Association schemes

R. A. Bailey
rab@mcs.st-and.ac.uk, r.a.bailey@qmul.ac.uk

G. C. Steward lecture,
Gonville and Caius College, Cambridge

10 May 2013

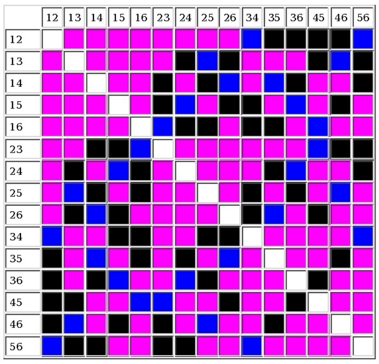
Association schemes: definition

An association scheme of rank r
on a finite set Ω (sometimes called points)
is a colouring of the elements of $\Omega \times \Omega$
(sometimes called edges)
by r colours such that

(i) one colour is exactly the main diagonal;
(ii) each colour is symmetric about the main diagonal;
(iii) if (α, β) is yellow
then there are exactly $p_{\mathrm{red,blue}}^{\mathrm{yellow}}$ points γ
such that (α, γ) is red and (γ, β) is blue
(for all values of yellow, red and blue).

The non-diagonal classes are called *associate classes*.

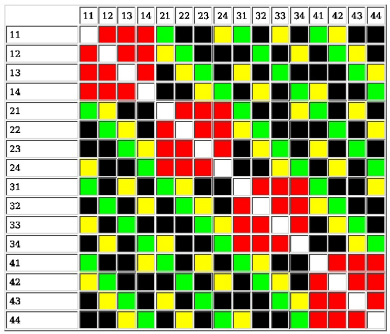
An association scheme with 15 points and 3 associate classes



If (α, β) is blue

α	β	
white	blue	1
blue	white	1
blue	blue	1
black	pink	4
pink	black	4
pink	pink	4

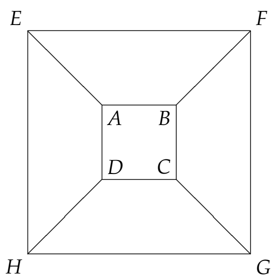
An association scheme defined by a Latin square

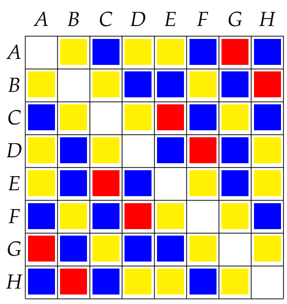


	1	2	3	4
1	*A*	*B*	*C*	*D*
2	*B*	*C*	*D*	*A*
3	*C*	*D*	*A*	*B*
4	*D*	*A*	*B*	*C*

different cells in same row	red
different cells in same column	green
different cells in same letter	yellow
other different cells	black

The association scheme defined by the cube





edge (distance 1)	yellow
distance 2	blue
opposite (distance 3)	red

Association schemes: alternative definition

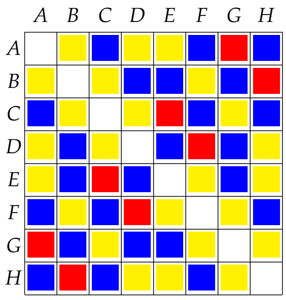
The adjacency matrix A_i for colour i is the $\Omega \times \Omega$ matrix with

$$A_i(\alpha, \beta) = \begin{cases} 1 & \text{if } (\alpha, \beta) \text{ has colour } i \\ 0 & \text{otherwise.} \end{cases}$$

Colour 0 is the diagonal, so

(i) $A_0 = I$ (identity matrix);
(ii) every A_i is symmetric;
(iii) $A_i A_j = \sum_k p_{ij}^k A_k$;
(iv) $\sum_i A_i = J$ (all-1s matrix).

One adjacency matrix for the cube



$$A_{\text{blue}} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

That hard condition

$$\begin{aligned} A_iA_j(\alpha,\beta) &= \sum_\gamma A_i(\alpha,\gamma)A_j(\gamma,\beta) \\ &= |\{\gamma : (\alpha,\gamma) \text{ has colour } i \text{ and } (\gamma,\beta) \text{ has colour } j\}| \\ &= p_{ij}^k \quad \text{if } (\alpha,\beta) \text{ has colour } k. \end{aligned}$$

So

$$A_iA_j = \sum_k p_{ij}^k A_k.$$

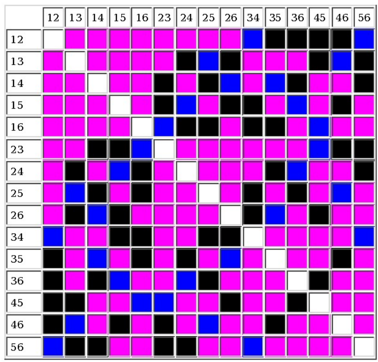
For an association scheme,
we turn counting into matrix multiplication.

