k} \underline{x}(\omega')$$

and decompose V into the simultaneous eigenspaces V_i:

$$V = V_0 \perp V_1 \perp \ldots \perp V_s \quad , \quad A_kV_i = p_{ik}V_i.$$

Let $\Pi_i : V \to V$ denote the projection onto V_i, then it is easy to see that

$$\langle \Pi_i\omega,\ \Pi_i\omega'\rangle = \langle \omega,\ \Pi_i\omega'\rangle = E_i(\omega,\omega').$$

(Note that $E_0,\ldots, E_s$ are the projections on the s+1 simultaneous eigenspaces of $A_0,\ldots, A_s$).
This leads to the following:

1) $\Omega_i := \{\Pi_i\omega \mid \omega\in\Omega\}$, has Gram and coordinate matrix E_i.

2) $\Omega_{ii} := \{\Pi_i\omega \otimes \Pi_i\omega \mid \omega\in\Omega\}$ has Grammatrix
$(E_i \circ E_i) = [<\Pi_i\omega, \Pi_i\omega'>^2]$.

(we remind the reader that the 2-tensor $\underline{a}\otimes\underline{b}$ has the components $(\underline{a}\otimes\underline{b})_{ij} = a_ib_j$, and that two 2-tensors have inner product

$$<\underline{a}\otimes\underline{b}, \underline{c}\otimes\underline{d}> = <\underline{a},\underline{c}><\underline{b},\underline{d}>)$$

3) $\Omega_{iii} := \{\Pi_i\omega \otimes \Pi_i\omega \otimes \Pi_i\omega \mid \omega\in\Omega\}$ has Grammatrix
$(E_i \circ E_i \circ E_i) = [<\Pi_i\omega, \Pi_i\omega'>^3]$.

The orthogonal projection Ω_i of the orthonormal frame Ω is spherical. Indeed, take $k = 0$ in the equation

$$nE_i \circ A_k = q_{ki}A_k.$$

Then we get

$$nE_i \circ I = q_{oi}I.$$

Hence

$<\Pi_i\omega, \Pi_i\omega> = q_{oi}/n$, $\omega\in\Omega$, and therefore Ω_i is a subset of a sphere.

In addition in [10] it is shown that Ω_i is a spherical 2-design in V_i, and that it is a spherical 3-design iff $b^i_{ii} = 0$, equivalently

$$\sum E_i \circ E_i \circ E_i = 0.$$

(Let X be a subset of the unit sphere in R^d. X is a spherical t-design if for $1 \le k \le t$ the sum of the values of any homogeneous harmonic polynomial of degree k over the points of X is zero.)

For $\{\omega, \omega'\}\in \Gamma_k$ the equation $nE_i \circ A_k = q_{ki}A_k$ reads

$$<\Pi_i\omega, \Pi_i\omega'> = \frac{1}{n}q_{ki}.$$

This is the addition formula in V_i, in particular in the Q-polynomial case when the q_{ki} are polynomials in q_{k1} of degree i.

The vectorspace V provides a setting for the subsets of the set Ω. For instance,

$$X = \{\omega_1,\ldots,\omega_m\} \subset \Omega = \{\omega_1,\ldots,\omega_n\},$$

is represented by the vector $\underline{x} = (1^m, 0^{n-m}) \in V$. The cardinality of X, of the intersection $X \cap Y$ of two subsets, and the average valency a_k

of Γ_k restricted to X are expressed by

$$|X| = \langle \underline{x}, \underline{x} \rangle , \quad |X \cap Y| = \langle \underline{x}, \underline{y} \rangle ,$$

$$a_k = \frac{\langle \underline{x}, A_k \underline{x} \rangle}{\langle \underline{x}, \underline{x} \rangle} \qquad \text{for } k = 0,1,\ldots,s.$$

For any $\underline{x}$, $\underline{y} \in V$, we define the distribution matrix $D(\underline{x},\underline{y})$ to be either side of the following equality:

3.7.1. Theorem. $$\sum_{k=0}^{s} \langle \underline{x}, A_k \underline{y} \rangle \frac{A_k}{v_k} = \sum_{i=0}^{s} \langle \underline{x}, E_i \underline{y} \rangle \frac{nE_i}{\mu_i}$$

Proof. With $A_k = \sum_{i=0}^{s} p_{ik} E_i$, $\Delta_\mu P = Q^T \Delta_v$ and $PQ = nI$, we see that:

$$\sum_{k=0}^{s} \langle \underline{x}, A_k \underline{y} \rangle \frac{A_k}{v_k} = \sum_{i=0}^{s} \sum_{j=0}^{s} \sum_{k=0}^{s} \langle \underline{x}, E_i \underline{y} \rangle E_j \frac{p_{ik} p_{jk}}{v_k} =$$

$$= \sum_{i=0}^{s} \sum_{j=0}^{s} \sum_{k=0}^{s} \langle \underline{x}, E_i \underline{y} \rangle E_j \frac{p_{ik} q_{kj}}{\mu_j} = \sum_{i=0}^{s} \langle \underline{x}, E_i \underline{y} \rangle \frac{nE_i}{\mu_i}$$

□

Putting $\underline{x} = \underline{y}$ we obtain the inner distribution

$$D(\underline{x},\underline{x}) = \sum_{k=0}^{s} \frac{\langle \underline{x}, A_k \underline{x} \rangle}{v_k} A_k = \sum_{i=0}^{s} \frac{\langle \underline{x}, E_i \underline{x} \rangle}{\mu_i} nE_i .$$

The transition of the coefficients

$$\frac{1}{v_k} \langle \underline{x}, A_k \underline{x} \rangle \quad \text{to} \quad \frac{1}{\mu_i} \langle \underline{x}, E_i \underline{x} \rangle$$

is well-known as the Mac Williams transform. It's significance stems from the nonnegativity of the inner product $\langle \underline{x}, E_i \underline{x} \rangle$.

Multiplication of $D(\underline{x},\underline{x})$ by E_i yields

$$\langle \underline{x}, \underline{x} \rangle \sum_{k=0}^{s} a_k q_{ki} = n \langle \underline{x}, E_i \underline{x} \rangle \geq 0.$$

With $\underline{a} = (a_0, a_1, \ldots, a_s)$, $a^0 = 1$, the constraints

$$Q^T \underline{a} \geq 0, \quad \underline{a} \geq 0, \quad |X| = 1 + a_1 + \ldots + a_s$$

provide a setting for application of the linear programming method. [15]. (For more details on the A-module, see appendix 3.2).

3.8. Cliques and codes.

Let $R = \{1,2,\ldots,r\} \subset \{1,2,\ldots,s\}$. For an association scheme $(\Omega, \{\Gamma_0, \Gamma_1, \ldots, \Gamma_s\})$ we define:

$X \subset \Omega$ is an R-clique if its elements have only relations Γ_k with $k \in R$, that is, if $\langle \underline{x}, A_k \underline{x} \rangle = 0$ for $r < k \leq s$.

$Y \subset \Omega$ is an R-code if its elements have no relations Γ_k with $k \in R$, that is if $\langle \underline{y}, A_k \underline{y} \rangle = 0$ for $1 \leq k \leq r$.

3.8.1. Theorem. For an R-clique X and an R-code Y we have

$$|X| \cdot |Y| \leq |\Omega|$$

If equality holds, then $|X \cap Y| = 1$.

Proof. $n|X| \cdot |Y| = n \langle \underline{x}, \underline{x} \rangle \langle \underline{y}, \underline{y} \rangle =$

$n \sum_{k} \langle \underline{x}, A_k \underline{x} \rangle \langle \underline{y}, A_k \underline{y} \rangle / v_k = n \langle D(\underline{x},\underline{x})\underline{y}, \underline{y} \rangle =$

$n^2 \sum_{i} \langle \underline{x}, E_i \underline{x} \rangle \langle \underline{y}, E_i \underline{y} \rangle / \mu_i \geq n^2 \langle \underline{x}, E_0 \underline{x} \rangle \langle \underline{y}, E_0 \underline{y} \rangle = \langle \underline{x}, \underline{j} \rangle^2 \langle \underline{y}, \underline{j} \rangle^2 =$

$|X|^2 |Y|^2$, hence

$$|X| \cdot |Y| \leq n = |\Omega|$$

(note that $\langle \underline{x}, E_i \underline{z} \rangle \geq 0$ and $E_0 \underline{z} = \frac{1}{n} \langle \underline{z}, \underline{j} \rangle \underline{j}$ for all $\underline{z}$).

If equality holds, then $|X| \cdot |Y| = n$, and we see above that

$$\sum_{i=0}^{s} \langle \underline{x}, E_i \underline{x} \rangle \langle \underline{y}, E_i \underline{y} \rangle / \mu_i = \langle \underline{x}, E_0 \underline{x} \rangle \langle \underline{y}, E_0 \underline{y} \rangle .$$

Hence $$\sum_{i=1}^{s} \langle \underline{x}, E_i \underline{x} \rangle \langle \underline{y}, E_i \underline{y} \rangle = 0.$$

This yields

$$E_i \underline{x} = 0 \text{ or } E_i \underline{y} = 0, \qquad \text{for } i = 1,2,\ldots, s$$

and therefore

$$\langle \underline{x}, E_i \underline{y} \rangle = \langle E_i \underline{x}, E_i \underline{y} \rangle = 0 \qquad \text{for } i = 1,2,\ldots s.$$

Then (note that $\sum_{i=0}^{s} E_i = I$)

$$|X \cap Y| = \langle \underline{x}, \underline{y} \rangle = \langle \underline{x}, I\underline{y} \rangle = \sum_{i=0}^{s} \langle \underline{x}, E_i\underline{y} \rangle = \langle \underline{x}, E_0\underline{y} \rangle$$
$$= \frac{1}{n} \langle \underline{x}, \langle \underline{y}, \underline{j} \rangle \underline{j} \rangle = \frac{1}{n} \langle \underline{x}, \underline{j} \rangle \langle \underline{y}, \underline{j} \rangle = \frac{1}{n} |X| \cdot |Y| = 1. \qquad \square$$

Dually, $X \subset \Omega$ is an R-design if $\langle \underline{x}, E_i\underline{x} \rangle = 0$, for $i \in R$, that is

if $E_i\underline{x} = 0$ for $i \in R$, that is,

if $\sum_{k=0}^{s} a_k q_{ki} = 0$, for $i \in R$.

3.8.2. Example. In $J(v,k)$ an R-design translates into a r-(v,k,λ) design.

3.8.3. Theorem. $|X| \cdot |Y| \geq |\Omega|$, for an R-design X and an (S\R)-design Y.

Proof. $|X|^2 \cdot |Y|^2 = n^2 \langle \underline{x}, E_0\underline{x} \rangle \langle \underline{y}, E_0\underline{y} \rangle = n^2 \sum_{i=0}^{s} \langle \underline{x}, E_i\underline{x} \rangle \langle \underline{y}, E_i\underline{y} \rangle / \mu_i$
$= n \sum_{k=0}^{s} \langle \underline{x}, A_k\underline{x} \rangle \langle \underline{y}, A_k\underline{y} \rangle / v_k \geq n \langle \underline{x}, \underline{x} \rangle \langle \underline{y}, \underline{y} \rangle = n|X| \cdot |Y|$,
which proves the assertion. $\square$

The vectors $\underline{x}, \underline{y} \in R\Omega$ are called design-orthogonal if
$\langle \underline{x}, E_i\underline{x} \rangle \langle \underline{y}, E_i\underline{y} \rangle = 0$ for $i = 1,2,\ldots, s$.
If so then $\langle \underline{x}, E_i\underline{y} \rangle = 0$ for $i = 1,\ldots, s$ (see the proof of theorem 3.8.1.) Hence

$$D(\underline{x},\underline{y}) = \langle \underline{x}, E_0\underline{y} \rangle nE_0 = \frac{1}{n} \langle \underline{x}, \underline{j} \rangle \langle \underline{y}, \underline{j} \rangle J.$$

Therefore , for $k = 0, 1,\ldots, s$ we have

$$\frac{1}{v_k} \langle \underline{x}, A_k\underline{y} \rangle = \sum_{i=0}^{s} \frac{p_{ik}}{v_k} \langle \underline{x}, E_i\underline{y} \rangle = \langle \underline{x}, E_0\underline{y} \rangle = \frac{1}{n} \langle \underline{x}, \underline{j} \rangle \langle \underline{y}, \underline{j} \rangle =$$
$$\frac{1}{v_0} \langle \underline{x}, A_0\underline{y} \rangle = \langle \underline{x}, \underline{y} \rangle$$ and this proves

3.8.4. Theorem. If $\underline{x}$ and $\underline{y}$ are design-orthogonal, then

$$D(\underline{x},\underline{y}) = \langle \underline{x}, \underline{y} \rangle J$$

Appendix 3.1. Minimal idempotents.

A.3.1.1. Definition. Let F denote a commutative field. An algebra over F is a set A on which an addition, multiplication and scalar multiplication is defined, such that

(i) A is a ring with unit element e.

(ii) A is a vectorspace over F of finite dimension.

(iii) $(\lambda a)b = a(\lambda b) = \lambda(ab)$, $1.a = a$, for all $a,b \in A$, $\lambda \in F$ (1 is the unit element of F).

In this paragraph we will also assume that the ring multiplication is commutative and that

$$a^2 = 0 \Rightarrow a = 0 \qquad \text{for all } a \in A .$$

For a more general treatment of the theory of associative algebras see [25], Ch. V.

A.3.1.2. Examples.

1) $A = C$, $F = R$.

2) In the theory of the cyclic codes, the algebra $A = F[x]/(x^n-1)$, with $F = GF(q)$, $(q,n) = 1$.

3) The Bose-Mesner algebra of an association scheme.

We will now investigate the structure of an algebra A.
First we recall the following definition:

A.3.1.3. Definition. An ideal B of A is a subring of A, such that $ab \in B$ for all $a \in A$ and $b \in B$.
An ideal $B \neq \{0\}$ of A is called minimal if for all ideals B' of A with $B' \subset B$ the following holds:

$$B' = \{0\} \qquad \text{or} \qquad B' = B$$

(0 is the unit element of the additive group of A).

A.3.1.4. Theorem. An ideal B of A is a subspace of A.

Proof. Clearly, $a + b \in B$ for all $a,b \in B$. Also, if $\lambda \in F$ and $b \in B$, then $\lambda b = \lambda(eb) = (\lambda e)b \in B$.

□

A.3.1.5. Theorem. Let M_1 and M_2 denote distinct minimal ideals of A.
Then $M_1M_2 = \{0\}$ $(M_1M_2 := \{ \sum_i m_1^{(i)}m_2^{(i)} \mid m_1^{(i)} \in M_1 , m_2^{(i)} \in M_2 \})$

Proof. Clearly, M_1M_2 is an ideal of A and $M_1M_2 \subset (M_1 \cap M_2)$.

Also $(M_1 \cap M_2) \subset M_1$ and $(M_1 \cap M_2) \neq M_1$.
(for $M_1 \neq M_2$ and M_1, M_2 are minimal).
Hence

$$M_1M_2 \subset M_1 \quad \text{and} \quad M_1M_2 \neq M_1.$$

Because

M_1 is minimal, this yields $M_1M_2 = \{0\}$.

□

A.3.1.6. Theorem. Let $M_0, M_1, \ldots, M_s$ denote distinct minimal ideals of A.
Then the ideal $M := M_0 + M_1 + \ldots + M_s$ is a direct sum.

Proof. If $0 = m_0 + \ldots + m_s$ for $m_i \in M_i$, $i = 0,\ldots,s$, then
with theorem A.3.1.5. we see that

$$0 = 0 \cdot m_i = m_i^2 \quad \text{for all } i = 0,\ldots,s.$$

Therefore $m_i = 0$ for all $i = 0,\ldots, s$.

Hence $M = M_0 \oplus M_1 \oplus \ldots \oplus M_s$. □

Theorem A.3.1.6. implies that there is only a finite number of minimal ideals in A (note that A has finite dimension).
Let $M_0, M_1, \ldots, M_s$ denote the minimal ideals of A Then:

A.3.1.7. Theorem. If $M = M_0 \oplus M_1 \oplus \ldots \oplus M_s$, then $M = A$.

