This preliminary chapter introduces the objects with which we will be working. We intend to move briskly, so only references to proofs and more in-depth discussions will be given. The following sections will define in turn: balanced incomplete block designs, error-correcting codes, weighing matrices and their generalizations, and finally association schemes.

§1. Balanced Incomplete Block Designs

This section presents some basic definitions and results about block designs that will be used throughout this work. Particular emphasis will be placed on matrix representations of such objects.

* * *

1.1. Definition and Necessary Conditions. A block design is simply a collection of subsets of a finite point set such that the points are regularly distributed amoungst the subsets in question. There are numerous directions to take with this vague understanding, but we only require the following.

1.1. Definition. Let X be a set of order v, called the set of varieties; and let $\mathscr{B} \subset \binom{X}{k}$, called the set of blocks, have order b. The ordered pair $\mathbf{D} = (X, \mathscr{B})$ is a *balanced incomplete block design* (henceforth BIBD) if there is a positive integer λ such that each 2-subset of varieties appears in λ blocks of $\mathscr{B}$.

The conditions placed on a finite set and a collection of its subsets in order to form a BIBD are quite strong, and we have at once the following result which can be shown using the elementary techniques of double counting (see **?**, for an abstract discussion).

1.2. Proposition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD with $|X| = v$, and $\mathscr{B} \subset \binom{X}{k}$ for which $|\mathscr{B}| = b$. Then:

(1.2.a) Every point of X occurs in $r = \frac{\lambda(v-1)}{k-1}$ blocks, and

(1.2.b) there are $b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)}$ blocks in $\mathscr{B}$.

1.3. Corollary. For the parameters v, k, λ of a BIBD, it must hold that

(1.3.a) $\lambda(v-1) \equiv 0 \bmod (k-1)$, and

(1.3.b) $\lambda v(v-1) \equiv 0 \bmod k(k-1)$.

If $\mathbf{D} = (X, \mathscr{B})$ is a BIBD with the parameters shown above, then we denote this property as BIBD(v, b, r, k, λ). As we have seen, however, the parameters b and r are expressible in terms of v, k, and λ; hence, we will usually shorten the denotation to BIBD(v, k, λ) whenever no confusion will arise.

Corollary **??** imposes some necessary conditions on the parameters of a BIBD. Our next result, due to **?**, is a strong necessary condition relating the number of points to the number of blocks of a BIBD, and it has far reaching consequences in the applications of designs to fields like statistics.

This most important result admits several interesting derivations employing techniques ranging from determinants to variance counting [1]).

1.4. Fisher's Inequality. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ). It follows that

(1.4.a) $b \geq v$.

The extremal case of Fisher's inequality is naturally very interesting and important. We single this case out thus.

1.5. Definition. Let $\mathbf{D} = (X, \mathscr{B})$ be some BIBD(v, b, r, k, λ). If $v = b$ (equiv. $k = r$), then we say that $\mathbf{D}$ is a *symmetric* balanced incomplete block design, or simply symmetric.

* * *

1.2. Related Configurations. Thus far, we have been thinking of designs strictly as subsets of some finite set. We can, however, broaden our view to include the following tool, and in so doing the theory of linear algebra can be brought to bear on the subject.

1.6. Definition. Let $\mathbf{D} = (\{x_0, \ldots, x_{v-1}\}, \{B_0, \ldots, B_{b-1}\})$ be a BIBD(v, b, r, k, λ), and let A be a $v \times b$ $(0,1)$-matrix defined by

$$\text{(1.6.a)}\quad A_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j, \text{ and} \\ 0 & \text{if } x_i \notin B_j. \end{cases}$$

We call A the *incidence matrix* of the design.

The next result is immediate. Note that we use I_n and J_n to denote the identity matrix and the all ones matrix, respectively, of n rows and n columns. Similarly, $\mathbf{1}_n$ and $\mathbf{0}_n$ will denote the column with n ones and the column with n zeros. For simplicity, the indices will at times be omitted.

1.7. Proposition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ), and let A be a $v \times b$ $(0,1)$-matrix. Then A is the incidence matrix of the design if and only if the following hold.

(1.7.a) $AA^t = rI_v + \lambda(J_v - I_v)$, and

(1.7.b) $\mathbf{1}_v^t A = k\mathbf{1}_b^t$.