How many edges of colour i at each point?

$$\begin{aligned} A_iA_i(\alpha,\alpha) &= \sum_\gamma A_i(\alpha,\gamma)A_i(\gamma,\alpha) \\ &= |\{\gamma : (\alpha,\gamma) \text{ has colour } i \text{ and } (\gamma,\alpha) \text{ has colour } i\}| \\ &= |\{\gamma : (\alpha,\gamma) \text{ has colour } i\}| \qquad \text{by symmetry} \\ &= p_{ii}^0. \end{aligned}$$

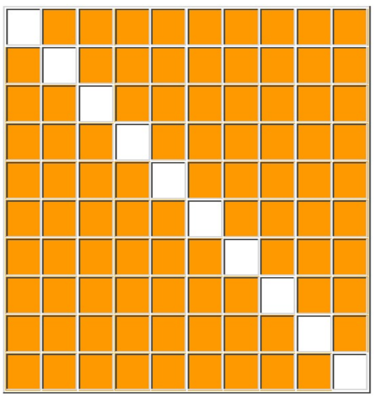
Put $a_i = p_{ii}^0$.
Then there are precisely a_i edges of colour i at each point.

How many edges of colour i at each point in this association scheme?



i	a_i
white	1
purple	8
blue	4
black	2

The trivial association scheme on 10 points

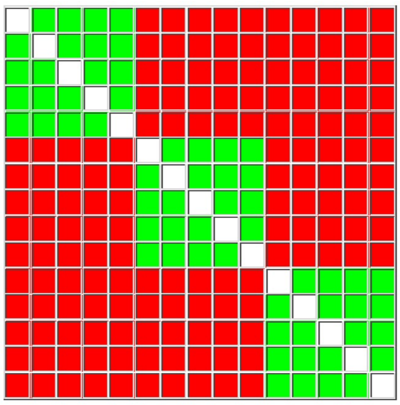


$A_0 = I$

$A_1 = J - I$

This is the only association scheme with rank 2.

The group divisible association scheme $GD(3,5)$.



The set Ω is partitioned into 3 "groups" of size 5.

Different points in the same "group" are 1st associates (green).

Points in different "groups" are 2nd associates (red).

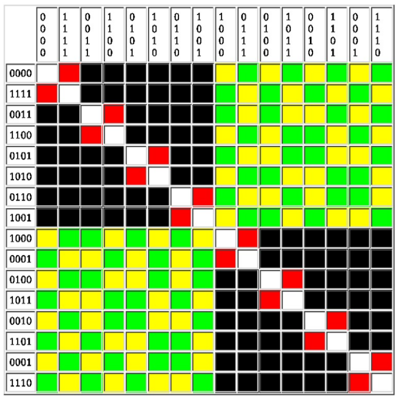
Association schemes in design of experiments

Suppose that we are going to do an experiment to compare 5 varieties of wheat.
We can use 15 plots of land in a single field.

If the plots are all alike, they form the trivial association scheme on 15 plots.

If the plots are not all alike, we may have to group them into three blocks: one block has the five plots near to the trees; another block has the five stony plots; and the third block has the five plots near to the stream. Now we have the group divisible association scheme GD(3,5).

The Hamming association scheme Hamm(4,2).

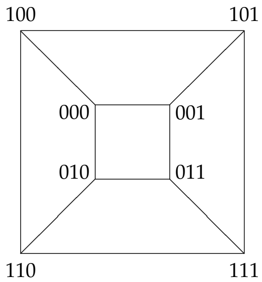


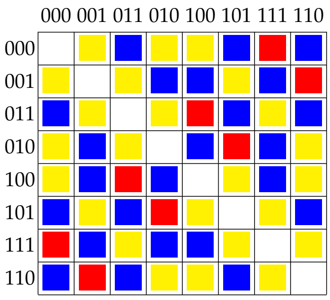
The points are vectors in Z_2^4.

How many equal coordinates?