Proof. Select an $m_i \in M_i \setminus \{0\}$ for all $i = 0,1,\ldots,s$ and let
$m := m_0 + m_1 + \ldots + m_s$.
We define the linear mapping $\phi_m : A \to M$ by

$$\phi_m(a) := ma \quad , \quad \text{for all } a \in A .$$

Assume that $A \neq M$.
Then $N := \{ a \in A \mid \phi_m(a) = 0 \} \neq \{0\}$. Because N is an ideal of A (this is easy to see), we can find a minimal ideal M_i of A such that $M_i \subset N$. But then $0 = \phi_m(m_i) = m_i^2$ and therefore $m_i = 0$. This is impossible hence $A = M$.

□

So $A = M_0 \oplus M_1 \oplus \ldots\ldots \oplus M_s$ and we can write

$$e = e_0 + e_1 + \ldots + e_s , \qquad e_i \in M_i \qquad i = 0,1,\ldots,s.$$

A.3.1.8. Theorem. (i) The e_i's are idempotents ($e_i^2 = e_i$, i= 0,1,...,s) and are called the minimal idempotents of A. Also $e_i e_j = 0$ if $i \neq j$.

(ii) If $a \in A$, then $a = a_0 + a_1 + \ldots + a_s$ where $a_i = ae_i$ (i + 0,1,...,s).

(iii) M_i is a field with unit element e_i (i = 0,1,...,s).

(iv) Let B be an ideal of A. Then B is the sum of a number of M_i's and B contains a unique idempotent that generates the ideal B. Also every idempotent of A is the sum of a number of e_i's.

Proof. Evident, with preceding theorems. □

A.3.1.9. Theorem. The dimension of M_i equals 1, for all i = 0,1,...,s , iff for all $a \in A$: A is the sum of the eigenspaces of the linear mapping $\phi_a : A \to A$ defined by

$$\phi_a(x) := ax , \quad \text{for all } x \in A .$$

Proof.

1) $\Leftarrow$ Let $i \in \{0,1,\ldots,s\}$ and $m_i \in M_i$.
Clearly an eigenspace of ϕ_{m_i} is an ideal of A. If $\varepsilon_1,\ldots,\varepsilon_t$ are the eigenspaces of ϕ_{m_i} for the eigenvalues $\lambda_1,\ldots,\lambda_t$, and $A = \varepsilon_1 \oplus \ldots \oplus \varepsilon_t$, then

$$\varepsilon_1 \oplus \ldots\ldots \oplus \varepsilon_t = M_0 \oplus M_1 \oplus \ldots\ldots \oplus M_s .$$

With theorem A.3.1.8 (iv) we see that there must be a ε_j such that $M_i \subset \varepsilon_j$.
Now $m_i = m_i e = m_i e_i = \phi_{m_i}(e_i) = \lambda_j e_i$.
Hence M_i has dimension 1 for all i= 0,1,...,s.

2) $\Rightarrow$ Let $a \in A$. Thus $a = \lambda_0 e_0 + \ldots + \lambda_s e_s$ and therefore $M_0,\ldots,M_s$ are the eigenspaces of ϕ_a. Hence A is the sum of the eigenspaces of the mapping ϕ_a.

□

We now return to the association scheme case, so let $\mathcal{A}$ be the Bose-Mesner algebra of an association scheme.
Consider again the linear mapping $\phi_a: A \to A$ defined by

$$\phi_A(X) := AX \quad , \quad \text{for all } X \in A \qquad (A \in A).$$

Then the mapping $\phi : A \to \phi_A := \{\phi_A \mid A \in A\}$ defined by

$$\phi(A) := \phi_A \quad , \quad \text{for all } A \in A, \text{ is an algebra isomorphism.}$$

Therefore, A and ϕ_A $(A \in A)$ have the same minimal polynomial (ψ_0 is the minimal polynomial of A if $\psi_0 \neq 0$, $\psi_0(A) = 0$, ψ_0 is monic, and if $\psi \neq 0$ and $\psi(A) = 0$, then degree$(\psi) \geq$ degree(ψ_0)).
Without proof we state the following theorem:

A.3.1.10. Theorem. Let M be a n x n matrix and $\lambda_1,\ldots,\lambda_p$ be distinct reals. Then:

M is diagonalizable with distinct eigenvalues $\lambda_1,\ldots,\lambda_p$ iff the minimal polynomial of M is

$$\psi_o(X) := \prod_{i=1}^{p}(x-\lambda_i).$$

A is symmetric for all $A \in A$, and therefore diagonalizable.
Then theorem A.3.1.10. and the fact that A and ϕ_A have the same minimal polynomial yield:
ϕ_A is diagonalizable for all $A \in A$, and therefore A is the sum of the eigenspaces of ϕ_A, for all $A \in A$. Therefore, with theorem A.3.1.9. we see that the minimal ideals of A have dimension 1. Hence the minimal idempotents of A constitute a basis of A (theorem A.3.1.8.(ii)).

Appendix 3.2. The A-module.

Let A be a commutative algebra over F, as described in appendix 3.1. with minimal ideals $M_0, M_1,\ldots, M_s$ and minimal idempotents $e_0, e_1,\ldots, e_s$; $e_i \in M_i$, $i = 0,1,\ldots,s$.

A.3.2.1. Definition. A vectorspace V over F of finite dimension is called A-module if there exists a mapping $\phi: A \times V \to V$, $\phi(a,v) = av$, such that for all $a_1, a_2 \in A$, $v \in V$ and $\lambda \in F$ the following holds:

(1) $(a_1 + a_2)v = a_1v + a_2v$

(2) $(a_1a_2)v = a_1(a_2v)$

(3) $ev = v$

(4) $a(v_1 + v_2) = av_1 + av_2$

(5) $a(\lambda v) = (\lambda a)v = \lambda(av)$.

Properties (4) and (5) imply that the mapping $f_a := \bigvee_{v \in V} av$ is a linear mapping of V into V ($a \in A$). The properties (1), (2), (5) say that the mapping $a \to f_a$ ($a \in A$) is a homomorphism of algebras of A into the algebra consisting of all linear maps of V into V.

A.3.2.2. Examples.

(1) A is a A-module.

(2) Every ideal of A is a A-module.

(3) The standard A-module V of an association scheme as described in paragraph 3.7. is a A-module.

A.3.2.3. Theorem. Let V be a A-module and define $V_i := e_iV$ for all $i = 0,\ldots,s$. Then

$$V = V_0 \oplus V_1 \oplus \ldots \oplus V_s.$$

Proof.

(1) Let $v \in V$. Then $v = ev = (e_0 + \ldots + e_s)v = e_0v + \ldots + e_sv$ and

$$e_iv \in V_i, \quad i = 0,1,\ldots,s.$$

(2) Assume that $0 = v_0 + v_1 + \ldots + v_s$ for certain $v_i \in V_i$. Let $i \in \{0,1,\ldots,s\}$. Then $v_i = e_iw$ for a certain $w \in V$. Hence, $e_iv_i = e_i^2w = e_iw = v_i$ and

$$e_jv_i = e_je_iw = 0 \cdot w = 0 \quad \text{for } j \neq i.$$

Therefore, for all $i = 0,1,\ldots,s$

$$0 = e_i \cdot 0 = e_i(v_0 + v_1 + \ldots + v_s) = e_iv_i = v_i.$$

Hence $V = V_0 \oplus V_1 \oplus \ldots \oplus V_s$.

If $\dim M_i = 1$ for a certain $i \in \{0,1,\ldots,s\}$, then V_i is an eigenspace of f_a for all $a \in A$, because if $a \in A$ and $v_i \in V_i$, then

$$f_a(v_i) = av_i = ae_iv_i = \lambda v_i \quad , \quad \lambda \in F.$$

Now consider the association scheme case with the standard A-module V described in paragraph 3.7.. In appendix 3.1. we have seen that all the M_i's have dimension 1, and therefore we see that $V_0,\ldots,V_s$ are the simultaneous eigenspaces of the matrices of the Bose-Mesner algebra A of the association scheme. If $\mu_i := \dim(V_i)$ $i = 0,1,\ldots,s$, we see that $\mu_i = \dim(V_i) = \dim(E_iV) = \operatorname{rank}(E_i) = \operatorname{trace}(E_i) = \operatorname{trace}(E_i \circ I) =$

$$\operatorname{trace}(\tfrac{1}{n} q_{oi} I) = q_{oi}.$$

Chapter 4.

Pseudo-cyclic Association Schemes.

General references are [3] , [22] , [24] , [25] .

4.1. A theorem.

Let $(\Omega, \{ id, \Gamma_1, \ldots\ldots, \Gamma_s \})$ denote an s-class association scheme on $n = |\Omega|$ points, with valencies $v_0, v_1, \ldots, v_s$, and multiplicities $\mu_0, \ldots, \mu_s$, and intersection numbers a_{ij}^k $(i,j,k = 0, \ldots, s)$ and character table $P = [p_{ik}]$ (see chapter 3).

4.1.1. Definition. The association scheme $(\Omega, \{ id, \Gamma_1, \ldots., \Gamma_s \})$ is called pseudo-cyclic if $\mu_1 = \mu_2 = \ldots = \mu_s$.

In chapter 3 we have seen that a strongly regular graph is a 2-class association scheme. For example, the pentagon graph P(5) is strongly regular with parameters $n = 5$, $k = 2$, $\lambda = 0$, $\mu = 1$ and spectrum

$$(2^1, \ \tfrac{1}{2}(-1-\sqrt{5})^2, \ \tfrac{1}{2}(-1+\sqrt{5})^2).$$

Therefore P(5) is a pseudo-cyclic association scheme, for $\mu_1 = \mu_2 = 2$. Note also that $v_1 = v_2 = 2$.
Moreover, all conference graphs are pseudo-cyclic 2-class association schemes with $v_1 = v_2$, since the parameters of a conference graph P(q) are $(q = p^r$, p prime and $q \equiv 1 \bmod 4)$

$$n = q \ , \ k = \tfrac{1}{2}(q-1) \ , \ \lambda = \tfrac{1}{4}(q-5) \ , \ \mu = \tfrac{1}{4}(q-1) \ .$$

The spectrum of P(q) is

$$([\tfrac{1}{2}(q-1)]^1, [\tfrac{1}{2}(-1-\sqrt{q})]^{\frac{1}{2}(q-1)}, [\tfrac{1}{2}(-1+\sqrt{q})]^{\frac{1}{2}(q-1)}).$$

Therefore $\mu_1 = \tfrac{1}{2}(q-1) = \mu_2$ and $v_1 = k = \tfrac{1}{2}(q-1) = n-1-k = v_2$.

The fact that a certain association scheme has all valencies equal does not always imply that it is pseudo-cyclic. For example the triangular graph T(7) has parameters

$$n = 21, \ k = 10, \ \lambda = 5, \ \mu = 4 \quad \text{and spectrum } (10^1, (-2)^{14}, 3^6) \ .$$

Hence, $v_1 = v_2 = 10$ and $\mu_1 = 14 \neq \mu_2 = 6$.

4.1.2. Theorem. The association scheme $(\Omega, \{ id, \Gamma_1, \ldots, \Gamma_s \})$ is pseudo-cyclic if and only if there exists an integer t such that

1) $v_1 = v_2 = \ldots = v_s = t$.

2) $\sum_{i=0}^{s} a_{ij}^{i} = t - 1$ for all $j = 1,2,\ldots, s$.

Proof. First, consider the following: we know that

(1) $p_{zi}p_{zj} = \sum_{k=0}^{s} a_{ij}^{k} p_{zk}$ $(i,j,z = 0,1,\ldots,s.)$

Also if $Q = [q_{ij}]$, then $PQ = QP = nI$, and this yields

(2) $\sum_{k=0}^{s} p_{ik}q_{kj} = \sum_{k=0}^{s} p_{ki}q_{jk} = n\delta_{ij}$ $(i,j = 0,1,\ldots, s)$

Furthermore, $p_{ok} = v_k$, $q_{ok} = \mu_k$, $p_{ko} = 1$ (because $p_{ko}E_k = A_0E_k = E_k$) and $q_{ko} = 1$ (because $(1/n)q_{ko}A_k = E_0 \circ A_k = (1/n)A_k$) for all $k = 0, 1,\ldots, s$.

With (2) this yields

(3) $\sum_{k=0}^{s} v_k = n$ and $\sum_{k=0}^{s} p_{ik} = 0$ for $i = 1,2,\ldots,s$

(4) $\sum_{k=0}^{s} \mu_k = n$ and $\sum_{k=0}^{s} q_{jk} = 0$ for $j = 1,2,\ldots,s$

(see chapter 3).

If we multiply (1) with q_{iz} and take the sum over i and z, then we get:

$$\sum_{i=0}^{s}\sum_{z=0}^{s} p_{zi}p_{zj}q_{iz} = \sum_{i=0}^{s}\sum_{z=0}^{s}\sum_{k=0}^{s} a_{ij}^{k}p_{zk}q_{iz}.$$

With (2) this yields

$$\sum_{z=0}^{s} n\, p_{zj} = \sum_{i=0}^{s}\sum_{k=0}^{s} n\, \delta_{ki}\, a_{ij}^{k}, \text{ and therefore}$$

(5) $\sum_{z=0}^{s} p_{zj} = \sum_{i=0}^{s} a_{ij}^{i}$ for all $j = 0,1,\ldots,s$.

$\Delta_\mu P = Q^T \Delta_v$ (see chapter 3) yields $\mu_z p_{zj} = v_j q_{jz}$, or

$$\frac{p_{zj}}{v_j} = \frac{q_{jz}}{\mu_z} \qquad j,z = 0,1,\ldots,s.$$

If we substitute this in (5), we obtain

$$(6)\quad \sum_{z=0}^{s} \frac{q_{jz}}{\mu_z} = \frac{1}{v_j} \sum_{i=0}^{s} a_{ij}^{i} \quad , \text{ for all } j = 0,1,\ldots,s.$$

Now we can prove the theorem.

(i) $\Longrightarrow$ If $(\Omega, \{id, \Gamma_1, \ldots, \Gamma_s\})$ is pseudo-cyclic, then

$$\mu_0 = 1,\ \mu_1 = \mu_1 = \ldots = \mu_s = t \quad , \text{ for a certain integer } t.$$

With (6) we see that

$$\sum_{i=0}^{s} a_{ij}^{i} = v_j \sum_{z=0}^{s} \frac{q_{jz}}{\mu_z} = v_j\left(1 + \frac{1}{t} \sum_{z=1}^{s} q_{jz}\right) .$$

If $j = 1,2,\ldots,s$ then (3) yields $\sum q_{jz} = -q_{jo} = -1$

and therefore

$$(7)\qquad \sum_{i=0}^{s} a_{ij}^{i} = v_j\left(1 - \frac{1}{t}\right) = v_j \frac{t-1}{t} \quad , \quad j = 1,2,\ldots,s.$$

This yields $t \mid v_j$ and therefore $t \leq v_j$ for $j = 1,2,\ldots,s.$

Also

$$st + 1 = \sum_{j=0}^{s} \mu_j = \sum_{j=0}^{s} v_j = 1 + \sum_{j=1}^{s} v_j.$$

Hence

$$v_1 = v_2 = \ldots = v_s = t.$$

If we substitute this in (7) we obtain

$$\sum_{i=0}^{s} a_{ij}^{i} = t - 1, \qquad \text{for all } j = 1,2,\ldots,s.$$

(ii) $\Longleftarrow$ Assume that $v_1 = v_2 = \ldots = v_s = t$

$$\text{and} \quad \sum_{i=0}^{s} a_{ij}^{i} = t - 1 \qquad \text{for } j = 1,2,\ldots,s.$$

For a certain integer t. Then (5) yields

$$(8)\quad \sum_{z=0}^{s} p_{zj} = \sum_{i=0}^{s} a_{ij}^{i} = t - 1 \qquad (j = 1,2,\ldots,s)$$

Consider

$$(1, t, t, \ldots, t)\, P = (1, t, t, \ldots, t) \begin{bmatrix} 1 & v_1 & v_2 & \ldots & v_s \\ 1 & p_{11} & p_{12} & \ldots & p_{1s} \\ 1 & p_{21} & p_{22} & \ldots & p_{2s} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & p_{s1} & p_{s2} & \ldots & p_{ss} \end{bmatrix}$$

This equals n (1,0,0,...,0) for:

$$1 + st = \sum_{i=0}^{s} v_i = n \qquad ((3)) \quad \text{and}$$

$$v_j + t \sum_{z=1}^{s} p_{zj} = v_j + t(t-1-v_j) = 0 \qquad ((8)).$$

Q is the unique matrix such that QP = nI. Hence

(1,t,t,....,t) is the first row of Q. The first row of Q is also $(\mu_0,\ldots,\mu_s)$. Hence

$$\mu_1 = \mu_2 = \ldots = \mu_s = t.$$

□

Remark. For T(7) : $\sum_{i=0}^{2} a_{i1}^{i} = 11$ and $\sum_{i=0}^{2} a_{i2}^{i} = 7.$

For P(q) : $\sum_{i=0}^{2} a_{i1}^{i} = \sum_{i=0}^{2} a_{i2}^{i} = \frac{1}{2}(q-3).$

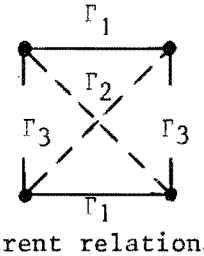
4.2. Pseudo-cyclic association schemes with 3 classes, on 28 vertices.

