Chapter 7

Block Designs

One simile that solitary shines

In the dry desert of a thousand lines.

Epilogue to the Satires, ALEXANDER POPE

The collection of all subsets of cardinality k of a set with v elements ($k < v$) has the property that any subset of t elements, with $0 \leq t \leq k$, is contained in precisely $\binom{v-t}{k-t}$ subsets of size k. The subsets of size k provide therefore a nice covering for the subsets of a lesser cardinality. Observe that the number of subsets of size k that contain a subset of size t depends only on v, k, and t and not on the specific subset of size t in question. This is the essential defining feature of the structures that we wish to study.

The example we just described inspires general interest in producing similar coverings without using all the $\binom{v}{k}$ subsets of size k but rather as small a number of them as possi-

ble. The coverings that result are often elegant geometrical configurations, of which the projective and affine planes are examples. These latter configurations form nice coverings only for the subsets of cardinality 2, that is, any two elements are in the same number of these special subsets of size k which we call blocks (or, in certain instances, lines).

A collection of subsets of cardinality k, called blocks, with the property that every subset of size t ($t \leq k$) is contained in the same number (say λ) of blocks is called a t-design. We supply the reader with constructions for t-designs with t as high as 5. Only recently a nontrivial 6-design has been found and no nontrivial 7-design is known. We then study in more depth the necessary numerical conditions for the existence of a symmetric 2-design contained in a result of Bruck, Ryser, and Chowla. A more recent result, due to Cameron, on extending symmetric 2-designs is included as well.

Special kinds of 2-designs, called Steiner triple systems, were studied in the nineteenth century by Woolhouse, Kirkman, and Steiner. Apart from their implicit connections to multiple transitive groups, 2-designs (known to statisticians as balanced incomplete block designs) arise explicitly from the statistical theories of Sir R. A. Fisher, most notably his analysis of variance. The rich combinatorial content of the theory of experimental design and the analysis of variance, initiated by Fisher and Yates, was further pursued by Bose and many of his students. Much of the material included in this chapter originated in their work. One such instance is the extension of Fisher's inequality from 2-designs to t-designs ($t \geq 2$). We devote a full section to this extension. The latter part of the chapter provides an introduction to association schemes, the Bose-Mesner algebra, and partial designs. Familiarity with finite fields, $GF(q)$, and finite-dimensional vector spaces over such fields is assumed in this chapter. The reader not exposed to these subjects is

referred to Appendix 2 and the references given there.

1 THE BASIC STRUCTURE OF t-DESIGNS

7.1

Let $P = \{1, 2, ..., v\}$ be a set of v elements that we call *points*. A subset of P with k elements is called a *k-subset*. We assume $0 \leq t \leq k < v$.

Definition. A $t-(v, k, \lambda_t)$ *design* is a pair (P, B), where B is a collection of k-subsets of P (called *blocks*) with the property that each t-subset of P occurs in exactly λ_t blocks. (With less stringent emphasis we call such a pair a *t-design*.)

By $\sum_s(P)$ we denote the collection of all $s-$subsets of P; $|\sum_s(P)| = \binom{v}{s}$. For notational ease, however, we simply write σ_s to convey the fact that σ_s is a s-subset.

As we pointed out in the introduction, $(P, \sum_k(P))$ is a $t-(v, k, \binom{v-t}{k-t})$ design, for all $0 \leq t \leq k$; this design is called the *complete design*. Our interest is in studying t-designs that are not complete, that is, t-designs in which not every k-subset is a block. Though by no means abundant, such structures do exist. Several small examples are given at the end of this section. Well-known families of t-designs ($2 \leq t \leq 5$) are described in greater detail in Section 2.

The result we now prove gives insight into the combinatorial structure of a t-design.

Proposition 7.1. *Let (P, B) be a $t-(v, k, \lambda_t)$ design.*

(a) *(P, B) is also an $i-(v, k, \lambda_i)$ design, with $\lambda_i = \binom{v-i}{t-i}\binom{k-i}{t-i}^{-1}\lambda_t$, for all $0 \leq i \leq t$.*

(Note that $\lambda_0 = |B|$.)

(b) *For σ_i and τ_j such that $0 \le i+j \le t$, the number of blocks α such that $\sigma_i \subseteq \alpha$ and $\tau_j \cap \alpha = \emptyset$* is $\binom{v-i-j}{k-i}\binom{v-t}{k-t}^{-1}\lambda_t$. (We denote this number by λ_i^j and observe that it depends on i and j only and not on the specific choice of the subsets σ_i and τ_j.)

(c) *If $v \ge k+t$, then*

$$(P, \{P-\alpha : \alpha \in B\})$$

is a $t-(v, v-k, \binom{v-t}{k}\binom{v-t}{k-t}^{-1}\lambda_t$ design [called the *complementary design* of (P,B)].

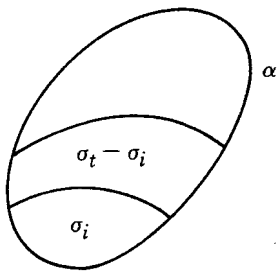
(d) *Let $a \in P$. Then*

$$(P-\{a\}, \{\alpha-\{a\} : \alpha \in B \text{ such that } a \in \alpha\})$$

is a $(t-1)-(v-1, k-1, \lambda_t)$ design [called the *derived design* of *(P,B)* at a] *and* $(P-\{a\}, \{\alpha : \alpha \in B \text{ and } a \notin \alpha\})$ *is a $(t-1)-(v-1, k, \binom{v-t}{k-t+1}\binom{v-t}{k-t}^{-1}\lambda_t$ design* [called the *residual design* of *(P,B)* at the point a].

Proof. (a) Count in two ways the set of ordered pairs

$$\{(\sigma_t - \sigma_i, \alpha) : \alpha \supseteq \sigma_t \supseteq \sigma_i,\ \alpha \in B\}.$$



Fix α first and obtain $\binom{k-i}{t-i}\lambda_t$ for an answer (with λ_i denoting the number of blocks containing σ_i). Fix $\sigma_t - \sigma_i$ first and obtain $\binom{v-i}{t-i}\lambda_t$ for an answer. This gives $\lambda_i = \binom{v-i}{t-i}\binom{k-i}{t-i}^{-1}\lambda_t$, an expression that is *independent* of the specific subset σ_i. (The reader

should observe that, in fact, $\bigcap_{\sigma_i \subseteq \alpha} \alpha = \sigma_i$ for $0 \leq i < t$ – or else $\lambda_i \leq \lambda_{i+1}$, leading to a contradiction.)

(b) Let $X = \{\alpha \in B : \sigma_i \subseteq \alpha\}$; $|X| = \lambda_i$. Let also $\{A_m : m \in \tau_j\}$ be a collection of subsets of X defined as follows:

$$A_m = \{\alpha \in B : \ \sigma_i \subseteq \alpha \text{ and } \{m\} \subseteq \alpha \cap \tau_j\}.$$

There are j such A_m's. Note that

$$|\bigcap_{m \in \sigma_r} A_m| = |\{\alpha \in B : \ \sigma_i \subseteq \alpha \text{ and } \sigma_r \subseteq \alpha \cap \tau_j| = \lambda_{i+r} \ (\sigma_r \subseteq \tau_j).$$

We want the number of blocks in X that are in none of the A_m's. By the principle of inclusion-exclusion (see Section 9.12) this number is

$$\lambda_i^j = |\bigcap_{m \in \sigma_r} \bar{A}_m| = \sum_{r=0}^{j} (-1)^r \sum_{\substack{\sigma_r \\ (\sigma_r \subseteq \tau_j)}} |\bigcap_{m \in \sigma_r} A_m|$$

$$= \sum_{i=0}^{j} (-1)^r \sum_{\sigma_r} \lambda_{i+r} = \sum_{i=0}^{j} (-1)^r \binom{j}{r} \lambda_{i+r}.$$

By (a) above $\lambda_s = \binom{v-s}{t-s}\binom{k-s}{t-s}^{-1}\lambda_t$. Hence $\lambda_i^j = c\lambda_t$ with

$$c = \sum_{i=0}^{j} (-1)^r \binom{j}{r} \binom{v-i-j}{t-i-r} \binom{k-i-r}{t-i-r}^{-1}.$$

Note that the constant c depends only on the parameters $v,\ k,\ t,\ i,\ j$ and not on the particular design. Taking the design $(P, \sum_k(P))$ we find in this case by direct computation $\lambda_t = \binom{v-t}{k-t}$ and $\lambda_i^j = \binom{v-i-j}{k-i}$. We thus obtain the simpler expression $c = \binom{v-i-j}{k-i}\binom{v-t}{k-t}^{-1}$. Thus $\lambda_i^j = \binom{v-i-j}{k-i}\binom{v-t}{k-t}^{-1}\lambda_t$.

(c) The number of blocks in $(P, \{P - \alpha : \alpha \in B\}$ containing a subset of t elements is λ_0^t in (P, B), which is well defined by part (b). In fact

$$\lambda_0^t = \binom{v-t}{k}\binom{v-t}{k-t}^{-1}\lambda_t,$$

which proves (c).

(d) To calculate how many blocks in the derived design contain a subset of $t-1$ points, let $\sigma_{t-1} \in \sum_{t-1}(P - \{a\})$. Look at $\sigma_t = \sigma_{t-1} \cup \{a\}$. The subset σ_t is in λ_t blocks of (P, B), all of which contain a. Therefore σ_{t-1} is in λ_t blocks of the derived design, as claimed.

In the case of the residual design, $t-1$ points from $P - \{a\}$ are in precisely

$$\lambda_{t-1}^1 = \binom{v-(t-1)-1}{k-t+1}\binom{v-t}{k-t}^{-1}\lambda_t = \binom{v-t}{k-t+1}\binom{v-t}{k-t}^{-1}\lambda_t.$$

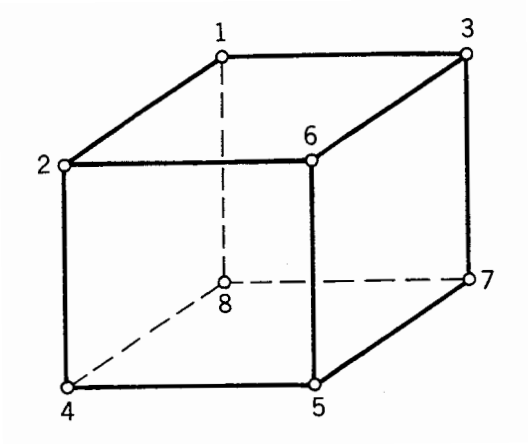
This proves (d) and concludes the proof of our proposition.

