Association Schemes[1]

Chris Godsil
Combinatorics & Optimization
University of Waterloo

---

[1] June 3, 2010

Preface

These notes provide an introduction to association schemes, along with some related algebra. Their form and content has benefited from discussions with Bill Martin and Ada Chan.

Contents

Chapter 1

Schemes and Algebras

Our first three chapters provide an introduction to the basic theory of association schemes and to some of their applications. In this chapter we introduce association schemes and describe their structure.

1.1 Definitions and Examples

We try to motivate the definitions to come. Suppose X is a graph with vertex set V and diameter d. For $i = 1, \ldots, d$ we define X_i to be the graph with vertex set V, where two vertices are adjacent in X_i if they are at distance i in X. (So $X = X_1$.) Let A_i denote the adjacency matrix of X_i, set A_0 equal to I and consider the matrix algebra $\mathbb{C}[\mathscr{A}]$ over $\mathbb{C}$ generated by $A_1, \ldots, A_d$.

If we identify the automorphism group of X with the set of permutation matrices that commute with A_1, then each automorphism of X lies in the commutant of $\mathbb{C}[\mathscr{A}]$. Thus, for example, if $\mathbb{C}[\mathscr{A}] = \mathrm{Mat}_{n\times n}(\mathbb{C})$, then the automorphism group of X must be the identity group. Since the matrices $A_0, \ldots, A_d$ are linearly independent, $\mathbb{C}[\mathscr{A}]$ has dimension at least $d+1$. This suggests that the case where $\dim(\mathbb{C}[\mathscr{A}]) = d+1$ should be interesting. In fact the dimension of $\mathbb{C}[\mathscr{A}]$ is $d+1$ if and only if the matrices $A_0, \ldots, A_d$ form an association scheme.

An *association scheme* with d classes is a set $\mathscr{A} = \{A_0, \ldots, A_d\}$ of 01-matrices such that

(a) $A_0 = I$.

(b) $\sum_{i=0}^{d} A_i = J$.

(c) $A_i^T \in \mathscr{A}$ for each i.

(d) $A_i A_j = A_j A_i \in \operatorname{span}(\mathscr{A})$.

Note that (b) implies that the matrices $A_0, \ldots, A_d$ are linearly independent, and (d) that the algebra they generate has dimension $d+1$. Since J is the sum of the A_i, it commutes with each A_i, which implies that all rows and columns of A_i have the same sum.

An association scheme is *symmetric* if each matrix in it is symmetric. We view $A_1, \ldots, A_d$ as adjacency matrices of directed graphs $X_1, \ldots, X_d$, with common vertex set V. We say two vertices u and v are *i-related* if uv is an arc in X_i.

1.1.1 Example. The *Johnson scheme $J(v,k)$*. The vertex set of this scheme is the set of all k-subsets of a fixed set of v elements. Two vertices α and β are i-related if $|\alpha \cap \beta| = k - i$. This scheme has k classes.

1.1.2 Example. The *Grassman scheme $J_q(v,k)$*. The vertex set is the set of all subspaces of dimension k of the vector space of dimension n over $GF(q)$. Subspaces α and β are i-related if $\dim(\alpha \cap \beta) = k - i$. This scheme has k classes.

1.1.3 Example. The *Hamming scheme $H(n,q)$*. Let Q be an alphabet of q symbols. The vertex set of $H(n,q)$ is Q^n, the set of all words of length n over Q. Two words are i-related if they differ in exactly i coordinate positions. This scheme has n classes.

1.1.4 Example. The *bilinear forms scheme*. The vertices are the $m \times n$ matrices over the field of q elements. Two matrices A and B are i-related if $\operatorname{rk}(A - B) = i$. The number of classes in this scheme is the minimum of m and n.

1.1.5 Example. The conjugacy classes of a finite group Γ. Let the congugacy classes of Γ be $C_0, \ldots, C_d$, where $C_0 = \{1\}$. The vertex set of this scheme consists of the elements of Γ, and two group elements g and h are i-related if $hg^{-1} \in C_i$. This is our first example of a scheme that is not symmetric.

1.1.6 Example. Let Z be the complete graph on n^2 vertices. A *parallel class* in Z is a subgraph isomorphic to nK_n. Two parallel classes are orthogonal is they are edge-disjoint. A *partial spread* is a set of pairwise orthogonal parallel classes $C_1, \ldots, C_t$. Define A_i to be the adjacency matrix of the i-parallel class, set $A_0 = I$ as usual and define

$$A_{t+1} = J - \sum_{i=1}^{t} A_i.$$

Then $A_0, \dots, A_{t+1}$ is a symmetric association scheme. (These schemes correspond to orthogonal arrays with index 1.)

1.2 Strongly Regular Graphs

The simplest association schemes are the schemes with one class. In this case we have $A_0 = I$ and $A_1 = J - I$; the directed graph X_1 is the complete graph itself. We cannot think of anything intelligent to say about this situation, so we turn to the next simplest case. These are the symmetric schemes with two classes, and are equivalent to strongly-regular graphs.

Rather than offer the necessary definitions, we consider a classical example. We consider graphs with diameter two and maximum degree k. If X is such a graph and $u \in V(X)$, then u has at most k neighbours, and at most $k(k-1)$ vertices lie at distance two from u. Therefore

$$|V(X)| \le 1 + k + k^2 - k = k^2 + 1.$$

If equality holds then X is k-regular and its girth is at least five. This leads us to study k-regular graphs on $k^2 + 1$ vertices with diameter two. Suppose X is such a graph and let A be its adjacency matrix.

We claim that

$$A^2 + A - (k-1)I = J. \tag{1.2.1}$$

This is an easy consequence of the fact that the ij-entry of A^2 is the number of walks of length two from i to j in X. The number of walks of length two that start and finish at the same vertex is the valency of the vertex, and therefore since X is regular, $(A^2)_{i,i} = k$. The number of walks of length two that start at a given vertex i and end at the adjacent vertex j is the number of triangles in X that contain the edge ij. Therefore $(A^2)_{i,j} = 0$ in this case. Finally if i and j are distinct and not adjacent in X then, since there are no 4-cycles in X and since the diameter of X is two, $(A^2)_{i,j} = 1$. Equation (1.2.1) follows from these facts.

We explain the connection with association schemes. The adjacency matrix $\overline{A}$ of the complement $\overline{X}$ of X is $J - I - A$. From (1.2.1)

$$\overline{A} = J - I - A = A^2 - kI.$$

Since $\overline{A}$ is thus a polynomial in A, it commutes with A. We also see that A^2 is a linear combination of I, A and $\overline{A}$. Since $AJ = JA = kJ$ we can also show that $A\overline{A}$

and $\overline{A}^2$ are linear combinations of I and $\overline{A}$. We conclude that the matrices I, A and $\overline{A}$ form a symmetric association scheme with two classes.

We can use (1.2.1) to obtain more information about our graphs. They key is that we can compute the eigenvalues of A.