As balanced incomplete block designs can more generally be regarded as finite incidence structures [2]), there can be related a number of further such objects. For our purposes, we will be interested in the following.

1.8. Definition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD, and let $B \in \mathscr{B}$. Then the *complement design* $\mathfrak{C}(\mathbf{D})$ is the pair $(X, \binom{X}{k} \backslash \mathscr{B})$. If $\mathbf{D}$ is symmetric, we have that the *derived design* $\mathfrak{D}(\mathbf{D})$ is the pair $(B_0, \{B \cap B_0 : B \in \mathscr{B} \text{ and } B \neq B_0\})$, and the *residual design* $\mathfrak{R}(\mathbf{D})$ is the pair $(X \backslash B_0, \{B - B_0 : B \in \mathscr{B} \text{ and } B \neq B_0\})$. When convenient, we will simply denote the complement, derived, and residual designs as $\mathfrak{C}$, $\mathfrak{D}$, and $\mathfrak{R}$, respectively.

The following result shows why, in part, these substructures are interesting.

1.9. Proposition. Let $\mathbf{D} = (X, \mathscr{B})$ be a BIBD(v, b, r, k, λ). Then

(1.9.a) $\mathfrak{C}$ is a BIBD$(v, b, b - r, v - k, b - 2r + \lambda)$.

If $\mathbf{D}$ is symmetric, then we further have that

(1.9.b) $\mathfrak{D}$ is a BIBD$(k, b - 1, k - 1, \lambda, \lambda - 1)$, and

(1.9.c) $\mathfrak{R}$ is a BIBD$(v - k, b - 1, k, k - \lambda, \lambda)$.

* * *

1.3. Isomorphisms of Designs. We conclude this section by briefly discussing isomorphisms of designs.

1.10. Definition. Let $\mathbf{D}_1 = (X_1, \mathscr{B}_1)$ and $\mathbf{D}_2 = (X_2, \mathscr{B}_2)$ be two BIBDs with the same parameters, and let $f : X_1 \to X_2$ be some bijection. If $f(\mathscr{B}_1) = f(\mathscr{B}_2)$, then we say that f is an *isomorphism* and that the two designs are *isomporhic*. For the case in which $\mathbf{D}_1 = \mathbf{D}_2$, we say that f is an *automorphism*. The collection of all automorphisms of a design $\mathbf{D}$ forms a group under composition called the *automorphism group* of the design.

In practice, one is usually concerned with the actions of isomorphisms on the incidence matrices of designs. In particular, two BIBD(v, b, r, k, λ)s with incidence matrices A_1 and A_2 are isomorphic if and only if there is a permutation matrix P of order v and a permutation matrix Q of order b such that

(1.10.a) $PA_1Q = A_2$ [3]).

1.11. Definition. As nothing essential is changed under the action of an isomorphism, one can then assume that the incidence matrix of a square design has the following form

(1.11.a) $$\begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}.$$

We will say that such an incidence matrix is in *normal form*.

* * *

§2. Error-Correcting Codes

In this section, the definitions of linear error-correcting codes will be given. We then move on to consider the famous generalized Hamming and simplex codes. As these are the only family of codes that we require, this section will be brief. The interested reader is refered to the standard references of **?** and **?** for a greater exposition of the subject.

* * *

2.1. Defintions. In essence a code is simply a finite collection of words over a given finite alphabet. There are many ways to formalize such a concept; for instance, we may consider a code to be a subset of functions from one finite set into another.

For the purposes at hand, however, we are interested in the case the alphabet is endowed with arithmetic sufficient to form a field in which case we may consider the code to be a linear subspace of an extension of the alphabet.

2.1. Definition. Let $H = (A \mid I_{n-k})$ be an $(n-k) \times n$ matrix over GF(q). The *linear code* $\mathscr{C}$ with parity check matrix H is given by $\mathscr{C} = \text{Null}(H) = \{x \in \text{GF}(q^n) : Hx^t = 0\}$, where the extension GF$(q^n)$ is interpreted here as a linear space over GF(q). We say that $\mathscr{C}$ is a linear $[n,k]_q$-code, where clearly $\dim(\mathscr{C}) = k$.

