# Spring 2023 Math 846

# Algebraic Combinatorics: Association Schemes
Paul Terwilliger

# Lecture 1

Our textbook is:

Bannai, Bannai, Ito, Tanaka. Algebraic Combinatorics. De Gruyter Series in Discrete Mathematics and Applications 5 (2021).

We will begin with Chapter 2. Chapter 1 is an elementary introduction, and mostly discusses special cases of the material in later chapters. Hopefully, we can cover Chapters 2–5.

In addition to the text, the following publications are handy references:

E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes.* Benjamin/Cummings, London, 1984.

A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs.* Springer-Verlag, Berlin, 1989.

W. Martin, H. Tanaka. Commutative association schemes. European J. Combin. 30 (2009) 1497–1525.

P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Suppl.* 10 (1973).

## 1 The definition of an association scheme

Let $X$ denote a nonempty finite set. We will speak of the Cartesian product $X \times X = \{(x, y)|x, y \in X\}$.

Recall the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ and integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.

**Definition 1.1.** For $d \in \mathbb{N}$, an *association scheme of class* $d$ is a sequence $\mathcal{X} = (X, \{R_i\}_{i=0}^d)$, where $X$ is a nonempty finite set, and $\{R_i\}_{i=0}^d$ are nonempty subsets of $X \times X$ such that:

(i) $R_0 = \{(x, x)|x \in X\}$;

(ii) $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$ (disjoint union);

(iii) for $0 \le i \le d$ there exists $i' \in \{0, 1, \dots, d\}$ such that $R_i^t = R_{i'}$, where

$$R_i^t = \{(y, x)|(x, y) \in R_i\};$$

(iv) for $0 \le i, j, k \le d$ there exists a natural number $p_{i,j}^k$ such that for all $(x, y) \in R_k$,

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

The elements of $X$ are called the *vertices* of $\mathcal{X}$. We call $R_i$ the $i^{\text{th}}$ *relation* of $\mathcal{X}$. The relation $R_0$ is called *trivial.* We call $p_{i,j}^k$ an *intersection number* of $\mathcal{X}$.

We mention two special cases of association schemes.

**Definition 1.2.** Referring to the association scheme $\mathcal{X}$ in Definition 1.1,

(i) $\mathcal{X}$ is *commutative* whenever

$$p^k_{i,j} = p^k_{j,i} \qquad (0 \leq i, j, k \leq d).$$

(ii) $\mathcal{X}$ is *symmetric* whenever

$$i' = i \qquad (0 \leq i \leq d).$$

**Lemma 1.3.** *A symmetric association scheme is commutative.*

*Proof.* Referring to Definition 1.1, assume that $\mathcal{X}$ is symmetric. For $0 \leq i, j, k \leq d$ we show that $p^k_{i,j} = p^k_{j,i}$. Pick $x, y \in X$ with $(x, y) \in R_k$. Then $(y, x) \in R^t_k = R_{k'} = R_k$.
Since $(x, y) \in R_k$,

$$p^k_{j,i} = |\{z \in X | (x, z) \in R_j \text{ and } (z, y) \in R_i\}|.$$

Since $(y, x) \in R_k$,

$$p^k_{i,j} = |\{z \in X | (y, z) \in R_i \text{ and } (z, x) \in R_j\}|.$$

For $z \in X$,

$$(x, z) \in R_j \text{ iff } (z, x) \in R_j \qquad (z, y) \in R_i \text{ iff } (y, z) \in R_i.$$

By these comments $p^k_{i,j} = p^k_{j,i}$. □

We give some examples of association schemes.

Consider a finite group $G$ acting on a set $X$. This action is called *transitive* whenever for all $x, y \in X$ there exists $g \in G$ such that $x^g = y$.

**Example 1.4.** Let $G$ denote a finite group acting transitively on a set $X$. Consider the action of $G$ on $X \times X$ such that

$$(x, y)^g = (x^g, y^g) \qquad g \in G, \quad x, y \in X.$$

Let $\{R_i\}^d_{i=0}$ denote the orbits of $G$ on $X \times X$, ordered such that $R_0 = \{(x, x) | x \in X\}$. Then $(X, \{R_i\}^d_{i=0})$ is an association scheme (not commutative in general).