First note that the all-ones vector $\mathbf{1}$ is an eigenvector for A; in fact

$$A\mathbf{1} = k\mathbf{1}$$

and so the corresponding eigenvalue of the valency k. Suppose λ is an eigenvalue of A with eigenvector z. We may assume that z is orthogonal to $\mathbf{1}$, whence $Jz = 0$. Therefore

$$0 = Jz = (A^2 + A - (k-1)I)z = (\lambda^2 + \lambda - k + 1)z$$

and so λ is a zero of the quadratic polynomial

$$t^2 + t - k + 1.$$

Denote the roots of this by θ and τ. Since $\theta\tau = 1 - k$ we may assume that $\theta > 0 > \tau$. Let m_θ and m_τ denote respectively the multiplicity of θ and τ as an eigenvalue of A. Since X has $k^2 + 1$ vertices and k is an eigenvalue with multiplicity at least one, we have

$$1 + m_\theta + m_\tau = k^2 + 1. \tag{1.2.2}$$

Also $\operatorname{tr}(A) = 0$ and consequently

$$k + m_\theta\theta + m_\tau\tau = 0. \tag{1.2.3}$$

These two equations imply that

$$m_\tau = \frac{\theta k^2 + k}{\theta - \tau} \tag{1.2.4}$$

The existence of this expression for the multiplicity of an eigenvalue is a consequence of the fact that we are dealing with an association scheme. The fact that its right side must be an integer provides a very useful constraint. The ensuing calculations show how we may put it to work.

We distinguish two cases. First, suppose that θ and τ are irrational. We have

$$0 = k + (m_\theta - m_\tau)\theta + m_\tau(\theta + \tau) = k - m_\tau + (m_\theta - m_\tau)\theta$$

and since $k - m_\tau$ is an integer and θ is irrational, it follows that $m_\theta - m_\tau = 0$. Then (1.2.3) yields that $k = m_\theta = m_\tau$ and so (1.2.2) now yields that $k^2 - 2k = 0$. The only useful solution to this is $k = 2$, when we see that $X = C_5$.

Thus we may assume that θ and τ are rational, and hence they are integers. Since θ and τ are the roots of $t^2 + t - k + 1$, we have

$$(\theta - \tau)^2 = 1 + 4(k-1) = 4k - 3$$

and therefore $4k - 3$ must be a perfect square. Since $4k - 3$ is odd, we may assume

$$4k - 3 = (2s+1)^2$$

and therefore

$$k = s^2 + s + 1.$$

From this it follows that $\theta = s$ and $\tau = -s - 1$ and consequently

$$m_\tau = \frac{(s^2+s+1)(s(s^2+s+1)+1)}{2s+1}$$

Now

$$4s^2 + 4s + 4 = (2s+1)^2 + 3$$

and

$$8s^3 + 8s^2 + 8s + 8 = 2s(2s+1)^2 + 3(2s+1) + 5 = (4s^2 + 4s + 3)(2s+1) + 5.$$

Hence there is a polynomial p with integer coefficients such that

$$32 m_\tau = p(s) + \frac{15}{2s+1}.$$

We conclude that m_τ is an integer if and only if $2s+1$ divides 15. This implies that

$$s \in \{1, 2, 7\}$$

and so

$$k \in \{3, 7, 57\}.$$

To summarise, we have shown that if there is a k-regular graph of diameter two on $k^2 + 1$ vertices, then k is 2, 3, 7 or 57 (and v is 5, 10, 50 or 3250). The case $k = 2$ is realized by C_5. The case $k = 3$ is realized by the Petersen graph and the case $k = 7$ by the famous Hoffman-Singleton graph. We do not know if there is a graph with valency 57. This is an old and famous open question.

1.3 The Bose-Mesner Algebra

The *Bose-Mesner algebra* of an association scheme $\mathscr{A} = \{A_0, \dots, A_d\}$ is the algebra generated by the matrices $A_0, \dots, A_d$; equivalently it is the complex span of these matrices. There is a second multiplication on the Bose-Mesner algebra which will prove to be very important. We define the Schur product $A \circ B$ of two matrices of the same order by

$$(A \circ B)_{i,j} := A_{i,j} B_{i,j}.$$

This is a commutative and associative product with J as unit. Since the set $\mathscr{A} \cup 0$ spans the Bose-Mesner algebra, and since this set is closed under Schur multiplication, it follows that the Bose-Mesner algebra is closed under Schur multiplication. Hence it is an algebra with respect to Schur multiplication. The Bose-Mesner algebra is also closed under complex conjugation and the transpose map.

A *coherent algebra* is a matrix algebra over $\mathbb{C}$ that is Schur-closed, closed under transpose and complex conjugation, and contains I and J. Any Bose-Mesner algebra is a commutative coherent algebra. We will discuss coherent algebras at greater length in Chapter **??**, but we offer some simple observations now.

1.3.1 Lemma. *A commutative coherent algebra is the Bose-Mesner algebra of an association scheme.* □

Define the *commutant* of a set of matrices to be the set of all matrices that commute with each element of the set.

1.3.2 Lemma. *The commutant of a set of $v \times v$ permutation matrices is a coherent algebra.*

Proof. It suffices to show that the commutant of a single permutation matrix P is a coherent algebra. The key point is then to show that the commutant of P is Schur-closed.

Suppose M and N commute with P. Then

$$P(M \circ N) = (PM) \circ (PN) = (MP) \circ (NP) = (M \circ N)P$$

and therefore the commutant of P is Schur-closed. □

A permutation group Γ on a set V is *generously transitive* if, for each pair of points u and v in V, there is an element γ of Γ such that

$$u\gamma = v, \quad v\gamma = u.$$

Clearly a generously transitive permutation group is transitive.

1.3.3 Lemma. *The commutant of a permutation group is the Bose-Mesner algebra of a symmetric association scheme if and only if the group is generously transitive.*

Proof. Let Γ be a permutation group on V. The commutant of Γ is a coherent algebra, so we need only decide when it is commutative. We note Γ acts as a group of permutations of $V \times V$, and the orbits of Γ form a partition of this set. Each orbit is a directed graph, and the adjacency matrices of the orbits form a basis for the commutant of Γ.

The set

$$\{(v, v) : v \in V\},$$

known as the diagonal of $V \times V$, is a union of orbits of Γ, and is a single orbit if and only if Γ is transitive. Suppose u and v are distinct. Then uv and vu lie in the same orbit if and only if there is an element of Γ that swaps u and v.

Hence if Γ is transitive, then it is generously transitive if and only if all matrices in the commutant of Γ are symmetric. Since the product of two symmetric matrices A and B is symmetric if and only if $AB = BA$, the lemma follows. □

This lemma can be used to verify that the schemes $J(v,k)$, $J_q(v,k)$, $H(n,q)$ and $\mathrm{Mat}_{m\times n}(\mathbb{F})$ are symmetric, with the stated number of classes.

1.4 Idempotents

Let $\mathbb{C}[\mathscr{A}]$ be the Bose-Mesner algebra of the association scheme

$$\mathscr{A} = \{A_0, \dots, A_d\}.$$

The matrices $A_0, \dots, A_d$ form a basis, each element of which is a Schur idempotent. In this section we identify a second basis, consisting of matrix idempotents.

Two idempotents E and F are *orthogonal* if $EF = 0$. For example, if E is an idempotent, then E and $I - E$ are orthogonal idempotents. We define a partial ordering on the idempotents of a commutative algebra $\mathbb{C}[\mathscr{A}]$. Suppose E and F are idempotents in $\mathbb{C}[\mathscr{A}]$. We write $E \le F$ if $FE = E$. This relation is reflexive, antisymmetric and transitive; therefore it is a partial order. A *minimal idempotent* is a minimal element of the set of non-zero idempotents. If E and F are idempotents, then $EF \le E, F$; it follows that if E and F are minimal, then they are orthogonal.

1.4.1 Theorem. *Let $\mathscr{B}$ be a commutative matrix algebra with identity over an algebraically closed field. Assume that if $N \in \mathscr{B}$ and $N^2 = 0$, then $N = 0$. Then $\mathscr{B}$ has a basis of pairwise orthogonal idempotents.*

Proof. As a first step, we show that each element of $\mathscr{B}$ is a linear combination of idempotents.