We have defined a linear code by its parity check matrix. An equivalent definition is to use the so-called *generator matrix* G. If $H = (A \mid I_{n-k})$ is the parity check matrix of the code, then $G = (I_k \mid -A^t)$. The code is then given by the linear span of the rows of G. Note that by construction, it follows that $GH^t = HG^t = O$.

The dual of a linear code $\mathscr{C}$ is given in the usual way by $\mathscr{C}^\perp = \{x \in \text{GF}(q^n) : xy^t = 0, \text{for every } y \in \mathscr{C}\}$. If H and G are the parity check and generator matrices of $\mathscr{C}$, then G and H are the parity check and generator matrices of $\mathscr{C}^\perp$, respectively.

In Definition **??**, there are two parameters explicitly given of a code, namely, the length n of the codewords and the dimension k of the linear space consisting of the codewords. Two more fundamental parameters for us are the minimum distance and the minimum weight defined thus.

2.2. Definition. Let $\mathscr{C}$ be a linear $[n,k]_q$-code, and let $x = x_0 \cdots x_{n-1}$ and $y = y_0 \cdots y_{n-1}$ be any two codewords of $\mathscr{C}$. Then:

(2.2.a) The *Hamming weight* of x is $\text{wt}(x) = \#\{i : x_i \neq 0\}$;

(2.2.b) the *Hamming distance* between x and y is $\text{dist}(x,y) = \#\{i : x_i \neq y_i\}$;

(2.2.c) the *minimum weight* of the code is $\text{wt}(\mathscr{C}) = \min_{x \in \mathscr{C} \setminus \{0\}} \text{wt}(x)$; and

(2.2.d) the *minimum distance* of the code is $\text{dist}(\mathscr{C}) = \min_{\substack{x,y\in\mathscr{C}\\ x\neq y}} \text{dist}(x,y)$.

If we wish to emphasize the distance $d = \text{dist}(\mathscr{C})$ of a code, we write $[n,k,d]_q$-code.

The Hamming distance can easily be seen to form a metric [4]) on GF(q^n). The next result is then clear (see **?**, Theorem 1.9).

2.3. Proposition. If $\mathscr{C}$ is any $[n,k,d]_q$-code, then

(2.3.a) for every $x, y \in \mathscr{C}$, it holds that $\text{dist}(x,y) = \text{wt}(x-y)$, hence $\text{dist}(\mathscr{C}) = \text{wt}(\mathscr{C})$.

* * *

2.2. The Hamming and Simplex Codes. The theory of error-correcting codes began with the seminal paper of Richard W. Hamming (**?**) who introduced redundancy for the purpose of error correction. In this paper, he also constructed a most useful family of codes aptly called the *Hamming codes*. The codes constructed by Hamming were binary; however, it is a simple matter to extend the construction to an arbitrary finite field.

2.4. Definition. Let H be the $n \times (q^n-1)/(q-1)$ matrix over GF(q) whose columns are representatives of the nonzero 1-dimensional subspaces of the extension field GF(q^n) over GF(q). The linear code $\mathscr{H}_{q,n}$ whose parity check matrix is H is called a *Hamming code*. The linear code $\mathscr{S}_{q,n}$ whose generator matrix is H is called a *simplex code*.

The following result is immediate.

2.5. Proposition. Let q be a prime power, $n > 1$, and let $v = (q^n-1)/(q-1)$. Then:

(2.5.a) $\mathscr{S}_{q,n}$ is a linear $[v,n]_q$-code, and

(2.5.b) $\mathscr{H}_{q,n}$ is a linear $[v, v-n]_q$-code.

It can be shown that $\mathscr{H}_{q,n}$ is a linear single-error correcting code. In what follows, however, the simplex code will play a central role. The reader may consult Theorem 3.9.27 of **?** for a derivation.

2.6. Theorem. Let q be a prime power, $n > 1$, and let $v = (q^n-1)/(q-1)$. Then a linear $[v,n]_q$-code $\mathscr{C}$ is a $\mathscr{S}_{q,n}$ code if and only if $\text{wt}(x) = q^{n-1}$, for every $x \in \mathscr{C}$.