*Proof.* We check the axioms in Definition 1.1.
(i), (ii) Clear.
(iii) For $0 \leq i \leq d$, $R^t_i$ is an orbit of $G$ on $X \times X$.
(iv) Let $0 \leq i, j, k \leq d$ and $(x, y) \in R_k$. We show that for $g \in G$, the following sets have the same size:

$$\{z \in X | (x, z) \in R_i \text{ and } (z, y) \in R_j\}, \tag{1}$$
$$\{w \in X | (x^g, w) \in R_i \text{ and } (w, y^g) \in R_j\}. \tag{2}$$

This holds because the map $z \mapsto z^g$ gives a bijection from (1) to (2). □

Consider a finite group $G$ acting on a set $X$. This action is called *generously transitive* whenever for all $x, y \in X$ there exists $g \in G$ such that $x^g = y$ and $y^g = x$.

**Example 1.5.** Referring to Example 1.4, the following are equivalent:

(i) the action of $G$ on $X$ is generously transitive;

(ii) for all $x, y \in X$ the ordered pairs $(x, y)$ and $(y, x)$ are in the same orbit of $G$ on $X \times X$;

(iii) the association scheme $(X, \{R_i\}_{i=0}^d)$ is symmetric.

*Proof.* Routine. □

**Example 1.6.** (Hamming association scheme $H(d, q)$). Fix integers $d, q \geq 1$. Fix a set $F$ with $|F| = q$. Define a set

$$X = F \times F \times \cdots \times F \qquad\qquad (d \text{ copies}).$$

For $x = (x_1, x_2, \ldots, x_d) \in X$ and $y = (y_1, y_2, \ldots, y_d) \in X$, define their *Hamming distance*

$$\partial(x, y) = |\{i | 1 \leq i \leq d, \;\; x_i \neq y_i\}|.$$

For $0 \leq i \leq d$ define

$$R_i = \{(x, y) | x, y \in X, \;\; \partial(x, y) = i\}.$$

Then $(X, \{R_i\}_{i=0}^d)$ is a symmetric association scheme, denoted $H(d, q)$.

*Proof.* This is a special case of Example 1.5, with $G$ defined as follows. Let $S_q$ denote the symmetric group on $F$, which consists of the permutations of $F$. Consider the direct sum $S = S_q \oplus S_q \oplus \cdots \oplus S_q$ ($d$ copies). Then $S$ acts on $X$ by permuting each copy of $F$. Next consider the symmetric group $S_d$. This group acts on $X$ by permuting the coordinates $1, 2, \ldots, d$. The group $G$ consists of the permutations of $X$ obtained by applying an element of $S$ followed by an element of $S_d$. The group $G$ is generously transitive on $X$. It is routine to check that $\{R_i\}_{i=0}^d$ are the orbits of $G$ on $X \times X$. □

# Lecture 2

**Example 1.7.** (Johnson association scheme $J(v, d)$). Fix integers $v, d \geq 1$ with $d \leq v/2$. Fix a set $V$ with $|V| = v$. Let the set $X$ consist of the subsets of $V$ that have cardinality $d$. For $0 \leq i \leq d$ define

$$R_i = \{(x, y) | x, y \in X, \;\; |x \cap y| = d - i\}.$$

Then $(X, \{R_i\}_{i=0}^d)$ is a symmetric association scheme, denoted $J(v, d)$.

*Proof.* This is a special case of Example 1.5, where $G = S_v$ is the symmetric group on $V$. The action of $G$ on $V$ induces an action of $G$ on $X$. The action of $G$ on $X$ is generously transitive. It is routine to check that $\{R_i\}_{i=0}^d$ are the orbits of $G$ on $X \times X$. □

**Example 1.8.** (Conjugacy classes of a finite group $G$). Let $G$ denote a finite group. Elements $x, y \in G$ are called *conjugate* whenever there exists $g \in G$ such that $gxg^{-1} = y$. Conjugacy is an equivalence relation, and the equivalence classes are called conjugacy classes. let $\{C_i\}_{i=0}^d$ denote the conjugacy classes, ordered such that $C_0 = \{\mathbf{1}\}$ (the identity element of $G$). Define $X = G$. For $0 \le i \le d$ define

$$R_i = \{(x, y) | x, y \in G, \;\; y^{-1}x \in C_i\}.$$

Then $(X, \{R_i\}_{i=0}^d)$ is a commutative association scheme.