In this section we discuss a method to construct a 3-class association scheme out of an existing one. Then we apply this method to the so called Mathon-scheme. Finally, it is pointed out that this pseudo-cyclic association scheme, together with Hollman's scheme, the one formed out of the Mathon-scheme by the mentioned construction, are the only pseudo-cyclic 3-class association schemes on 28 vertices.

4.2.1. A Construction.

Consider a 3-class association scheme $(X, \{I = \Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3\})$ with a subset Y, consisting of four points a, b, c, d, such that

(i) For all $x \in Y = \{a,b,c,d\}$ the relations (x,a), (x,b), (x,c) and (x,d) are distinct:



(ii) All $x \in X\backslash Y$ have only two different relations to the points of Y, say Γ_i and Γ_j and each relation appears exactly twice.

For instance $(x,a),(x,b) \in \Gamma_i$ and $(x,c),(x,d) \in \Gamma_j$, x is said to be of type $\{i,j\}$.

From (X,Γ) a new association scheme (X,Δ), with the same intersection numbers can be constructed as following.

(i) For $(x,y) \in (Y \times Y) \cup (X\backslash Y \times X\backslash Y)$ we define
$(x,y) \in \Delta_i \Leftrightarrow (x,y) \in \Gamma_i$.

(ii) For $(x,y) \in (X\backslash Y) \times Y$ and x of type $\{i,j\}$ we define
$(x,y) \in \Delta_i \Leftrightarrow (x,y) \in \Gamma_j$.

These definitions provide a new association scheme.

Proof. We will show that for $(x,y) \in \Delta_k$

$$|\Delta_i(x) \cap \Delta_j(y)| = a_{ij}^k, \quad \text{where } \Delta_i(x) := \{z \mid (x,z) \in \Delta_i\}$$

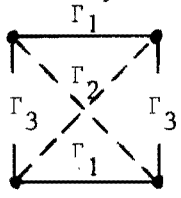
Furthermore $\Delta_i^*(x) := \Delta_i(x) \cap Y$ and $\Delta_i^{**}(x) := \Delta_i(x)\backslash Y$.

The proof is divided into three cases.

Case 1. Let $x \in Y$ and $y \in Y$.

$$\begin{aligned}
\text{Then } |\Delta_i(x) \cap \Delta_j(y)| &= |\Delta_i^*(x) \cap \Delta_j^*(y)| + |\Delta_i^{**}(x) \cap \Delta_j^{**}(y)| = \\
&= |\Gamma_i^*(x) \cap \Gamma_j^*(y)| + |\Gamma_j^{**}(x) \cap \Gamma_i^{**}(y)| = \quad (+) \\
&= |\Gamma_j^*(x) \cap \Gamma_i^*(y)| + |\Gamma_j^{**}(x) \cap \Gamma_i^{**}(y)| = \\
&= |\Gamma_j(x) \cap \Gamma_i(y)| = a_{ji}^k = a_{ij}^k.
\end{aligned}$$

Remark (+) can easily be seen by the inspection of



Case 2. Let $x \in X\backslash Y$ and $y \in X\backslash Y$.

$$\begin{aligned}
\text{Then } |\Delta_i(x) \cap \Delta_j(y)| &= |\Delta_i^*(x) \cap \Delta_j^*(y)| + |\Delta_i^{**}(x) \cap \Delta_j^{**}(y)| = \\
&= |\Gamma_i^*(x) \cap \Gamma_j^*(y)| + |\Gamma_i^{**}(x) \cap \Gamma_j^{**}(y)| = \\
&= |\Gamma_i(x) \cap \Gamma_j(y)| = a_{ij}^k.
\end{aligned}$$

Case 3. Let $x \in X \setminus Y$ and $y \in Y$.

Without loss of generality we can assume that $y = a$. Let $\{k,l\}$ be the type of x and assume $i \notin \{k,l\}$.

Define

$$V := \{z \in \Gamma_i(x) \mid \{z\} \times Y \cap \Gamma_j\} \neq \emptyset$$
$$W := \{z \in V \mid (z,a) \notin \Gamma_j\}.$$

Since $V \cap Y = \emptyset$ $(i \notin \{k,l\})$ and $(x,a) \in \Gamma_1$ the following holds

$$\Delta_i(x) \cap \Delta_j(a) = W \qquad \text{and} \qquad |W| = |V| - a_{ij}^{1}.$$

Now define $S := \{(z,u) \in \Gamma_i(x) \times Y \mid z \in \Gamma_j(u)\}$, $N := |S|$.

If $(x,u) \in \Gamma_1$ then the number of $z \in S$ is a_{ij}^{1}.

If $(x,u) \in \Gamma_k$ then the number of $z \in S$ is a_{ij}^{k}.

This gives us $N = 2a_{ij}^{1} + 2a_{ij}^{k}$.

If $z \in V$ then two $y \in Y$ satisfy $(z,y) \in \Gamma_j$.

So $N = 2 \cdot |V|$.

This gives us $2a_{ij}^{1} + 2a_{ij}^{k} = 2 \cdot |V| = 2 \cdot |W| + 2a_{ij}^{1}$.

or $|W| = |\Delta_i(x) \cap \Delta_j(y)| = a_{ij}^{k}$.

The case $i \in \{k,l\}$ is proved analogously. □

The scheme of Mathon.

If a group G has a generously transitive action on a set Ω, i.e. $\forall_{\alpha,\beta \in \Omega} \exists_{g \in G} [\alpha^g = \beta,\ \beta^g = \alpha]$ then the orbits of G on $\Omega \times \Omega$, that is the sets $\{(\alpha^g, \beta^g) \mid g \in G\}$, form an association scheme (see 3.2.4.). Now let O be a hyperoval in $P = PG(2,8)$. The 73 lines of P are divided in $\binom{10}{2} = 45$ secants and 28 passants. Consider the group of linear transformations on $V = (F_8^3)$, $Gl(3,8)$. The subgroup of $GL(3,8)$ that maps the hyperoval on itself.

acts generously transitive on Ω, the set of passants. The so constructed scheme has been described first by Mathon. Hollman has shown that we can construct another association scheme out of Mathon's scheme with the method described at the beginning of this section.
More precisely,if we take the hyperoval

$$O = \{(1,0,0),(0,1,0),(\xi,\xi^2,1) \mid \xi \in GF(8)\} ,$$

then

$$Y = \{\infty, O_1, O_2, O_3\} ,$$

where $\quad \infty = (1,\alpha^3,\alpha^3)^\perp , \quad O_1 = (1,\alpha^5,\alpha^5)^\perp$

$$O_2 = (1,\alpha^6,\alpha^6)^\perp , \quad O_3 = (1,1,1)^\perp$$

satisfies the conditions (i) and (ii) of 4.2.1. (α is primitive in GF(8) with $\alpha^3 = \alpha+1$).
Note that the four passants meet in one point viz. (0,1,1).

Pseudo-cyclic 3-class association schemes.

In pseudo-cyclic association schemes all non-trivial multiplicities are the same. For a 3-class scheme that means

$$|\Omega| = 3t+1 \quad \text{and} \quad \mu_1 = \mu_2 = \mu_3 = t.$$

This is equivalent to

$$v_1 = v_2 = v_3 = t \quad \text{and} \quad \sum_{k=0}^{3} a_{ik}^{k} = t-1.$$

To find the intersection numbers the following lemmas are needed :

4.2.2. Lemma. $\quad \sum_{t=0}^{3} a_{1i}^{t} a_{tj}^{m} = \sum_{k=0}^{3} a_{1k}^{m} a_{ji}^{k}$, for all i,j,1,m.

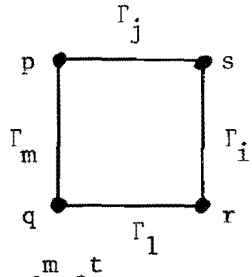
Proof 1. Since the Bose-Mesner algebra of an association scheme is commutative and associative:

$$(A_iA_j)A_1 = (A_jA_i)A_1 = A_j(A_iA_1)$$

so

$$\begin{aligned}(a_iA_j)A_1oA_m &= (\sum_k a_{ij}^k A_k)A_1oA_m = (\sum_k a_{ij}^k A_kA_1)oA_m \\ &= (\sum_k a_{ij}^k (\sum_s a_{k1}^s A_s))oA_m \\ &= \Sigma_k \sum_s a_{ij}^k a_{k1}^s (A_soA_m) \\ &= (\sum_k a_{ij}^k a_{k1}^m)A_m\end{aligned}$$

and analogously $A_j(A_iA_l)oA_m = (\sum_t a^t_{li}a^m_{tj})A_m$



Proof 2. Take p and q such that $(p,q) \in \Gamma_m$, and count the number of squares pqrs with $(q,r) \in \Gamma_l$, $(r,s) \in \Gamma_i$ and $(s,p) \in \Gamma_j$.
The number of s is $\sum_t a^m_{tj}$. If $(q,s) \in \Gamma_t$ there are a^t_{il} r's with $(s,r) \in \Gamma_k$.
So the total number of different squares is $\sum_t a^m_{tj}a^t_{il}$.

The number of r is $\sum_k a^m_{lk}$. If $(p,q) \in \Gamma_k$ then the number of s with $(s,r) \in \Gamma_i$ is a^k_{ij}.
So the number of squares is also $\sum_k a^m_{lk}a^k_{ij}$,
That gives us $\sum_{t=0}^{3} a^m_{tj}a^t_{il} = \sum_{k=0}^{3} a^m_{lk}a^k_{ij}$. □

4.2.3. Corollary. $a^j_{li} = a^l_{ji}$ for all $l,t > 0$.

Proof. Take $m = 0$ in 4.2.2. With $a^0_{ii} = t$ the result follows. □

4.2.4. Corollary. $\sum_k a^j_{kk} = t-1$, if $j > 0$.

Proof. Take $l = i = k$ in 4.2.3. then $a^j_{kk} = a^k_{jk}$.
So $t-1 = \sum_k a^k_{jk} = \sum_k a^j_{kk}$. □

4.2.5. Lemma. $\sum_{k=0}^{s} a^i_{jk} = v_j$, $\sum_{k=1}^{s} a^i_{ik} = v_i-1$, for all i and j.

Proof. Count the points that have relation j to a fixed point. □

4.2.6. Theorem. The intersection matrices are

$$\left[a^1_{ij}\right] = \begin{bmatrix} t-r-s-1 & s & r \\ s & r & t-r-s \\ r & t-r-s & s \end{bmatrix} \qquad \left[a^2_{ij}\right] = \begin{bmatrix} s & r & t-r-s \\ r & t-r-s-1 & s \\ t-r-s & s & r \end{bmatrix}$$

$$\left[a^3_{ij}\right] = \begin{bmatrix} r & t-r-s & s \\ t-r-s & s & r \\ s & r & t-r-s-1 \end{bmatrix}$$

Proof. Let $s := a^1_{12}$ and $r := a^1_{13}$.
From 4.2.5. we know $a^1_{11} = t-r-s-1$.
Since $[a^1_{ij}]$ is symmetric $a_{21} = s$ and $a^1_{31} = r$.
With 4.2.4.

$$a^1_{11} + a^1_{22} + a^1_{33} = t-1 = t-r-s-1 + a^1_{22} + a^1_{33}.$$

So $$a^1_{22} + a^1_{33} = r+s \qquad (*)$$

With 4.2.5. $$s + a^1_{22} + a^1_{33} = t \qquad (**)$$

$$r + a^1_{23} + a^1_{33} = t \qquad (***)$$

(*), (**), (***) lead to $a^1_{22} = r$, $a^1_{33} = s$ and
$a^1_{23} = a^1_{32} = t-r-s$.

The matrices $[a^2_{ij}]$ and $[a^3_{ij}]$ can be found from $[a^1_{ij}]$ with 4.2.3., 4.2.4. and 4.2.5.

□

4.2.7. Theorem. For r and s and t holds

$$1+2(r+s)-3(r-s)^2 = (1+3(r+s)-2t)^2.$$

Proof. Application of lemma 4.2.2. in the case 1 = i = 2, j = 1 gives

$$\sum_{t=0}^{s} a^t_{22} a^1_{t1} = \sum_{k=0}^{s} a^k_{12} a^k_{12}$$

So

$$r(t-r-s-1)+(t-r-s-1)s+sr = s^2+r^2+(t-r-s)^2 \quad \text{or}$$

$$1+2(r+s)-3(r-s)^2 = (1+3(r+s-2t)^2.$$

□

Equation 4.2.7. has integer solutions r, s, t iff

$L^2 + 27M^2 = 4V$ has integer solutions.

Here $L = 6t-2-9(r+s)$, $M = r-s$, $V = 3t+1$.

In the schemes on 28 vertices we have the unique solution
$V = 28$, $L = \pm 2$, $M = \pm 2$ or without loss of generality
$r = 4$, $s = 2$, $t = 9$.

Thus the intersection matrices in our case are uniquely determined viz.

$$\left[a^{1}_{ij}\right] = \begin{bmatrix} 2 & 2 & 4 \\ 2 & 4 & 3 \\ 4 & 3 & 2 \end{bmatrix} \qquad \left[a^{2}_{ij}\right] = \begin{bmatrix} 2 & 4 & 3 \\ 4 & 2 & 2 \\ 3 & 2 & 4 \end{bmatrix} \qquad \left[a^{3}_{ij}\right] = \begin{bmatrix} 4 & 2 & 3 \\ 2 & 2 & 4 \\ 3 & 4 & 2 \end{bmatrix}$$

The schemes of Mathon and Hollman are the only pseudo-cyclic 3-class association schemes on 28 vertices. This is partly the result from the uniqueness of the intersection numbers. Hollmann has shown that the two association schemes are the only ones with these intersection numbers by detailed examination of substructures of the scheme.

4.3. Pseudo-cyclic Association schemes from PSL(2,q), $q = 2^m$.

Let $V(2,q)$, $q = 2^m$, denote the vectorspace of dimension 2, over the Galois field F_q. The projective special linear group $PSL(2,q)$ is the group of the permutations of the projective points of $PG(1,q)$ (these are the lines through the origin of $V(2,q)$) induced by the linear maps of $V(2,q)$ into $V(2,q)$ with determinant 1.
We recall the following definitions and lemmas from group theory.

4.3.1. Definitions. Let G denote a transformation group of a set A.
G is called k-transitive on A if for all
$x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k \in A$,
$x_i \neq x_j$, $y_i \neq y_j$, $i,j = 1,2,\ldots,k$, $i \neq j$,
there is a $g \in G$ such that

$$g(x_i) = y_i \quad , \quad \text{for all } i = 1,2,\ldots,k.$$

If this g is unique, then G is called sharply k-transitive on A.
If $x_1, x_2, \ldots, x_m \in A$, then the stabilizer $G_{x_1,\ldots,x_m}$ of $x_1,\ldots, x_m$ is defined as

$$G_{x_1,\ldots,x_m} = \{g \in G \mid g(x_i) = x_i \ , \ i = 1,2,\ldots,m\}.$$

(Clearly, $G_{x_1,\ldots,x_m}$ is a subgroup of G).