Suppose $A \in \mathscr{B}$. Let $\psi(t)$ be the minimal polynomial of A and assume that

$$\psi(t) = \prod_{i=1}^{k} (t - \theta_i)^{m_i}.$$

If

$$\psi_i(t) := \frac{\psi(t)}{(t-\theta_i)^{m_i}},$$

then the polynomials $\psi_1, \dots, \psi_k$ are coprime, and therefore there are polynomials $f_1(t), \dots, f_k(t)$ such that

$$1 = \sum_i f_i(t)\psi_i(t).$$

Therefore

$$I = \sum_i f_i(A)\psi_i(A). \tag{1.4.1}$$

If $i \neq j$, then $\psi_i(A)\psi_j(A) = 0$ because ψ divides $\psi_i\psi_j$. Hence if we multiply both sides of (1.4.1) by $f_i(A)\psi_i(A)$, we find that

$$f_i(A)\psi_i(A) = (f_i(A)\psi_i(A))^2.$$

Thus $f_i(A)\psi_i(A)$ is an idempotent, which we denote by E_i. We note that $E_iE_j = 0$ if $i \neq j$. Since ψ divides $(t-\theta_i)^{m_i}\psi_i(t)$, we have

$$(A - \theta_i I)^{m_i} E_i = 0.$$

Consequently

$$[(A - \theta_i I)E_i]^{m_i} = 0,$$

and, given our hypothesis, it follows that $(A-\theta_i I)E_i = 0$. We may rewrite (1.4.1) as

$$I = E_1 + \cdots + E_k$$

and so

$$A = AE_1 + \cdots + AE_k = \theta_1 E_1 + \cdots + \theta_k E_k.$$

This expresses A as a linear combination of idempotents.

We have shown that $\mathscr{B}$ is spanned by idempotents. The essential problem that remains is to show that minimal idempotents exist. Suppose E and F are distinct idempotents and $E \le F$. Then

$$F(I-E) = F - E \neq 0$$

but $E(I-E) = 0$. Hence the column space of E must be a proper subspace of the column space of F. Therefore if $E_1, \ldots, E_m$ are distinct idempotents and

$$E_1 \le \cdots \le E_m$$

then $m \le n+1$. We conclude that minimal idempotents exist.

Now we prove that each idempotent is a sum of minimal idempotents. Suppose F is an idempotent and E is a minimal idempotent. If $EF \neq 0$, then $EF \le E$ and therefore $EF = E$. This also shows that distinct minimal idempotents are orthogonal. Let F_0 be the sum of the distinct minimal idempotents E such that $E \le F$. Then F_0 is an idempotent. If $F_0 \neq F$ then $F - F_0$ is an idempotent and so there is a minimal idempotent below it, which contradicts our choice of F_0. We conclude that $\mathscr{B}$ is spanned by minimal idempotents. □

Suppose $\mathscr{B}$ is a Schur-closed algebra that contains J over some field. Then 1.4.1 implies that $\mathscr{B}$ has a basis of 01-matrices. Of course this can be proved more directly (and with less effort).

A matrix N is nilpotent if $N^k = 0$ for some k. Theorem 1.4.1 asserts that a commutative matrix algebra with identity has a basis of orthogonal idempotents if there are no non-zero nilpotent matrices in it. Since a non-zero linear combination of pairwise orthogonal idempotents cannot be nilpotent, this condition is necessary too. A commutative algebra is *semisimple* if it contains no non-zero nilpotent elements.

1.5 Idempotents for Association Schemes

We will apply the theory of the last section to Bose-Mesner algebras.

1.5.1 Theorem. *Suppose $\mathscr{B}$ is a commutative subalgebra of $\mathrm{Mat}_{v\times v}(\mathbb{C})$ that is closed under conjugate transpose and contains the identity. Then $\mathscr{B}$ has a basis of matrix idempotents $E_0,\dots,E_d$ such that*

(a) $E_iE_j = \delta_{i,j}E_i$.

(b) The columns of E_i are eigenvectors for each matrix in $\mathbb{C}[\mathscr{A}]$.

(c) $\sum_{i=0}^{d} E_i = I$.

(d) $E_i^* = E_i$. □

Proof. Suppose $N \in \mathbb{C}[\mathscr{A}]$ and $N^2 = 0$. Then

$$0 = (N^*)^2N^2 = (N^*N)^2$$

and hence

$$0 = \mathrm{tr}((N^*N)^2) = \mathrm{tr}((N^*N)^*(N^*N)).$$

If $H := N^*N$, then $\mathrm{tr}(H^*H) = 0$ if and only if $H = 0$, so we deduce that $N^*N = 0$. But then $\mathrm{tr}(N^*N) = 0$ and therefore $N = 0$. Hence $\mathbb{C}[\mathscr{A}]$ satisfies the hypotheses of Theorem 1.4.1, and so it has a basis of pairwise orthogonal idempotents, which we denote by $E_0,\dots,E_d$. Thus (a) is proved.

If $A \in \mathbb{C}[\mathscr{A}]$, then

$$A = \sum_i a_iE_i$$

for suitable scalars a_i. Since the idempotents E_i are orthogonal,

$$AE_r = a_rE_r.$$

This shows that the columns of E_r are eigenvectors for A, and the scalars a_i are eigenvalues of A. So (c) is proved.

Since $I \in \mathbb{C}[\mathscr{A}]$, it is a linear combination of $E_0,\dots,E_d$:

$$I = \sum_i a_iE_i.$$

Since the scalars a_i are eigenvalues for I, they must all equal 1. Hence (d) holds.

Finally we show that the idempotents E_i are Hermitian. Since $\mathbb{C}[\mathscr{A}]$ is closed under transpose and complex conjugation, $E_i^* \in \mathbb{C}[\mathscr{A}]$. Therefore there are scalars $a_0,\dots,a_d$ such that

$$E_i^* = \sum_j a_jE_j$$

and so

$$E_i^* E_i = f_i E_i.$$

Since $\operatorname{tr}(E_i^* E_i) > 0$ and $\operatorname{tr}(E_j) > 0$, it follows that $f_i \neq 0$. But E_i^* is a minimal idempotent, and therefore $f_j = 0$ if $j \neq i$. This implies that E_i^* is a scalar multiple of E_i, but $\operatorname{tr}(E_i) = \operatorname{tr}(E_i^*)$, and therefore $E_i^* = E_i$. $\square$

This theorem applies immediately to the Bose-Mesner algebra of an association scheme. In this case $\frac{1}{v}J \in \mathscr{B}$; since this is an idempotent with rank one, it must be minimal and therefore it is equal to one of the idempotents E_i. It is conventional to assume it is E_0.

If A_i is Schur idempotent in $\mathscr{A}$, so is A_i^T. If E_j is a matrix idempotent, so is E_j^T (which is equal to $\overline{E}_j$). We adopt the useful convention that

$$A_{i'} := A_i^T$$

and

$$E_{j'} := E_j^T = \overline{E}_j.$$

Note that $v_{i'} = v_i$ and $m_{j'} = m_j$.

To give a better idea of the power of 1.4.1, we use it to derive one of the basic results in linear algebra. A complex matrix A is *normal* if $AA^* = A^* A$. We adopt the convention that the algebra generated by a set of matrices always contains the identity.