*Proof.* We apply Example 1.4. The group $G$ acts on $X = G$ by left and right multiplication. The left action is $G \times X \to X, (g, x) \mapsto gx$. The right action is $G \times X \to X, (h, x) \mapsto xh^{-1}$. The two actions commute. Combining the two actions, we get an action of $G \oplus G$ on $X$ such that $(g, h)$ sends $x \mapsto gxh^{-1}$ for all $(g, h) \in G \oplus G$ and $x \in X$. The action of $G \oplus G$ on $X$ is transitive. Next we check that the orbits of $G \oplus G$ on $X \times X$ are $\{R_i\}_{i=0}^d$. Pick any $(x, y) \in X \times X$ and $(u, v) \in X \times X$ that are in the same orbit of $G \oplus G$. We show that $y^{-1}x$ and $v^{-1}u$ are conjugate. By assumption, there exists $(g, h) \in G \oplus G$ such that $gxh^{-1} = u$ and $gyh^{-1} = v$. We have

$$v^{-1}u = \big(gyh^{-1}\big)^{-1}\big(gxh^{-1}\big) = hy^{-1}g^{-1}gxh^{-1} = hy^{-1}xh^{-1}$$

so $y^{-1}x$ and $v^{-1}u$ are conjugate. Conversely, pick any $(x, y) \in X \times X$ and $(u, v) \in X \times X$ such that $y^{-1}x$ and $v^{-1}u$ are conjugate. We show that $(x, y)$ and $(u, v)$ are in the same orbit of $G \oplus G$ on $X \times X$. By assumption there exists $h \in G$ such that $v^{-1}u = hy^{-1}xh^{-1}$. Rearranging this equation, we obtain $uhx^{-1} = vhy^{-1}$; denote this common value by $g$. We have $gxh^{-1} = u$ and $gyh^{-1} = v$. Therefore $(g, h) \in G \oplus G$ sends $(x, y)$ to $(u, v)$. Consequently $(x, y)$ and $(u, v)$ are in the same orbit of $G \oplus G$ on $X \times X$. We have shown that $(X, \{R_i\}_{i=0}^d)$ is an association scheme. Next, we check that this association scheme is commutative. For $0 \le i, j, k \le d$ we show that $p_{i,j}^k = p_{j,i}^k$. Pick $(x, y) \in R_k$. Note that $xy^{-1}$ is conjugate to $y^{-1}x$, so $(y^{-1}, x^{-1}) \in R_k$. Consider the following sets:

$$\{z \in X | (x, z) \in R_i \text{ and } (z, y) \in R_j\}, \tag{3}$$

$$\{w \in X | (y^{-1}, w) \in R_j \text{ and } (w, x^{-1}) \in R_i\}. \tag{4}$$

The sets (3) and (4) have cardinality $p_{i,j}^k$ and $p_{j,i}^k$ respectively. These cardinalities are the same, because the map $z \mapsto z^{-1}$ gives a bijection from (3) to (4). We have shown that $(X, \{R_i\}_{i=0}^d)$ is commutative. □

**Problem 1.9.** Referring to the association scheme in Example 1.8, assume that $G$ is the symmetric group $S_n$. For small $n = 2, 3, 4, ..$ describe the conjugacy classes and find the intersection numbers.

**Problem 1.10.** Find the intersection numbers of the Hamming association scheme $H(2, 4)$. Show that $H(2, 4)$ contains four vertices that are mutually in relation one (4-clique). Construct an association scheme that has the same intersection numbers as $H(2, 4)$ and has no 4-clique. This association scheme is called the Shrikhande scheme.