4.3.2. Lemma. Let G be a finite group of permutations on a set A, T an orbit of G, $a \in T$ and G_a the stabilizer of a. Then

$$|G| = |G_a| \cdot |T| .$$

4.3.3. Lemma. Let G be a permutation group on a set A, $a \in A$. Then G is k-transitive on A iff G is transitive on A and G_a is (k-1)-transitive on $A \setminus \{a\}$.

4.3.4. Theorem. PSL(2,q) is sharply 3-transitive on the points of PG(1,q).

Proof. Let $G := PSL(2,q)$ and let Ω be the set of the points of PG(1,q).

1) Consider two elements x,y of $\Omega \setminus \{<(1,0)>, <(0,1)>\}$

Then $x = <(a,1)>$, $y = <(b,1)>$, $a,b \in F_q \setminus \{0\}$.

Consider the matrix

$$A = \begin{bmatrix} a^{-\frac{1}{2}}b^{\frac{1}{2}} & 0 \\ 0 & a^{\frac{1}{2}}b^{-\frac{1}{2}} \end{bmatrix}$$

Clearly, $A \in G_{<(1,0)>,<(0,1)>}$ and

$<(a,1)A> = <(a^{\frac{1}{2}}b^{\frac{1}{2}}, a^{\frac{1}{2}}b^{-\frac{1}{2}})> = <(b,1)>$.

Hence, $G_{<(1,0)>,<(0,1)>}$ is transitive on $\Omega \setminus \{<(0,1)>,<(1,0)>\}$

Moreover, $G_{<(1,0)>}$ is transitive on $\Omega \setminus \{<(1,0)>\}$ for,

if

$$B := \begin{bmatrix} a^{\frac{1}{2}} & 0 \\ a^{\frac{1}{2}} & a^{-\frac{1}{2}} \end{bmatrix}$$

then $B \in G_{<(1,0)>}$ and

$<(1,0)B> = <(a^{\frac{1}{2}}, a^{-\frac{1}{2}})> = <(a,1)>$, for all $a \in F_q \setminus \{0\}$.

With lemma 4.3.3. we see that $G_{<(1,0)>}$ is 2-transitive on $\Omega \setminus \{<(1,0)>\}$.

2) If

$$C = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

then $C \in G$ and $<(1,0)C> = <(0,1)>$, and therefore, G is transitive on Ω. Then with 2) and lemma 4.3.3. we see that G is 3-transitive on Ω.

3) It is easy to see that the matrices of G that fix $<(1,0)>$ and $<(0,1)>$ are of the form

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \quad , \; a \in F_q \setminus \{0\}.$$

Also $<(1,1)\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}> = <(a,a^{-1})> = <(a^2,1)> = <(1,1)>$ iff $a = 1$ (for $a^2 = 1 \Rightarrow a = 1$ in F_q , $q = 2^m$).

Hence, the only matrix of G that fixes $<(1,0)>$, $<(0,1)>$ and $<(1,1)>$ is I_{2x2}.

Now let $x_1, x_2, x_3 \in V(2,q)$, $y_1, y_2, y_3 \in V(2,q)$,
$x_i \neq x_j$, $y_i \neq y_j$ $i \neq j$,
then there are $A \in G$ and $B \in G$ such that

$$<x_1A> = <y_1B> = <(1,0)> \quad , \quad <x_2A> = <y_2B> = <(0,1)> \quad ,$$

$$<x_3A> = <y_3B> = <(1,1)> \qquad \text{(Because G is 3-transitive on } \Omega).$$

Hence, $<x_iAB^{-1}> = <y_i>$, $i = 1,2,3$.
If $<x_iD> = <y_i>$, $i = 1,2,3$, then $A^{-1}DB$ fixes $<(0,1)>$, $<(1,0)>$ and $<(1,1)>$ and therfore $A^{-1}DB = I$ or $D = AB^{-1}$. Hence, G is sharply 3-transitive on Ω.

□

We want to use PSL(2,q) to define a pseudo-cyclic association scheme. To do this, we consider another permutation group that is isomorphic with PSL(2,q).

Let V(3,q) , $q = 2^m$, denote the 3-dimensional vectorspace over F_q and let Q be the quadratic form $Q(x) = x_0^2 + x_1x_2$, $x = (x_0,x_1,x_2) \in V(3,q)$.

The bilinear form corresponding to Q is

$(x,y) := Q(x+y) - Q(x) - Q(y) = x_1y_2 - x_2y_1 = x_1y_2 + x_2y_1 \quad x,y \in V(3,q)$

Clearly, $R := <(1,0,0)>$ is the radical of (,) (in other words $((1,0,0),y) = 0$ for all $y \in V(3,q)$). Also, the q+1 projective points $<x>$ of PG(2,q) with $Q(x) = 0$ constitute an oval C in PG(2,q) and the projective lines through R are the tangents of C (hence, R is the nucleus of C).

The projective orthogonal group PO(3,q) is the group of the permutations of PG(2,q) induced by the linear transformations A of V(3,q) with $Q(x) = Q(xA)$, for all $x \in V(3,q)$ (hence, if $A \in PO(3,q)$, then $(x,y) = (xA, yA)$ holds for all $x,y \in V(3,q)$).
Let $N := \{\langle x\rangle \in PG(2,q) \mid Q(x) \neq 0\} \setminus \{R\}$, T the set of the tangents of C, S the set of the secants of C and E the set of the passants of C.
Clearly, $\langle(1,0,0)A\rangle = \langle(1,0,0)\rangle$ for all $A \in PO(3,q)$
$(((1,0,0)A,y) = ((1,0,0),yA^{-1}) = 0$ for all $y \in V(3,q))$,
and therefore $\{R\}$ is an orbit of PO(3,q) on the points of PG(2,q).
We shall see that PO(3,q) has 3 orbits on the points of PG(2,q), viz. $\{R\}$, C and N, and PO(3,q) has 3 orbits on the lines of PG(2,q) viz. T, S and E. But first, consider the following:
Let $A \in PO(3,q)$. Then A is a nonsingular 3 x 3 matrix such that $Q(x) = Q(xA)$ for all $x \in V(3,q)$. Because
$\langle(1,0,0)A\rangle = \langle(1,0,0)\rangle$, A is of the form

$$A = \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & b_{11} & b_{12} \\ a_2 & b_{21} & b_{22} \end{bmatrix} . \qquad Q(x) = Q(xA) \text{ yields}$$

$$x_0^2 + x_1x_2 = a_0^2x_0^2 + (a_1^2 + b_{11}b_{12})x_1^2 + (a_2^2 + b_{21}b_{22})x_2^2 + (b_{11}b_{22} + b_{21}b_{12})x_1x_2$$

for all $x \in V(3,q)$.
Hence,

$$a_0 = 1 \ , \ a_1 = (b_{11}b_{12})^{\frac{1}{2}}, \ a_2 = (b_{21}b_{22})^{\frac{1}{2}}, \quad \det(b_{ij}) = 1.$$

Apparently, the matrices of PO(3,q) are of the form

$$A = \begin{bmatrix} 1 & 0 & 0 \\ a_1 & b_{11} & b_{12} \\ a_2 & b_{21} & b_{22} \end{bmatrix} , \ a_i = (b_{i1}b_{i2})^{\frac{1}{2}}, \ i = 1,2 \ , \quad \det(bij) = 1.$$

Then, with the map $\phi : PO(3,q) \to PSL(2,q)$,

$$\phi\left(\begin{bmatrix} 1 & 0 & 0 \\ a_1 & b_{11} & b_{12} \\ a_2 & b_{21} & b_{22} \end{bmatrix}\right) := \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} ,$$

it is clear that the groups PO(3,q) and PSL(2,q) are isomorphic. Furthermore, the permutation representation of PO(3,q) on C is isomorphic with the permutation representation of PSL(2,q) on PG(1,q), for:

if $\Pi : C \to PG(1,q)$ is the map $\Pi(\langle(x_0,x_1,x_2)\rangle) := \langle(x_1,x_2)\rangle$, then $\langle(x_0,x_1,x_2)\rangle A\Pi = \langle(x_0,x_1,x_2)\rangle\Pi\phi(A)$.

With theorem 4.3.4. this yields

4.3.5. Theorem. PO(3,q) is sharply 3-transitive on the points of C, and therefore also on the lines of T (for, a $T \in T$ is of the form $R + \langle x\rangle$, $\langle x\rangle \in C$).

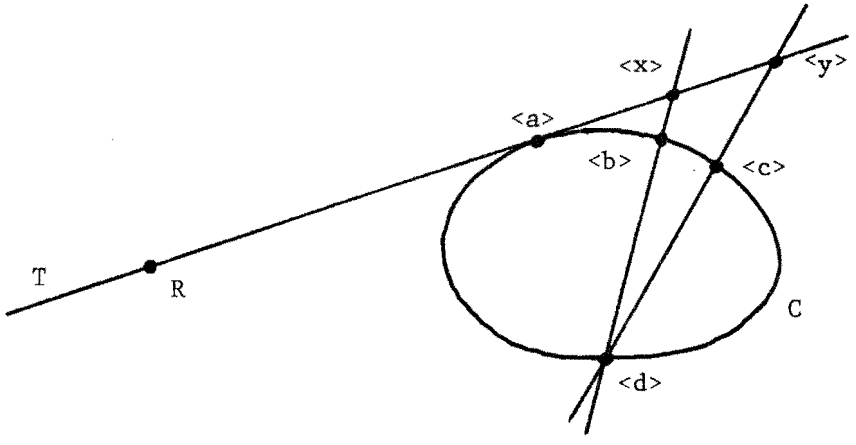
4.3.6. Theorem. The action of PO(3,q) on the points of PG(2,q) has 3 orbits, viz. {R}, C and N.

Proof. 1) We have seen above that {R} is an orbit.

2) Clearly, C is an orbit, for $\langle xA\rangle \in C$ for all $x \in C$, $A \in PO(3,q)$ $(0 = Q(x) = Q(xA))$ and PO(3,q) is transitive on C (4.3.5.).

3) If $\langle x\rangle \in N$ and $A \in PO(3,q)$, then $\langle xA\rangle \in N$ $(QxA) = Q(x) \neq 0$, and R is an orbit). To prove that PO(3,q) is transitive on N, it is sufficient to show that PO(3,q) is transitive on $N \cap T$, for a $T \in T$, because each point of N is on a line of T and PO(3,q) is transitive on T (4.3.5.). So let $T \in T$, $\langle x\rangle, \langle y\rangle \in N \cap T$. Let $\langle a\rangle := T \cap C$ and select $\langle d\rangle \in C$, $\langle d\rangle \neq \langle a\rangle$.

Define $\langle b\rangle := (\langle d\rangle+\langle x\rangle) \cap C$ and $\langle c\rangle := (\langle d\rangle+\langle y\rangle) \cap C$.



Because PO(3,q) is 3-transitive on C, there is a $A \in PO(3,q)$ such that $\langle a\rangle A = \langle a\rangle$, $\langle d\rangle A = \langle d\rangle$, $\langle b\rangle A = \langle c\rangle$; note that A is linear.
Then,

$$\langle x\rangle A = ((R + \langle a\rangle) \cap (\langle b\rangle + \langle d\rangle))A = (R + \langle a\rangle) \cap (\langle b\rangle A + \langle d\rangle A)$$
$$= (R + \langle a\rangle) \cap (\langle c\rangle + \langle d\rangle) = \langle y\rangle .$$

Hence PO(3,q) is transitive on N, and therefore N is an orbit.
Because $PG(2,q) = \{R\} \cup C \cup N$, we have proved the theorem. □

4.3.7. Theorem. The action of PO(3,q) on the lines of PG(2,q) has 3 orbits, viz. T, S and E. Also, PO(3,q) is generously transitive on the lines of E.

Proof. 1) Because C is an orbit of PO(3,q) on the points of PG(2,q), it is easy to see that T is an orbit of PO(3,q) on the lines of PG(2,q).
2) S is also an orbit, for C is an orbit of PO(3,q) on the points of PG(2,q) and PO(3,q) is 2-transitive on C.
3) Because N is an orbit of PO(3,q) on the points of PG(2,q), and because the lines of E only have points of N, it is clear that $EA \in E$, for all $E \in E$ and $A \in PO(3,q)$.
For all $\langle a\rangle \in N$, we define the linear map $A_a : V(3,q) \to V(3,q)$ by

$$xA_a := x + \frac{(x,a)}{Q(a)}\, a \quad , \quad \text{for all } x \in V(3,q).$$

Then $A_a \in PO(3,q)$, for

$$Q(xA_a) = Q(x + \frac{(x,a)}{Q(a)}\, a) = Q(x) + \frac{(x,a)^2}{Q^2(a)}\, Q(a) + \frac{(x,a)}{Q(a)}\, (x,a) = Q(x),$$

for all $x \in V(3,q)$.
Also, because $xA_a = x$ if $(x,a) = 0$, A_a fixes all the points of the tangent $R + \langle a\rangle$ (note that $(R,a) = (a,a) = 0$. Note also that $A_a \neq I$).
Moreover, A_a has order 2 for

$$xA_a^2 = (x + \frac{(x,a)}{Q(a)}\, a)A_a = x + \frac{(x,a)}{Q(a)}\, a + \frac{(x,a)}{Q(a)}\, a = x$$

for all $x \in V(3,q)$.
Let $\langle a\rangle \in N$, $\langle b\rangle \in (\langle a\rangle + R) \cap N$. Then $b = a + \lambda(1,0,0)$ and

$$xA_aA_b = (x + \frac{(x,a)}{Q(a)}\, a)A_b = x + \frac{(x,b)}{Q(b)}\, b + \frac{(x,a)}{Q(a)}\, a = xA_bA_a \text{ , for}$$

all $x \in V(3,q)$.

Hence, if $\langle a\rangle = \langle b\rangle$, then $A_a A_b = I$, and if $\langle a\rangle \neq \langle b\rangle$, then

$A_a A_b = A_b A_a = A_c$, where $c = a + \frac{Q(a)}{\lambda}(1,0,0) = \lambda^{-2}(Q(b)a+Q(a)b)$,

$\langle c\rangle \in (\langle a\rangle + R) \cap N$.

With this we see that for every $T \in T$ the set

$$H(T) := \{I\} \cup \{A_a \mid \langle a\rangle \quad T \cup N\}$$

is an elementary Abelian subgroup of PO(3,q) of order $q = 2^m$.

Also, the elements of H(T) fix all the points of T.

Now, let E_1 and E_2 be distinct lines of E. Then E_1 and E_2 meet in a point $\langle a\rangle \in N$. Let $T := \langle a\rangle + R$ (then $T \in T$).

Clearly, if $A_b \in H(T)\backslash\{I\}$ and $\langle b\rangle \neq \langle a\rangle$, then A_b cannot fix E_1 (otherwise $A_b = I$). Therefore, $H(T)_{E_1} = \{I, A_a\}$.

($H(T)_{E_1}$ is the H(T)-stabilizer of E_1). Then, with lemma 4.3.2. we see that the H(T)-orbit that contains E_1 has length

$$\frac{|H(T)|}{|H(T)_{E_1}|} = \frac{q}{2}.$$

Hence the H(T) orbit that contains E_1 consists of the q/2 lines of E through $\langle a\rangle$ (note that H(T) fixes $\langle a\rangle$). Therefore, there is an $A \in H(T) \subset PO(3,q)$ such that $E_2 = E_1 A$, and because A has order 2, $E_2 A = E_1$. Hence PO(3,q) is generously transitive on E and E is the third (and last) orbit of PO(3,q) on the lines of PG(2,q).

□

Now, consider the following:

Let $\Gamma_0, \Gamma_1, \ldots, \Gamma_s$ denote the orbits of the action of PO(3,q) on $E \times E$, where Γ_0 is the orbit $\{(EA, EA) \mid A \in PO(3,q)\}$, for a certain $E \in E$. Clearly, $\Gamma_0 = \{(E,E) \mid E \in E\}$, for PO(3,q) is transitive on E.