1.5.2 Theorem. *If A is normal, then A is unitarily similar to a diagonal matrix.*

Proof. The algebra generated by A and A^* is commutative and closed under conjugate-transpose. Hence it has a basis of orthogonal idempotents $F_1, \ldots, F_d$. Since each F_i is Hermitian, the condition $F_i F_j = 0$ implies the column spaces of F_i and F_i are orthogonal. If follows that there is an orthogonal basis of eigenvectors of A. $\square$

Notes

There a number of useful references for association schemes. Bannai and Ito [**?**], is the oldest of these, but carries its age well. It views the subject from a group theoretic viewpoint. Bailey's book [**?**] is more recent and views association schemes from the viewpoint of design theory. Since this is the origin of the subject, this is a very natural approach. We note that Bailey restricts herself to what we call symmetric association schemes; for design theory this is very natural. However it excludes the association schemes arising from the conjugacy classes of a finite group and as the only real cost in allowing non-symmetric schemes is the use of $\mathbb{C}$ rather than $\mathbb{R}$, and we have happily chosen to pay it.

Brouwer, Cohen and Neumaier's book on distance-regular graphs [**?**] offers a lot of information on association schemes. Zieschang [**?**] allows his association schemes to be infinite and/or non-commutative. For an algebraist this can be very interesting, but the resulting theory does not seem to have much contact with the combinatorial questions that we are interested in.

The classic source of information on association schemes (in the sense we use the term) is Delsarte's thesis [**?**]. A copy of this is available online at `http://users.wpi.edu/~martin/RESEARCH/philips.pdf`. One of Delsarte's main contributions was to demonstrate that the theory of association schemes provides an extremely useful framework for work in coding theory.

Chapter 2

Parameters

To each association scheme there are four associated families of parameters: the eigenvalues,the dual eigenvalues, the intersection numbers and the Krein parameters. We introduce these and present a few of their applications. We will see that the algebraic structure of an association scheme is entirely determined by its eigenvalues.

2.1 Eigenvalues

There are scalars $p_i(j)$ such that

$$A_i = \sum_{r=0}^{d} p_i(r) E_r, \qquad (i = 0, \dots, d) \tag{2.1.1}$$

and scalars $q_i(j)$ such that

$$E_j = \frac{1}{v} \sum_{r=0}^{d} q_j(r) A_r. \qquad (j = 0, \dots, d) \tag{2.1.2}$$

The scalars $p_i(j)$ are called the *eigenvalues* of the scheme. Since they are eigenvalues of the 01-matrices A_i, they are algebraic integers. Note that

$$A_i J = p_i(0) J$$

and therefore $p_i(0)$ is equal to the common value of the row sums of A_i. We define

$$v_i := p_i(0),$$

call $v_0, \dots, v_d$ the *valencies* of the scheme. Because $I = \sum_i E_i$, we also have $p_0(i) = 1$ for each i.

The eigenvalues of A_i^T are the numbers $\overline{p_i(j)}$, for $i = 0, 1, \dots, d$.

The scalars $q_i(j)$ are the *dual eigenvalues* of the scheme. Since

$$E_0 = \frac{1}{v} \sum_i A_i,$$

we have $q_0(i) = 1$. The columns of E_i are eigenvectors for each matrix in $\mathbb{C}[\mathscr{A}]$, and so its column space is an eigenspace for $\mathbb{C}[\mathscr{A}]$. The dimension of this eigenspace is the rank of E_i. Since E_i is an idempotent, all its eigenvalues are equal to 1 and

$$\operatorname{rk}(E_i) = \operatorname{tr}(E_i).$$

The quantities $\operatorname{tr}(E_i)$ are the *multiplicities* of the scheme. From refEA we have

$$\operatorname{tr}(E_i) = \frac{1}{v} \sum_i q_i(r) \operatorname{tr}(A_r).$$

Now $\operatorname{tr}(A_r) = 0$ if $r \neq 0$ and $\operatorname{tr}(A_0) = v$, so we find that

$$\operatorname{tr}(E_i) = q_i(0).$$

We use m_i to denote $\operatorname{tr}(E_i)$.

The *eigenmatrix* of $\mathbb{C}[\mathscr{A}]$ is the $(d+1) \times (d+1)$ matrix P given by

$$P_{i,j} = p_j(i).$$

The dual eigenmatrix Q is the $(d+1) \times (d+1)$ matrix Q given by

$$Q_{i,j} = q_j(i).$$

From 2.1.1 and 2.1.2, we have

$$PQ = vI.$$

One consequence of this is that the dual eigenvalues of $\mathbb{C}[\mathscr{A}]$ are determined by the eigenvalues. As we proceed we will see that much of the structure of an association scheme is determined by its eigenmatrix.

2.2 Strongly Regular Graphs

A graph X is *strongly regular* if it is neither complete nor empty and there are integers k, a and c such that:

(a) X is regular with valency k.

(b) Any two adjacent vertices have exactly a common neigbours.

(c) Any two distinct non-adjacent vertices have exactly c common neighbours.

If A is the adjacency matrix of X, these conditions are equivalent to the two matrix equations

$$AJ = kJ, \qquad A^2 = kI + aA + c(J - I - A).$$

It is usually better to write the second of these as

$$A^2 - (a - c)A - (k - c)I = cJ.$$

A strongly regular graph on v vertices with parameters k, a and c as above is called a $(v, k; a, c)$ strongly regular graph.

It is straightforward to use the above matrix equations to show that if A is the adjacency matrix of a strongly regular graph, then

$$I, A, J - I - A$$

form an association scheme with two classes. Conversely, any association scheme with two classes arises from a strongly regular graph.

Suppose A_1 is the adjacency matrix of a strongly regular graph X and $\mathscr{A}$ is the corresponding association scheme, with matrix idempotents E_0, E_1 and E_2. If X is k-regular, then

$$A_0 = E_0 + E_1 + E_2, \quad A_1 = kE_0 + \theta E_1 + \tau E_2.$$

This equations determine two columns of the eigenmatrix P. Since $A_2 = J - I - A_1$, we also have

$$A_2 = (v - 1 - k)E_0 - (\theta + 1)E_1 - (\tau + 1)E_2.$$

Therefore

$$P = \begin{pmatrix} 1 & k & v-1-k \\ 1 & \theta & -\theta-1 \\ 1 & \tau & -\tau-1 \end{pmatrix}$$

from which we compute that

$$Q = \frac{1}{\theta-\tau}\begin{pmatrix}\theta-\tau & -k-(v-1)\tau & k+(v-1)\theta\\ \theta-\tau & v-k+\tau & k-v-\theta\\ \theta-\tau & \tau-k & k-\theta\end{pmatrix}$$

The entries in the first row of Q give the multiplicities of the eigenvalues of the graph. One consequence of this is that the ratio

$$\frac{\theta(v-1)+k}{\theta-\tau}$$

must be an integer. Constraints of this form play a major role in the theory of distance-regular graphs.

2.3 Intersection Numbers

Suppose $\mathscr{A}$ is a scheme with d classes. Since $\mathbb{C}[\mathscr{A}]$ is closed under multiplication, there are constants $p_{i,j}(k)$ such that

$$A_iA_j = \sum_{k=0}^{d} p_{i,j}(k)A_k.$$

We call these the *intersection numbers* of the scheme. We see that

$$p_{i,j}(k)A_k = A_k \circ (A_iA_j),$$

from which it follows that the intersection numbers are non-negative integers. We see also that

$$p_{i,j}(k) = \frac{\operatorname{sum}(A_k\circ(A_iA_j))}{vv_k} = \frac{\operatorname{tr}(A_k^TA_iA_j)}{vv_k}. \tag{2.3.1}$$

We define the *intersection matrices* $B_0,\dots,B_d$ by

$$(B_i)_{j,k} := p_{i,j}(k).$$

If π denotes the relation partition of $V(\mathscr{A})$ with respect to v, then $B_i = A/\pi$. Hence the matrices $B_0,\dots,B_d$ generate a commutative algebra of $(d+1)\times(d+1)$ matrices which is isomorphic to $\mathbb{C}[\mathscr{A}]$ as an algebra. (However it is not Schur-closed in general.)