§3. Weighing Matrices and Their Generalizations

This section focuses on a third combinatorial configuration, namely, weighing matrices together with their generalizations. We begin with a brief look at weighing matrices themselves before moving onto to consider two generalizations. The first generalization is allowing the entries of a weighing matrix to be chosen from a finite group. This idea is then synthesized with the ideas of §1. Finally, we allow the entries of a weighing matrix to be taken from sets of indeterminants and consider the utility of such an approach.

* * *

3.1. Weighing Matrices. We begin the following definition.

3.1. Definition. Let W be a $(-1, 0, 1)$-matrix of order n. W is a *weighing matrix* of *order* n and *weight* k if

(3.1.a) $WW^t = kI_n$.

If $n = k$, then we say that W is a *Hadamard matrix*. If $n - 1 = k$, then we say that W is a *conference matrix*. In any event, we write $\mathrm{W}(n, k)$ to denote this property.

There are many useful generalizations of weighing matrices. We will take this up generally in the following sections, but for now we note the following special case. Note that we use A^* to denote the conjugate (Hermitian) transpose of a complex matrix A.

3.2. Definition. Let $G = \{\exp(\frac{2\pi im}{p}) : 0 \leq m < p\}$, and let W be a $(0, G)$-matrix of order v. We say that W is a *Butson weighing matrix* of *order* v and *weight* k if

(3.2.a) $WW^* = kI_n$,

and we write $\mathrm{BW}(v, k; p)$ to denote this property.

A result that is useful in studying properties of complex weighing matrices is the following that can be found in **?**.

3.3. Lemma. Let p be a prime, and let ξ be a primitive complex p-th root of unity. Then $\sum_{i=0}^{n} a_i \xi^i = 0$ for some $n < p$ and $a_i \in \mathbf{N}$ if and only if $n = p - 1$ and $a_0 = \cdots = a_n$.

We now move on to consider some generalizations of a weighing matrix.

* * *

3.2. Generalized Bhaskar Rao Designs. In the previous section, we defined a weighing matrix as a square matrix over $\{-1, 0, 1\}$. We then extended this definition to include those matrices over $\{0\}$ together with the complex p-th roots of unity. More generally, we can have weighing matrices over any finite group.

Before we can do this, however, we need to extend the conjugate transpose to group matrices. To accomplish this, let A be some matrix over a finite group G, and define $\overline{A}$ by $\overline{A}_{ij} = A_{ij}^{-1}$, that is, the matrix obtained by taking the group inverse of the nonzero entries of A. Finally, define $A^* = \overline{A}^t$. We then have the following.

3.4. Definition. Let G be some finite group, and let A be a $v \times b$ $(0, G)$-matrix such that

$$\text{(3.4.a)} \quad AA^* = rI_v + \frac{\lambda}{|G|}\left(\sum_{g \in G} g\right)(J_v - I_v),$$

for some positive integers r and λ, and such that there are k non-zero entries in every column. We then say that A is a *generalized Bhaskar Rao design* (henceforth GBRD), and we write GBRD$(v, k, \lambda; G)$ to denote this property. If we need to stress the remaining parameters, then we write GBRD$(v, b, r, k, \lambda; G)$.

It is clear that replacing the nonzero entries of a GBRD with unity furnishes a BIBD. Hence, we see that Fisher's Inequality applies. Again we single out the extremal case of the inequality.

3.5. Definition. A *balanced generalized weighing matrix* is a GBRD$(v, b, r, k, \lambda; G)$ in which $v = b$ (equiv. $k = r$). We use the denotation BGW$(v, k, \lambda; G)$. A BGW$(v, k, \lambda; G)$ in which $v = k$ is called a *generalized Hadamard matrix*, and we denote this as GH(G, λ) where $\lambda = v/|G|$. If $G = \mathrm{EA}(q)$, the elementary abelian group [5]) of order q, then we write GH(q, λ) instead.

BGW matrices are quite useful in the construction of other combinatorial designs (see, for example, **?** [**?**, **?**]), and satisfy a number of properties. For a detailed discussion of BGW matrices, the interested reader may consult **?**.

* * *

3.3. Isomorphisms of BGW matrices. As before, we can impose an equivalence on the set of all $v \times b$ $(0, G)$-matrices, which will play an important part in what is to come.