Because PO(3,q) is generously transitive on E, $(E, \{\Gamma_0, \Gamma_1, \ldots, \Gamma_s\})$ is an association scheme (this we have seen in chapter 3. Note also that $\Gamma_0 = id$.).

4.3.8. Theorem. The association scheme $(E, \{id, \Gamma_1, \ldots, \Gamma_s\})$ is pseudo-cyclic.

Proof. We will show that $v_1 = v_2 = \ldots = v_s = q+1$ and

$$\sum_{i=1}^{s} a_{ij}^{i} = q \quad , \text{ for all } j = 1,\ldots,n,$$

for the valencies and intersection numbers of the association scheme (this is equivalent with the fact that the association scheme is pseudo-cyclic (theorem 4.1.2.)).

1) Let $E_1, E_2 \in \mathcal{E}$ and assume that $(E_1, E_2) \in \Gamma_i \quad (i \in \{1,\ldots,s\})$. Then,

$$v_i = \frac{|PO(3,q)_{E_1}|}{|PO(3,q)_{E_1,E_2}|} \qquad \text{for:}$$

let $A := \{E \in \mathcal{E} \mid (E_1,E) \in \Gamma_i\}$. It is clear that $v_i = |A|$.
But A is also the $PO(3,q)_{E_1}$ orbit that contains E_2.
Lemma 4.3.2. yields

$$v_i = |A| = \frac{|PO(3,q)_{E_1}|}{|PO(3,q)_{E_1,E_2}|}$$

Because PO(3,q) is sharply 3-transitive on the q+1 points of the oval C, it is easy to see that PO(3,q) has order $(q+1)q(q-1)$.
Also lemma 4.3.2. and the fact that PO(3,q) is transitive on $\mathcal{E}$ yield

$$\frac{|PO(3,q)|}{|PO(3,q)_{E_1}|} = |\mathcal{E}| = q^2+q+1-q+1-\binom{q+1}{2} = \tfrac{1}{2}q(q-1).$$

Hence, $|PO(3,q)_{E_1}| = (q+1)q(q-1)/\tfrac{1}{2}q(q-1) = 2(q+1)$.

Let $\langle a\rangle := E_1 \cap E_2$. Then $\langle a\rangle \in \mathcal{N}$ and the transitivity of PO(3,q) on $\mathcal{N}$ yields

$$|PO(3,q)_{\langle a\rangle}| = \frac{|PO(3,q)|}{|\mathcal{N}|} = \frac{(q+1)q(q-1)}{q^2-1} = q.$$

If $T = R + \langle a\rangle$, then H(T) is a subgroup of $PO(3,q)_{\langle a\rangle}$ and we have seen that $|H(T)| = q$ (see the proof of theorem 4.3.7.).
But then, $H(T) = PO(3,q)_{\langle a\rangle}$, and therefore,

$$PO(3,q)_{E_1,E_2} = (PO(3,q)_{\langle a\rangle})_{E_1,E_2} = H(T)_{E_1,E_2} = H(T)_{E_1} = \{ I, A_a \}.$$

Hence,

$$v_i = \frac{|PO(3,q)_{E_1}|}{|PO(3,q)_{E_1,E_2}|} = 2(q+1)/2 = q+1 \quad \text{for all } i = 1,2,\ldots,s.$$

2) Let $j \in \{1,2,\ldots,s\}$. Because $a^0_{0j} = 0$, we have to show that

$$\sum_{i=1}^{s} a^i_{ij} = q$$

Select a $E \in E$. Clearly, the number of pairs $(E', E'') \in E \times E$ such that $(E,E') \in \Gamma_i$, $(E,E'') \in \Gamma_k$ and $(E',E'') \in \Gamma_j$ is $v_i a^i_{jk}$, and also $v_k a^k_{ij}$ $(i,j,k = 1,\ldots,s)$. Thus $a^i_{jk} = a^k_{ij}$ (because $v_i = v_k$), for all $i,j,k = 1,\ldots,s$, and in particular, $a^i_{ij} = a^j_{ii}$ $(i,j = 1,\ldots,s)$. Hence,

$$\sum_{i=1}^{s} a^i_{ij} = \sum_{i=1}^{s} a^j_{ii} \quad , \quad (j = 1,\ldots,s).$$

Let $E_1, E_2, E_3 \in E$, $E_1 \neq E_2$, $E_1 \neq E_3$, $E_2 \neq E_3$ and $E_1 \cap E_2 = E_2 \cap E_3 = E_1 \cap E_3 = \langle a \rangle$. $(\langle a \rangle \in N)$.
All the relations (except the identity) betwwen E_1, E_2, E_3 are different, for:

if $(E_1,E_2) \in \Gamma_i$ and $(E_1,E_3) \in \Gamma_i$ for a certain $i \in \{1,\ldots,s\}$, then there exists an $A \in PO(3,q)$ such that $E_1A = E_1$ and $E_2A = E_3$, and thus,

$\langle a \rangle A = (E_1 \cap E_2)A = E_1 \cap E_3 = \langle a \rangle$. But then, $A \in (PO(3,q)_{\langle a \rangle})_{E_1} = H(T)_{E_1} = \{I, A_a\}$, where $T = R + \langle a \rangle$, and this is not possible for $E_2A_a = E_2 \neq E_3$. So, the relations must be different. Now, consider 2 lines of E, say E_1 and E_2 that are in relation Γ_j. We have seen above that a line $E_3 \in E \setminus \{E_1,E_2\}$, that has relation Γ_i with E_1 and E_2 $(i \in \{1,\ldots,s\})$ cannot go through $\langle a \rangle := E_1 \cap E_2$. So, $E_3 = \langle b \rangle + \langle c \rangle$, $\langle b \rangle \in E_1$, $\langle c \rangle \in E_2$, $\langle b \rangle \neq \langle a \rangle \neq \langle c \rangle$. For the same reason a line $E_4 \in E \setminus \{E_1,E_2,E_3\}$ that has relation Γ_k with E_1 and E_2 $(k = 1,\ldots,s)$, cannot meet E_3 in $\langle b \rangle$ or $\langle c \rangle$, (otherwise two relations between E_1, E_3, E_4 or E_2, E_3, E_4 would be the same, and that is impossible). Then it is easy to see that

$$(*) \qquad \sum_{i=1}^{s} a^i_{ij} = \sum_{i=1}^{s} a^j_{ii} \leq q \quad , \quad \text{for all } j = 1,\ldots,s.$$

Let $E \in E$. Then the number of pairs $(E',E'') \in E \times E$, $E' \neq E''$, $E \neq E'$, $E \neq E''$, such that relation(E,E') = relation(E,E''), equals

$$\sum_{j=1}^{s} \sum_{i=1}^{s} a^i_{ij} v_i .$$

But this is also $\sum_{i=1}^{s} v_i(v_i-1)$.

Because $v_1 = v_2 = \ldots = v_s = q+1$, this yields

$$\sum_{j=1}^{s} \sum_{i=1}^{s} a_{ij}^{i} = nq.$$

With (*) this yields $\sum_{i=1}^{s} a_{ij}^{i} = q$ for all $j = 1,\ldots,s$.

□

4.3.9. Remark. If we extend PO(3,q) with the field isomorphism $\lambda \to \lambda^2$ ($\lambda \in F_q$) that has order m, then we obtain a group, called PΣO(3,q) of order $m(q+1)q(q-1)$ that also fixes the oval C. (if $x_0^2+x_1+x_2 = 0$ then $(x_0^2)^2+x_1^2x_2^2 = (x_0^2+x_1x_2)^2 = 0$). Furthermore, the orbits of PΣO(3,q) on $E \times E$ are unions of orbits of PO(3,q) on $E \times E$. This way we obtain a new association scheme. For example, if $q = 2^4 = 16$, then we get a 3-class association scheme on 120 points with valencies $v_1 = 17$, $v_2 = 2\cdot 17 = 34$, $v_3 = 68$ and intersection numbers

a_{ij}^1	1	2	3
1	0	8	8
2	8	2	24
3	0	24	36

a_{ij}^2	1	2	3
1	4	1	12
2	1	12	20
3	12	20	36

a_{ij}^3	1	2	3
1	2	6	9
2	6	10	18
3	9	18	40

With these parameters, it is easy to see that if we take the first and second class together we obtain a 2-class association scheme on 120 points or in other words, a strongly regular graph on 120 vertices. If $q = 2^p$, p prime, then the association scheme obtained with the orbits of PΣO(3,q) on $E \times E$ is pseudo-cyclic with valencies (q+1)p.

Appendix 4.1. The action of PSL(2,q) on PG(2,q), $q = 2^m$.

Let $q := 2^m$. In paragraph 4.3. we have seen that PSL(2,q) is isomorphic with PO(3,q), and that the action of PO(3,q) on the lines of PG(2,q) has 3 orbits. Hence, PSL(2,q) induces an action on PG(2,q), that has 3 orbits on the lines of PG(2,q). Another proof of this fact is as follows:

Let V := V(2,q) and let S be the space of all symmetric linear maps $A : V \to V$, that is (with respect to any orthonormal basis) the space

of all symmetric matrices $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ $a,b,c \in F_q$

(In fact, $S = Sym^{(2)}(V)$, the space of all symmetric 2-tensors over V). Obviously, $\dim(S) = 3$.

For any symmetric 2-tensors ϕ and ψ, with matrices Φ and Ψ with respect to an orthonormal basis $\{\underline{e}_1,\underline{e}_2\}$ of V, the <u>trace inner product</u>

$$(\phi,\psi) := \sum_{i,j=1}^{2} \Phi_{ij} \cdot \Psi_{ij}$$

is independent of the orthonormal basis $\{\underline{e}_1,\underline{e}_2\}$, and serves as an inner product for S. Special elements of S are the <u>projections</u>. For any $\underline{a} \in V\backslash\{\underline{0}\}$ the projections onto the subspace $<\underline{a}>$ is the 2-tensor $\underline{a} \otimes \underline{a}$, that is the symmetric idempotent linear map having $<\underline{a}>$ as its image, that is the symmetric matrix

$$\begin{bmatrix} a_1^2 & a_1a_2 \\ a_1a_2 & a_2^2 \end{bmatrix} \qquad \text{for } \underline{a} = (a_1,a_2).$$

A.4.1.1. <u>Lemma.</u> If $\underline{a}$, $\underline{b}$, $\underline{c} \in V$ are pairwise independent, then $\underline{a} \otimes \underline{a}$, $\underline{b} \otimes \underline{b}$, $\underline{c} \otimes \underline{c}$ are independent.

<u>Proof.</u> Without loss of generality we can take $\underline{c} = \alpha\underline{a} + \beta\underline{b}$, $\alpha\beta \neq 0$. Then,

$$\underline{c} \otimes \underline{c} = \alpha^2(\underline{a} \otimes \underline{a}) + \beta^2(\underline{b} \otimes \underline{b}) + \alpha\beta(\underline{a} \otimes \underline{b} + \underline{b} \otimes \underline{a}).$$

Since $\underline{a}$ and $\underline{b}$ are independent vectors, the 3 summands on the right hand side are independent symmetric 2-tensors.

So, $\underline{a} \otimes \underline{a}$, $\underline{b} \otimes \underline{b}$ and $\underline{c} \otimes \underline{c}$ are also independent $(\alpha\beta \neq 0)$.

□

A.4.1.2. <u>Lemma.</u> If $\underline{a}$, $\underline{b} \in V$ are independent, then $D := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $(D \in S)$, $\underline{a} \otimes \underline{a}$, $\underline{b} \otimes \underline{b}$ are independent.

<u>Proof.</u> Same as lemma A.4.1.1. In fact, for any independent $\underline{a}$, $\underline{b} \in V$, the 2-tensor $\underline{a} \otimes \underline{b} + \underline{b} \otimes \underline{a}$ is a multiple of D.

□

The map $\phi : V \to S$ defined by $\forall_{\underline{a} \in V} (\phi(\underline{a}) := \underline{a} \otimes \underline{a})$,

induces a map of the q+1 points of $PG(1,F_q)$ onto the q+1 points of an oval in $PG(,2,F_q)$. This follows from lemma A.4.1.1.. From lemma A.4.1.2. we infer that the nucleus of this oval is the projective point $<D>$.

PSL(2,q) induces an action on PG(2,q). Indeed, for $\sigma \in PSL(2,q)$ define $\bar{\sigma}$ by linear extension of

$$\forall_{\underline{a} \in V} [\bar{\sigma}(\underline{a} \otimes \underline{a}) := \sigma(\underline{a}) \otimes \sigma(\underline{a})] .$$

Under this action, the nucleus <D> is fixed and the oval is fixed setwise.

A.4.1.3. Lemma. PSL(2,q) has 3 orbits on the points of PG(2,q).

Proof. <D>is one orbit; the oval is one orbit.
Take any $p \neq$ <D>outside the oval. Call
$p_1 :=$ (oval) $\cap$ $(p \cup$ <D>$)$, $p_3 :=$ (oval) $\cap$ $(p \cup p_2)$, for any $p_2 \neq p_1$ on the oval. Then

$$p = (\text{<D>} \cup p_1) \cap (p_3 \cup p_2), \text{ so}$$

p_1, p_2, p_3 determine p. Now, we have seen that PSL(2,q) acts 3-transitively on the points of PG(1,q) (theorem 4.3.4.), hence on the points of the oval. Therefore, the points $\neq$ <D> outside the oval form an orbit. □

A.4.1.4. Theorem. The action of PSL(2,q) on the lines of PG(2,q) has 3 orbits, viz. the q+1 tangents, the $\frac{1}{2}q(q-1)$ passants and the $\frac{1}{2}q(q+1)$ secants of the oval.

Proof. The tangents are represented by $\langle \underline{a} \otimes \underline{a} \rangle$ + <D> , and the secants by $\langle \underline{a} \otimes \underline{a} \rangle + \langle \underline{b} \otimes \underline{b} \rangle$, where $\underline{a} \otimes \underline{a}$, $\underline{b} \otimes \underline{b}$ are on the oval. Then, it is easy to see that the tangents and the secants each form an orbit.
But so do the passants, since there are 3 orbits altogether. This follows from the fact ([18] p. 21) that any group of automorphisms of PG(2,q) has equally many orbits on points and on lines, since the incidence matrix is nonsingular. □

Chapter 5.

Few distance sets.

5.1. Spherical s-distance sets. (Ref. [16]).

Let X, of finite cardinality n, denote a subset of the unit sphere

$$\Omega_d = \{\xi \in R^d \mid \langle \xi, \xi \rangle = 1\},$$

in Euclidean R^d with inner product

$$\langle \xi, \eta \rangle = \xi_1 \eta_1 + \ldots + \xi_d \eta_d .$$

Assume that the vectors of X admit only s inner products $\neq 1$, say $\alpha_1, \ldots, \alpha_s$ (s is called the degree of X).
In other words, the vectors of X admit s distances $\neq 0$. Then X is called a spherical s-distance set.

5.1.1. Example. Consider the case s = 1. Projection of an orthonormal basis in R^{d+1} onto the hyperplane

$$x_1 + \ldots + x_{d+1} = 0,$$

yields a set X of d+1 vectors in R^d having

$$I_{d+1} - \frac{1}{d+1} J_{d+1}$$

as their Gram matrix of inner products. Hence, the vectors of X lie on a sphere and admit only one distance $\neq 0$. In other words, X is a spherical one-distance set in R^d, called the regular simplex.