The intersection numbers are determined by the eigenvalues of the scheme. The eigenvalue of $A_k^T A_i A_j$ on the column space of E_ℓ is

$$p_i(\ell) p_j(\ell) \overline{p_k(\ell)}$$

whence 2.3.1 implies that

$$p_{i,j}(k) = \frac{1}{v v_k} \sum_{\ell=0}^{d} m_\ell p_i(\ell) p_j(\ell) \overline{p_k}(\ell).$$

Let $X_1, \ldots, X_d$ be the graphs of an association scheme. If X_i has diameter s then the matrices

$$A_i^0, \ldots, A_i^s$$

are linearly independent. (It might be easier to see that the first $s+1$ powers of $A_i + I$ are linearly independent.) Therefore the diameter of X_i is bounded above by d, the number of classes of the scheme.

An association scheme with d classes is *metric* with respect to the i-th relation if the diameter of X_i is d. If the scheme is metric with respect to the i-th relation, then X_i is said to be a *distance-regular graph*. The Johnson scheme, the Grassman scheme, the Hamming scheme and the bilinear forms scheme are all metric with respect to their first relation. A primitive strongly regular graph is primitive with respect to each non-identity relation. An association scheme may be metric with respect to more than one relation. The standard example is the Johnson scheme $J(2k+1, k)$, which is metric with respect to A_1 and A_k.

If $\mathscr{A}$ is metric with respect to A_i and $s \leq d$, then $(I + A_i)^s$ is a linear combination of exactly $s+1$ distinct Schur idempotents. It is customary to assume $i = 1$, and to order the Schur idempotents so that $(I + A_1)^s$ is a linear combination of $A_0, \ldots, A_s$. With this convention, the intersection matrix B_1 is tridiagonal.

2.4 Krein Parameters

We consider the parameters dual to the intersection numbers. Let $\mathscr{A}$ be a scheme on v vertices with d classes. Then there are constants $q_{i,j}(k)$ such that

$$E_i \circ E_j = \frac{1}{v} \sum_{k=0}^{d} q_{i,j}(k) E_k. \tag{2.4.1}$$

We call these constants the *Krein parameters* of the scheme. We have

$$q_{i,j}(k)E_k = vE_k(E_i \circ E_j)$$

and therefore

$$q_{i,j}(k) = v\frac{\operatorname{tr}(E_k(E_i \circ E_j))}{m_k} = v\frac{\operatorname{sum}(\overline{E}_k \circ E_i \circ E_j)}{m_k}$$

Now

$$\overline{E}_k \circ E_i \circ E_j = \frac{1}{v^3}\sum_{\ell=0}^{d} q_i(\ell)q_j(\ell)\overline{q_k(\ell)}A_\ell$$

which yields

$$q_{i,j}(k) = \frac{1}{vm_k}\sum_{\ell=0}^{d} q_i(\ell)q_j(\ell)\overline{q_k(\ell)}v_\ell = \frac{m_i m_j}{v}\sum_{\ell=0}^{d}\frac{\overline{p_\ell(i)}\,\overline{p_\ell(j)}p_\ell(k)}{v_\ell^2}.$$

(Here the second equality is derived using 2.3.1). We see that the Krein parameters are determined by the eigenvalues of the scheme.

If M is a square matrix and $p(t)$ a polynomial, we define the *Schur polynomial* $p \circ M$ to be the matrix with

$$(p \circ M)_{i,j} = p(M_{i,j}).$$

We define the *Schur diameter* of a matrix M to be the least integer s such that there is a polynomial p with degree s and $p \circ M$ is invertible. (If A is the adjacency matrix of a directed graph, the diameter of the graph is the least integer s such that there is a polynomial p of degree s and $p \circ A$ is Schur invertible.)

2.4.1 Lemma. *If E is a square matrix with Schur diameter s, the Schur powers*

$$J, E, \dots, E^{\circ s}$$

are linearly independent.

Proof. If $E^{\circ(r+1)}$ lies in the span U_r of the first r Schur powers of E, then U_r is invariant under Schur multiplication by E_r. Therefore U_r contains all Schur polynomials in E. If $r < s$, no Schur polynomial in E is invertible, which contradicts our hypothesis. It follows that spaces $U_0, \dots, U_s$ form a strictly increasing sequence, and this implies the lemma. □

Let $\mathscr{A}$ be an association scheme with d classes. If E_i is a matrix idempotent of $\mathscr{A}$ with Schur diameter s, then $s \le d$. We say $\mathscr{A}$ is *cometric* with respect to E_i if the Schur diameter of E_i is d. The Johnson scheme, the Grassman scheme, the Hamming scheme and the bilinear forms scheme are all cometric. A primitive strongly regular graph is primitive with respect to each non-identity idempotent. If $\mathscr{A}$ is cometric with respect to the idempotent E, then it is conventional to order the idempotents so that $E^{\circ r}$ is a linear combination of $E_0, \dots, E_r$.

In the following we make use of the Kronecker product of matrices. What we need is summarised in Section 4.1.

Examples show that the Krein parameters need not be non-negative integers, or even rational. We do have the following.

2.4.2 Theorem. *The Krein parameters are non-negative real numbers.*

Proof. From (2.4.1), we see that the Krein parameters are the eigenvalues of the matrix $vE_i \circ E_j$. The matrices E_i and E_j are positive semidefinite, and therefore $E_i \otimes E_j$ is a positive semidefinite matrix. The matrix $E_i \circ E_j$ is a principal submatrix of this Kronecker product, and therefore it is positive semidefinite too. Hence its eigenvalues are non-negative real numbers. □

We offer a second proof that the Krein parameters are non-negative real numbers.

Let $\mathscr{A}$ be an association scheme on v vertices and let $e_1, \dots, e_v$ denote the standard basis for $\mathbb{C}^v$. Define $\mathscr{T}$ by

$$\mathscr{T} = \sum_{i=1}^{v} e_i \otimes e_i \otimes e_i.$$

2.4.3 Lemma. *Let $\mathscr{A}$ be an association scheme. Then*

$$q_{i,j}(k) = \frac{v}{m_k} \|(E_i \otimes E_j \otimes E_{k'})\mathscr{T}\|^2,$$

and $q_{i,j}(k) = 0$ if and only if $(E_i \otimes E_j \otimes E_{k'})\mathscr{T} = 0$.

Proof. We have

$$\operatorname{sum}(E_i \circ E_j \circ E_k) = \mathscr{T}^*(E_i \otimes E_j \otimes E_k)\mathscr{T}.$$

Since $E_i \otimes E_j \otimes E_k$ is idempotent and self-adjoint,

$$\operatorname{sum}(E_i \circ E_j \circ E_k) = \|(E_i \otimes E_j \otimes E_k)\mathscr{T}\|^2.$$

Both claims of the lemma follow. □

If $q_{i,j}(k) = 0$, then $E_k(E_i \circ E_j) = 0$ and therefore each column of $E_{k'} = E_k^T$ is orthogonal to each column of $E_i \circ E_j$. We will need the following strengthening of this result.

2.4.4 Lemma. *Let $\mathscr{A}$ be an association scheme on v vertices. If $q_{i,j}(k) = 0$ and x, y and z are three elements of $\mathbb{C}^v$, then $E_{k'}z$ is orthogonal to $E_i x \circ E_j y$.*

Proof. We have

$$\mathscr{T}^*(E_i \otimes E_j \otimes E_{k'})(x \otimes y \otimes z) = \mathbf{1}^*(E_i x \circ E_j y \circ E_{k'} z).$$

The right side is zero if and only if $E_{k'}z$ is orthogonal to $E_i x \circ E_j y$. The left side is zero if $q_{i,j}(k) = 0$. □

Suppose $\mathscr{A}$ is cometric with respect to E_1. A *harmonic polynomial* of degree i is defined to be an element of the column space of E_i. A *polynomial function* of degree i is a linear combination of harmonic polynomials with degree at most i. The previous result implies that if f is a polynomial with degree 1 and g is a polynomial with degree i, then $f \circ g$ has degree at most $i+1$. Note that $f \circ g$ is just the usual product of functions.