4 white
3 yellow
2 black
1 green
0 red

The cube association scheme is Hamm(3,2)





edge (distance 1)	yellow	2 equal coordinates
distance 2	blue	1 equal coordinate
opposite (distance 3)	red	0 equal coordinates

Association schemes in coding theory

You receive the following top-secret message:

SHOOT BORDS

Should you

SHOOT BORIS?

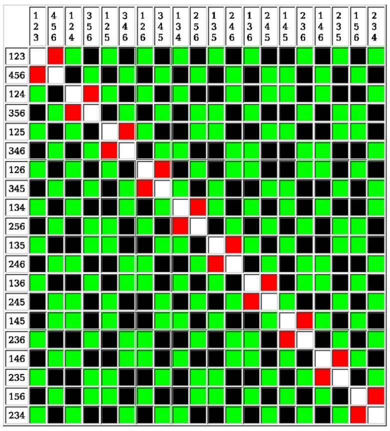
SHOOT BIRDS?

SHOOT LORDS?

SHOOT BONDS?

Coded versions of possible messages should have large Hamming distance between them.

The Johnson association scheme J(6,3).

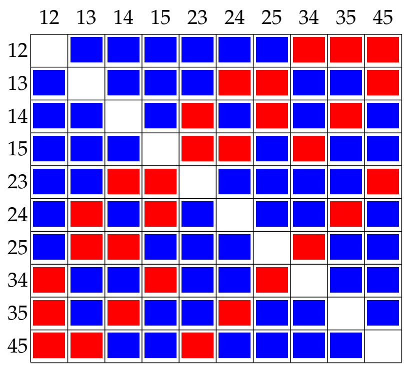


The points are subsets of size 3 of a set of size 6.

What is the size of their intersection?

3 white
2 green
1 black
0 red

Association schemes in genetics



Types of offspring from cross-breeding five pure breeds of dog.
Two different types may have one or zero parental lines in common. This is J(5,2).

How do we verify the hard condition?

We need to evaluate A_iA_j for $0 \le i \le r-1$ and $0 \le j \le r-1$.

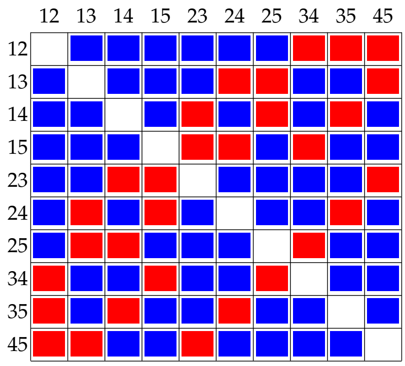
$A_0 = I$ and $IA_i = A_iI = A_i$, so
we only need to evaluate A_iA_j for $1 \le i \le r-1$ and $1 \le j \le r-1$.

If A_i does not have a constant number of 1s in each row and column then we do not have an association scheme.
If A_i has exactly a_i entries 1 in each row and column then $A_iJ = a_iJ$. So
$A_i(A_0 + \cdots + A_{r-1}) = A_iJ = a_iJ = a_i(A_0 + \cdots + A_{r-1})$. So
we only need to evaluate A_iA_j for $1 \le i \le r-2$ and $1 \le j \le r-2$.

If $A_iA_j = \sum_k p_{ij}^k A_k$ then A_iA_j is symmetric, so
$A_iA_j = (A_iA_j)^\top = A_j^\top A_i^\top = A_jA_i = \sum_k p_{ij}^k A_k$, so
we only need to evaluate A_iA_j for $1 \le i \le j \le r-2$.

When $r = 3$ we only need to evaluate A_1^2.

Where can I get to in two red steps?

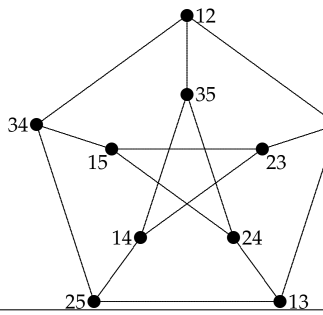


$A_{\text{red}}^2 = 3I + 0A_{\text{red}} + 1A_{\text{blue}}.$

Strongly regular graphs

A graph is strongly regular if

- every point is in p_{11}^0 edges;
- every edge is in p_{11}^1 triangles;
- every non-edge is in p_{11}^2 two-paths;
- the graph is neither null nor complete.