7.2

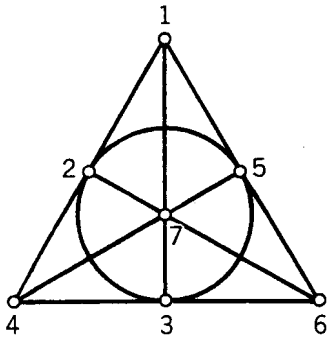
As an example, consider

$$\begin{array}{cccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 & 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 & 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 8 & 8 & 8 & 8 & 8 & 8 & 8 & 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \tag{7.1}$$

with $P = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and blocks B the columns of (7.1). Then one can directly check that (P, B) is a $3-(8, 4, 1)$ design. The checking can be facilitated by interpreting the blocks of (7.1) as the six faces, the six diagonal planes, plus the two "skewed" blocks 2 3 5 8 and 4 6 7 1 of the cube below:



Assertions (a) through (d) made in Proposition 7.1 can also be verified with enough ease by examining the figure above. The design (P, B) turns out to be self-complementary. Its derived design, at $a = 8$, is perhaps better known in its more graphical form



(7.2)

The residual design at $a = 8$ consists of the last seven blocks of (7.1). This residual design turns out to be, in this case, the complementary design of the derived design of (P, B) at $a = 8$. Hadamard matrices provide us with perhaps the largest supply of 3-designs. The design we just examined is the smallest example of an infinite family of 3-designs that can be obtained from Hadamard matrices. A description of the general method of construction is given in the next section.

Another 3-design, not of the Hadamard kind, is listed below:

$$\begin{array}{cccccccccccccc}
1 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 4 & 4 & 5 & 1 & 1 & 1 \\
2 & 3 & 5 & 6 & 3 & 6 & 7 & 4 & 7 & 5 & 8 & 6 & 2 & 2 & 2 \\
4 & 8 & 9 & 7 & 5 & 9 & 8 & 6 & 9 & 7 & 9 & 8 & 3 & 5 & 6 \\
T & T & T & T & T & T & T & T & T & T & T & T & 9 & 7 & 8 \\
\end{array} \tag{7.3}$$

$$\begin{array}{ccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 4 & 5 \\
3 & 3 & 4 & 4 & 7 & 3 & 3 & 4 & 4 & 5 & 4 & 5 & 6 & 6 & 6 \\
4 & 5 & 5 & 6 & 8 & 4 & 6 & 5 & 7 & 8 & 5 & 7 & 8 & 7 & 7 \\
7 & 6 & 8 & 9 & 9 & 8 & 7 & 6 & 9 & 9 & 9 & 8 & 9 & 8 & 9 \\
\end{array}$$

The symbol T abbreviates 10. We invite the reader to examine this design and possibly attach geometrical interpretations to it.

2 CONSTRUCTIONS OF t-DESIGNS

In the next few pages we describe several methods of constructing t-designs with $2 \leq t \leq 5$. Outlines of proofs, along with some references, are given in the latter part of the section.

Large families of 2- and 3-designs can be constructed through Hadamard matrices. A $n \times n$ matrix H with entries 1 and -1 is called a *Hadamard matrix* if $H'H = nI$ $(= HH')$. Here H' denotes the transpose of the matrix H. Observe that multiplying rows and columns of a Hadamard matrix by -1 leads again to a Hadamard matrix.

A Hadamard matrix may exist only if n is a multiple of 4 or if n is 2 or 1. It is not known whether a Hadamard matrix exists for every multiple of 4 but it appears that they do exist in abundance. We quickly mention some known families of Hadamard matrices.

For $A = (a_{ij})$ a $n \times n$ matrix and B a $m \times m$ matrix we denote by $A \otimes B$ the matrix $(a_{ij}B)$ and call it the *tensor product* of A with B; $A \otimes B$ is $nm \times nm$. The matrix $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ is a 2×2 Hadamard matrix. It can easily be verified that if H and G are Hadamard matrices, then so is $H \otimes G$. By repeatedly tensoring a Hadamard matrix of order 2 with itself we conclude that Hadamard matrices of order 2^n exist for all $n \geq 0$. It is known that a Hadamard matrix of order $q + 1$ exists, where q is a prime power and $q \equiv 3$ (modulo 4). There also exists a Hadamard matrix of order $2(q + 1)$ for q a prime power congruent to 1 modulo 4. In fact it is known that *if there exists a Hadamard matrix of order h ($h > 1$), then there exists a Hadamard matrix of order $h(q + 1)$, where q is an odd prime power.*

7.3 The Hadamard 2-Designs

Let H be a Hadamard matrix of order n ($n \geq 8$).

Make 1's in the first row and column of H, by multiplying suitable rows and columns of H by -1. Delete the first row and column. In the remaining $(n-1) \times (n-1)$ matrix each

row generates a block: it consists of the indices of the columns in which the 1's occur. The resulting structure is a $2 - (n - 1, \frac{n}{2} - 1, \frac{n}{4} - 1)$ design.

This construction is reversible. In other words, by starting out with any $2 - (n - 1, \frac{n}{2} - 1, \frac{n}{4} - 1)$ design we can produce a Hadamard matrix of order n by reversing the steps above.

7.4 The Paley Designs

A special case of the above construction are the Paley designs (these are 2-designs). Consider $GF(q)$, the field with q elements, where $q \equiv 3$ (modulo 4); q is a power of a prime. The points are the elements of $GF(q)$. The blocks are $\{Q + a : a \in GF(q)\}$, where Q is the set of nonzero squares in $GF(q)$. [An element $x \in GF(q)$ is said to be a square in $GF(q)$ if $x = y^2$, for some $y \in GF(q)$.]

As an example, let $q = 11$. Then $Q = \{1, 3, 4, 5, 9\}$ and the resulting 2-design is

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 2 \\ 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 2 & 3 \\ 5 & 6 & 7 & 8 & 9 & 10 & 11 & 1 & 2 & 3 & 4 \\ 9 & 10 & 11 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8. \end{array} \tag{7.4}$$

7.5 The Hadamard 3-Designs

Let H be a Hadamard matrix of order n ($n \geq 8$).

Make 1's in the first row by multiplying suitable columns by -1. The points are the (indices of) columns of H. Blocks are given as follows: each row (other than the first) gives two blocks; the columns in which 1 appears is one, and the (remaining) columns in which -1 appears is the other.

The resulting design is a $3 - (n, \frac{n}{2}, \frac{n}{4} - 1)$ design. This construction is reversible as well. The design in (7.1) is the smallest example in this family.

Another way of constructing 2-designs is through projective and affine geometries.

A *projective geometry* over $GF(q)$ is the collection of subspaces of a vector space of finite dimension over $GF(q)$. The *points* of the geometry are the subspaces of dimension 1. A (projective) subspace is identified with the set of points it contains. Points have (projective) dimension 0 and, in general, a (projective) subspace is assigned dimension 1 less than the vector space dimension of the subspace it comes from. Subspaces of projective dimension 1 are called *lines*, those of projective dimension 2 are called *planes*.

An *affine geometry* of dimension n is the collection of cosets of subspaces of a vector space of dimension n over $GF(q)$. The geometric dimension here equals the usual vector space dimension of the underlying subspace. *Points* are just vectors (or cosets of the 0 subspace). An (affine) subspace is identified with the points it contains. The affine subspaces of dimension 1 are called *lines* and those of dimension 2 are called *planes*.

Projective and affine geometries contain 2- and 3-designs. Sections 7.6 and 7.7 give the details of these constructions along with a couple of illustrative examples.

7.6 The Projective Geometries

In a projective geometry of (projective) dimension n over $GF(q)$ the subspaces of a given projective dimension m $(2 \leq m \leq n-1)$ form a

$$2 - \left(\frac{q^{n+1}-1}{q-1}, \frac{q^{m+1}-1}{q-1}, \begin{bmatrix} n-1 \\ m-1 \end{bmatrix} (q) \right)$$

design, where $\begin{bmatrix} n \\ k \end{bmatrix}(x)$ denotes the Gaussian polynomial.

When $m = n-1$ we obtain a symmetric

$$2 - \left(\frac{q^{n+1}-1}{q-1}, \frac{q^{n}-1}{q-1}, \frac{q^{n-1}-1}{q-1} \right)$$

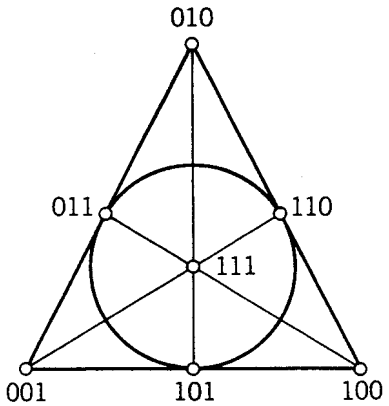
design. [A 2-design (P, B) is said to be *symmetric* if the number of blocks equals the number of points, i.e., if $\lambda_0 = |B| = |P| = v$.] We denote this symmetric design by $PG(n, q)$. Note that $PG(n, 2)$ is a Hadamard 2-design for all $n \geq 2$.

Example. Let us construct $PG(2, 2)$. We start with a vector space V of dimension 3 over $GF(2)$. The space V contains eight vectors: 000, 100, 010, 001, 110, 101, 011, 111. There are $(2^3 - 1)/(2 - 1) = 7$ subspaces of dimension 2 in V; each is a solution to one of the following equations: $x = 0$, $y = 0$, $z = 0$, $x + y = 0$, $x + z = 0$, $y + z = 0$, and $x + y + z = 0$ (where x, y, and z denote the three coordinate axes). The subspaces are (with 000 omitted):

$$\left\{\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{matrix}\right\}, \quad \left\{\begin{matrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{matrix}\right\}, \quad \left\{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{matrix}\right\}, \quad \left\{\begin{matrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{matrix}\right\},$$

$$\left\{\begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{matrix}\right\}, \quad \left\{\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}\right\}, \quad \text{and} \quad \left\{\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{matrix}\right\},$$

This gives rise to the following projective picture:



in which the reader will recognize the design displayed in (7.2).

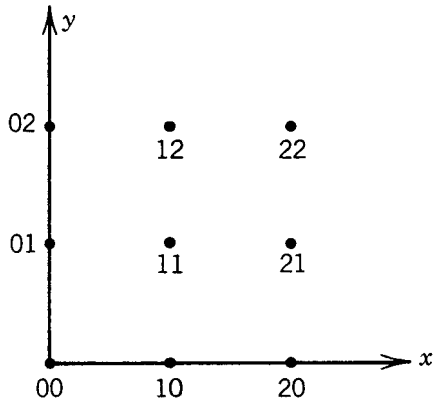
7.7 The Affine Geometries

In an affine geometry of (affine) dimension n over $GF(q)$ the subspaces of a given affine dimension m $(2 \le m \le n-1)$ form a $2-(q^n, q^m, \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}(q))$ design, where $\begin{bmatrix} n \\ k \end{bmatrix}(x)$ denotes the Gaussian polynomial.