**Problem 1.11.** (Cyclotomic association schemes, I). Let $\mathrm{GF}(q)$ denote a finite field with $q$ elements. Let $\mathrm{GF}(q)^*$ denote the multiplicative group. This group consists of the nonzero elements of $\mathrm{GF}(q)$, and the group operation is multiplication. It is known that $\mathrm{GF}(q)^*$ is cyclic; let $\omega$ denote a generator of $\mathrm{GF}(q)^*$. Define $X = \mathrm{GF}(q)$. Define $R_0 = \{(x,x)|x \in X\}$. For $1 \le i \le q-1$ define $R_i = \{(x,y)|x,y \in X, \;\; x-y=\omega^{i-1}\}$. Show that $(X, \{R_i\}_{i=0}^{q-1})$ is a commutative association scheme.

**Problem 1.12.** (Cyclotomic association schemes, II). We refer to Problem 1.11. Let $d$ denote a divisor of $q-1$ and define $r = (q-1)/d$. Let $H_r = \langle \omega^d \rangle$ denote the subgroup of $\mathrm{GF}(q)^*$ generated by $\omega^d$. Note that $|H_r| = r$. For $1 \le i \le d$ define the coset $C_i = \omega^{i-1}H_r$. For notational convenience, define the set $C_0 = \{0\}$. Define $X = \mathrm{GF}(q)$. Define $R_0 = \{(x,x)|x \in X\}$. For $1 \le i \le d$ define $R_i = \{(x,y)|x,y \in X, \;\; x-y \in C_i\}$. Show that $(X, \{R_i\}_{i=0}^{d})$ is a commutative association scheme.

# 2 The Bose-Mesner algebra

In this section we consider association schemes using linear algebra. We start with some notation.

Let $\mathbb{C}$ denote the field of complex numbers. Let $X$ denote a nonempty finite set. Let $M_X(\mathbb{C})$ denote the algebra over $\mathbb{C}$ consisting of the matrices that have rows and columns indexed by $X$ and all entries in $\mathbb{C}$. Let $I \in M_X(\mathbb{C})$ denote the identity matrix. The matrix $J \in M_X(\mathbb{C})$ has all entries 1. Let $A \in M_X(\mathbb{C})$. For $x, y \in X$ the $(x,y)$-entry of $A$ is denoted $A_{x,y}$ or $A(x,y)$. The transpose of $A$ is denoted $A^t$ or ${}^tA$. For $A, B \in M_X(\mathbb{C})$ define a matrix $A \circ B \in M_X(\mathbb{C})$ with $(x,y)$-entry $A_{x,y}B_{x,y}$ for $x, y \in X$. We call $A \circ B$ the *entrywise product* or *Hadamard product* of $A$ and $B$.

Let $\mathcal{X} = (X, \{R_i\}_{i=0}^{d})$ denote an association scheme. For $0 \le i \le d$ define $A_i \in M_X(\mathbb{C})$ that has entries

$$A_i(x,y) = \begin{cases} 1 & \text{if } \;(x,y) \in R_i; \\ 0 & \text{if } \;(x,y) \notin R_i \end{cases} \qquad\qquad x, y \in X.$$

We call $A_i$ the $i^{\text{th}}$ *associate matrix for* $\mathcal{X}$, or the *adjacency matrix of* $\mathcal{X}$ *for* $R_i$. In terms of these matrices, the conditions (i)–(iv) in Definition 1.1 become:

(i) $A_0 = I$;

(ii) $J = \sum_{i=0}^{d} A_i$;

(iii) for $0 \le i \le d$ there exists $i' \in \{0, 1, \ldots, d\}$ such that $A_i^t = A_{i'}$;

(iv) for $0 \le i, j \le d$ there exist natural numbers $p_{i,j}^k$ $(0 \le k \le d)$ such that

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

The scheme $\mathcal{X}$ is commutative if and only if

$$A_i A_j = A_j A_i \qquad (0 \le i \le d).$$

The scheme $\mathcal{X}$ is symmetric if and only if

$$A_i^t = A_i \qquad (0 \le i \le d).$$

By the above conditions (i)–(iv), the matrices $\{A_i\}_{i=0}^d$ form a basis for a subalgebra $\mathcal{M}$ of $M_X(\mathbb{C})$ that contains $J$ and is closed under transpose. Note that $\mathcal{M}$ is closed under Hadamard multiplication, because

$$A_i \circ A_j = \delta_{i,j} A_i \qquad (0 \le i, j \le d).$$

We call $\mathcal{M}$ the *adjacency algebra* of $\mathcal{X}$. If $\mathcal{X}$ is commutative, then we call $\mathcal{M}$ the *Bose-Mesner algebra* of $\mathcal{X}$.