5.1.2. Example. Consider the case s = 2. In R^2 the maximum n equals 5, attained by the vertices of the regular pentagon. In R^3 the maximum n equals 6, attained by the vertices of the octahedron, but also by any 6 of the 12 vertices of the icosahedron which do not contain an antipodal pair (such sets have inner product $\pm 5^{-\frac{1}{2}}$).
For general R^d, at least $n = \frac{1}{2}d(d+1)$ may be achieved, viz. the $\binom{d+1}{2}$ points with coördinates $(1^2, 0^{d-1})$, which in R^{d+1} lie on the hyperplane

$$x_1 + x_2 + \ldots + x_{d+1} = 2.$$

5.1.3. Theorem. (absolute bound).

$$n \leq \binom{d+s-1}{d-1} + \binom{d+s-2}{d-1}, \quad \text{for the cardinality } n \text{ of a spherical } s\text{-distance set in } R^d.$$

Proof. [26] For each vector $y \in X$ we define the function

$$F_y(\xi) := \prod_{i=1}^{s} (\langle y,\xi\rangle - \alpha_i) \quad , \ \xi \in \Omega_d.$$

($\alpha_1, \alpha_2, \ldots, \alpha_s$ are the admissable inner products $\neq 1$ in X.)
These are n polynomials of degree $\leq s$ in the variables $\xi_1, \ldots, \xi_d$, restricted to Ω_d. The linear space of all such polynomials is Pol(s), and has dimension

$$\binom{d+s-1}{d-1} + \binom{d+s-2}{d-1} \qquad \text{(see 5.1.5.)}.$$

The polynomials $F_y(\xi)$, $y \in X$ are linearly independent, for:
let

$$\sum_{y\in X} c_y F_y(\xi) \equiv 0 \ , \ \xi \in \Omega_d, \quad \text{for } c_y \in R, \ y \in X.$$

Since

$$F_y(x) = \delta_{x,y} \prod_{i=1}^{s} (1-\alpha_i) \quad \text{for all } x,y \in X,$$

we find

$$c_y \prod_{i=1}^{s} (1-\alpha_i) = 0 \quad \text{for all } y \in X.$$

This yields $c_y = 0$ for all $y \in X$ (note that $\alpha_i \neq 1$).
Thus, the n polynomials $F_y(\xi)$, $y \in X$, are linearly independent in Pol(s). Therefore, n cannot exceed the dimension

$$\binom{d+s-1}{d-1} + \binom{d+s-2}{d-1}$$

of Pol(s).

□

5.1.4. Remark. If $s = 1$ then $n \leq d+1$. Equality holds for the regular simplex. If $s = 2$, then $n \leq \frac{1}{2}d(d+3)$. The only known cases for which $n = \frac{1}{2}d(d+3)$ are $(n,d) = (5,2), (27,6), (275,22)$.

5.1.5. Remark. The linear space Pol(s) of the polynomials of degree $\leq s$, restricted to Ω_d is the direct sum of the linear spaces Hom(s) and Hom(s-1), where Hom(s) is the space of the homogeneous polynomials of degree s, restricted to Ω_d. (In other words, the span of the monomials $\xi_1^{\alpha_1}, \ldots\ldots, \xi_d^{\alpha_d}$, $\alpha_1 + \ldots + \alpha_d = s$, restricted to Ω_d).

The dimension of Hom(s) is $\binom{d+s-1}{d-1}$, and therefore, the dimension of Pol(s) is

$$\binom{d+s-1}{d-1} + \binom{d+s-2}{d-1} .$$

5.2. The mod p bound.

In some cases we can obtain an upper bound, which is better than the one given in 5.1.3. (For a more general approach see [7]).
First we prove the following lemma:

5.2.1. Lemma. Let M denote a subset of R of finite, positive cardinality. If $ZM \subset pZM$, for a certain prime p, then $M = \{0\}$.

Proof. Assume that $ZM \subset pZM$ for a certain prime p.
QM is a linear space over Q of finite dimension f. We select a basis $e_1, e_2, \ldots, e_f$ in QM and denote every $m \in QM$ by the unique vector $(q_1, q_2, \ldots, q_f)$ with

$$m = \sum_{i=1}^{f} q_i e_i \quad , \qquad q_i \in Q.$$

If $q_i \neq 0$, then we can write

$$q_i = p^{\alpha_1} \prod_{j=1}^{\infty} p_j^{\beta_{ij}}, \text{ where } p_j \text{ is prime, } \alpha_i, \beta_{ij} \in Z$$

(Note that this factorization is unique).
For $m \in (QM)\backslash\{0\}$ we define

$$p(m) := \min\{\alpha_i \mid q_i \neq 0\} .$$

Since $ZM \subset pZM$, and therefore $ZM = pZM$, the following holds:

$$\min_{m \in pZM\backslash\{0\}} p(m) = \min_{m \in ZM\backslash\{0\}} p(m)$$

But also:

$$\min_{m \in pZM\backslash\{0\}} p(m) = 1 + \min_{m \in ZM\backslash\{0\}} p(m) \qquad (*)$$

It is easy to see that $p(m+n) \geq \min p(m), p(n)$, and therefore

$$\min_{m \in ZM\backslash\{0\}} p(m) = \min_{m \in M\backslash\{0\}} p(m).$$

With (*), this yields

$$\min_{m \in M\backslash\{0\}} p(m) = 1 + \min_{m \in M\backslash\{0\}} p(m).$$

M has finite, positive cardinality, and therefore the above yields $M = \{0\}$.

□

5.2.2. Theorem. (mod p bound)

Let $X \subset \Omega_d$, of cardinality n, denote a spherical s-distance set in R^d with admissable inner products $\alpha_1,\ldots,\alpha_s$ $(\neq 1)$.
Assume that for a certain integer k: $k\alpha_i \in Z$, for all $i = 1,\ldots, s$.
If p is a prime such that $k\alpha_i \not\equiv k \bmod p$, $i = 1,\ldots,s$, then

$$n \leq \binom{d+s_p-1}{d-1} + \binom{d+s_p-2}{d-1} \quad ,$$

where s_p is the cardinality of the set $\{k\alpha_i \bmod p \mid i = 1,\ldots,s\}$.

Proof. Let $\{k\alpha_i \bmod p \mid i = 1,\ldots,s\} = \{\beta_1,\ldots,\beta_{s_p}\}$

Define for each vector $y \in X$ the function:

$$F_y(\xi) := \prod_{i=1}^{s_p}(k\langle y,\xi\rangle - \beta_i) \quad , \xi \in \Omega_d.$$

These $F_y(\xi)$, $y \in X$ are n polynomials in $\mathrm{Pol}(s_p)$. They are linearly independent, for:

let

$$\sum_{y\in X} m_y F_y(\xi) \equiv 0 \quad , \xi \in \Omega_d \text{ , for } m_y \in R \text{ , } y \in X.$$

Since

$$F_y(y) = \prod_{i=1}^{s_p} (k\langle y,y\rangle - \beta_i) \not\equiv 0 \bmod p \ ,$$

and

$$F_y(x) = \prod_{i=1}^{s_p} (k\langle y,x\rangle - \beta_i) \equiv 0 \bmod p \ , \quad x \neq y \ ,$$

we find

$$m_x F_x(x) = - \sum_{y\neq x} m_y F_y(x) \in pZM \ , \ x \in X.$$

Because $F_x(x) \not\equiv 0 \bmod p$, $x \in X$, we obtain $m_x \in pZM$, $x \in X$.
Hence, $M \subset pZM$, and so $ZM \subset pZM$.
The lemma 5.2.1. yields $M = \{0\}$.
Hence, the n polynomials $F_y(\xi)$, $y \in X$ are linearly independent in $\mathrm{Pol}(s_p)$. Therefore, n cannot exceed the dimension

$$\binom{d+s_p-1}{d-1} + \binom{d+s_p-2}{d-1} \quad \text{of } \mathrm{Pol}(s_p).$$

□

5.2.3. Example. Let X be a set of binary d-vectors with weight 7 and with admissable inner products ($\neq 7$) 0,2,4,6. Then X is a sperical four-distance set in R^d.
With theorem 5.1.3. we obtain $(1/24)(d+7)(d+2)(d+1)$ as an upperbound for the cardinality n of X. But, if we use theorem 5.2.2. with k=1 and p=2 we have $s_p=1$, and this yields

$$n \leq \binom{d}{d-1} + \binom{d-1}{d-1} = d+1.$$

Until now we have only spoken of spherical few-distance sets in R^d. But what about general few-distance sets in R^d?

Let X denote a s-distance set in R^d with admissable distances ($\neq 0$) $\alpha_1, \ldots, \alpha_s$. If we use the same techniques as for spherical s-distance sets, in other words, if we define the polynomials

$$F_y(\xi) := \prod_{i=1}^{s} (\|y-\xi\|^2 - \alpha_i^2) \ , \ y \in X,$$

which are linearly independent, we only get

$$|X| \leq \binom{d+s}{d} + \binom{d+s-1}{d} \ ,$$

the same bound as for spherical s-distance sets in R^{d+1}.
But it is possible to choose $\binom{d+s-1}{d}$ polynomials f_i with the property that the set

$$\{F_y \mid y \in X\} \cup \{f_i \mid i = 1, \ldots, \binom{d+s-1}{d}\}$$

remains independent, and therefore find

$$|X| \leq \binom{d+s}{d} \ . \qquad \text{ref: [5].}$$

5.3. Equiangular lines.

Equiangular lines in R^d are lines through $\underline{0}$ in R^d that admit only one angle $\neq 0$.
Note that a set of equiangular lines in R^d is a one-distance set in (d-1)-dimensional elliptic geometry.

We will nowstate an absolute bound for the cardinality of such a set (in 5.4. we will give an interesting example of a set of equiangular lines, and in 5.5. we will investigate the ralation between equiangular line sets and other combinatorial structures).See also [28].

5.3.1. Theorem. (absolute bound)

$n \leq \frac{1}{2}d(d+1)$, for the cardinality n of a set of equiangular lines in R^d.

Proof. First, note that the linear space of the symmetric 2-tensors in R^d has dimension $\frac{1}{2}d(d+1)$. Recall that the 2-tensor $(\underline{a} \otimes \underline{b})$ has components $(\underline{a} \otimes \underline{b})_{ij} = a_i b_j$; $\underline{a}, \underline{b} \in R^d$ and that two 2-tensors have inner product

$$\langle \underline{a} \otimes \underline{b}, \underline{c} \otimes \underline{d} \rangle = \langle \underline{a},\underline{c} \rangle \langle \underline{b},\underline{d} \rangle \text{ , hence}$$
$$\langle \underline{a} \otimes \underline{a}, \underline{b} \otimes \underline{b} \rangle = \langle \underline{a},\underline{b} \rangle^2 \qquad (*)$$

Let L, of finite cardinality n, denote a set of equiangular lines in R^d with admissable angle ($\neq 0$) ϕ.

We select a unit vector along each line and denote the set of those n vectors with X.

The Gram-matrix of the vectors of X is $I_n + C_n \cos(\phi)$,

where $$C_n = \begin{bmatrix} 0 & & \pm 1 \\ & \ddots & \\ \pm 1 & & 0 \end{bmatrix}.$$

With property $(*)$, it follows that the Gram matrix of the vectors $\underline{x} \otimes \underline{x}$, $x \in X$ is

$$I_n + (J_n - I_n) \cos^2(\phi),$$

which has only positive eigenvalues ($\lambda_1 = \sin^2(\phi) + n \cos^2(\phi)$, $\lambda_2 = \ldots = \lambda_n = \sin^2(\phi)$).

Therefore, the n vectors $\underline{x} \otimes \underline{x}$, $x \in X$ are linearly independent in the linear space of the symmetric 2-tensors in R^d, of dimension $\frac{1}{2}(d+1)d$. Hence, $n \leq \frac{1}{2}d(d+1)$. □

5.3.2. Remark. This theorem can also be derived with the proof of 5.1.3., viz. the vectors of X admit 2 inner products $\neq 1$ ($\cos(\phi)$ and $-\cos(\phi)$). The polynomials $F_y(\xi)$ are in this case

$$F_y(\xi) = \langle y,\xi\rangle^2 - \cos^2(\phi) = \langle y,\xi\rangle^2 - \langle \xi,\xi\rangle\cos^2(\phi),\ \xi \in \Omega_d.$$

Hence, the $F_y(\xi)$ are n independent polynomials in Hom(2) of dimension $\frac{1}{2}d(d+1)$, and therefore $n \leq \frac{1}{2}d(d+1)$.

5.4. Sets of equiangular lines in R^d with angle arccos(1/3).

Let X_d denote a set of equiangular lines in R^d with admissable angle arccos(1/3). We are interested in the maximum cardinality of X_d, which we denote by $v_{1/3}(d)$.
We claim that

d =	3	4	5	6	7	8	. . . .	15	d ≥ 16
$v_{1/3}(d)$ =	4	6	10	16	28	28	. . . .	28	2(d-1) .

Proof. The problem is to find a maximum set X of unit vectors in R^d with admissable inner products($\neq$1) 1/3 and -1/3 (*).

1) d = 3. We can always find 3 vectors in R^3 with the above property, say $\underline{p}_1$, $\underline{p}_2$, $\underline{p}_3$ ($\langle \underline{p}_i,\underline{p}_i\rangle = 1$, for i = 1,2,3).
There are 2 non-equivalent cases:
(i) $\langle \underline{p}_i,\underline{p}_j\rangle = -1/3$ for all $i \neq j$
(ii) $\langle \underline{p}_i,\underline{p}_j\rangle = 1/3$ for all $i \neq j$.
All other possibilities lead to a set of lines produced by (i) or (ii).
Important is the fact that $\underline{p}_1$, $\underline{p}_2$, $\underline{p}_3$ must be independent in R^3.
Therefore. all other vectors $\underline{p}$ with property (*) can be written as

$$\underline{p} = \alpha_1\underline{p}_1 + \alpha_2\underline{p}_2 + \alpha_3\underline{p}_3 .$$

Then we find that case (i) yields one additional vector,viz. $\underline{p} = -\underline{p}_1 - \underline{p}_2 - \underline{p}_3$. Case (ii) does not produce any additional vectors. Hence, $v_{1/3}(3) = 4$. A maximum set is:

$$\underline{p}_1 = \frac{1}{\sqrt{3}}\begin{bmatrix}1\\-1\\-1\end{bmatrix} \quad \underline{p}_2 = \frac{1}{\sqrt{3}}\begin{bmatrix}-1\\1\\-1\end{bmatrix} \quad \underline{p}_3 = \frac{1}{\sqrt{3}}\begin{bmatrix}-1\\-1\\1\end{bmatrix} \quad \underline{p}_4 = \frac{1}{\sqrt{3}}\begin{bmatrix}1\\1\\1\end{bmatrix}$$

2) To prove the cases $d \geq 4$, we first investigate the structure of maximum vector sets X in R^d with $\langle \underline{p},\underline{p}\rangle = 1$, $\underline{p} \in X$. and other admissable inner products 1/3 and -1/3.

First, note that it is always possible to select 3 vectors of length 1 and mutual inner products -1/3 (if not, then the Gram matrix may be put in the form $(2/3)I + (1/2)J$, and this yields $\leq d$ vectors). Call these vectors $\underline{p}_1$, $\underline{p}_2$, $\underline{p}_3$. The vector $\underline{p}_4 := -\underline{p}_1-\underline{p}_2-\underline{p}_3$ must also be in X, for, X is maximal (i.e. the set is tetrahedrally closed). So, X must contain 4 vectors (a maximum set) $\underline{p}_1$, $\underline{p}_2$, $\underline{p}_3$, $\underline{p}_4$ of length 1, mutual inner products -1/3, that lie in R^3. Other elements of X must lie outside R^3. Therefore, we have to look for vectors $\underline{x} \in R^d$ outside R^3 with

$$\langle \underline{x},\underline{x}\rangle = 1, \quad \langle \underline{x},\underline{p}_i\rangle = (1/3)\varepsilon_i \quad , \quad \varepsilon_i = \pm 1 \quad , \; i = 1,2,3,4.$$

$\underline{p}_1+\underline{p}_2+\underline{p}_3+\underline{p}_4 = \underline{0}$ yields $\varepsilon_1+\varepsilon_2+\varepsilon_3+\varepsilon_4 = 0$. Hence, there are 3 non-equivalent possibilities for the ε_i's , viz.