When $m = n-1$ we obtain a $2-(q^n, q^{n-1}, (q^{n-1}-1)/(q-1))$ design. [We denote this design by $AG(n,q)$. An affine plane is $AG(2,q)$.]

In an affine geometry of (affine) dimension n over $GF(2)$ the subspaces of a given affine dimension m $(2 \le m \le n-1)$ form a $3-(2^n, 2^m, \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}(2))$ design, with $\begin{bmatrix} n \\ k \end{bmatrix}(x)$ being the Gaussian polynomial. $AG(n,2)$ is a Hadamard 3-design. Design (7.1) is such an example, that is, it is $AG(3,2)$.

Example. Let us construct $AG(2,3)$, the affine plane over $GF(3)$. We have nine vectors:



$AG(2,3)$ consists of four subspaces of dimension 1 (each coming with 2 cosets):

$x=0$			$y=0$			$x+2y=0$			$x+y=0$		
00	10	20	00	01	02	00	10	01	00	10	02
01	11	21	10	11	12	11	21	12	12	22	11
02	12	22	20	21	22	22	02	20	21	01	20.

With an immediately obvious relabeling of points (1 through 9) we can write $AG(2,3)$ as follows:

1	4	7	1	2	3	1	4	2	1	4	3
2	5	8	4	5	6	5	8	6	6	9	5
3	6	9	7	8	9	9	3	7	8	2	7.

(7.5)

$AG(2,3)$ is indeed a $2-(9,3,1)$ design with the columns of (7.5) as blocks.

7.8 The Multiply Transitive Groups

The t-transitive groups provide yet another way of constructing t-designs, $2 \leq t \leq 5$. A permutation group G acting on a set P is called *t-transitive* if for any two ordered t-tuples with distinct entries $(x_1, \ldots, x_t)$ and $(y_1, \ldots, y_t)$ there exists $g \in G$ such that $g(x_1) = y_1, \ldots, g(x_t) = y_t$; $x_i, y_i \in P$, $1 \leq i \leq t$.

Let G act t-transitively on P and let $\alpha \in \sum_k(P)$, with $k > t$. Define $B = \{g(\alpha) : g \in G\}$. [We understand by $g(\alpha)$ the k-subset $\{g(x) : x \in \alpha\}$.] Then (P, B) is a $t-(v,k,\lambda_t)$ design. Since $\binom{v}{t}\binom{k}{t}^{-1}\lambda_t = \lambda_0 = |G|/|G_\alpha|$ we obtain $\lambda_t = \binom{k}{t}\binom{v}{t}^{-1}|G||G_\alpha|^{-1}$; here G_α denotes the (set) stabilizer of α, that is, $G_\alpha = \{g \in G : g(\alpha) = \alpha\}$. Sometimes the designs generated through this process actually turn out to be complete designs.

As nontrivial examples, the Mathieu groups M_{12} and M_{24} act 5-transitively on 12 and 24 points, respectively. They are known to generate the Mathieu designs $5-(12,6,1)$

and $5-(24,8,1)$ in the manner described above. We outline a construction and list the Mathieu $5-(12,6,1)$ design in its entirety in Section 7.9. There exist many 2-transitive groups. Through the process just described they can be used to generate 2-designs.

7.9 Construction through Linear Codes

We illustrate now a method of construction of t-designs through the use of linear codes. Identify a vector space of dimension n over $GF(q)$ with $(GF(q))^n$, that is, n-tuples with entries from $GF(q)$. A subspace C of dimension m in $(GF(q))^n$ is called a (n,m) *linear code*; $|C| = q^m$. Let $x \in C$; the set of nonzero coordinates of x is called its *support*; the number of nonzero coordinates of x is called the *weight* of x and is denoted by $w(x)$.

Let us agree to write the vectors of $(GF(q))^n$ as row vectors. A *generating matrix* $G(C)$ for the (n,m) linear code C is a $m \times n$ matrix whose rows form a basis for C [over $GF(q)$].

Designs can sometimes be obtained by the following process: The distinct supports of the vectors of minimal (nonzero) weight of certain (quite select) linear codes over $GF(q)$ form the blocks of a t-design $(2 \leq t \leq 5)$.

Example. Let C be the linear code of $(GF(2))^8$ with generating matrix

$$G(C) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Apart from the 0 vector and (11111111) all of the 14 remaining vectors in C have minimal

(nonzero) weight 4. They are:

$$
\begin{array}{cccccccc|c}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2\ 5\ 6\ 8 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 3\ 5\ 7\ 8 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 4\ 6\ 7\ 8 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 2\ 3\ 6\ 7 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 2\ 4\ 5\ 7 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 3\ 4\ 5\ 6 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 2\ 3\ 4\ 8 \\
\multicolumn{8}{c|}{\longleftrightarrow} & \\
1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1\ 3\ 4\ 7 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1\ 2\ 4\ 6 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1\ 2\ 3\ 5 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1\ 4\ 5\ 8 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1\ 3\ 6\ 8 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1\ 2\ 7\ 8 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1\ 5\ 6\ 7
\end{array}
$$

The supports of these vectors give a $3-(8,4,1)$ design; this is the same as design (7.1) in Section 1. [The permutation

$$
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 2 & 4 & 7 & 6 & 8 \end{pmatrix}
$$

carries in fact the blocks of this design into those of (7.1).]

Another Example. Consider the (distinguished) (12,6) linear code C over $GF(3)$, whose

elements we write as -1, 0, 1, with generating matrix:

$$G(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & -1 & -1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & -1 & 0 & -1 \end{bmatrix}.$$

The code C is called the *Golay ternary code*. The minimal (nonzero) weight in C is 6 [it takes a bit of puzzling over $G(C)$ to actually see this]. A computer search finds 264 vectors of weight 6 in C. Since a vector and its negative have the same support, there will be at most 132 distinct supports for the 264 vectors of weight 6. As it turns out there are precisely 132 distinct supports. These 132 supports are the blocks of a $5-(12,6,1)$ design, called the *Mathieu* 5-*design* on 12 points. The design is listed on page 270, with rows as blocks.

7.10 The Method of Differences

Let G be an Abelian group with addition as group operation. For a subset α of size k of G consider the list of $k(k-1)$ (ordered) differences of its elements. Call a collection of k-subsets $\alpha_1, \alpha_2, \ldots, \alpha_m$ a *set of generating blocks* if among the $mk(k-1)$ differences coming from these k-subsets each nonzero element of G occurs λ times.

If $\alpha_1, \ldots, \alpha_m$ is a set of generating blocks, then the collection of k-subsets $\{\alpha_i + a : a \in G\}$, $1 \le i \le m$, is a $2-(v,k,\lambda)$ design, with the elements of G as points. (Here $v = |G|$, $\lambda_1 = mk$, and $\lambda_0 = mv$.)

To illustrate this method of construction we take G to be the Abelian (cyclic) group with 13 elements. The difficulty always rests in selecting a set of generating blocks (especially since sometimes they do not exist). In this case take $\alpha_1 = \{1, 3, 9\}$ and $\alpha_2 = \{2, 6, 5\}$. The list of differences is:

$$\text{from } \alpha_1 : 1-3 = 11,\ 1-9 = 5,\ 3-9 = 7, 9-3 = 6,\ 9-1 = 8,\ 3-1 = 2$$

$$\text{from } \alpha_2 : 2-6 = 9,\ 2-5 = 10,\ 6-5 = 1,\ 5-6 = 12,\ 5-2 = 3,\ 6-2 = 4.$$

We conclude that λ equals 1 in this case. By expanding the two blocks we obtain the $2-(13, 3, 1)$ design listed below:

1	2	3	4	5	6	7	8	9	10	11	12	13
3	4	5	6	7	8	9	10	11	12	13	1	2
9	10	11	12	13	1	2	3	4	5	6	7	8

2	3	4	5	6	7	8	9	10	11	12	13	1
6	7	8	9	10	11	12	13	1	2	3	4	5
5	6	7	8	9	10	11	12	13	1	2	3	4

7.11 Construction through Hypergraphs

A *hypergraph* H is simply a collection of subsets (called *edges*) of a set. We also assume that every element of the set is on at least one edge. An *automorphism group* G of H is a group of permutations on the elements of the set that preserves the edges of H. Nontrivial designs with t as high as 5 (and possibly 6) have been obtained as follows:

Take the edges of H as the points of the design. Then G has a natural action on the subsets of k edges. Unions of certain (carefully selected) orbits under this action form a

t-design ($2 \leq t < k$).

As a small example, let H be the set of (ordinary) edges of the complete graph on five vertices. Our prospective design will thus have $\binom{5}{2} = 10$ points.

1 2 4 10 11 12	1 4 6 8 10 12	1 3 4 9 10 11
1 3 8 10 11 12	1 4 7 9 10 12	1 3 5 6 8 10
1 5 9 10 11 12	1 5 6 8 9 12	1 3 5 7 10 11
1 6 7 10 11 12	1 5 7 8 10 12	1 3 5 8 9 11
2 3 5 10 11 12	2 3 4 5 7 12	1 3 6 7 9 11
2 6 9 10 11 12	2 3 4 9 10 12	1 3 7 8 9 10
2 7 8 10 11 12	2 3 5 6 9 12	1 4 5 6 10 11
3 4 6 10 11 12	2 3 6 8 10 12	1 4 5 7 9 11
3 7 9 10 11 12	2 3 7 8 9 12	1 4 5 8 9 10
4 5 7 10 11 12	2 4 5 8 10 12	1 4 6 7 8 9
4 8 9 10 11 12	2 4 6 7 10 12	1 4 7 8 10 11
5 6 8 10 11 12	2 4 6 8 9 12	1 5 6 7 8 11
1 2 3 9 11 12	2 5 6 7 8 12	1 5 6 7 9 10
1 2 5 7 11 12	2 5 7 9 10 12	1 6 8 9 10 11
1 2 6 8 11 12	3 4 5 6 8 12	2 3 4 5 6 10
1 3 4 7 11 12	3 4 6 7 9 12	2 3 4 5 8 9
1 3 5 6 11 12	3 4 7 8 10 12	2 3 4 6 7 8
1 4 5 8 11 12	3 5 6 7 10 12	2 3 4 6 9 11
1 4 6 9 11 12	3 5 8 9 10 12	2 3 4 7 10 11