2.5 The Frame Quotient

Let $\mathscr{A}$ be an association scheme with d classes on the vertex set v. Let e_u be the characteristic vector of the vertex u and let H be the matrix

$$H := (A_0 e_u, A_1 e_u, \cdots, A_d e_u).$$

Then H is the characteristic matrix of the relation partition relative to the vertex u, and an easy computation shows that the column space of V is A-invariant. Hence there are $(d+1) \times (d+1)$ matrices $B_0, \dots, B_d$ such that

$$A_r H = H B_r.$$

Since

$$A_r A_i e_u = \sum_{j=0}^{d} p_{r,i}(j) A_j e_u,$$

we find that

$$(B_r)_{i,j} = p_{r,j}(i).$$

The matrices B_r are the *intersection matrices* of the scheme. They form an algebra of $(d+1)\times(d+1)$ matrices isomorphic to the Bose-Mesner algebra of $\mathscr{A}$, because

$$B_r B_s = \sum_{i=0}^{d} p_{r,s}(i) B_i.$$

There are also matrices $F_0,\dots,F_d$ such that $E_r H = HF_r$ and

$$B_r = \sum_{i=0}^{d} p_r(i) F_i.$$

Since $E_r^2 = E_r$, we have $HF_r = HF_r^2$ and since the columns of H are linearly independent, it follows that F_r is an idempotent and

$$I = \sum_r F_r.$$

As $\operatorname{tr}(F_r)$ is a positive integer, this implies that $\operatorname{tr}(F_r)=1$ for all r. Therefore

$$\operatorname{tr}(B_{r'} B_s) = \sum_i p_{r'}(i) p_s(i) = \sum_i \overline{p_r(i)} p_s(i) = (P^* P)_{r,s}.$$

One consequence of this is that the entries of P^*P are integers.

2.5.1 Theorem. *Let P be the eigenmatrix of the association scheme $\mathscr{A}$, let p be a prime and let $\mathbb{F}$ denote $GF(p)$. Then $\mathbb{F}[\mathscr{A}]$ contains a non-zero nilpotent matrix if and only if p divides*

$$v^{d+1} \prod_{i=0}^{d} \frac{v_i}{m_i}.$$

Proof. Let $G = P^*P$ viewed as a matrix over $\mathbb{F}$. Suppose $M \in \mathbb{F}[\mathscr{A}]$ and $MH = HN$. By changing u if needed, we may assume that $MH \neq 0$. If $M^2 = 0$ then $HN^2 = 0$ and therefore $N^2 = 0$. Hence $(B_r N)^2 = 0$ for each r and so

$$\operatorname{tr}(B_{r'} N) = 0$$

for all r. Since N is an $\mathbb{F}$-linear combination of $B_0,\dots,B_d$, this implies that the null space of G is not zero.

Suppose conversely that the null space of G is not zero. If $Gx = 0$ where $x \neq 0$ and

$$N := \sum_r x_r B_r,$$

then $\mathrm{tr}(B_{r'}N) = 0$ for all r. Therefore $\mathrm{tr}(N^k) = 0$ when $k > 0$, and so N is nilpotent.

We conclude that $\mathbb{F}[\mathscr{A}]$ contains a nilpotent element if and only if $\det(G) = 0$ mod p. As we will see in Section 3.1,

$$P^* D_m P = v D_v$$

and therefore

$$\det(P^* P) = \det(v D_v) / \det(D_m).$$

The theorem follows immediately. □

The expression

$$v^{d+1} \prod_{i=0}^{d} \frac{v_i}{m_i}$$

is known as the *Frame quotient* of the scheme. It is known that for each k and any prime p,

$$|\{i : p^k | m_i\}| \le |\{i : p^k | v v_i\}|.$$

One consequence of the previous theorem is that $\mathbb{F}[\mathscr{A}]$ is semisimple if and only if the Frame quotient is not divisible by p, the characteristic of $\mathbb{F}$.

The Frame quotient of the Petersen graph is

$$1000 \frac{18}{20} = 900.$$

It is not a surprise that this quotient is a perfect square, since the following simple observation holds.

2.5.2 Lemma. *If the eigenvalues of an association scheme are integers, the Frame quotient is the square of an integer.* □

Notes

There is little to say about this section; our approach is straightforward and fairly standard. We have not addressed the problem of determining the parameters of an association scheme. The actual approach taken will depend on how the scheme is presented. If the scheme is the centralizer of a multiplicity free permutation representation of a group, then it may be possible to use character theory. In general though the problem is usually difficult for association schemes with more than three classes.

Chapter 3

An Inner Product

Here we find that the Bose-Mesner algebra of an association scheme is an inner product space. The inner product can be computed in two different ways, and both the matrix and the Schur idempotents form orthogonal bases relative to it. This leads immediately to one of the most important application of association schemes, namely the linear programming method developed by Delsarte [**?**].

3.1 An Inner Product

There is one important property of Bose-Mesner algebras still to be discussed. If $M, N \in \mathrm{Mat}_{m\times n}(\mathbb{C})$, we define

$$\langle M, N\rangle := \mathrm{tr}(M^* N).$$

As is well known, this is a complex inner product on $\mathrm{Mat}_{m\times n}(\mathbb{C})$. Note that

$$\langle N, M\rangle = \overline{\langle M, N\rangle}.$$

If $\mathrm{sum}(M)$ denotes the sum of the entries of the matrix M, then

$$\mathrm{tr}(M^* N) = \mathrm{sum}(\overline{M} \circ N)$$

and therefore

$$\langle M, N\rangle = \mathrm{sum}(\overline{M} \circ N).$$

It follows that the Bose-Mesner algebra of an association scheme $\mathscr{A}$ is an inner product space. If

$$\mathscr{A} = \{A_0, \dots, A_d\}$$

then $\mathscr{A}$ is an orthogonal set: if $i \neq j$, then $A_i \circ A_j = 0$ and therefore

$$\langle A_i, A_j \rangle = \operatorname{sum}(A_i \circ A_j) = 0.$$

Similarly if $i \neq j$, then $E_i E_j = 0$ and

$$\langle E_i, E_j \rangle = \operatorname{tr}(E_i^* E_j) = \operatorname{tr}(E_i E_j) = 0.$$

We have

$$\langle A_i, E_j \rangle = \operatorname{tr}(A_i^T E_j) = \operatorname{tr}(\overline{p_i(j)} E_j) = m_j \overline{p_i(j)}$$

and

$$\langle A_i, E_j \rangle = \operatorname{sum}(A_i \circ E_j) = q_j(i) v_i.$$

Hence we have the important relation:

$$\frac{q_j(i)}{m_j} = \frac{\overline{p_i(j)}}{v_i}. \tag{3.1.1}$$

We express this last identity in matrix terms. Let D_m be the $(d+1) \times (d+1)$ diagonal matrix with i-th diagonal entry equal to m_i and let D_v be the $(d+1) \times (d+1)$ diagonal matrix with i-th diagonal entry equal to v_i. Then 3.1.1 implies that

$$QD_m^{-1} = D_v^{-1} P^*$$

or equivalently that

$$Q = D_v^{-1} P^* D_m$$

Since $PQ = vI$, it also follows that

$$vD_v = P^* D_m P.$$

3.2 Orthogonal Projection

Now suppose $M \in \operatorname{Mat}_{v \times v}(\mathbb{C})$ and let $\widehat{M}$ denote the orthogonal projection of M onto $\mathbb{C}[\mathscr{A}]$. Then

$$\widehat{M} = \sum_{i=0}^{d} \frac{\langle A_i, M \rangle}{\langle A_i, A_i \rangle} A_i,$$

since $A_0, \ldots, A_d$ is an orthogonal basis for $\mathbb{C}[\mathscr{A}]$. But we also have

$$\widehat{M} = \sum_{j=0}^{d} \frac{\langle E_j, M \rangle}{\langle E_j, E_j \rangle} E_j.$$

This yields a new proof of the following important result, which I am ascribing to J. J. Seidel.