3.6. Definition. Two $v \times b$ $(0, G)$-matrices A_1 and A_2 are said to be *monomially equivalent* if there are monomial $(0, G)$-matrices P and Q of orders v and b, respectively, such that

$$\text{(3.6.a)} \quad PA_1Q = A_2 \text{ [6])}.$$

In order to extend normality to BGW matrices, we begin by altering somewhat Definition **??** as in Part V of **?**.

3.7. Definition. let G be some finite group, and let A be a $v \times b$ $(0, G)$-matrix. If A has k non-zero entries in every column, and if there is an element $c \in (\frac{\lambda}{|G|}G)\backslash\{1\} \subset \mathbf{Z}[G]$ such that

(3.7.a) $AA^* = rI_v + c(J_v - I_v)$,

then we say that A is a c-GBRD$(v, k, \lambda - 1; G)$, or a c-GBRD$(v, b, r, k, \lambda - 1; G)$ if more precision required.

We can now properly extend the idea of normality to BGW matrices.

3.8. Definition. A BGW$(v, k, \lambda; G)$ is said to be in *normal form* if it has the form

(3.8.a) $\begin{pmatrix} \mathbf{0}_{v-k} & A_1 \\ \mathbf{1}_k & A_2 \end{pmatrix}$.

Note that of necessity, A_1 is a GBRD$(v - k, v - 1, k, k - \lambda, \lambda; G)$ and A_2 is a c-GBRD$(k, v - 1, k - 1, \lambda, \lambda - 1; G)$. These have the parameters of the residual and derived designs of a square BIBD(v, k, λ), hence we call them, respectively, a residual GBRD and a derived c-GBRD.

* * *

3.4. Orthogonal Designs. In the previous subsection, we covered one generalization of weighing matrices, namely, we allowed the nonzero enetries to come from a finite group. In this subsection, we pursue another generalization in a different direction. In particular, instead of allowing the nonzero entries to come from some group, we will take the nonzero entries to be indeterminants—real, complex, or quaternary [7]).

We begin with the case of real indeterminants.

3.9. Definition. Let $x_1, \ldots, x_u$ be real, commuting indeterminants, and let X be an $n \times n$ matrix with entries from $\{0, \pm x_1, \ldots, \pm x_u\}$. We say that X is an *orthogonal design* if

(3.9.a) $XX^t = \left(\sum_i s_i x_i^2\right) I_n$.

We say that the orthogonal design is of order n and type $(s_1, \ldots, s_u)$, and we write X is an OD$(n; s_1, \ldots, s_u)$. If $\sum_i s_i = n$, then we say that the OD is *full*.

We now extend Definition **??** to the case of complex and quaternary numbers.

3.10. Definition. Let $z_1, \ldots, z_u$ be complex (resp. quaternary), commuting indeterminants, and let X be a matrix of order n with entries from $\{0, \varepsilon_1 z_1, \ldots, \varepsilon_u z_u\}$ and $\{\varepsilon_1 z_1^*, \ldots, \varepsilon_u z_u^*\}$, where each $\varepsilon_t \in \{\pm 1, \pm i\}$ (resp. $\varepsilon_t \in \{\pm 1, \pm i, \pm j, \pm k\}$). In the event that

$$\text{(3.10.a)} \quad XX^* = \left(\sum_i s_i |z_i|^2 \right) I_n,$$

then we say that X is a *complex* (resp. *quaternary*) orthogonal design of type $(s_1, \ldots, s_u)$. We write X is a COD$(n; s_1, \ldots, s_u)$ (resp. QOD$(n; s_1, \ldots, s_u)$).

Equivalence of orthogonal designs is the same as for BGW matrices where the monimal matrices have nonzero entries in set $\{1, i, j, k\}$, and where we also allow a permutation of symbols.

* * *

3.5. Sequences and Circulants. Let A be an $n \times n$ matrix with first row $(a_0, \ldots, a_{n-1})$. Recall that A is *circulant* if $A_{ij} = a_{j-i}$, where the indices are calculated modulo n. In this way, the entire matrix is determined by its first row; moreover, if A and B are two circulants of the same dimension, then A^t, $A+B$, and AB are also circulant matrices. Therefore, to effect a study of circulant matrices, we can profitably study sequences.