1	7	8	9	11	12		4	5	6	9	10	12		2	3	5	6	8	11
2	3	4	8	11	12		4	5	7	8	9	12		2	3	5	7	8	10
2	3	6	7	11	12		6	7	8	9	10	12		2	3	5	7	9	11
2	4	5	6	11	12		1	2	3	4	5	11		2	3	6	7	9	10
2	4	7	9	11	12		1	2	3	4	7	9		2	3	8	9	10	11
2	5	8	9	11	12		1	2	3	4	8	10		2	4	5	6	7	9
3	4	5	9	11	12		1	2	3	5	6	7		2	4	5	7	8	11
3	5	7	8	11	12		1	2	3	5	9	10		2	4	5	9	10	11
3	6	8	9	11	12		1	2	3	6	8	9		2	4	6	8	10	11
4	6	7	8	11	12		1	2	3	6	10	11		2	4	7	8	9	10
5	6	7	9	11	12		1	2	3	7	8	11		2	5	6	7	10	11
1	2	3	4	6	12		1	2	4	5	6	8		2	5	6	8	9	10
1	2	3	5	8	12		1	2	4	5	7	10		2	6	7	8	9	11
1	2	3	7	10	12		1	2	4	6	7	11		3	4	5	6	7	11
1	2	4	5	9	12		1	2	4	6	9	10		3	4	5	7	9	10
1	2	4	7	8	12		1	2	4	8	9	11		3	4	5	8	10	11
1	2	5	6	10	12		1	2	5	6	9	11		3	4	6	8	9	10
1	2	6	7	9	12		1	2	5	7	8	0		3	4	7	8	9	11
1	2	8	9	10	12		1	2	5	8	10	11		3	5	6	7	8	9
1	3	4	5	10	12		1	2	6	7	8	10		3	5	6	9	10	11
1	3	4	8	9	12		1	2	7	9	10	11		3	6	7	8	10	11
1	3	5	7	9	12		1	3	4	5	6	9		4	5	6	7	8	10
1	3	6	7	8	12		1	3	4	5	7	8		4	5	6	8	9	11
1	3	6	9	10	12		1	3	4	6	7	10		4	6	7	9	10	11
1	4	5	6	7	12		1	3	4	6	8	11		5	7	8	9	10	11

Take the block size to be 4. The automorphism group in question will be S_5, the symmetric group on the five vertices. The three orbits with orbit representatives $\{12, 14, 23, 34\}$, $\{12, 13, 14, 15\}$, and $\{12, 13, 23, 45\}$ form a $3-(10, 4, 1)$ design. By drawing out the subgraphs corresponding to these three orbit representatives one can easily check that any three edges of the complete graph on five vertices is contained in exactly one image of one of our initial three subgraphs. The 5-transitivity of S_5 is what simplifies things significantly in this particular example.

The list of construction procedures that we gave is by no means exhaustive. Generating projective planes through complete sets of latin squares is but one example of well-known constructions that we do not include. Of special interest would be constructions that lead to nontrivial t-designs with high values of t. For $t \geq 7$ no such constructions are yet known.

A Justification That the Methods of Construction Described so Far Indeed Generate the t-Designs We Claimed They Do: Hadamard Matrices

In the introductory pages to this section we discussed Hadamard matrices and their existence in particular. A necessary condition for a Hadamard matrix H of order n to exist (with $n \geq 4$) is that n actually be a multiple of 4. Indeed, multiplying suitable rows of H by -1 makes the first column of H consist of all 1's. Look now at the first three columns only. Denote by x the number of rows of the form $(1, 1, 1)$, by y those of the form $(1, 1, -1)$, by z and w those of the form $(1, -1, 1)$ and $(1, -1, -1)$, respectively. (Then $x+y+z+w = n$.) Writing in terms of x, y, z, w the fact that any pair of the three distinct columns are orthogonal, we obtain a system of linear equations with solution

$x = y = z = w$ $(= n/4)$. Since x is obviously integral we conclude that 4 divides n, necessarily.

Hadamard matrices are well researched, existence being a central problem. Many constructions are known, of which we mentioned several. We refer the reader to the expository article [17] and the references contained therein for the detailed proofs.

The Hadamard 2-Designs (Section 7.3)

Let the first row and column of H consist of 1's only. Fix the first column and two additional (distinct) columns; the two additional columns correspond to two distinct points in our prospective design. Then the number of blocks containing these two points equals the number of vectors of the form $(1, 1, 1)$ across the three columns, minus one. The "minus one" is the vector $(1, 1, 1)$ from the *first* row of H which has in effect been deleted. From our previous discussion, in which we showed that the dimension of a Hadamard matrix must be a multiple of 4, we know that there are precisely $n/4$ vectors of the form $(1, 1, 1)$. Hence two (arbitrary) points are always in precisely $\frac{n}{4} - 1$ blocks. We thus have a 2-design with $\lambda_2 = \frac{n}{4} - 1$.

The Paley Designs (Section 7.4)

Let Q be the set of nonzero squares in $GF(q)$, with q equal to 3 modulo 4. The first thing to observe is that -1 is not a square in such a field. [If it were we could write $-1 = w^2$ or $1 = w^4$. Since the nonzero elements of $GF(q)$ form a group with respect to multiplication, the order of w must divide the order of the group, that is, 4 must divide $q - 1$. This contradicts the fact that q equals 3 modulo 4.] The second observation is that d $(\neq 0)$ is a square if and only if $-d$ is not a square. One can see this by recalling

that the multiplication structure of $GF(q)$ is in fact a cyclic group. If ξ generates this group, then the even powers of ξ are the (nonzero) squares in $GF(q)$; there are $\frac{1}{2}(q-1)$ of these. The remaining half are not squares. It is also clear that not both d and $-d$ can be squares because then -1 would also be a square, as their quotient. This tells us that the set of nonsquares of $GF(q)$ is precisely $\{-d : d \text{ a nonzero square in } GF(q)\}$.

The points of our design are the q elements of the field $GF(q)$ and the blocks are the subsets $\{Q + a : a \in GF(q)\}$. To check that we do indeed have a 2-design we have to show that every two (distinct) elements of $GF(q)$ are in the same number of blocks. Let x and y be two such elements. Then

$$\begin{aligned}
|\{\alpha \ : \ & \{x,y\} \in \alpha,\ \alpha \text{ block}\}| \\
&= |\{a \in GF(q) : \{x,y\} \in Q + a\}| \\
&= |\{a \in GF(q) : x - a \in Q \text{ and } y - a \in Q\}| \\
&= |\{a \in GF(q) : x - a = \alpha^2 \text{ and } y - a = \beta^2, \text{ with } \alpha, \beta \neq 0\}| \\
&= |\{(\alpha^2, \beta^2) : \alpha^2 - \beta^2 = x - y, \ \alpha \text{ and } \beta \neq 0\}|.
\end{aligned}$$

Now if $x - y$ is a square, say γ^2, then (dividing out by γ^2) one can see that $\alpha^2 - \beta^2 = \gamma^2$ has the same number of solutions as the equation $s^2 - u^2 = 1$. If $x - y$ is not a square, then we pointed out that $-(x - y)$ must be a square, say δ^2 , and $\alpha^2 - \beta^2 = -\delta^2$ has again precisely as many solutions as $u^2 - s^2 = 1$ (or $s^2 - u^2 = 1$) does. This constant number of solutions is therefore independent of x and y and it equals the number of blocks containing two points. We have thus proved that the sets $\{Q + a : a \in GF(q)\}$ form a 2-design. The reader might wish to compute its parameters as functions of q only. [*Hint*: Find $k = |Q|$ first, then λ_1.]

The Hadamard 3-Designs (Section 7.5)

Assume, without loss, that the first row of the Hadamard matrix has all its entries equal to 1. With each row (other than the first) we associate two blocks. Observe that we do not affect these two blocks if we multiply the row by -1.

Select now three columns of H; this corresponds to selecting three distinct points. The number of blocks containing these three points equals the number of vectors of the form $(1,1,1)$ or $(-1,-1,-1)$ across the three columns (excepting the first row). Multiply now by -1 all the rows in which $(-1,-1,-1)$ occurs across the three columns. The number of blocks containing the three points equals now the number of rows having $(1,1,1)$ across the three columns, minus one. We subtract one because the first row does not generate blocks. We know (see the proof for Hadamard 2-designs) that there are precisely $n/4$ vectors of the type $(1,1,1)$ throughout H in the three columns. Three points are therefore contained in $\frac{n}{4}-1$ blocks.

The Projective Geometries (Section 7.6)

In a vector space V of dimension $n+1$ over $GF(q)$ fix two (distinct) subspaces of dimension 1. The two subspaces of dimension 1 necessarily generate a subspace W of dimension 2. The number of subspaces of dimension $m+1$ (with $2 \leq m \leq n$) containing W equals the number of subspaces of dimension $m-1$ in the quotient space V/W. The number of such subspaces equals $\begin{bmatrix} n-1 \\ m-1 \end{bmatrix}(q)$, where $\begin{bmatrix} n \\ k \end{bmatrix}(x)$ denotes the Gaussian polynomial (see Section 6 in Chapter 3). Since the number of subspaces of dimension $m+1$ containing two distinct subspaces of dimension 1 is independent of the choice of the two one-dimensional subspaces [as it always equals $\begin{bmatrix} n-1 \\ m-1 \end{bmatrix}(q)$], we conclude that the structure so defined is a

2-design.

The projective geometries do not generate 3-designs in the same manner. For if we choose three (projective) points they may generate a subspace of (vector space) dimension 2 or 3. In the former case they will be in $\begin{bmatrix} n-1 \\ m-1 \end{bmatrix}(q)$ subspaces of (vector space) dimension $m+1$, while in the latter case they will be in $\begin{bmatrix} n-2 \\ m-2 \end{bmatrix}(q)$ such subspaces.

We leave to the reader the task of computing the remaining parameters of these 2-designs. After doing so it is easy to check that when $m = n-1$ we obtain a symmetric design.

The Affine Geometries (Section 7.7)

The affine geometry consists of parallel classes of cosets. When selecting two distinct points this allows us to choose one as the origin, without loss of generality. It is now clear that the number of (affine) subspaces of dimension m containing the origin and the other point (call it x) equals the number of (vector space) subspaces of dimension m containing the one-dimensional subspace generated by x. There are $\begin{bmatrix} n-1 \\ m-1 \end{bmatrix}(q)$ such m-dimensional subspaces, where n is the dimension of the whole vector space [over $GF(q)$]. This number is independent of the original choice of the two points. We thus have a 2-design. The other parameters are even easier to establish and we omit these details.

In a vector space over $GF(2)$ the situation is even nicer (due mostly to the lack of room!). Select three distinct points among which one is the origin (without loss). Then necessarily the other two must be linearly independent (as vectors) and hence must span a subspace of (vector space) dimension 2. The number of affine subspaces of affine dimension m containing the three points equals the number of (vector space) subspaces of dimension

m that contain them. There are $\begin{bmatrix} n-2 \\ m-2 \end{bmatrix}$ (2) of these. We thus have a 3-design.

The Multiply Transitive Groups (Section 7.8)

The Mathieu groups M_{12} and M_{24} mentioned in Section 7.8 are 5-transitive groups on 12 and 24 letters, respectively. We refer the reader to [13, pp. 637 and 648] for proofs of 5-transitivity. A general treatment of permutation groups can be found in [14].