$p_{11}^0 = 3$

$p_{11}^1 = 0$

$p_{11}^2 = 1$

Association schemes of rank 3

An association scheme has rank 3
if and only if
each of its non-identity classes forms the edges of a strongly regular graph.

Distance-regular graphs

Suppose that a graph G with v vertices is connected and simple (no multiple edges) and has diameter (maximum distance) d.
Let A_i be the $v \times v$ matrix whose (α, β)-entry is equal to

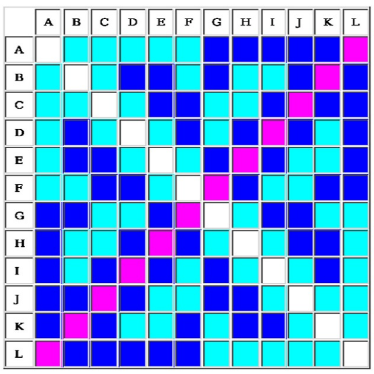
$$\begin{cases} 1 & \text{if the distance from } \alpha \text{ to } \beta \text{ in } G \text{ is } i \\ 0 & \text{otherwise} \end{cases}$$

The graph G is distance-regular if A_1A_i is a linear combination of A_{i-1}, A_i and A_{i+1} for all i.

Theorem
If G is distance-regular with diameter d then its distance classes form an association scheme of rank $d+1$.

If $r \ge 4$ then not all association schemes of rank r arise in this way.

The icosahedral association scheme



The 12 vertices and 30 edges of the icosahedron form a distance-regular graph with diameter 3.

distance 1	turquoise
distance 2	blue
distance 3	purple

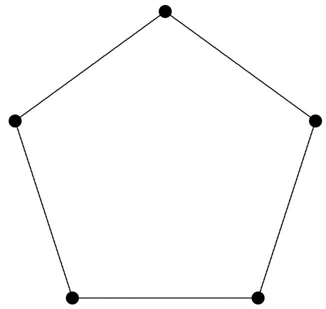
I have a wonderful cardboard model of this ... but it was too large to fit on the train.

Cyclic association schemes (circuits)

The n-circuit is an association scheme with rank

$$1 + \left\lfloor \frac{n-1}{2} \right\rfloor.$$

If the distance from α to β is d then (α, β) has colour d.



These are also distance-regular graphs.

Association schemes and permutation groups

If G is a transitive permutation group on Ω, it induces a permutation group on $\Omega \times \Omega$. Give (α, β) the same colour as (γ, δ) if and only if there is some g in G with $(\alpha^g, \beta^g) = (\gamma, \delta)$. The colour classes are the orbitals of G.

- Transitivity $\Longrightarrow$ (i);
- the orbitals are self-paired $\Longleftrightarrow$ (ii);
- (iii) is always satisfied.

The Bose–Mesner algebra

(i) $A_0 = I$ (identity matrix);
(ii) every A_i is symmetric;
(iii) $A_iA_j = \sum_k p_{ij}^k A_k$;
(iv) $\sum_i A_i = J$ (all-1s matrix).

Let $\mathcal{A}$ be the set of all real linear combinations of the A_i.

This is a real vector space. The matrices $A_0, \ldots, A_{r-1}$ are linearly independent (in position (α, β), only one of the A-matrices is non-zero), so one basis for $\mathcal{A}$ is $\{A_0, A_1, \ldots, A_{r-1}\}$, and the dimension of $\mathcal{A}$ is equal to the rank of the association scheme.

Condition (iii) shows that $\mathcal{A}$ is closed under multiplication, so it is an algebra.

$A_iA_j = A_jA_i$ for all i and j, so $\mathcal{A}$ is a commutative algebra.

Real symmetric matrices

Theorem

If A is an $n \times n$ real symmetric matrix then the following hold.

(i) *All eigenvalues of A are real.*
(ii) *If the distinct eigenvalues of A are $\lambda_1, \ldots, \lambda_s$, then the minimal polynomial of A is $(X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_s)$.*
(iii) *Eigenvectors of A corresponding to different eigenvalues are orthogonal to each other (w. r. t. the usual inner product).*
(iv) *A is diagonalizable, which means that $\mathbb{R}^n$ has a basis consisting of eigenvectors of A, which means that $\mathbb{R}^n = W_1 \oplus \cdots \oplus W_s$, where W_i is the eigenspace for eigenvalue λ_i.*
(v) *Let Q_i be the matrix of orthogonal projection onto W_i (this means that $Q_iv = v$ if $v \in W_i$ and $Q_iv = 0$ if $v \in W_i^\perp$). Then Q_i is a polynomial in A.*

How do you find the eigenvalues of a real symmetric matrix A?