Our next goal is to define adjacency algebras in a more abstract way.

**Lemma 2.1.** *Let $\mathcal{M}$ denote a nonzero subspace of the vector space $M_X(\mathbb{C})$. Assume that $\mathcal{M}$ is closed under Hadamard multiplication. Then $\mathcal{M}$ has a basis $\{A_i\}_{i=0}^d$ such that $A_i \circ A_j = \delta_{i,j} A_i$ for $0 \le i, j \le d$. This basis is unique up to permutation of $A_0, A_1, \ldots, A_d$.*

*Proof.* For $A \in \mathcal{M}$ define the support set

$$\mathrm{Sup}(A) = \{(x, y) | x, y \in X, \quad A_{x,y} \ne 0\}.$$

For nonzero $\alpha \in \mathbb{C}$ we have

$$\mathrm{Sup}(\alpha A) = \mathrm{Sup}(A).$$

For $A, B \in \mathcal{M}$ we have

$$\mathrm{Sup}(A \circ B) = \mathrm{Sup}(A) \cap \mathrm{Sup}(B).$$

For $A \in \mathcal{M}$, we say that $A$ is *minimal* whenever (i) $A \ne 0$; and (ii) there does not exist a nonzero $B \in \mathcal{M}$ such that $\mathrm{Sup}(B) \subsetneq \mathrm{Sup}(A)$. Assume that $A \in \mathcal{M}$ is minimal. Then for all $B \in \mathcal{M}$, either $\mathrm{Sup}(A) \subseteq \mathrm{Sup}(B)$ or $\mathrm{Sup}(A) \cap \mathrm{Sup}(B) = \emptyset$. For minimal elements $A, B \in \mathcal{M}$, either $\mathrm{Sup}(A) = \mathrm{Sup}(B)$ or $\mathrm{Sup}(A) \cap \mathrm{Sup}(B) = \emptyset$. For minimal elements $A, B \in \mathcal{M}$ such that $\mathrm{Sup}(A) = \mathrm{Sup}(B)$, there exists a nonzero $\alpha \in \mathbb{C}$ such that $B = \alpha A$; otherwise there exists a linear combination of $A, B$ that is nonzero and has its support properly contained in the common support of $A$ and $B$. For a minimal element $A \in \mathcal{M}$ the nonzero entries of $A$ are all the same; otherwise the previous assertion is contradicted with $B = A \circ A$. A minimal element $A \in \mathcal{M}$ is called *normalized* whenever its nonzero entries are equal to 1. Every minimal element of $\mathcal{M}$ is a scalar multiple of a normalized minimal element. Let $\{A_i\}_{i=0}^d$ denote an ordering of the normalized minimal elements of $\mathcal{M}$. By construction $A_i \circ A_j = \delta_{i,j} A_i$ for $0 \le i, j \le d$. Consequently $\{A_i\}_{i=0}^d$ are linearly independent. For $A \in \mathcal{M}$ we have

$$A \in \mathrm{Span}\{A_i | 0 \le i \le d, \quad \mathrm{Sup}(A_i) \subseteq \mathrm{Sup}(A)\}.$$

By these comments $\{A\}_{i=0}^d$ is a basis for the vector space $\mathcal{M}$. The uniqueness assertion is clear. $\square$

**Lemma 2.2.** *For $A \in M_X(\mathbb{C})$ the following are equivalent:*

(i) *the diagonal entries of $A$ are all the same;*

(ii) *$I \circ A$ is a scalar multiple of $I$.*

*Proof.* Routine. □

**Definition 2.3.** A subspace $\mathcal{M}$ of $M_X(\mathbb{C})$ is *homogeneous* whenever each $A \in \mathcal{M}$ satisfies the equivalent conditions (i), (ii) in Lemma 2.2.