3.2.1 Theorem. *If the matrices* $A_0,\dots,A_d$ *form an association scheme on* v *vertices with idempotents* $E_0,\dots,E_d$ *and* $M\in \mathrm{Mat}_{v\times v}(\mathbb{C})$*, then*

$$\widehat{M}=\sum_{i=0}^{d}\frac{\langle A_i,M\rangle}{vv_i}A_i=\sum_{j=0}^{d}\frac{\langle E_j,M\rangle}{m_j}E_j.$$

Proof. We note that

$$\langle A_i,A_i\rangle=\mathrm{sum}(A_i\circ A_i)=\mathrm{sum}(A_i)=vv_i$$

and

$$\langle E_j,E_j\rangle=\mathrm{tr}(E_j)=m_j. \qquad \square$$

The way to view this result is that the first expression for $\widehat{M}$ gives us its entries, while the second gives us its eigenvalues. The set

$$\{i:1\le i\le d,\ \langle M,A_i\rangle\ne 0\}$$

is called the *degree set* of M, and its size is the *degree* of M. The set

$$\{i:1\le i\le d,\ \langle M,E_i\rangle\ne 0\}$$

is called the *dual degree set* of M, and its size if the *dual degree* of M.

3.3 Linear Programming

Suppose $\mathscr{A}$ is an association scheme with vertex set V and d classes. If C is a subset of V, its *degree set* if the set of integers i such that some pair of distinct vertices in C is i-related. (This usage is consistent with the usage introduced at the end of the previous section.) The degree set of C is a subset of $\{1,\dots,d\}$. If $R\subseteq\{1,\dots,d\}$, we call a subset C of V an R*-clique* if the degree set of C is contained in R. If thedegree set of C is disjoint from R, we call it an R*-coclique.* A clique in X_i is an $\{i\}$-clique.

Suppose y is the characteristic vector of an R-clique in $\mathscr{A}$ and $M=yy^T$. Then the projection $\widehat{M}$ of M onto the Bose-Mesner algebra of $\mathscr{A}$ satisfies

(a) $\widehat{M}\succcurlyeq 0$.

(b) If $i \notin R \cup \{0\}$, then $\widehat{M} \circ A_i = 0$.

Since

$$\widehat{M} = \sum_{i=0}^{d} \frac{y^T A_i y}{v v_i} A_i = \sum_{i=0}^{d} \frac{y^T E_i y}{m_i} E_i$$

we have

$$\operatorname{tr}(\widehat{M}) = \frac{y^T y}{v} = \frac{|C|}{v}$$

and

$$\operatorname{sum}(\widehat{M}) = \frac{y^T J y}{v} = \frac{|C|^2}{v}.$$

Accordingly

$$|C| = \frac{\operatorname{sum}(\widehat{M})}{\operatorname{tr}(\widehat{M})}.$$

We summarise our conclusions.

3.3.1 Theorem. *Let $\mathscr{A}$ be an association scheme with d classes and let C be an R-clique in it. Then*

$$|C| \le \max_M \frac{\operatorname{sum}(M)}{\operatorname{tr}(M)},$$

where M runs over the positive semidefinite matrices in $\mathbb{C}[\mathscr{A}]$ such that $M \circ A_i = 0$ if $i \notin R \cup \{0\}$. □

We next derive a bound on the size of an R-coclique. Let N be a matrix in $\mathbb{C}[\mathscr{A}]$ such that

(a) $N \succcurlyeq 0$.

(b) If $i \notin R \cup \{0\}$, then $N \circ A_i \le 0$.

Assume

$$N = \sum_i a_i A_i = \sum_i b_i E_i$$

and let x be the characteristic vector of an R-coclique S. If $i \in R$ then $x^T A_i x = 0$ and, if $i \notin R \cup \{0\}$, then $a_i x^T A_i x \le 0$. Consequently

$$x^T N x = \sum_i a_i x^T A_i x \le a_0 x^T x = a_0 |S|$$

and

$$x^T Nx = \sum_j b_j x^T E_j x \geq b_0 x^T E_0 x \geq \frac{b_0}{v}|S|^2.$$

Hence

$$|S| \leq v\frac{a_0}{b_0} = v\frac{\operatorname{tr}(N)}{\operatorname{sum}(N)}.$$

Thus we have the following. (Note that $\operatorname{tr}(N) = a_0 v$ and $\operatorname{sum}(N) = b_0 v$.)

3.3.2 Theorem. *Let $\mathscr{A}$ be an association scheme with d classes and let S be an R-coclique in it. Then*

$$|S| \leq \min_N v\frac{\operatorname{tr}(N)}{\operatorname{sum}(N)}$$

where N runs over the set of positive semidefinite matrices in $\mathbb{C}[\mathscr{A}]$ such that $N \circ A_i \leq 0$ if $i \notin R \cup \{0\}$.

From this theorem we also see that

$$\frac{v}{|S|} \geq \max_N \frac{\operatorname{sum}(N)}{\operatorname{tr}(N)}$$

where N runs over the set of positive semidefinite matrices in $\mathbb{C}[\mathscr{A}]$ such that $N \circ A_i \leq 0$. Hence the same inequality holds when N runs over the smaller set of positive semidefinite matrices in $\mathbb{C}[\mathscr{A}]$ such that $N \circ A_i = 0$ if $i \notin R \cup \{0\}$. It follows from Theorem 3.3.1 that if C is an R-clique, then

$$\frac{v}{|S|} \geq |C|.$$

Thus we have proved that if C is an R-clique and S is an R-coclique in $\mathscr{A}$, then

$$|C||S| \leq v. \tag{3.3.1}$$

This inequality is due to Delsarte. We offer an alternative derivation of it in Section 4.6.

If P is the matrix of eigenvalues of $\mathscr{A}$ and $a = (a_0, \dots, a_d)$, then the eigenvalues of the matrix $M = \sum_i a_i A_i$ are the entries of the vector Pa. Since

$$\operatorname{tr}(M) = va_0, \qquad \operatorname{sum}(M) = ve_0^T Pa,$$

we see that $|S|$ is bounded above by the value of the following linear program

$$\begin{aligned} \max e_0^T Pa \\ a_0 = 1, a_i = 0 \text{ if } i \in R \\ Pa \geq 0 \\ a \geq 0. \end{aligned}$$

Alternatively, suppose $b = (b_0, \dots, b_d)$. Then the entries of the matrix $N = \sum_j b_j E_j$ are the entries of the vector $P^{-1}b$. Since $PQ = vI$ and

$$\operatorname{sum}(N) = b_0, \qquad \operatorname{tr}(N) = e_0^T Qb,$$

we see that $|S|$ is bounded above by the reciprocal of the value of the linear program

$$\begin{aligned} \min e_0^T Qb \\ b \geq 0 \\ b_0 = 1, e_i^T Qb \leq 0 \text{ if } i \in R. \end{aligned}$$

In working with these linear programs, it can be useful to recall that $Q = D_v^{-1} P^* D_m$. If in the last linear program we replace the constraints $e_i^T Qb \leq 0$ by $e_i^T Qb = 0$, the resulting linear program is dual to the first.