Constructions through Linear Codes (Section 7.9)

A result of Assmus and Mattson (see [13, p. 177]) gives sufficient conditions for constructing t-designs from codes. Families of 5-designs have been generated by this method.

The 5-design of Mathieu (on 12 points) that we have listed in its entirety has been generated by the author on a CDC 6600 computer. We list the design as a successive three point extension of the affine plane $AG(2,3)$, that is, of the $2-(9,3,1)$ design, see (7.5). The reader will observe that the one point extension is the design listed in (7.3), which is a $3-(10,4,1)$ design.

The Method of Differences (Section 7.10)

Let x and y be two distinct elements of G. For a fixed i we refer to $\{\alpha_i + a : a \in G\}$ as the cycle generated by the block α_i. Suppose x and y are in a block β. The block β is in some cycle, say the cycle generated by α_i. Then $\beta = \alpha_i + a$, for some a in G, and in particular $x = c+a$ and $y = d+a$, with c and d elements of α_i. The mapping $\beta \to (c,d)$ is a bijection between the blocks containing x and y and the ordered pairs in the generating blocks whose differences equal $x - y$. There are, by construction, λ such pairs for any nonzero element of G. There are hence λ blocks containing two distinct elements of G. We thus have a 2-design.

Construction through Hypergraphs (Section 7.11)

We mention here the general approach of constructing t-designs through hypergraphs which the reader can find in [16]. Let O_j^k denote the jth orbit in the action of the group G on the k-subsets of edges of H, and let O_i^t denote the ith orbit of G on the t-subsets of edges of H $(2 \leq t < k)$. For a t-subset σ_t in O_i^t denote by a_{ij} the number of k-subsets of O_j^k in which σ_t is contained. The number a_{ij} is well defined in the sense that it only depends on O_i^t and O_j^k and not on the specific choice of σ_t in O_i^t. (This is clearly so because of the transitive action of G within an orbit.) Form the matrix $A(t,k) = (a_{ij})$ with the rows indexed by the orbits of the t-subsets of edges. The following statement is now self-evident:

If there exists a vector x with entries 0 and 1 such that $A(t,k)x = \lambda_t x$ then there exists a $t-(v,k,\lambda_t)$ design. (Hence v is the total number of edges of the hypergraph H.)

It is generally complicated to even determine the dimensions of the matrix $A(t,k)$. This involves the counting of orbits under the action of a group. A substantial theory has been developed in Chapter 6 to handle just this problem. Computing the entries of $A(t,k)$ is no less complicated a task. Much of the work undertaken in this direction involves significant computer interaction.

3 FISHER'S INEQUALITY

7.12

Fisher proved the inequality that bears his name for 2-designs. This inequality informs us that *in a* $2-(v,k,\lambda_2)$ *design we must necessarily have at least as many blocks as points*, that is, $\lambda_0 \geq v$.

The original proof, which Fisher gave, goes as follows: Denote by J the matrix with all its entries 1 and by I the identity matrix. Let $N = (n_{ij})$ be the $v \times \lambda_0$ incidence matrix of points versus blocks; that is, $n_{ij} = 1$ if point i belongs to block j and 0 otherwise. Then NN' is a $v \times v$ matrix with all its diagonal entries equal to λ_1 and all its off diagonal entries equal to λ_2. Write therefore $NN' = (\lambda_1 - \lambda_2)I + \lambda_2 J$. The matrix $NN' - (\lambda_1 - \lambda_2)I = \lambda_2 J$ has rank 1 and its nonzero eigenvalue is $\lambda_2 v$ (the value of the rows sums of $\lambda_2 J$). This tells us that NN' has eigenvalues $(\lambda_1 - \lambda_2) + v\lambda_2 = \lambda_1 + (v-1)\lambda_2$ of multiplicity 1, and $\lambda_1 - \lambda_2$ of multiplicity $v - 1$. All these eigenvalues are strictly positive [since $\lambda_1 - \lambda_2 = 0$ implies $(v-1)(k-1)^{-1}\lambda_2 = \lambda_2$, or $k = v$, which we do not allow]. Hence the matrix NN' is *nonsingular*. The rank of N must therefore be v and thus N must have at least v columns, that is, $\lambda_0 \geq v$. This ends the proof of Fisher's inequality for 2-designs.

A 2-design in which the number of blocks actually equals the number of points is called *symmetric*. Examples are the Hadamard $2 - (n-1, \frac{n}{2} - 1, \frac{n}{4} - 1)$ designs and the $PG(n, q)$'s of which the projective planes are special cases. Symmetry has strong geometric implications concerning the intersections of blocks. Our next result shows what these implications are.

Proposition 7.2. *In a* $2 - (v, k, \lambda_2)$ *design the following conditions are equivalent*:

(i) $\lambda_0 = v$.

(ii) $\lambda_1 = k$.

(iii) *Any two distinct blocks intersect in* λ_2 *points.*

Proof. Observe that $\lambda_0 = v(v-1)k^{-1}(k-1)^{-1}\lambda_2 = vk^{-1}\lambda_1$. From this it directly follows that (i) and (ii) imply each other. Let N denote the incidence matrix between points and

blocks. We know that N has rank v (from the proof of Fisher's inequality, which we just gave).

Assume condition (i). This implies that N is a $v \times v$ (nonsingular) matrix. The matrix N satisfies $NJ = JN$ [this simply being condition (ii), which (i) implies]. Since N commutes with J and since $NN' = (\lambda_1 - \lambda_2)I + \lambda_2 J$, we conclude that N commutes also with NN'. Then $N'N = N^{-1}(NN')N = N^{-1}N(NN') = NN' = (\lambda_1 - \lambda_2)I + \lambda_2 J$. The matrix $N'N$ has as (i, j)th entry the cardinality of the intersection of the blocks i and j. The fact that $N'N = (\lambda_1 - \lambda_2)I + \lambda_2 J$ tells us that any two distinct blocks intersect in λ_2 points; this is statement (iii). We thus showed that (i) implies (iii).

To see that (iii) implies (i) think of the blocks as "points" and of the points as "blocks" with a "point" belonging to a "block" if the block contains the respective point. Statement (iii) tells us that any two "points" are in λ_2 "blocks." Our "points" and "blocks" form therefore a $2 - (\lambda_0, \lambda_1, \lambda_2)$ design. Fisher's inequality written for this design gives $v \geq \lambda_0$. In our original $2 - (v, k, \lambda_2)$ design we have $\lambda_0 \geq v$. Hence $\lambda_0 = v$ and we conclude the proof of our proposition.

The reader should observe the nice *duality* between points and blocks that exists in a symmetric design. Results about points could be dualized into results concerning blocks and conversely.

7.13

The several extensions of Fisher's inequality to t-designs are described in the remaining pages of Section 3. We follow the vector space approach given in [3], although shorter proofs involving matrices exist. To start with we prove Fisher's inequality for t-designs

with even t:

$*$ *Let* (PB) *be a* $t-(v,k,\lambda_t)$ *design with* $t=2s$ *(and* $v \geq k+s$*). Then* $\lambda_0 \geq \binom{v}{s}$.

Proof. Let V be a vector space (over the real numbers) with basis indexed by $\sum_s(P)$; $\dim V = \binom{v}{s}$. Consider the subspace

$$V(B) = \left\langle \hat{\alpha} = \sum_{\sigma_s \subseteq \alpha} \sigma_s : \alpha \in B \right\rangle$$

spanned by the λ_0 vectors $\hat{\alpha}, \alpha \in B$. (In writing $\sum_{\sigma_s \subseteq \alpha} \sigma_s$ we identify σ_s in the sum with the basis vector whose index is σ_s.)

We claim that $V(B) = V$. [If we show this, then the number of vectors in the span of $V(B)$ is at least equal to the number of vectors in the basis of V, that is, $|V(B)| = \lambda_0 \geq \binom{v}{s}$, as is to be shown.]

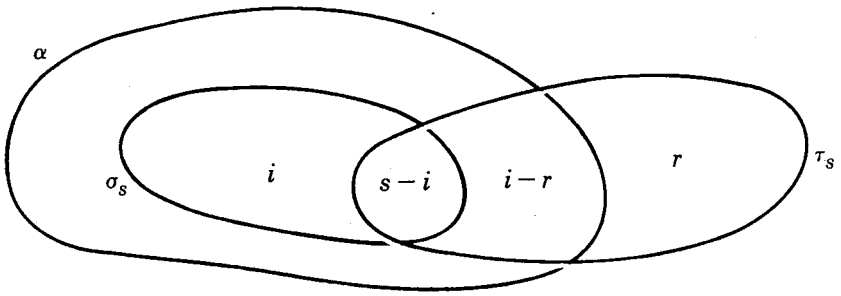
Let $\tau_s \in \sum_s(P)$ be fixed. Denote

$$e_i = \sum_{|\sigma_s \cap \tau_s| = s-i} \sigma_s;$$

(note that $e_0 = \tau_s$) and

$$f_i = \sum_{|\alpha \cap \tau_s| = s-i} \hat{\alpha},$$

for $i = 0, 1, \ldots, s$. (Clearly $f_i \in V(B)$, $0 \leq i \leq s$.) We can express f_r as a linear combination of the e_i's. (The figure below captures the details.) For $\sigma_s \in \sum_s(P)$ with $|\sigma_s \cap \tau_s| = s - i$ the coefficient of σ_s in f_r is: the number of blocks α such that $\sigma_s \subseteq \alpha$ and $|\alpha \cap \tau_s| = s - r$.



(To see this fix r points in τ_s; there are then $\lambda_i^r+(s-i)+(i-r) = \lambda_s^r-r+i$ blocks α as above that omit these specific r points.) The required coefficient is therefore $\binom{s-(s-i)}{r}\lambda^r_{s-r+i}$. Hence

$$f_r = \sum_{i=r}^{s} \binom{i}{r} \lambda^r_{s-r+i} e_i, \qquad 0 \le r \le s.$$

The associated matrix is $\left(\binom{i}{r}\lambda^r_{s-r+i}\right)_{0\le r\le s, r\le i\le s}$ (the rows being indexed by r). This is an upper triangular matrix; its diagonal elements, λ_s^i, are in fact nonzero since

$$\lambda_s^i = 0 \quad \text{if and only if } \binom{v-s-i}{k-s}\binom{v-t}{k-t}^{-1}\lambda_t = 0$$
$$\text{if and only if } k+s > v$$

(but our hypothesis assumes $v \ge k+s$). Hence the matrix $\left(\binom{i}{r}\lambda^r_{s-r+i}\right)$ is *nonsingular* and we may solve for $e_0 = \tau_s$ as a linear combination of the f_r's. This shows that $\tau_s \in V(B)$ and hence $V \subseteq V(B)$, which establishes the claim and concludes the proof.