- Solve the equation $\det(A - xI) = 0$ (Cambridge Maths students).
- Put it into Matlab (Lisbon Statistics students).
- If the matrix is patterned, guess an eigenvector and try it (RAB).
- Find the minimal polynomial.

The easy fruit

If u is the all-1 vector then $A_iu = a_iu$ (because A_i has a_i non-zero entries in each row and column).

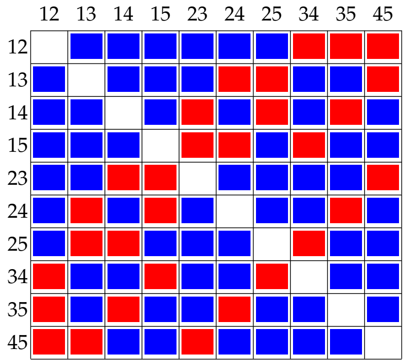
So u is an eigenvector of all matrices in $\mathcal{A}$, so we can confine the rest of our search to vectors which are orthogonal to u.

A lucky guess for the cube

$$A_{\text{blue}} = \begin{array}{c} A \\ B \\ C \\ D \\ E \\ F \\ G \\ H \end{array} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

We have found an eigenvector with eigenvalue -1.

Finding the minimal polynomial: I



$$A_{\text{red}}^2 = 3I + 0A_{\text{red}} + 1A_{\text{blue}} \quad \text{and} \quad A_{\text{red}}J = 3J.$$

Finding the minimal polynomial: II

$$A_{\text{red}}^2 = 3I + 0A_{\text{red}} + 1A_{\text{blue}} \quad \text{and} \quad A_{\text{red}}J = 3J.$$

Put $A = A_{\text{red}}$.

$$A^2 = 3I + (J - A - I) \quad \text{and} \quad AJ = 3J.$$

$$A^2 = 2I - A + J.$$

$$A^3 = 2A - A^2 + AJ = 2A - (2I - A + J) + 3J = -2I + 3A + 2J.$$

$$A^3 - 2A^2 - 5A + 6I = 0.$$

The minimal polynomial is $X^3 - 2X^2 - 5X + 6 = (X-3)(X^2 + X - 2) = (X-3)(X-1)(X+2)$.

Commuting projectors

Theorem

Let P be the matrix of orthogonal projection onto the subspace U, and let Q be the matrix of orthogonal projection onto the subspace V. If $PQ = QP$ then PQ is the matrix of orthogonal projection onto the subspace $U \cap V$.

Proof.

$(PQ)^2 = PQPQ = P^2Q^2 = PQ$, so PQ is idempotent. Since PQ is also symmetric, it is the matrix of orthogonal projection onto its image. Call this W.

$$v \in W \Rightarrow PQv = v \Rightarrow P^2Qv = Pv \Rightarrow PQv = Pv \Rightarrow v = Pv \Rightarrow v \in U.$$

Similarly, $v \in W \Rightarrow v \in V$, so $W \subseteq U \cap V$.

If $v \in U \cap V$ then $v = Pv = Qv$ so $PQv = Pv = v$ so $v \in W$.

Therefore $U \cap V \subseteq W$, and so $U \cap V = W$. □

Commuting symmetric matrices

Theorem

Let A and B be real symmetric $n \times n$ matrices. If $AB = BA$ then there are mutually orthogonal subspaces $W_1, \ldots, W_s$ such that

- $\mathbb{R}^n = W_1 \oplus \cdots \oplus W_s$;
- *each W_i is contained in an eigenspace of A and an eigenspace of B;*
- *the matrix of orthogonal projection onto each subspace is a polynomial in A and B.*

Proof.

Let the eigenprojectors of A be $P_1, \ldots, P_m$ and the eigenprojectors of B be $Q_1, \ldots, Q_t$. The former are polynomials in A, and the latter are polynomials in B, so they commute.
Apply the previous theorem to each nonzero product P_iQ_j.
$I = I^2 = (P_1 + \cdots + P_m)(Q_1 + \cdots + Q_t) = \sum_i \sum_j P_iQ_j$,
so $\bigoplus_k W_k$ is the whole space. □

Mutual eigenspaces of the Bose–Mesner algebra

The Bose–Mesner algebra $\mathcal{A}$ consists of symmetric matrices, is commutative, and has dimension r, where r is the rank of the association scheme.
So there are mutually orthogonal subspaces $W_1, \ldots, W_s$ of $\mathbb{R}^n$ such that if $M \in \mathcal{A}$ then each eigenspace of M is either one of the W_i or the direct sum of two or more of $W_1, \ldots, W_s$.