What we are particularly interested with here is the following.

3.11. Definition. Let $\mathcal{A} = \{A_i\}$ be a finite collection of circulant matrices of the same dimension over a commutative ring R endowed with an involution $\cdot^*$. The collection $\mathcal{A}$ is said to be *complementary* if

$$\text{(3.11.a)} \quad \sum_i A_i A_i^* = aI, \text{ for some } a \in R,$$

where, as usual, $(m_{ij})^* = (m_{ji}^*)$.

Note, however, that we can state this in terms of sequences. First, a definition.

3.12. Definition. Let $a_0 = (a_{0,0}, \ldots, a_{0,n-1})$ be a sequence in a commutative ring R with the involution $\cdot^*$. The *j-th aperiodic* and *j-th periodic autocorrelations* of the sequence a are given respectively by

$$\text{(3.12.a)} \quad N_j(a) = \sum_{i=0}^{n-j-1} a_{0,i} a_{0,i+j}^*, \text{ and}$$

$$\text{(3.12.b)} \quad P_j(a) = \sum_{i=0}^{n-1} a_{0,i} a_{0,i+j}^*, \text{ indices calculated modulo } n.$$

If $a_1 = (a_{1,0}, \ldots, a_{1,n-1}), \ldots, a_m = (a_{m,1}, \ldots, a_{m,n-1})$ are any other sequence in R, then $a_0, \ldots, a_m$ are *complementary* if

(3.12.c) $\sum_i P_j(a_i) = 0$, for every $j \in \{1, \ldots, n-1\}$.

For the case in which $m = 1$, we say that we have a *Golay pair*.

We see immediately that $P_j(a) = N_j(a) + N_{n-j}(a)^*$; hence, if $N_j(a) + N_j(b) = 0$, for every $j \in \{1, \ldots, n-1\}$, then a and b are complementary. However, vanishing periodic autocorrelations does not in general imply vanishing aperiodic autocorrelations.

The importance of the periodic correlation is given by the fact that if the first row of the circulant A continues to be $a = (a_0, \ldots, a_{n-1})$, then the first row of AA^* is given by $(\sum_i |a_i|^2, P_{n-1}(a), \ldots, P_1(a))$. So we see that complementary circulants and complementary sequences are one and the same.

Complementary sequences and orthogonal designs are connected in an intimate way; in fact, complementary sequences offer many elegant constructions of ODs. To make the connection precise, we need to allow sequence elements to be indeterminants whether real, complex, or quaternary, and where the involution is taken to be conjugation.

3.13. Proposition. Let $\{z_1, \ldots, z_u\}$ be commuting quaternary indeterminants, and let $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ be complementary sequences with entries from $\{0, \varepsilon_0 z_0, \ldots, \varepsilon_u z_u\}$, where $\varepsilon_t \in \{\pm 1, \pm i, \pm j, \pm k\}$, such that $\sum_i (|a_i|^2 + |b_i|^2) = \sum_i s_i x_i^2$. Then

(3.13.a) $\begin{pmatrix} A & B \\ -B^* & A^* \end{pmatrix}$

is a QOD$(2n; s_1, \ldots, s_u)$, where A and B are the circulants with first rows a and b, respectively.

The matrix (**??**) will feature as a submatrix in our later work where the sequences will be composed of matrices. We will need one further idea before we proceed.

3.14. Definition. Let $a = (a_0, \ldots, a_{n-1})$ and $b = (b_0, \ldots, b_{n-1})$ be two sequences over a ring with involution $\cdot^*$. The *j-th cross-correlation* of a by b is given by

(3.14.a) $C_j(a, b) = \sum_{i=0}^{n-1} a_i b_{i+j}^*$, for each $j \in \{1, \ldots, n-1\}$.

If A has first row $a = (a_0, \ldots, a_{n-1})$, and if B has first row $b = (b_0, \ldots, b_{n-1})$, then the first row of the circulant AB^* is $(\sum_i a_i b_i^*, C_{n-1}(a, b), \ldots, C_1(a, b))$. Note, however, that $C_j(a, b)$ is not in general equal to $C_j(b, a)$. So, care must be taken in extending Proposition **??** since amicability is required in maintaining orthogonality when substituting into an OD.