(i) $\varepsilon_1 = \varepsilon_4 = 1$, $\varepsilon_2 = \varepsilon_3 = -1$

(ii) $\varepsilon_1 = \varepsilon_3 = -1$, $\varepsilon_2 = \varepsilon_4 = 1$

(iii) $\varepsilon_1 = \varepsilon_2 = -1$, $\varepsilon_3 = \varepsilon_4 = 1$

We can write $\underline{x} = \underline{h} + \underline{c}$ where $\underline{h} \in R^3$, $\underline{c} \in R^d$, and $\underline{c} \perp R^3$.
Then $\langle \underline{h},\underline{p}_i\rangle = (1/3)\varepsilon_i$ and therefore there are 3 possibilities for $\underline{h}$:

(i) $\underline{h}_1 = \frac{1}{4}(\underline{p}_1-\underline{p}_2-\underline{p}_3+\underline{p}_4)$

(ii) $\underline{h}_2 = \frac{1}{4}(-\underline{p}_1+\underline{p}_2-\underline{p}_3+\underline{p}_4)$

(iii) $\underline{h}_3 = \frac{1}{4}(-\underline{p}_1-\underline{p}_2+\underline{p}_3+\underline{p}_4)$

In other words, the elements of $X\setminus\{\underline{p}_1,\underline{p}_2,\underline{p}_3,\underline{p}_4\}$ can be written as $\underline{h}_1+\underline{c}_1$, $\underline{h}_2+\underline{c}_2$, $\underline{h}_3+\underline{c}_3$ where $\underline{c}_1,\underline{c}_2,\underline{c}_3 \perp R^3$.
$\{\underline{h}_i+\underline{c} \mid \underline{h}_i+\underline{c} \in X\}$ (i = 1,2,3) is called a pillar. $\underline{h}_i$ is the socle of the pillar.

The question is: how can we "fill" the pillars?

Case 1 : one pillar.

Assume that the first pillar is filled (or the second or the third), and that the other two are empty. Let Y be the set of the vectors $\underline{h}_1 + \underline{c}$ in the pillar.

The Gram matrix G of the vectors of Y is $G = I + (1/3)A$,

where $A = \begin{bmatrix} 0 & & \pm 1 \\ & \ddots & \\ \pm 1 & & 0 \end{bmatrix}$.

Because the vectors of Y can be written as $\underline{h}_1 + \underline{c}$, we can also say that $G = (1/3)J + C$, where C is the Gram matrix of the $\underline{c}$'s (note that $\langle \underline{h}_1, \underline{h}_1 \rangle = 1/3$). This yields

$$C = \frac{2}{3} \begin{bmatrix} 1 & & 0/-1 \\ & \ddots & \\ 0/-1 & & 1 \end{bmatrix}$$

Hence, for 2 different vectors $\underline{h}_1 + \underline{c}$ and $\underline{h}_1 + \underline{c}'$ in the same pillar, $\underline{c}$ and $\underline{c}'$ have angle 90° or 180°. The $\underline{c}$'s lie in (d-3)-dimensional space and therefore there are at most 2(d-3) vectors $\underline{c}$ with the above property. Hence, if one pillar is full and the other two empty, then the full pillar contains 2(d-3) vectors.

Case 2 : two pillars, three pillars.

Consider the first pillar with a vector $\underline{h}_1 + \underline{c}_0$, and the second with s vectors $\underline{h}_2 + \underline{c}_1$, ... , $\underline{h}_2 + \underline{c}_s$, where $\underline{c}_1$,...., $\underline{c}_s$ is an orthogonal s-set $\perp R^3$ (hence, $0 \le s \le d-3$).
The Gram matrix of the vectors $\underline{h}_1 + \underline{c}_0$, $\underline{h}_2 + \underline{c}_1$,....., $\underline{h}_2 + \underline{c}_s$ in the pillars is

$$G = I + \frac{1}{3} \begin{bmatrix} 0 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & & & \\ \pm 1 & & J_s - I_s & \\ \pm 1 & & & \end{bmatrix}$$

But also

$$G = \frac{1}{3} \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & & & & \\ \vdots & & J_s & & \\ 0 & & & & \end{bmatrix} + C ,$$

where C is the Gram matrix of $\underline{c}_0, \ldots, \underline{c}_s$ (note $\langle \underline{h}_1, \underline{h}_2 \rangle = 0$).

This yields $$C = \frac{2}{3}\begin{bmatrix} 1 & \pm\frac{1}{2} & \cdots & \pm\frac{1}{2} \\ \pm\frac{1}{2} & & & \\ \vdots & & I_s & \\ \pm\frac{1}{2} & & & \end{bmatrix}.$$

C is a Gram matrix and therefore $\det(C) \geq 0$.
Henc, $1-\frac{1}{4}((\pm 1)^2 + \ldots + (\pm 1)^2) = 1 - \frac{1}{4}s \geq 0$. This yields $s \leq 4$.
Because a pillar can only be filled with elements $\underline{h}_i + \underline{c}$ where the $\underline{c}$'s form a double-orthogonal set (angles 90° and 180°), we can state:
If more than one pillar is filled, each pillar can not contain more than 8 vectors. Thus, if we fill more than one pillar, we obtain at most $4 + 3 \cdot 8 = 28$ vectors with property (*).
Now we can continue with the proof.

3) $d = 4$. If we fill one pillar, we get: $v_{1/3}(4) \geq 4 + 2 = 6$.
Assume that in the first pillar we have a vector $\underline{h}_1 + \underline{c}$, and in the second a vector $\underline{h}_2 + \underline{c}_2$. The Gram-matrix of $\underline{c}_1$ and $\underline{c}_2$ is:

$$C = \frac{2}{3}\begin{bmatrix} 1 & \pm\frac{1}{2} \\ \pm\frac{1}{2} & 1 \end{bmatrix}.$$

C has rank 2. But because $\underline{c}_1, \underline{c}_2 \in R^4$ and $\perp R^3$, C must have rank ≤ 1.
Hence, we can only fill one pillar. This yields $v_{1/3}(4) = 6$.

4) $d = 5$. If we fill one pillar we get: $v_{1/3}(5) \geq 4 + 4 = 8$.
Assume that one pillar (the first) contains one vector $\underline{h}_1 + \underline{c}_1$ and another (the second) contains two vectors $\underline{h}_2' + \underline{c}_2$ and $\underline{h}_2 + \underline{c}_2'$ with $\langle \underline{c}_2, \underline{c}_2' \rangle = 0$. The Gram-matrix of the $\underline{c}$'s is:

$$C = \begin{bmatrix} 1 & \pm\frac{1}{2} & \pm\frac{1}{2} \\ \pm\frac{1}{2} & 1 & 0 \\ \pm\frac{1}{2} & 0 & 1 \end{bmatrix}, \text{ which has rank 3.}$$

But the $\underline{c}$'s are in R^5 and $\perp R^3$, and therefore C must have rank ≤ 2.
Hence, if we fill all three pillars, we can put at most 2 vectors in each pillar.
This yields $v_{1/3}(5) \leq 4 + 3 \cdot 2 = 10$.

Now consider the (-1,1) adjacency matrix C of the Petersen-graph:

$$C = \begin{bmatrix} A_5 & J-2I \\ J-2I & -A_5 \end{bmatrix} \qquad \text{where} \quad A_5 = \begin{bmatrix} 0 & - & + & + & - \\ - & 0 & - & + & + \\ + & - & 0 & - & + \\ + & + & - & 0 & - \\ - & + & + & - & 0 \end{bmatrix} .$$

C satisfies $C^2 = 9I$ and $CJ = 3J$.
Hence, C has smallest eigenvalue -3 of multiplicity 5 , and largest eigenvalue 3 of multiplicity 5.
If we use theorem 5.5.1. in the next paragraph, we find that C leads to a set of 10 lines in R^5 with angle arccos(1/3).
This yields $v_{1/3}(5) = 10$.

5) d = 6. In the same way as for d = 5, we can show that $v_{1/3}(6) \leq 4 + 3 \cdot 4 = 16$ (each pillar can not contain more than 4 vectors).
Consider now the following vectors in R^6:

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} .$$

Change in each vector the ones in each of the following combinations:

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix} .$$

This way we get 16 vectors in R^6 with $\cos(\alpha) = \pm(1/3)$.
Hence, $v_{1/3}(6) = 16$.

6) d = 7. If we fill one pillar, we get $v_{1/3}(7) \leq 4 + 2(7-3) = 12$.
If we fill all three pillars, we get $v_{1/3}(7) \leq 4 + 3 \cdot 8 = 28$.

Consider the incidence matrix of the Fano plane:

$$F = \begin{bmatrix} 1&1&0&1&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \\ 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 1&0&1&0&0&0&1 \end{bmatrix}.$$

If we change in each of the rows of F the ones in each of the following combinations:

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} -1 \\ -1 \\ 1 \end{bmatrix},$$

we obtain 28 vectors in R^7 with $\cos(\alpha) = \pm(1/3)$.
Hence, $v_{1/3}(7) = 28$.

7) $d = 8, 9, \ldots, 15$. If we fill one pillar we obtain less (or no more, (d=15)) than 28 vectors. Therefore $v_{1/3}(7) = v_{1/3}(8) = \ldots$ $\ldots = v_{1/3}(15) = 28$.

8) $d \geq 16$. If we fill one pillar we obtain more than 28 vectors. Therefore, $v_{1/3}(d) = 4 + 2(d-3) = 2(d-1)$. □

5.5. Two-graphs. (Ref: [30], [33]).

5.5.1. Theorem. There is a 1-1 correspondence between sets of equiangular lines and switching classes of graphs.

Proof.

1) Consider a switching class S of graphs on n points. Let C be the (-1,1) adjacency matrix of such a graph, with smallest eigenvalue -s of multiplicity n-d. Then $I + (1/s)C$ is positive semidefinite of rank d. Therefore, $I + (1/s)C$ is the Gram matrix of n vectors in R^d of length 1, and with inner products $\pm(1/s)$. Hence, these n vectors determine n equiangular lines in R^d with angle $\arccos(1/s)$. Switching w.r.t. a vertex of the considered graph is equivalent to changing the direction of the unit vector on the corresponding line. Therefore, all the graphs of S yield the same set of equiangular lines.
2) Consider a set X of n equiangular lines spanning R^d. Select a unit vector along each line. We may write the Gram matrix of these vectors as $I + C\cos(\alpha)$, where C is the (-1,1) adjacency matrix of a graph on n points, α the angle between the lines.

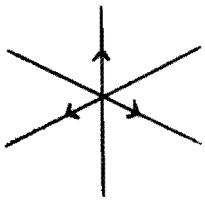
If we choose another set of unit vectors that also produces X, then the Gram matrix of these vectors can be put in the form $I + C'\cos(\alpha)$, where $C' = DCD$, $D = \mathrm{diag}(\pm 1)$. Hence, the graphs of C and C' are switching equivalent.

□

5.5.2. Definition. A two-graph (Ω,Δ) is a set Ω and a collection Δ of triples in Ω, such that every 4-subset of Ω contains an even number of triples of Δ.
If there exists an integer k, such that every pair in Ω occurs in k triples of Δ, then we call the two-graph (Ω,Δ) regular.

Let Ω, of cardinality n, denote a set of equiangular lines in R^d with angle $0 < \phi < \pi/2$. We select along each line a vector and define the following graph on those n vectors:
2 vectors are adjacent iff the angle between the vectors is obtuse.

A triple of lines in Ω is called good if we can choose 3 vectors along the lines, one along each line, such that all three angles are obtuse.
e.g.



A triple of lines in Ω is called bad if we can choose 3 vectors along the lines, one along each line, such that all three angles are acute.
Observe that a triple of lines is either good or bad, and that there is no third possibility.
To be more precise, consider a good triple of lines in Ω. If we choose any three vectors along the lines (one along each line), then the graph of these vectors is

or

If the triple is bad, then the graph is

 or 

For the vertices a and b ($a \neq b$) of a graph, we define the following:

$[ab] := 1$ if ab is a nonedge,

$[ab] := -1$ if ab is an edge.

The following can be easily verified:
a triple of lines in Ω is good iff for the vertices a,b,c of the corresponding graph $[ab][ac][bc] = -1$ holds, and it is bad iff $[ab][bc][ac] = 1$.
Call $[abc] := [ab][ac][bc]$.
We claim that every 4-subset X of Ω contains an even number of good triples.

Proof. Consider the graph corresponding with X on 4 vertices a,b,c,d. The triples are abc, abd, acd, bcd. $[abc][abd][acd][bcd] = 1$, holds because every $[xy]$, $x,y = a,b,c,d$; $x \neq y$ occurs exactly twice in the product. Hence, the number of good triples in X is even. □

5.5.2. Example. The 6 diagonals of the icosahedron make up 20 triples. Among these, 10 are bad. Every diagonal occurs in five bad triples, every pair of diagonals in two bad triples.

We have shown above that a set of equiangular lines in R^d is a two-graph.
Likewise, the converse holds (this we state without proof).
Hence, we can formulate the conclusions of this paragraph as follows:

5.5.3. Theorem. Two-graphs, switching classes of graph, and sets of dependent equiangular lines are equivalent structures.

Chapter 6.

Some problems from combinatorial geometry.

6.1. Introduction.

In this chapter we will deal with some problems of the Hungarian mathematician Paul Erdös, in the area of combinatorial geometry. First we will discuss sets of points with angles that are smaller than $\pi/2$ and $\pi/3 + \gamma$, respectively, where γ is small. (see [14] and [19]).

Secondly we examine sets of points in which each triangle is isosceles, the so called isosceles sets, first introduced by L.M. Kelly. These will turn out to be closely related to two-distance sets (see[4]).

6.2. Sets of points with no obtuse angles.

Paul Erdös conjectured many years ago that in d-dimensional R-space the maximum number of points f(d), with all angles not larger than $\pi/2$ equals 2^d and is realized by the d-dimensional hypercube $\{0,1\}^d$, that is $\{\underline{x} \in R^d \mid x_i \in \{0,1\},\ i = 1,2,..,d\}$. A simple proof for this conjecture was given by L. Danzer and B. Grünbaum [14].

If also no right angles are allowed, one can easily see that $f(2) = 3$, Croft proved $f(3) = 5$ and we will show the following result by Erdös and Füredi.

6.2.1. Theorem.[19]. The maximum number of points in R^d that provide only sharp angles is larger than $(1.15)^d$, for large d.

Proof. Consider the collection of vertices from the d-cube $\{0,1\}^d$. For any vertex a we define $A := \{i \mid a_i = 1\}$. The triangle (a,b,c) has a right angle in c iff

$$(A \cap B) \subset C \subset (A \cup B) \qquad (*)$$

Since (a,b,c) right in c means $\langle a-c, b-c\rangle = 0$ which is equivalent to

$$\forall_{1\le i\le d} [\ a_i = c_i \ \text{ or } \ b_i = c_i\ ] .$$

So

$$\text{if } c_i = 1 \quad \text{then} \quad \neg(a_i = b_i = 0) \quad : \quad C \subset A \cup B \ ,$$
$$\text{if } c_i = 0 \quad \text{then} \quad \neg(a_i = b_i = 1) \quad : \quad A \cap B \subset C \ .$$

We see now that the combinations $(0,0,1)$ and $(1,1,0)$ for (a_i,b_i,c_i) make the triangle (a,b,c) acute in c.
Now choose $2m$ points $a^1,\ldots,a^{2m}$ at random. That implies

$$\text{prob}(a_i^j = 0) = \text{prob}(a_i^j = 1) = \tfrac{1}{2}.$$

It is clear now that

$$\text{prob}((a,b,c) \text{ satisfy } (*)) = (\tfrac{3}{4})^d.$$

So

$$E(\#(a,b,c) \text{ with } (*)) = 2m(2m-1)(2m-2)(\tfrac{3}{4})^d.$$

We are now looking for an m which satisfies $E(..) \leq m$. This results in the inequality

$$2m(2m-1)(2m-2)(\tfrac{3}{4})^d \leq m \ .$$

This inequality holds if

$$8m^3(\tfrac{3}{4})^d \leq 1 \quad \text{or} \quad m = (\tfrac{2}{\sqrt{3}})^{d-8} \ .$$

We know now that we can find $2m$ points with at most m right triangles. If we remove one point from all those triangles, there are still m points left and no right triangles.
So

$$f(d) \geq m = (\frac{2}{\sqrt{3}})^{d-8} > (1.15)^d \quad \text{for sufficiently large d.}$$

□

Remark. Some of the counting in this proof can be done much better. However, it was not our intention to get the best possible result, but only to show that the maximal number of points is exponential in d.