**Proposition 2.4.** *Let $\mathcal{M}$ denote a subspace of the vector space $M_X(\mathbb{C})$ that satisfies* (i)–(v) *below:*

(i) *$I, J \in \mathcal{M}$;*

(ii) *$\mathcal{M}$ is closed under matrix multiplication;*

(iii) *$\mathcal{M}$ is closed under Hadamard multiplication;*

(iv) *$\mathcal{M}$ is closed under the transpose map;*

(v) *$\mathcal{M}$ is homogeneous.*

*Then there exists an association scheme $\mathfrak{X} = (X, \{R_i\}_{i=0}^d)$ that has adjacency algebra $\mathcal{M}$. Also, $\mathfrak{X}$ is commutative if and only if $AB = BA$ for all $A, B \in \mathcal{M}$. Moreover, $\mathfrak{X}$ is symmetric if and only if $A^t = A$ for all $A \in \mathcal{M}$.*

*Proof.* Since $\mathcal{M}$ is closed under Hadamard multiplication, by Lemma 2.1 there exists a basis $\{A_i\}_{i=0}^d$ for $\mathcal{M}$ such that $A_i \circ A_j = \delta_{i,j} A_i$ for $0 \le i, j \le d$. Since $\mathcal{M}$ contains $J$, we have $J = \sum_{i=0}^d A_i$. Since $\mathcal{M}$ is homogeneous and contains $I$, we see that one of the matrices $\{A_i\}_{i=0}^d$ must equal $I$; without loss we many assume that $A_0 = I$. Since $\mathcal{M}$ is closed under the transpose map, $\mathcal{M}$ contains the matrices $\{A_i^t\}_{i=0}^d$. Observe that the matrices $\{A_i^t\}_{i=0}^d$ form a basis for $\mathcal{M}$, and satisfy $A_i^t \circ A_j^t = \delta_{i,j} A_i^t$ for $0 \le i, j \le d$. By the uniqueness assertion in Lemma 2.1, the sequence $\{A_i^t\}_{i=0}^d$ is a permutation of the sequence $\{A_i\}_{i=0}^d$. In other words, for $0 \le i \le d$ there exists $i' \in \{0, 1, \ldots, d\}$ such that $A_i^t = A_{i'}$. Since $\mathcal{M}$ is closed under matrix multiplication, for $0 \le i, j \le d$ there exist scalars $p_{i,j}^k \in \mathbb{C}$ $(0 \le k \le d)$ such that

$$A_i A_j = \sum_{k=0}^d p_{i,j}^k A_k.$$

For $0 \le k \le d$ we have $p_{i,j}^k \in \mathbb{N}$ because the nonzero entries of $A_i, A_j, A_k$ are equal to 1. For $0 \le i \le d$ define

$$R_i = \{(x, y) | A_i(x, y) = 1\}.$$

By the above comments, the sequence $(X, \{R_i\}_{i=0}^d)$ is an association scheme, with associate matrices $\{A_i\}_{i=0}^d$ and adjacency algebra $\mathcal{M}$. The assertions about commutativity and symmetry are clear. □

# 3 Commutative association schemes

Throughout this section, we assume that $\mathcal{X} = (X\{R_i\}_{i=0}^d)$ is a commutative association scheme. By assumption,

$$p_{i,j}^k = p_{j,i}^k \qquad (0 \leq i, j, k \leq d).$$

Recall that for $x, y \in X$ and $0 \leq i \leq d$,

$$(x, y) \in R_i \text{ iff } (y, x) \in R_{i'}.$$

For $x \in X$ and $0 \leq i \leq d$ define

$$\Gamma_i(x) = \{y \in X | (x, y) \in R_i\}.$$

For $0 \leq i, j, k \leq d$ and $(x, y) \in R_k$,

$$p_{i,j}^k = |\Gamma_i(x) \cap \Gamma_{j'}(y)|.$$

Define

$$k_i = p_{i,i'}^0 \qquad (0 \leq i \leq d). \tag{5}$$

For $x \in X$,

$$k_i = |\Gamma_i(x)| \qquad (0 \leq i \leq d).$$

**Lemma 3.1.** *We have*

(i) $k_0 = 1$;

(ii) $k_i = k_{i'} \qquad (0 \leq i \leq d)$;

(iii) $|X| = \sum_{i=0}^d k_i$.