Much more can be said about this most useful topic. The interested reader is may consult **?** and **?** for a wealth of material.

§4. Association Schemes

This fourth and final preliminary section briefly touches on association schemes, a fundamental abstract object used as a unifying tool across the otherwise disparate fields of combinatorics. It is composed of two sections. The first will introduce the basic ideas via strongly regular graphs, the simplest nontrivial example of an association scheme. The second moves on to consider these objects in general. Only enough theory is developed in order to be applied in later chapters.

* * *

4.1. Defintion. We begin with the following definition.

4.1. Definition. Let X be a finite set of v elements, and let $\mathscr{R} = \{R_0, \ldots, R_d\}$ be a collection of relations on X. We say that the ordered pair $\mathfrak{X} = (X, \mathscr{R})$ is an *association scheme* with d *classes* whenever the following are satisfied.

(4.1.a) $R_0 = \{(x, x) : x \in X\}$;

(4.1.b) $R_i \cap R_j = \emptyset$ and $X \times X$ is the disjoint union of $R_0, \ldots, R_d$;

(4.1.c) $R_i^t = R_{i'}$ for some $i' \in \{0, \ldots, d\}$, where $R_i^t = \{(x, y) : (y, x) \in R_i\}$; and

(4.1.d) Given $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k. We call the p_{ij}^k, the *intersection numbers* of the scheme.

The scheme $\mathfrak{X}$ is *commutative* if

(4.1.e) $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \{0, \ldots, d\}$.

The scheme is *symmetric* if

(4.1.f) $i = i'$, for every $i \in \{0, \ldots, d\}$.

We denote p_{ii}^0 as k_i, the *valency* of the relation R_i.

Unless otherwise stated, we will assume that the association schemes we are working with are commutative.

* * *

4.2. Adjacency Algebras. The importance of association schemes resides in the following equivalent definition.

4.2. Definition. Let $\mathfrak{X} = (X, \mathscr{R})$ be a d-class assocation scheme. For $i \in \{0, \ldots, d\}$, define the $v \times v$ $(0,1)$-matrix A_i with rows and columns indexed by elements of X by $(A_i)_{xy} = 1$ if and only if $(x, y) \in R_i$. We call A_i the *adjacency matrix* of the relation R_i. Then Definition **??** is equivalent to the following.

(4.2.a) $A_0 = I$;

(4.2.b) $A_0 + \cdots + A_d = J$;

(4.2.c) $A_i^t = A_{i'}$ for some $i' \in \{0, \ldots, d\}$; and

(4.2.d) $A_i A_j = \sum_k p_{ij}^k A_k$, for every $i, j \in \{0, \ldots d\}$.

If $\mathfrak{X}$ is commutative, then

(4.2.e) $A_i A_j = A_j A_i$, for each $i, j \in \{0, \ldots, d\}$.

If $\mathfrak{X}$ is symmetric, then

(4.2.f) $A_i^t = A_i$, for every $i \in \{0, \ldots, d\}$.

By **??**, the adjacency matrices of the scheme are $\mathbf{C}$-linearly independent and generate a subspace $\mathfrak{U}$ of $\mathrm{Mat}_v(\mathbf{C})$ of dimension $d+1$. By **??**, $\mathfrak{U}$ is closed under standard matrix multiplication. We call $\mathfrak{U}$ the *adjacency algebra* of the association scheme $\mathfrak{X}$.

We further have that $A_i \circ A_j = \delta_{ij} A_i$. Therefore, $A_0, \ldots, A_d$ also generate a commutative algebra $\hat{\mathfrak{U}}$ with Schur multiplication for which they are primitive idempotentsdual-scheme. We therefore also call the adjacency matrices the *Schur idempotents* of the scheme.

Assume an ordering of $X = \{x_0, \ldots, x_{v-1}\}$, and take e_{x_i} to be the standard vector with i-th position equal to 1 and 0 elsewhere. Take V to be the Hermitian space with the standard orthonormal basis $\{e_x : x \in X\}$.

Since we are assuming commutativity, the adjacency matrices $A_0, \ldots, A_d$ are pairwise commuting, normal matrices. So, they share an eigenbasis, and by the Spectral Theorem for normal matrices, $V = \bigoplus_{i=1}^r V_i$, where the V_i are maximal common eigenspaces.