Occasionally Fisher's inequality allows us to conclude the nonexistence of certain t-designs. Consider, for example, whether or not a $6-(120m, 60m, (20m-1)(15m-1)(12m-1))$ design exists. The numbers

$$\lambda_i = \frac{\binom{120m-i}{6-i}}{\binom{60m-i}{6-i}}(20m-1)(15m-1)(12m-1)$$

are indeed all integers, $0 \le i \le 6$. However, Fisher's inequality requires $\lambda_0 \ge \binom{120m}{3}$. But

in this case

$$\begin{aligned}\lambda_0 &= \frac{\binom{120m}{6}}{\binom{60m}{6}}(20m-1)(15m-1)(12m-1)\\ &= 2(120m-1)(40m-1)(24m-1),\end{aligned}$$

which is strictly less than $\binom{120m}{3}$. A 6-design with these parameters, therefore, cannot exist.

7.14

We next give a version of Fisher's inequality for t-designs with odd t.

∗ *Let (P,B) be a $t-(v,k,\lambda_t)$ design with $t=2s+1$ (and $v-1\geq k+1$). Then $\lambda_0\geq 2\binom{v-1}{s}$.*

Proof. Let $a\in P$. Form the derived and residual designs on $P-\{a\}$; both of these are $2s$-designs on $v-1$ points. Applying Fisher's inequality (for even t) to each one of these leads to $\lambda_0\geq\binom{v-1}{s}+\binom{v-1}{s}$.

The lower bound on λ_0 can be sharpened with additional assumptions on the design:

∗ *Let (P,B) be a $t-(v,k,\lambda_t)$ design with $t=2s$ (and $v\geq k+s$). Assume that there exists a partition of the blocks $B=B_1\cup B_2\cup\cdots\cup B_r$ such that (P,B_i) is a $s-(v,k,\lambda_s(i))$ design, $1\leq i\leq r$. Then $\lambda_0\geq\binom{v}{s}+r-1$.*

Proof. With the same notation as in the proof of Fisher's inequality we recall that

$$V=V(B)=\langle\hat{\alpha}:\ \alpha\in B\rangle,\qquad \text{where } \hat{\alpha}=\sum_{\sigma_s\in\alpha}\sigma_s.$$

From our assumption we have

$$\sum_{\alpha\in B_i}\hat{\alpha}=\sum_{\alpha\in B_i}\sum_{\sigma_s\in\alpha}\sigma_s=\sum_{\text{all}}\sum_{\substack{\alpha\\ \sigma_s\subseteq\alpha}}\sigma_s=\lambda_s(i)\sum_{\text{all}}\sigma_s \tag{7.6}$$

[We understand $\sum_{\text{all}}$ to mean the sum of all σ_s with $\sigma_s \in \sum_s(P)$.] Choose now (and fix) $\alpha_i \in B_i$, $i = 1, 2, \ldots, r$. Expression (7.6) can be written as

$$\hat{\alpha}_i = \lambda_s(i) \sum_{\text{all}} \sigma_s - \sum_{\substack{\alpha \in B_i \\ \alpha \neq \alpha_i}} \hat{\alpha}.$$

Hence

$$\begin{aligned} V &= V(B) = \langle \hat{\alpha} : \alpha \in B \rangle \\ &= \left\langle \sum_{\text{all}} \sigma_s \text{ and } \hat{\alpha} : \text{ with } \alpha \in B - \{\alpha_1, \ldots, \alpha_r\} \right\rangle. \end{aligned}$$

V is therefore spanned by $\lambda_0 - r + 1$ vectors; thus $\lambda_0 - r + 1 \geq \binom{v}{s}$ = dimension of V, as desired. This ends the proof.

A design whose blocks can be partitioned as above is often called *resolvable*. An example is design (7.5) from Section 7.7. Verify the inequality we just proved for this example.

7.15

We next investigate when equality is achieved in Fisher's inequality.

A nonnegative integer μ is called an *intersection number* for the t-design (P, B) if there exist two *distinct* blocks α and β $(\in B)$ such that $|\alpha \cap \beta| = \mu$.

$*$ *Let* (P, B) *be a* $t - (v, k, \lambda_t)$ *design, with* $t = 2s$ *(and* $v \geq k + s$*). Suppose* (P, B) *has precisely* s *distinct intersection numbers:* $\mu_s < \mu_{s-1} < \cdots < \mu_1$ $(< k = \mu_0)$*. Then* $\lambda_0 = \binom{v}{s}$.

Proof. Let W be a vector space (over the real numbers) with basis indexed by α, $\alpha \in B$;

dim $W = \lambda_0$. For $\sigma_s \in \sum_s(P)$ define

$$\sigma_s^* = \sum_{\substack{\alpha \\ \alpha \supseteq \sigma_s}} \alpha.$$

Consider the subspace

$$W(S) = \langle \sigma_s^* : \sigma_s \in \sum_s(P) \rangle.$$

We prove that $W(S) = W$. [Observe that all σ_s^*'s are *distinct* and there are $\binom{v}{s}$ of them. If $W(S) = W$, then the span of $W(S)$ contains at least as many vectors as a basis of W; hence $\lambda_0 \geq \binom{v}{s}$ – we already know that $\lambda_0 \geq \binom{v}{s}$ by Fisher's inequality. Therefore $\lambda_0 \geq \binom{v}{s}$.]

Fix $\alpha \in B$. We prove that $\alpha \in W(S)$. Set

$$h_i = \sum_{\substack{\beta \in B \\ |\beta \cap \alpha| = \mu_i}} \beta, \qquad 0 \leq i \leq s.$$

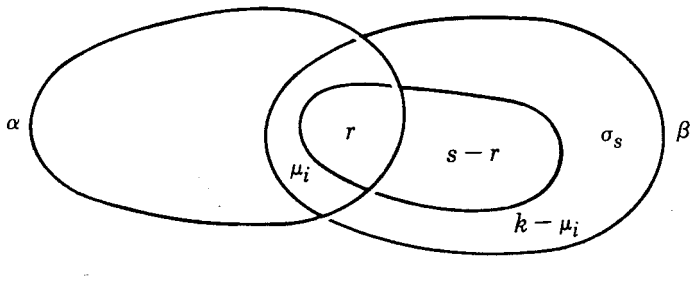
For consistency of notation we denote the block size k by μ_0. (Observe that $h_0 = \alpha$.) Let also

$$g_r = \sum_{\substack{\sigma_s \in \sum_s(P) \\ |\sigma_s \cap \alpha| = r}} \sigma_s^*, \qquad 0 \leq r \leq s.$$

The g_r's are of course in $W(S)$. We claim that

$$g_r = \sum_{i=0}^{s} \binom{\mu_i}{r} \binom{k - \mu_i}{s - r} h_i.$$

To see this fix $\beta \in B$, $|\beta \cap \alpha| = \mu_i$. We then want to count the number of σ_s such that $\sigma_s \subseteq \beta$ and $|\sigma_s \cap \alpha| = r$. There are $\binom{\mu_i}{r}\binom{k-\mu_i}{s-r}$ such choices as displayed below:



Form the matrix

$$\left(\binom{\mu_i}{r}\binom{k-\mu_i}{s-r}\right)_{\substack{0\le r\le s.\\ 0\le i\le s}}$$

If we show that this matrix is nonsingular, then we can solve for $h_0 = \alpha$ as a linear combination of g_r's and hence prove that $\alpha \in W(S)$; thus $W \subseteq W(S)$ and we are done.

To prove nonsingularity denote by v_r the rth row of our matrix, that is, $v_r = \left(\binom{\mu_0}{r}\binom{k-\mu_0}{s-r}, \ldots, \binom{\mu_s}{r}\binom{k-\mu_s}{s-r}\right)$. Assume $\sum_{r=0}^{s} c_r v_r = 0$ and consider the polynomial

$$f(x) = \sum_{r=0}^{s} c_r \binom{x}{r}\binom{k-x}{k-r}$$

[by $\binom{x}{r}$ we mean $[x]_r/r! = x(x-1)\cdots(x-r+1)/r!$]. The polynomial $f(x)$ has degree *at most* s. But $x = \mu_0, \mu_1, \ldots, \mu_s$ are all roots of $f(x)$ ($s+1$ of them!). Hence $f(x) \equiv 0$ for all x. Suitable choices of x give $c_r = 0$, for $0 \le r \le s$. The rows v_r of our matrix are therefore linearly independent; this establishes the nonsingularity and ends our proof.

7.16

We conclude Section 3 with a result that summarizes most of the previous ones. The reader should compare it with Proposition 7.2.

Fisher's Inequality. *Let (P, B) be a $t-(v,k,\lambda_t)$ design with $t = 2s$* (and $v \ge k+s$). *Then*

(i) $\lambda_0 \geq \binom{v}{s}$.

(ii) *The number of distinct intersection numbers for* (P, B) *is greater than or equal to* s.

(iii) $\lambda_0 = \binom{v}{s}$ *if and only if the number of distinct intersection numbers for* (P, B) *equals* s.

Proof. Statement (i) is Fisher's inequality in its initial form. To prove (ii) suppose there are u distinct intersection numbers with $u < s$. (P, B) is a $2s$-design, hence also a $2u$-design. The immediately previous result now gives $\lambda_0 = \binom{v}{u}$; but Fisher's inequality assures $\lambda_0 \geq \binom{v}{s} > \binom{v}{u}$, a contradiction [because $s \leq v-k$ and $s < k$ implies $0 \leq s < v/2$; in this range $u < s$ implies $\binom{v}{u} < \binom{v}{s}$].

To establish (iii) it remains to be shown that if $\lambda_0 = \binom{v}{s}$ then there are at most s (distinct) intersection numbers for (P, B). As in the first proof of Fisher's inequality (Section 7.13) we let V be the vector space over the real numbers freely spanned by σ_s, with $\sigma_s \in \sum_s(P)$; dimension of $V = \binom{v}{s}$. Let also $V(B) = \langle \hat{\alpha} : \alpha \in B \rangle$ with $\hat{\alpha} = \sum_{\sigma_s \subseteq \alpha} \sigma_s$. We know that $V(B) = V$ (see Section 7.13). Since we assume $\lambda_0 = \binom{v}{s}$ the vectors $\{\hat{\alpha} : \alpha \in B\}$ must be in fact a *basis* for V.