The method used in the proof of 6.2.1. can be used to solve the problem of finding an upperbound of the maximum cardinality of sets in R^d with the property that all 3-subsets determine "near"-equiangular triangles. We need the following lemma.

6.2.2. Lemma. Let $X = \{1,2,\ldots,d\}$. $\forall_{\varepsilon\in\{0,1\}}$ there exists a collection $F = \{F_1, F_2, \ldots\}$ of subsets F_i from X, with $|F_i| = k$ such that

1) $|F_i \cap F_j| < \varepsilon k \quad , \quad i \neq j$

2) $|F| > (1 + 0.4\ \varepsilon^2)^d$.

Proof. Take F_i's with $|F_i \cap F_j| < \varepsilon k$. Assume that we have found n:

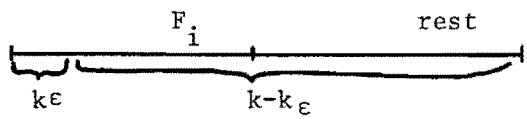
$$F_1, F_2, \ldots\ldots, F_n.$$

Define $G_n := \{G \subset X \mid |G| = k\ ,\ \exists_i \ |G \cap F_i| > k\varepsilon\}$.

As long as the cardinality of G does not exceed $\binom{d}{k}$ we can find an F_{n+1}.

For any i the number of G's with $|G \cap F_i| \geq k\varepsilon$,
is at most

$$\binom{k}{k\varepsilon}\binom{d-k\varepsilon}{k-k\varepsilon}.$$



It now follows

$$|G_n| \leq n\binom{k}{k\varepsilon}\binom{d-k\varepsilon}{k-k\varepsilon}.$$

So in the end at least

$$n \geq \binom{d}{k} \Big/ \binom{k}{k\varepsilon}\binom{d-k\varepsilon}{k-k\varepsilon}.$$

Choose now $k \simeq \frac{1}{4}d\varepsilon$. We find with Stirling's formula
$(n \simeq n^n e^{-n}\sqrt{2\pi n})$ that

$$|F| = n \geq (1 + 0.4\ \varepsilon^2)^d. \qquad \square$$

6.2.3. Theorem. [19] The maximum cardinality of a set in R^d with the property that all its 3-subsets determine angles smaller than $\pi/3 + \gamma$, where γ is a small real, is higher than

$$(1 + \tfrac{1}{2}\gamma^2)^d.$$

Proof. The k-subsets of a d-set as used in lemma 6.2.2. can be considered as vertices x of the d-cube, lying in the hyperplane

$$\sum_{i=1}^{d} x_i = k$$

If we take three vertices x,y,z out of F then

$$\begin{aligned} \langle y-x, z-x\rangle &\geq k-2\varepsilon k \quad , \\ \langle y-x, y-x\rangle &\leq (2k)^{\frac{1}{2}} \quad , \\ \langle z-x, z-x\rangle &\leq (2k)^{\frac{1}{2}} \quad . \end{aligned}$$

Thus $\cos(\angle yxz) \geq \frac{k-2\varepsilon k}{2k} = \frac{1}{2} - \varepsilon$.

Since $\cos(\pi/3 + \gamma) \simeq \frac{1}{2} - \frac{1}{2}\sqrt{3}\,\gamma$ we find $\varepsilon \simeq \sqrt{\frac{3}{4}}\gamma$.

So

$$f(d) \geq (1 + 0.4\,\varepsilon^2)^d \simeq (1 + 8/15\,\gamma^2)^d > (1 + \tfrac{1}{2}\gamma^2)^d.$$

□

6.3. Isosceles point sets in R^d.

An isosceles set in R^d is a collection X of points, such that any triple among them determines an isosceles triangle. The terminology that we use is the following :

(i) Let $X = \{x_1, x_2, \ldots, x_v\}$, then the affine hull aff(X) is defined as

$$\mathrm{aff}(X) := \{ \textstyle\sum_{i=1}^{v} a_i x_i \mid \sum a_i = 1\}.$$

We assume that $\mathrm{aff}(X) = R^d$.

(ii) For any subset $X_1 \subset X$, $\dim(X_1)$ is the dimension of $\mathrm{aff}(X_1)$.

(iii) A(X) represents the set of distances between points of X.

(iv) For $a \in A(X)$ let X_a be the graph defined on the set X, with two points joined by an edge iff their distance equals a.

(v) Finally X is called <u>decomposable</u> if X can be partitioned into X_1 and X_2 with $|X_2| > 1$, such that each point of X_1 has the same distance to all points of X_2, this distance may be different for distinct points of X_1, though.

6.3.1. <u>Lemma.</u> If X is decomposable, and (X_1, X_2) is a decomposition for X, then

$$\dim(X_1) + \dim(X_2) \leq \dim(X) \ .$$

Proof. Let P be the orthogonal projection on $\mathrm{aff}(X_2)$. Then for any $x_1 \in X_1$, Px_1 is the center of a sphere in $\mathrm{aff}(X_2)$, containing X_2. Since X_2 spans $\mathrm{aff}(X_2)$, P maps X_1 onto a single point. Therefore the flats $\mathrm{aff}(X_1)$ and $\mathrm{aff}(X_2)$ are orthogonal and the result follows. □

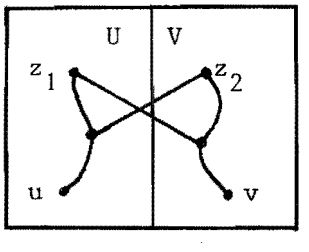
6.3.2. Theorem. If X is indecomposable then it is a two-distance set.

Proof. First we examine the case that there is some distance a for which X_a is disconnected. Then we look at the case where there is some a for which X_a has diameter larger than two. Finally we consider the case that X_a has diameter two for each $a \in A(X)$.

Case 1. Suppose there is an $a \in A(X)$ such that X_a is disconnected, then X is decomposable, for let X_2 be a component of X_a having more than one point. From the isosceles property it now follows that any point not in X_2 has the same distance to all points in X_2.

Case 2. Now suppose X_a is connected for all $a \in A(X)$ and let b be a distance such that there are two points, u and v, at distance three in X_b. Let a be the Euclidean distance between u and v. We claim that X is a two-distance set.

Let U be the set of points in X that are closer to u than to v in the graph X_b and let $V = X \setminus U$. For any z in U there is a (u,z) path entirely in U. So by the isosceles property v and z have distance a. Similarly u has Euclidean distance a to any point in V. Now take $z_1 \in U$ and $z_2 \in V$ and let P_1 be a shortest (z_1,u) path, P_2 a shortest (z_2,v) path. If z_1 is adjacent to z_2 in X_b, they have distance b. If z_1 is not adjacent to any point in P_2 then they have distance a by the isosceles property. Similarly if z_2 is not adjacent to any point of P_1. Now if both points do have a neighbour on the other path it is clear from the picture that the following holds:



$$d_b(v,z_1) \leq d_b(v,z_2) \leq d_b(u,z_2) \leq d_b(u,z_1) ,$$

where $d_b(x,y)$ is the "distance" of x and y in X_b.

This is a contradiction.

Now for any further distance c the graph X_c cannot be connected, since U and V are only joined by distances a and b.
Therefore X is a two-distance set.

Case 3. Suppose now that X_a is connected for every distance a, and has diameter 2. Suppose there are three distances. Call them a, b and c. We will construct an infinite subset of X, thus obtaining a contradiction.
Let z be an arbitrary point in X and a_1 a point at distance a from z. In X there is a point b_1 having distance b to both z and a_1 for the diameter of X_b is 2. Similarly we can find a point c_1 having distance c to both z and b_1. Since c_1a_1 is part of the triangle $c_1a_1b_1$, c_1a_1 is either c or b, but since it is also a side of the triangle c_1a_1z it is either a or c, and therefore it has to be c. Now let a_2 be a point at distance a from both c_1 and z and define b_2, c_2, a_3, . . . in the way indicated above, we will show that at each step at the construction of the infinite set the last constructed point has the same distance to all previous constructed points. Suppose the last point we added was a_k, we assume that our induction assumption holds for all points preceding a_k, i.e. if d_j is a point of the sequence, where d = a, b or c and $j < k$, then d_j has distance d to all points preceding d_j. By definition a_k has distance a to z and c_{k-1}.
Comparing the triangles za_kb_j and $c_{k-1}a_kb_j$ we see that a_kb_j is a. Similarly, comparing the triangles za_kc_j and $b_{j+1}a_kc_j$ (where $j+1 < k$) we conclude that a_kc_j is a. Finally the triangles $b_{k-1}a_ka_j$ and $c_{k-1}a_ka_j$ force a_ka_j to be a. Since every point has a different distance to its predecessors all points we obtain in this way are new, therefore we constructed an infinite subset of X, a contradiction.
Therefore X is a two-distance set. □

Remark. Cases 2 and 3 can be considered as the proof of the following pure graph-theoretic theorem:
Let K_n (the complete graph on n vertices) be edge-coloured with k colours, such that every triangle has at most two colours, and for each colour, the induced graph on that colour is connected. Then k = 2.

6.3.3. Theorem.[4]. Let X be an isosceles set in R^d, then

$$\text{card}(X) \leq \tfrac{1}{2}(d+1)(d+2) .$$

Equality implies that X is a two-distance set, or a spherical two-distance set together with its center.

Proof. The proof is by induction. If d = 1 then 3 is the maximum cardinality and X is a spherical set together with it's center. For d = 2 Kelly proved that the maximum is 6, realized by the centered regular pentagon.
Now let d > 2. If X is a two-distance set then we have the required inequality (see 5.2.).Now suppose X is decomposable, (X_1,X_2) being a decomposition.

Case 1. dim $X_1 \neq 0$. Since $|X_2| > 1$ we have $0 < \dim(X_1) < d$. Let $d_1 = \dim(X_1)$, then by induction we have

$$|X| \leq \tfrac{1}{2}(d_1+1)(d_1+2) + \tfrac{1}{2}(d-d_1+1)(d-d_1+2) < \tfrac{1}{2}(d+1)(d+2).$$

Case 2. $\dim(X_1) = 0$. In this case X_1 is a single point and therefore X_2 is spherical. If X_2 is not a two-distance set it is decomposable say $X_2 = (X_2',X_2'')$. But now $(X_1 \cup X_2',X_2'')$ is a decomposition of X as in case 1. This finishes the proof.

□

References.

1. E. Bannai, E. Bannai and D. Stanton: An upper bound for the cardinality of an s-distance set in real Euclidean space. Combinatorica 1 (1981), 99-102.

2. E. Bannai, A. Blokhuis, Ph. Delsarte and J.J. Seidel: The addition formula for hyperbolic space. To appear in: J. Comb. Theory Ser. A.

3. N. Biggs and A.T. White: Permutation groups and combinatorial structures. Cambridge: Cambridge University Press, 1979 (London Mathematical Society lecture notes series; 33).

4. A. Blokhuis: Isosceles point sets in R^d. Eindhoven: Technological University Dept. of Math. and Comp. Sci., 1981 (T.H.-Memo 1981-10).

5. A. Blokhuis: Few-distance sets in E^d and H^d. Eindhoven: Technological University. Dept. of Math. and Comp. Sci., 1982 (T.H.-Memo 1982-08).

6. A. Blokhuis: An upperbound for the cardinality of a set of equiangular lines in $R^{d,1}$. Eindhoven:Technological University. Dept. of Math. and Comp. Sci., 1981 (T.H.-Memo 1981-08).

7. A. Blokhuis and N.M. Singhi: Bounds on sets with few distances modulo a prime in metric spaces of strength t. Eindhoven: Technological University. Dept. of Math. and Comp. Sci., 1981 (T.H.-Memo 1981-06).

8. 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.

9. P.J. Cameron, J.-M. Goethals, J.J. Seidel and E.E. Shult: Line graphs, rootsystems and elliptic geometry. J. Algebra 43 (1976), 305-327.

10. P.J. Cameron, J.-M. Goethals and J.J. Seidel: The Krein condition, spherical designs, Norton algebras and permutation groups. Proc. K.N.A.W. Amsterdam Ser. A 81 (=Indag. Math. 40) (1978), 196-206.

11. P.J. Cameron and J.H. van Lint: Graphs, codes and designs. Cambridge: Cambridge University Press, 1980 (London Mathematical Society lecture notes series; 43).

12. P. Coebergh van de Braak: Constructions and an existence result of uniquely decodable codepairs for the two-access adder channel. Eindhoven: Technological University. Dept. of Math. and Comp. Sci.,1982 (Master thesis; 244).

13. D.M. Cvetković, M. Doob and H. Sachs: Spectra of graphs, theory and applications. Berlin: Deutscher Verlag der Wissenschaften, 1980.

14. L. Danzer and B. Grünbaum: Über zwei Probleme bezüglich konvexe Körper van P. Erdös und von V.L. Klee. Math. Z. 79 (1962), 95-99.

15. Ph. Delsarte: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Supplement nr 10(1973) (Thesis).

16. Ph. Delsarte, J.-M. Goethals and J.J. Seidel: Spherical codes and designs. Geom. Dedicata 6 (1977), 363-388.

17. Ph. Delsarte: Pairs of vectors in the space of an association scheme. Philips Res. Rep. 32 (1977), 373-411.

18. P. Dembowski: Finite geometries. Berlin etc.: Springer, 1968.

19. P. Erdös and Z. Füredi: The greatest angle among n points in d-dimensional Euclidean space. In: Combinatorial mathematics (Proc. Intern. colloquium Marseille, 1981); ed. by C. Berge et al. Amsterdam: North-Holland Publ. Comp., 1983 (North-Holland mathematics studies; 75) (Annals of discrete mathematics; 17) (in press).

20. P. Frankl and R.M. Wilson: Intersection theorems with geometric consequences. Combinatorica 1 (1981), 357-368.

21. W. Haemers: Eigenvalue techniques in design and graph theory. Amsterdam: Mathematisch Centrum,1981 (MC Tracts; 121) (Thesis).

22. D.G. Higman: Classical groups. Eindhoven: Technological University, 1978 (TH Report 78 WSK-04).

23. H. Hollmann: A new family of pseudocyclic association schemes. To appear in: J. Comb. Theory Ser. A.

24. H. Hollmann: Pseudo-cyclic 3-class association schemes on 28 points. To appear in: Discrete Math.

25. B. Huppert: Endliche Gruppen I. Berlin etc.: Springer, 1967.

26. T. Koornwinder: A note on the absolute bound for systems of lines. Proc. K.N.A.W. Amsterdam Ser. A 79 (=Indag. Math. 38) (1976), 152-153.

27. D.G. Larman, G.A. Rogers and J.J. Seidel: On 2-distance sets in Euclidean space. Bull. London Math. Soc. 9 (1977), 261-267.

28. P.W.H. Lemmens and J.J. Seidel: Equiangular lines. J.Algebra 24 (1973), 494-512.

29. J.H. van Lint, J.J. Seidel: Equilateral point sets in elliptic geometry. Proc. K.N.A.W. Amsterdam Ser. A 69 (=Indag. Math. 28) (1966), 335-348.

30. J.J. Seidel: A survey of two-graphs. In: Teorie Combinatorie, Tomo I (Proc. intern. coll. Roma, 1973). Roma: Accad. Naz. Linzei, 1976; 481-511.

31. J.J. Seidel: Strongly regular graphs of L_2 type and triangular type. Proc. K.N.A.W. Amsterdam Ser. A 70 (=Indag. Math. 29) (1976), 188-196.

32. J.J. Seidel: Graphs and two-distance sets. In: Combinatorial Mathematics VIII; ed by K.L. McAvaney. Berlin etc.: Springer 1981 (Lecture notes in mathematics; 884); 90-98.

33. J.J. Seidel and D.E. Taylor: Two-graphs a second survey. In: Algebraic methods in graph theory, Vol. 2; ed. by L. Lovász and V.T. Sós. Amsterdam: North-Holland Publ. Comp., 1981 (Colloquia mathematica Societas János Bolyai; 25);689-711.

34. J.A. Thas: Combinatorics of partial geometries and generalized quadrangles. In Higher combinatorics; ed. by M. Aigner. Dordrecht: Reidel, 1977; 183-199.

35. P. Turan: On the theory of graphs. Colloq. Math. 3 (1954), 19-30.