3.4 Cliques and Cocliques

We use the theory of the previous section to derive some specific bounds. Let $\mathscr{A}$ be an association scheme on v vertices with d classes.

Suppose first that C is a 1-clique, that is, a clique in the graph X_1 with adjacency matrix A_1. We seek to use Theorem 3.3.1 to obtain an upper bound on $|C|$. If $M \in \mathbb{C}[\mathscr{A}]$ and $M \circ A_i = 0$ if $i \neq 0, 1$, then

$$M = aI + bA_1.$$

Hence

$$\frac{\operatorname{sum}(M)}{\operatorname{tr}(M)} = \frac{av + bvv_1}{av} = 1 + v_1 \frac{b}{a}.$$

Here v_1 is the valency of X_1, and want to choose a and b to maximise the last term, subject to the condition that $M \succcurlyeq 0$. Since our objective function depends only on the ratio b/a, we may assume $b = \pm 1$. If $b = -1$, then the least eigenvalue of $aI - A_1$ is $a - v_1$, and we maximise our objective function by taking $a = v_1$. The value of the objective function is 2. If $b = 1$ and the least eigenvalue of A_1 is τ, then the least eigenvalue of $aI + A_1$ is $a + \tau$ and we maximise our objective function by taking $a = -\tau$. This gives a bound

$$|C| \le 1 - \frac{v_1}{\tau}.$$

This bound is never less than 2, and so it is the linear programming bound on a 1-clique.

3.4.1 Lemma. *If X is a graph in an association scheme with valency k and least eigenvalue τ, then*

$$\omega(X) \le 1 - \frac{k}{\tau}. \qquad \square$$

By using Theorem 3.3.2, we can derive an upper bound on the size of a 1-coclique in a union of classes from an association scheme. Suppose A is the adjacency matrix of such a graph X with valency k, and that its least eigenvalue is τ. If $N := A - \tau I$, then $N \succcurlyeq 0$ and

$$\operatorname{tr}(N) = -v\tau, \qquad \operatorname{sum}(N) = vk - v\tau$$

By Theorem 3.3.2, this results in the bound

$$\alpha(X) \le \frac{v}{1 - \frac{k}{\tau}}.$$

This bound actually holds for all regular graphs. Note that here we did not need to solve the linear program in Theorem 3.3.2, any matrix which satisfies the conditions provides an upper bound.

We give an application of the inequality (3.3.1). Let $\mathscr{A}$ be the Hamming scheme $H(n, q)$. Let B_e denote the ball of radius e about the zero word in the Hamming graph. Then

$$\beta_e := |B_e| = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Any two words in B_e are at distance at most $2e$. If $R := \{2e+1, \dots, n\}$, then B_e is an R-coclique, while an R-clique is a code with minimum distance $2e+1$. So (3.3.1) yields that

$$|C| \le \frac{q^n}{\beta_e};$$

in coding theory this is the *sphere-packing bound*.

Note that if C is an R-clique and D is an R-coclique, then $|C \cap D| \le 1$. Hence if we could partition the vertex set V of $\mathscr{A}$ into disjoint copies of an R-coclique D, no code has more than one vertex in any cell of this partition and so we trivially get the bound $|C| \le |V|/|D|$. Suppose q is a prime power and the vertices of the Hamming scheme $H(n,q)$ are taken to be the vectors in $V(n,q)$. If D is an R-coclique and a subspace, then the cosets of D partition the vertices of $H(n,q)$ into copies of D and therefore any S-clique contains at most $q^n/|D|$ vertices. The above result enables us to derive the same bound, given only a single copy of D. From a coding theorist's viewpoint, association schemes provide a tool which enables us to extend results about linear codes to the general case. This crucial fact is due to Delsarte.

3.5 Feasible Automorphisms

Let $\mathscr{A}$ be an association scheme with d class on v vertices. Let P be a $v \times v$ permutation matrix. Then P is an automorphism of $\mathscr{A}$ if it commutes with each Schur idempotent A_i or equivalently if it commutes with each matrix in $\mathbb{C}[\mathscr{A}]$.

We derive a necessary condition for P to be an automorphism, due to G. Higman.

Let σ denote the permutation associated with P. Define $v_i(\sigma)$ to be the number of vertices u in the scheme such that u is i-related to u. Then

$$v_i(\sigma) = \operatorname{sum}(P \circ A_i).$$

We compute the projection $\widehat{P}$ of P onto $\mathbb{C}[\mathscr{A}]$:

$$\widehat{P} = \sum_{i=0}^{d} \frac{v_i(\sigma)}{v v_i} A_i = \sum_{i=0}^{d} \frac{\langle P, E_i \rangle}{m_i} E_i.$$

Therefore

$$\widehat{P} E_j = \sum_{i=0}^{d} \frac{v_i(\sigma)}{v v_i} p_i(j) E_j = \frac{\langle P, E_j \rangle}{m_j} E_j$$

and consequently

$$\langle P, E_j \rangle = \frac{m_j}{v} \sum_{i=0}^{d} \frac{p_i(j)}{v_i} v_i(\sigma).$$

We claim that if P is an automorphism, then $\langle P, E_j\rangle$ must be an algebraic integer. For since E_j is idempotent and Hermitian, we may write it as

$$E_j = UU^*$$

where U is a $v \times m_j$ matrix such that $U^*U = I$. Hence

$$\langle P, E_j\rangle = \operatorname{tr}(E_j P) = \operatorname{tr}(UU^*P) = \operatorname{tr}(U^*PU).$$

If P commutes with E_j, then

$$PUU^* = UU^*P$$

and therefore

$$PU = U(U^*PU).$$

This implies that the characteristic polynomial of U^*PU divides the characteristic polynomial of P, and therefore $\operatorname{tr}(U^*PU)$ is a sum of eigenvalues of P. Hence it is an algebraic integer.

We apply this theory to the Petersen graph. Suppose σ is an automorphism of this graph which maps each vertex to an adjacent vertex. Thus

$$v_0(\sigma) = 0,\ v_1(\sigma) = 10,\ v_2(\sigma) = 0.$$

The eigenvalues of the Petersen graph are -2, 1 and 3 with respective multiplicities 4, 5 and 1. If E_1 is the matrix idempotent associated to the eigenvalue 1 and A_1 is the adjacency matrix of the Petersen graph, then

$$\langle P, E\rangle = \frac{5}{10} \times \frac{1}{3} \times 10 = \frac{4}{3}.$$

Since $4/3$ is not an algebraic integer, we conclude that no automorphism of the Petersen graph maps each vertex to an adjacent vertex.

Suppose H is a projection that commutes with $\mathbb{C}[\mathscr{A}]$. Then the above argument yields that

$$\langle H, E_j\rangle = \frac{m_j}{v} \sum_{i=0}^{d} \frac{p_i(j)}{v_i} \langle H, A_i\rangle$$

is a non-negative integer. (The value of this observation is unclear, but in principle it could be used to show that certain equitable partitions do not exist.)

Notes

The observation that the Bose-Mesner algebra of an association scheme is an inner product space is surprising useful, and allows a comparatively easy approach to the linear programming method. Nonetheless the results in this chapter are all standard. The linear programming method was developed in [**?**] by Delsarte. The method developed in Section 3.5 is an unpublished idea of G. Higman, and is used in [**?**] to show that a Moore graph of diameter two and valency 57 cannot be vertex transitive.