Since $J = \sum_i A_i$, we find the eigenspace corresponding to the eigenvalue v is spanned by $\mathbf{1}_v$, i.e. it is 1-dimensional and hence maximal. It follows that this space is equal to V_i for some i. We can assume, then, that $i = 0$.

If we take E_i to be the orthogonal projection $V \to V_i$ with respect to the basis $\{e_x : x \in X\}$, then we can assume that $E_0 = |X|^{-1} J$, and we have $E_0 + \cdots + E_d = I$. Moreover, there is a unitary matrix Λ such that $\Lambda^* E_i \Lambda = \mathrm{diag}(0, \ldots, 0, \underbrace{1, \ldots, 1}_{m_i}, 0, \ldots, 0)$, where we have used m_i to denote $\dim(V_i)$. The numbers m_i, for $i \in \{0, \ldots, d\}$, are called the *multiplicities* of the scheme.

It can be shown (see **?**, Theorem 3.1) that the projection matrices $E_0, \ldots, E_d$ are primitive idempotents of $\mathfrak{U}$ and form a dual basis of $\mathfrak{U}$. It follows that there are constants P_{ij} and Q_{ij}, for $i, j \in \{0, \ldots, d\}$, called the *eigenvalues* and *dual-eigenvalues* of the scheme, such that $A_j = \sum_i P_{ij} E_i$ and $E_j = |X|^{-1} \sum_i Q_{ij} A_i$. Using these constants, we form the matrices P and Q with (i, j)-th entry given by P_{ij} and Q_{ij}, respectively, and we call these matrices the *first* and *second character tables* of the scheme. By what has been said, we have at once that $PQ = QP = vI$.

* * *

Notes

1. This technique is famously used in the justification of Hoffman's co-clique bound (see **?**, Proposition 1.3.2). In **?** and **?**, it is used to great effect in the context of designs.

2. By an incidence structure is meant a triple $S = (X, \mathscr{B}, I)$, where $I \subseteq X \times \mathscr{B}$. We say that X is the point set, $\mathscr{B}$ the block set, and I the set of flags. If $(x, B) \in I$, then the point x and block B are said to be incident. See **?** and **?** for a standard treatment of incidence. See **?** for study of incidence in the context of design theory.

3. This is more generaly given as the orbits of the action of $S_v \times S_b$ on the set of binary $v \times b$ matrices defined by $\mu(A, (P, Q)) = P^t A Q$, where the transposition is necessary in order to properly define a right action.

4. Recall that a metric space is a pair (X, ϱ), where X is a nonempty set, and where $\varrho : X \to \mathbf{R}_{\geq 0}$ is a map satisfying, for all $x, y, z \in X$, (a) $\varrho(x, y) \geq 0$ with equality iff $x = y$; (b) $\varrho(x, y) = \varrho(y, x)$; and (c) $\varrho(x, y) \leq \varrho(x, z) + \varrho(z, y)$. We then say that ϱ is a metric.

5. If $q = p^n$, for some prime p, then $\mathrm{EA}(q) \simeq \underbrace{C_p \times \cdots \times C_p}_{n}$.

6. Let H and $K \leq S_v$ be finite groups. Recall that the wreath product $H \wr K$ is the semi direct product $H^v \rtimes K$ where $k(h_0, \ldots, h_{v-1})k^{-1} = (h_{k^{-1}0}, \ldots, h_{k^{-1}(v-1)})$. Let $H_1 = G \wr S_v$, let $H_2 = G \wr S_b$, and let $H = H_1 \times H_2$. We define an action of H on the set of all $v \times b$ $(0, G)$-matrices by $\mu(A, (P, Q)) = P^* A Q$. The monomially equivalent matrices are composed precisely by the orbits of this action.

7. Recall that the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ is defined with anticommutative multiplication given by $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$. We then take the quaternion algebra to be the $\mathbf{R}$-algebra $\{a_1 + a_i i + a_j j + a_k k : a_1, a_i, a_j, a_k \in \mathbf{R}\}$. Conjugation is extended to the quaternion algebra by $(a_1 + a_i i + a_j j + a_k k)^* = a_1 - a_i i - a_j j - a_k k$.