Fix $\alpha \in B$. Then put $\mu_\beta = |\beta \cap \alpha|$ for $B \ni \beta \neq \alpha$. We show that μ_β is the root of a polynomial $f(x)$ (independent of α) of degree $\leq s$. To prove this let

$$m_i = \sum_{|\sigma_s \cap \alpha| = i} \sigma_s, \qquad 0 \leq i \leq s$$

and let

$$n_r = \sum_{\beta \in B} \binom{\mu_\beta}{r} \hat{\beta}, \qquad 0 \leq r \leq s.$$

We first show that $n_r = \sum_{i=0}^{s} c_r^i m_i$, $0 \le r \le s$ where $c_r^i = \sum_{j=0}^{i} \binom{i}{j}\binom{k-i}{r-j}\lambda_{s+r-j}$ (independent of α). Take σ_s, $|\sigma_s \cap \alpha| = i$. The coefficient of σ_s in the sum n_r is $\sum_{\beta,\sigma_s\subseteq\beta}\binom{\mu_\beta}{r}$, that is, it equals the number of ordered pairs (β, σ_r) such that $\sigma_s \subseteq \beta$ and $\sigma_r \subseteq \alpha \cap \beta$. (We may, however, think that this number depends on α.) Let us compute it another way: for any $\sigma_r \subseteq \alpha$ with $|\sigma_r \cap \sigma_s| = j$, the number of blocks β such that (β, σ_r) satisfy $\sigma_s \subseteq \beta$ and $\sigma_r \subseteq \alpha \cap \beta$ is λ_{s+r-j}. Thus the coefficient of σ_s in n_r is $\sum_{j=0}^{i}\binom{i}{j}\binom{k-i}{r-j}\lambda_{s+r-j}$, which we denote by c_r^i. It is now clear that c_r^i is independent of α. Hence $n_r = \sum_{i=0}^{s} c_r^i m_i$, as claimed.

The $s+1$ vectors $n_r - c_r^s m_s$, $0 \le r \le s$, are contained in the span $\langle m_0, \ldots, m_{s-1}\rangle$; this span is of dimension at most s. Therefore the $s+1$ vectors mentioned above must be linearly dependent. Let $a_0, a_1, \ldots, a_s$ be constants, not all zero, such that

$$\sum_{r=0}^{s} a_r(n_r - c_r^s m_s) = 0.$$

Or

$$\sum_{r=0}^{s} a_r \left[\sum_{\beta\in B}\binom{\mu_\beta}{r}\hat{\beta} - c_r^s\hat{\alpha}\right] = 0$$

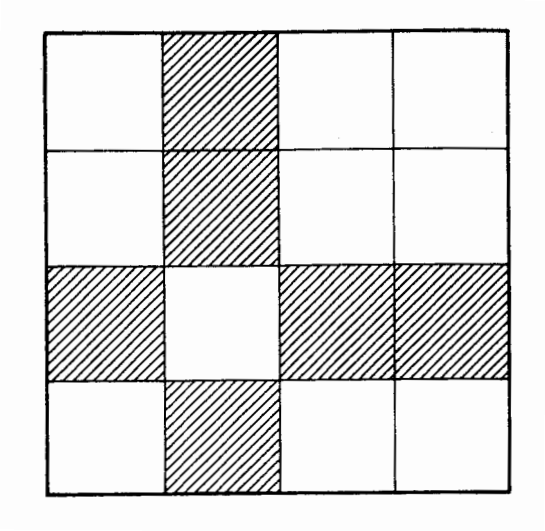
(observe that $m_s = \sum_{|\sigma_s\cap\alpha|=s}\sigma_s = \sum_{\sigma_s\subseteq\alpha}\sigma_s = \alpha$). Since $\{\hat{\beta} : \beta \in B)$ is a basis for V, for $\beta \ne \alpha$ the coefficient $\sum_{r=0}^{s} a_r\binom{\mu_\beta}{r}$ of $\hat{\beta}$ above must be 0. That is, for any $\beta \ne \alpha$ the intersection number μ_β is a root of the polynomial

$$f(x) = \sum_{r=0}^{s} a_r\binom{x}{r}$$

of degree *at most* s [recall again that $\binom{x}{r} = [x]_r/r!$]. The coefficients c_r^s are [and hence $f(x)$ is] independent of the block α; all intersection numbers are therefore roots of $f(x)$ (of which there are at most s). This ends the proof.

EXERCISES

1. Let P be the set of 16 small squares displayed below. To each small square attach the subset of the remaining 6 squares in the same row or column with it (see the figure below):



Show that the 16 subsets of size 6 thus obtained are the blocks of a symmetric 2-design.

2. Construct a Hadamard matrix of order 8 and one of order 12.

3. Suppose H is a Hadamard matrix having constant row and column sums. By taking as the ith block the index of the columns in the ith row of H in which the $+1$'s occur we obtain a symmetric 2-design. Prove this and find the parameters of the design. (Concerning the construction of such designs observe that the 4×4 Hadamard matrix $2I - J$ has constant row and column sums; this property is preserved under taking tensor products.)

4. Can a $2-(16,10,3)$ design exist? [*Hint*: Compute the determinant of NN' where N is the incidence matrix of points versus blocks.]

5. In a $2-(v,k,\lambda_2)$ design the number of blocks not disjoint from a given block α is at least

$$k(\lambda_1-1)^2((k-1)(\lambda_2-1)+\lambda_1-1)^{-1}.$$

Equality holds if and only if any block not disjoint from α intersects α in a constant number of points. Prove this.

6. List the 21 blocks of the projective plane $PG(2,4)$.

7. Three distinct points on the surface of an ordinary sphere determine a unique circle. Can you think of discrete analogs of this? [*Hint*: The sphere can be conveniently visualized as the field of complex numbers with a point at infinity. Given any two triples of distinct points there exists a map of the form $(az+b)(cz+d)^{-1}$, with $ad-bc\neq 0$, which sends one triple into the other. This allows a geometrical interpretation of the 3-design in (7.3).]

8. Show that a $2-(7,3,1)$ design must necessarily be $PG(2,2)$.

9. Show that a $3-(8,4,1)$ design must necessarily be $AG(3,2)$.

4 EXTENDING SYMMETRIC DESIGNS

7.17

Much of the material in the following three sections concerns symmetric 2-designs. Extending such structures means, roughly speaking, finding a larger t-design (with $t\geq 3$)

that contains the initial symmetric design. The motivating examples for such a study may well have been the symmetric Hadamard 2-designs that are contained in the Hadamard 3-designs, as the derived designs at a point – see again examples (7.1) and (7.2). The formal definitions and terminology are given below.

Let (P, B) be a $t-(v, k, \lambda_t)$ design. For an element a not in P let $\overline{P} = P \cup \{\alpha\}$. A $(t+1)$-design $(\overline{P}, \overline{B})$ is said to be an *extension* of (P, B) if (P, B) is the derived design at a of $(\overline{P}, \overline{B})$. A design that admits an extension is called *extendable*.

7.18

We now prove the following result due to Cameron:

If (P, B) *is a symmetric extendable* $2-(v, k, \lambda)$ *design* (with $k \leq v-1$), *then one of the following holds*:

(i) (P, B) *is a Hadamard* 2*-design with* $v = 4\lambda + 3$ *and* $k = 2\lambda + 1$.

(ii) $v = (\lambda+2)(\lambda^2+4\lambda+2)$, $k = \lambda^2+3\lambda+1$.

(iii) $v = 111$, $k = 11$, $\lambda = 1$.

(iv) $v = 495$, $k = 39$, $\lambda = 3$.

Proof. Let $\overline{D} = (\overline{P}, \overline{B})$ be an extension of (P, B). Then $\overline{D}$ is a $3-(v+1, k+1, \lambda_3(\overline{D}))$ design, with $\lambda_1(\overline{D}) = v$, $\lambda_2(\overline{D}) = k$, and $\lambda_3(\overline{D}) = \lambda$. For all $a \in \overline{P}$, set $\overline{D}_a = (\overline{P} - \{a\}, \{\alpha - \{a\} : a \in \alpha \in \overline{B}\})$; $\overline{D}_a = (P, B)$ for some $a \in \overline{P}$. Clearly $\overline{D}_a$ is a symmetric $2-(v, k, \lambda)$ design. So the *only* intersection number of $\overline{D}_a$ is λ (see Proposition 7.2). This implies that the only intersection numbers of $\overline{D}$ are $\lambda+1$ and 0.

Fix $\alpha \in \overline{B}$ and define $\overline{D}_\alpha = (\overline{P} - \alpha, \{\beta \in \overline{B} : \beta \cap \alpha = \emptyset\})$. We claim that $\overline{D}_\alpha$ is a

$2-(v-k,k+1,(k-\lambda)(\lambda+1)^{-1})$ design.

Let $a,b\in\overline{P}$; $a,b\notin\alpha$. Count the cardinality of the set $\{(\beta,c):\ a,b\in\beta-\alpha\ \text{ and }\ c\in\beta\cap\alpha;\ \beta\ \in\ \overline{B}\}$ in two different ways. We obtain (recalling that $c\ \in\ \beta\cap\alpha$ implies $|\beta\cap\alpha|=\lambda+1$)

$$|\{\beta\in\overline{B}:\ a,b\in\beta\ \text{ and }\ \beta\cap\alpha\neq\emptyset\}|(\lambda+1)=\lambda(k+1).$$

It follows that $|\{\beta\ \in\ \overline{B}\ :\ a,b\ \in\ \beta\ \text{ and }\ \beta\cap\alpha\ =\ \emptyset\}|\ =\ \lambda_2(\overline{D})-\lambda(k+1)(\lambda+1)^{-1}\ =\ k-\lambda(k+1)(\lambda+1)^{-1}=(k-\lambda)(\lambda+1)^{-1}>0$ (if $k=\lambda$, then $k=v$, contrary to our assumption). This proves that $\overline{D}_\alpha$ is a $2-(v-k,k+1,(k-\lambda)(\lambda+1)^{-1})$ design.

In particular, in $\overline{D}_\alpha$ the block size should not exceed the number of points, which means $v-k\geq k+1$.

1. Suppose $v-k=k+1$. Since (P,B) is a symmetric design we have $\lambda_0=v$ and hence also $k=\lambda_1=((v-1)/(k-1))\lambda$; replacing $v=2k+1$ gives $\lambda=\frac{1}{2}(k-1)$. Or, solving for k, $k=2\lambda+1$ and then $v=4\lambda+3$, which is (i).

2. If $v-k=k+2$, then $(\lambda_1\ =)\ k=(v-1)(k-1)^{-1}\lambda=(2k+1)(k-1)^{-1}\lambda$, or $\lambda=k(k-1)(2k+1)^{-1}$, which is not an integer. Hence this case can never happen.