*Proof.* Routine. □

**Proposition 3.2.** *We have*

(i) $p_{i,0}^k = \delta_{i,k} \qquad (0 \leq i, k \leq d)$;

(ii) $p_{0,j}^k = \delta_{j,k} \qquad (0 \leq j, k \leq d)$;

(iii) $p_{i,j}^0 = \delta_{i,j'} k_i \qquad (0 \leq i, j \leq d)$;

(iv) $p_{i,j}^k = p_{i',j'}^{k'} \qquad (0 \leq i, j, k \leq d)$;

(v) $k_i = \sum_{j=0}^d p_{i,j}^k \qquad (0 \leq i, k \leq d)$;

(vi) $k_\ell p_{i,j}^\ell = k_i p_{\ell,j'}^i = k_j p_{i',\ell}^j \qquad (0 \leq i, j, \ell \leq d)$;

(vii) $\sum_{\alpha=0}^{d} p^{\alpha}_{i,j} p^{\ell}_{k,\alpha} = \sum_{\alpha=0}^{d} p^{\alpha}_{k,i} p^{\ell}_{\alpha,j} \qquad (0 \le i,j,k,\ell \le d)$.

*Proof.* (i)–(iv) Routine.
(v) Fix $(x, y) \in R_k$. Partition $\Gamma_i(x)$ according to how its elements are related to $y$. This gives

$$\Gamma_i(x) = \cup_{j=0}^{d} (\Gamma_i(x) \cap \Gamma_{j'}(y)) \qquad \text{(disjoint union)}.$$

In this equation, take the cardinality of each side.
(vi) The three common values are equal to $|X|^{-1}$ times the number of 3-tuples $(x, y, z)$ such that $(x, y) \in R_\ell$ and $(x, z) \in R_i$ and $(z, y) \in R_j$.
(vii) In the equation $A_k(A_i A_j) = (A_k A_i)A_j$, write each side as a linear combination of $\{A_\ell\}_{\ell=0}^{d}$, and compare coefficients. □

As we study the Bose-Mesner algebra of $\mathcal{X}$, we will use the following linear algebra result.

**Lemma 3.3.** *Let $\mathcal{M}$ denote a nonzero subspace of the vector space $M_X(\mathbb{C})$. Assume that:*

(i) *$\mathcal{M}$ is closed under matrix multiplication;*

(ii) *$AB = BA$ for all $A, B \in \mathcal{M}$;*

(iii) *$\mathcal{M}$ is closed under the conjugate-transpose map.*

*Then $\mathcal{M}$ has a basis $\{E_i\}_{i=0}^{d}$ such that $E_i E_j = \delta_{i,j} E_i$ for $0 \le i, j \le d$. This basis is unique up to permutation of $E_0, E_1, \ldots, E_d$.*

*Proof.* □

**Definition 3.4.** Referring to Lemma 3.3, we call $\{E_i\}_{i=0}^{d}$ the *primitive idempotents* of $\mathcal{M}$.

**Lemma 3.5.** *For the subspace $\mathcal{M}$ in Lemma 3.3, its primitive idempotents satisfy $\overline{E}_i^t = E_i$ for $0 \le i \le d$.*

*Proof.* The subspace $\mathcal{M}$ contains $\overline{E}_i^t$ for $0 \le i \le d$. The matrices $\{\overline{E}_i^t\}_{i=0}^{d}$ form a basis for $\mathcal{M}$, and $\overline{E}_i^t \overline{E}_j^t = \delta_{i,j} \overline{E}_i^t$ for $0 \le i, j \le d$. By the uniqueness statement in Lemma 3.3, the sequence $\{\overline{E}_i^t\}_{i=0}^{d}$ is a permutation of the sequence $\{E_i\}_{i=0}^{d}$. For $0 \le i \le d$ we have $\overline{E}_i^t E_i \ne 0$, so $\overline{E}_i^t = E_i$. □