Let P_j be the orthogonal projector onto W_j.
Then P_j is a polynomial in $A_0, A_1, \ldots, A_{r-1}$, so $P_j \in \mathcal{A}$.

$P_1, \ldots, P_s$ are linearly dependent because $P_jP_k = 0$ if $j \neq k$.

Let c_{ij} be the eigenvalue of A_i on W_j. Then

$$A_i = \sum_{j=1}^{s} c_{ij}P_j \qquad \text{for } i = 0, \ldots, r-1.$$

Hence $\{P_1, \ldots, P_s\}$ is another basis for $\mathcal{A}$, and so $s = r$.

Strata

The subspaces $W_1, \ldots, W_r$ are called strata.

The projectors P_j are sometimes called minimal idempotents.

The dimension $d_j = \dim(W_j)$ is sometimes called the (number of) degrees of freedom for W_j.

The 1-dimensional space spanned by the all-1 vector is always a stratum.

The character table

We have seen that if c_{ij} is the eigenvalue of A_i on W_j then

$$A_i = \sum_{j=1}^{r} c_{ij} P_j \qquad \text{for } i = 0, \ldots, r-1.$$

Let C be the $r \times r$ matrix with entries c_{ij}. The columns of C are called the characters of the association scheme, and C is called the character table of the association scheme.

(The conventions are slightly different from those in group theory.)

To express P_j as a linear combination of the A_i, we need C^{-1}.

Two bases

$\{A_0, \ldots, A_{r-1}\}$ and $\{P_1, \ldots, P_r\}$ are both bases for $\mathcal{A}$.
$\{A_0, \ldots, A_{r-1}\}$ is more useful for interpretation, and is easier for doing addition.
$\{P_1, \ldots, P_r\}$ is easier for doing multiplication, including finding inverses (and generalized inverses).

To transfer back and forth between the two bases, we need to know both C and C^{-1}.

Theorem

$$C^{-1} = \frac{1}{|\Omega|} \operatorname{diag}(d_1, \ldots, d_r) C^\top \operatorname{diag}\left(\frac{1}{a_0}, \ldots, \frac{1}{a_{r-1}}\right).$$

In general, there is no easy way of finding C, and no natural labelling for the strata.

Possible generalizations

- Allow A_i and $A_i^\top$ to be two different colours, but still insist on commutativity (P. Delsarte, coding theory, 1973, thesis)
- Allow A_i and $A_i^\top$ to be two different colours, but do not insist on commutativity (natural approach for permutation groups, I. Schur, 1933; H. Wielandt, 1964; D. G. Higman, 1964, 1967) (now called homogeneous coherent configurations)
- Allow the diagonal to be more than one class, which forces the loss of commutativity and symmetry (called coherent configurations by D. G. Higman).

Some history: I

- Relevant idea for permutation groups (I. Schur, 1933).
- Definition of association scheme, in design of experiments (R. C. Bose and K. R. Nair, 1939).
- A strongly regular graph on 100 points with valency 22 (D. M. Mesner, 1956, thesis).
- Bose–Mesner algebra (Bose and Mesner, 1959).
- Multidimensional association schemes (J. N. Srivastava, 1961, thesis; Bose and Srivastava, 1964; much more by Srivastava over the years).
- Effectively homogeneous coherent configurations, but unnamed (C. R. Nair, 1964)
- A strongly regular graph on 100 points with valency 22 and large automorphism group (D. G. Higman and C. C. Sims, 1968).
- Cellular algebras (B. Yu. Weisfeiler and A. A. Lehman, 1968, possibly earlier in Russian?; much more by others in the U.S.S.R. over the years).

Some history: II

- Coherent configurations (Higman, 1975, 1976, after ten years of lecturing on them).
- Breakdown of barriers with U.S.S.R., and realisation that cellular algebras are the same as coherent configurations (1990).
- Death of Mesner, and realisation that he had pre-discovered the Higman–Sims graph (2002).
- Death of Higman (13/2/2006).
- Death of Srivastava (18/11/2010).
- Realisation that multidimensional association schemes are the same as coherent configurations (2011).