**Lemma 3.6.** *We refer to the subspace $\mathcal{M}$ in Lemma 3.3.*

(i) *Assume that $I \in \mathcal{M}$. Then $I = \sum_{i=0}^{d} E_i$.*

(ii) *Assume that $J \in \mathcal{M}$. Then $|X|^{-1}J$ is a primitive idempotent of $\mathcal{M}$ (denoted $E_0$).*

(iii) *Assume that $\mathcal{M}$ is closed under both the transpose map and complex conjugation. Then for $0 \le i \le d$ there exists $\hat{i} \in \{0, 1, \ldots, d\}$ such that $E_i^t = E_{\hat{i}} = \overline{E}_i$.*

*Proof.* (i) There exists scalars $\{\alpha_i\}_{i=0}^d$ in $\mathbb{C}$ such that $I = \sum_{i=0}^d \alpha_i E_i$. For $0 \le i \le d$ we have

$$E_i = E_i I = E_i \sum_{j=0}^d \alpha_j E_j = \alpha_i E_i,$$

so $\alpha_i = 1$.
(ii) There exists scalars $\{\beta_i\}_{i=0}^d$ in $\mathbb{C}$ such that $J = \sum_{i=0}^d \beta_i E_i$. At least one of $\{\beta_i\}_{i=0}^d$ is nonzero. Without loss, we may assume $\beta_0 \neq 0$. We have $JE_0 = \beta_0 E_0$. Note that $J^2 = |X|J$, so

$$JE_0 = |X|^{-1} J^2 E_0 = |X|^{-1} JE_0 J = |X|^{-1} sJ,$$

where $s$ is the sum of all the entries of $E_0$. By these comments $E_0$ is a scalar multiple of $J$. Using $E_0^2 = E_0$ we obtain $E_0 = |X|^{-1} J$.
(iii) The subspace $\mathcal{M}$ contains $E_i^t$ for $0 \le i \le d$. The matrices $\{E_i^t\}_{i=0}^d$ form a basis for $\mathcal{M}$ such that $E_i^t E_j^t = \delta_{i,j} E_i^t$ for $0 \le i, j \le d$. By the uniqueness statement in Lemma 3.3, the sequence $\{E_i^t\}_{i=0}^d$ is a permutation of the sequence $\{E_i\}_{i=0}^d$. In other words, for $0 \le i \le d$ there exists $\hat{i} \in \{0, 1, \ldots, d\}$ such that $E_i^t = E_{\hat{i}}$. By Lemma 3.5 we have $\overline{E}_i = E_i^t = E_{\hat{i}}$. □

We return our attention to the commutative association scheme $\mathcal{X} = (X, \{R_i\}_{i=0}^d)$.

**Proposition 3.7.** *The Bose-Mesner algebra* $\mathcal{M}$ *of* $\mathcal{X}$ *has a basis* $\{E_i\}_{i=0}^d$ *that satisfies*

(i) $E_0 = |X|^{-1} J$;

(ii) $E_i E_j = \delta_{i,j} E_i$ *for* $0 \le i, j \le d$;

(iii) $I = \sum_{i=0}^d E_i$;

(iv) *for* $0 \le i \le d$ *there exists* $\hat{i} \in \{0, 1, \ldots, d\}$ *such that* $E_i^t = E_{\hat{i}} = \overline{E}_i$.

*Proof.* Note that $\mathcal{M}$ satisfies the conditions of Lemma 3.3 and Lemma 3.6. □

The matrices $\{E_i\}_{i=0}^d$ form a basis for $\mathcal{M}$. Since $\mathcal{M}$ is closed under Hadamard multiplication, for $0 \le i, j \le d$ there exist $q_{i,j}^k \in \mathbb{C}$ $(0 \le k \le d)$ such that

$$E_i \circ E_j = |X|^{-1} \sum_{k=0}^d q_{i,j}^k E_k. \tag{6}$$

The scalars $q_{i,j}^k$ are called the *Krein parameters* of $\mathcal{X}$. Shortly we will show that $q_{i,j}^k$ is real and nonnegative for $0 \le i, j, k \le d$.