3. Assume $v-k>k+2$. Then

$$\begin{aligned}\lambda_0(\overline{D}_\alpha)\ &=\ \frac{(v-k)(v-k-1)}{(k+1)k}\lambda_2(\overline{D}_\alpha)=\frac{(v-k)(v-k-1)(k-\lambda)}{(k+1)k(\lambda+1)}\\ &=\ \left\{\text{since }\ \lambda=\frac{k(k-1)}{v-1}\right\}=\frac{(v-k)^2(v-k-1)}{(k+1)(k^2-k+v-1)}\geq v-k\end{aligned}$$

(this being Fisher's inequality applied to $\overline{D}_\alpha$). Or, equivalently,

$$v^2-(3k+2)v-(k+1)(k^2-2k-1)\geq 0. \tag{7.7}$$

Consider the quadratic $x^2 - (3k+2)x - (k+1)(k^2-2k-1)$ with roots $x = \frac{1}{2}[(3k+2) \pm k\sqrt{4k+5}]$. Since $x = \frac{1}{2}[(3k+2) - k\sqrt{4k+5}] \leq 1$ for all integral k, the solution to (7.7) is

$$v \geq \frac{1}{2}[(3k+2) + k\sqrt{4k+5}]. \tag{7.8}$$

Put $\sqrt{4k+5} = 3 + 2\mu$, for $\mu > 0$. Then $k = \mu^2 + 3\mu + 1$ and (7.8) becomes $v \geq \mu^3 + 6\mu^2 + 10\mu + 4 = (\mu+2)(\mu^2+4\mu+2)$. Hence

$$\lambda = \frac{k(k-1)}{v-1} \leq \frac{(\mu^2+3\mu+1)(\mu^2+3\mu)}{\mu^3+6\mu^2+10\mu+3} = \frac{(\mu^2+3\mu+1)(\mu+3)\mu}{(\mu^2+3\mu+1)(\mu+3)} = \mu,$$

so that $k = \mu^2 + 3\mu + 1 \geq \lambda^2 + 3\lambda + 1$,or

$$k + 1 \geq (\lambda+1)(\lambda+2). \tag{7.9}$$

But $\lambda_0(\overline{D}) = (v+1)v/(k+1)$, which shows that $k+1$ divides $(v+1)v$. [Since $\lambda = k(k-1)/(v-1)$, we have $(v+1)v = \lambda^{-2}(k^2-k+\lambda)(k^2-k+2\lambda)$.] Therefore $k+1$ divides $(k^2-k+\lambda)(k^2-k+2\lambda)$; looking at the remainder we finally conclude that

$$k+1 \text{ divides } 2(\lambda+1)(\lambda+2). \tag{7.10}$$

Conditions (7.9) and (7.10) restrict k very much. In fact we can only have

$$k+1 = 2(\lambda+1)(\lambda+2) \quad \text{or} \quad k+1 = (\lambda+1)(\lambda+2).$$

Assume $k+1 = 2(\lambda+1)(\lambda+2)$. Since $\lambda = k(k-1)/(v-1)$, λ divides $k(k-1) = (2\lambda^2+6\lambda+3)(2\lambda^2+6\lambda+2)$; looking at the remainder we conclude that λ divides 6. Hence $\lambda = 1, 2, 3,$ or 6. For $\lambda = 2$ or 6, $k+1$ does not divide $v(v+1)$. Thus $\lambda = 1$ or 3, giving cases (iii) and (iv), respectively.

The case $k+1 = (\lambda+1)(\lambda+2)$ gives $\lambda = \mu$, leading to (ii); in this case $v = (\lambda+2)(\lambda^2+4\lambda+2)$ and we obtain a $2-((\lambda+1)^2(\lambda+3),(\lambda+1)(\lambda+2),(\lambda+1))$ design for $\overline{D}_\alpha$. This ends the proof.

7.19

Consequence. *If (P,B) is a twice or three times extendable symmetric 2-design, then (P,B) is the unique $2-(21,5,1)$ design. There is no four times extendable symmetric 2-design.*

Proof. Let (P,B) be a symmetric twice extendable $2-(v,k,\lambda)$ design. Counting the number of blocks in the second extension [and using the fact that $\lambda_i = \binom{v-i}{k-i}\binom{k-i}{t-i}$; $i=0,1$] we find that $(k+1)(k+2)$ divides $v(v+1)(v+2)$. For the various possibilities for (P,B) listed in the previous result this leads to:

(i) $(2\lambda+3)$ divides $4(\lambda+1)(4\lambda+3)(4\lambda+5)$ which, upon looking at the remainder, tells us that $(2\lambda+3)$ divides 3; this cannot happen.

(ii) $\lambda^2+3\lambda+3$ divides

$$(\lambda+1)(\lambda+2)(\lambda^2+4\lambda+2)(\lambda^2+5\lambda+5)(\lambda^3+6\lambda^2+10\lambda+6),$$

leading us to conclude that $\lambda^2+3\lambda+3$ divides $\lambda+6$ (again upon looking at the remainder). This can only happen for $\lambda = 1$. Then (P,B) is a $2-(21,5,1)$ design, the 21 point projective plane $PG(2,4)$. There is up to isomorphism a unique such object and it is actually three times extendable [leading to the Mathieu $5-(24,8,1)$ design]. Since $4\cdot5\cdot6\cdot7\cdot8\cdot9$ does not divide $20\cdot21\cdot22\cdot23\cdot24\cdot25$ it is not four times extendable.

(iii) 13 does not divide $111\cdot112\cdot113$.

(iv) Finally, 41 does not divide $495 \cdot 496 \cdot 497$.

5 ON THE EXISTENCE OF SYMMETRIC DESIGNS

Necessary conditions for a $2-(v,k,\lambda_2)$ design to exist are that $\lambda_i = \binom{v-i}{2-i}\binom{k-i}{2-i}^{-1}\lambda_2$, $i = 0, 1$, be integers and that $\lambda_0 \geq v$ (which is Fisher's inequality). These conditions are in general far from being sufficient. Even with the additional assumption of symmetry they do not suffice. In this section we give another necessary condition for the existence of a (symmetric) 2-design. The result is known as Bruck, Ryser, and Chowla's (BRC) theorem. Since in this section we discuss 2-designs we write λ for λ_2.

7.20

The proof of the BRC theorem is based on rational congruences, Witt's cancellation law, and a result of Lagrange in number theory. We first define what is meant by rational congruence.

Two square and symmetric matrices A and B with rational entries (and of the same dimension) are called *rationally congruent* (written $A \overset{c}{=} B$) if there exists a nonsingular matrix P with rational entries such that $P'AP = B$. (The relation $\overset{c}{=}$ is an equivalence relation, and this is easy to check.)

The result of Lagrange to which we made reference is the following:

Lagrange's Result. *For any positive integer m we have $mI_4 \overset{c}{=} I_4$.*

[Here, and throughout this section, I_n denotes the $n \times n$ identity matrix. Lagrange's original result states that any positive integer m is the sum of four squares, that is,

$m = a^2 + b^2 + c^2 + d^2$ with a, b, c, d nonnegative integers. But then

$$\begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ d & c & -b & -a \\ c & -d & -a & b \end{pmatrix} I_4 \begin{pmatrix} a & b & d & c \\ b & -a & c & -d \\ c & d & -b & -a \\ d & -c & -a & b \end{pmatrix} = mI_4$$

showing that $mI_4 \overset{c}{=} I_4$, as stated above.]

The other result that we need is the following.

Witt's Cancellation Law. *If* $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \overset{c}{=} \begin{pmatrix} C & 0 \\ 0 & D \end{pmatrix}$ *and* $A \overset{c}{=} C$, *then* $B \overset{c}{=} D$.

The proofs of these two results are included in Appendix 3.

7.21

We now state and prove the BRC theorem:

The Theorem of Bruck, Ryser, and Chowla. *Suppose* v, k, λ *are natural numbers such that a symmetric* $2 - (v, k, \lambda)$ *design exists* (and $0 \leq k + 2 \leq v$). *Then*

(i) *If* v *is even* $k - \lambda$ *must be a square.*

(ii) *If* v *is odd the Diophantine equation*

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a solution in integers x, y, *and* z, *not all zero.*

Proof. Let (P, B) be a symmetric $2 - (v, k, \lambda)$ design. Denote by N the $v \times v$ incidence matrix (points versus blocks) of (P, B). Then $NN' = (\lambda_1 - \lambda)I_v + \lambda J$, where J is the

$v \times v$ matrix with all its entries 1. By observing that $NN' - (\lambda_1 - \lambda)I_v = \lambda J$ is a matrix of rank 1 it follows immediately that the eigenvalues of NN' are $\lambda_1 - \lambda$ (of multiplicity $v-1$) and $\lambda_1 + (v-1)\lambda$ (of multiplicity 1); see the proof of Fisher's inequality in Section 7.12 for a more detailed derivation. We can now write

$$\det NN' \;=\; (\lambda_1 + (v-1)\lambda)(\lambda_1 - \lambda)^{v-1} = k\lambda_1(\lambda_1 - \lambda)^{v-1} \tag{7.11}$$

where $\det NN'$ denotes the determinant of NN'. [To explain the last sign of equality recall that $\lambda_1 = (v-1)(k-1)^{-1}\lambda$.]

(a) The assumption of symmetry implies $\lambda_1 = k$. Expression (7.11) is thus rewritten as

$$(\det N)^2 = \det NN' = k^2(k-\lambda)^{v-1}. \tag{7.12}$$

Since $v-1$ is odd and since the left-hand side of (7.12) is a square it must be that each prime in the prime factorization of $k - \lambda$ occurs at an even power. Hence $k - \lambda$ is necessarily a square. This ends the proof of part (i) of the theorem.

(b) Form the $(v+1) \times (v+1)$ matrix

$$\overline{N} = \begin{bmatrix} N & \mathbf{1} \\ \mathbf{1}' & k\lambda^{-1} \end{bmatrix}$$

(with $\mathbf{1}$ the vector with all entries 1) and let

$$D = \mathrm{diag}(1, \ldots, 1, -\lambda), \;\; E = \mathrm{diag}(k-\lambda, \ldots, k-\lambda, -(k-\lambda)\lambda^{-1}).$$

Matrices D and E are diagonal, of dimension $v+1$.

Then $NN' = (\lambda_1 - \lambda)I_v - \lambda J$, $\lambda_1 = (v-1)(k-1)^{-1}\lambda$, and $\lambda_1 = k$ allow us to write

$$\overline{N}D\overline{N}' \;=\; \begin{bmatrix} N & \mathbf{1} \\ \mathbf{1}' & k\lambda^{-1} \end{bmatrix} \begin{bmatrix} I_v & 0 \\ 0 & -\lambda \end{bmatrix} \begin{bmatrix} N' & \mathbf{1} \\ \mathbf{1}' & k\lambda^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} N & -\lambda\mathbf{1} \\ \mathbf{1}' & -k \end{bmatrix} \begin{bmatrix} N' & \mathbf{1} \\ \mathbf{1}' & k\lambda^{-1} \end{bmatrix} = \begin{bmatrix} NN' - \lambda J & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{bmatrix}$$

$$= \begin{bmatrix} (k-\lambda)I_v & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{bmatrix} = E.$$

Hence

$$D \stackrel{c}{=} E. \tag{7.13}$$

By Lagrange's result we know that $mI_4 \stackrel{c}{=} I_4$. Extending this trivially to direct sums of matrices we can write

$$mI_n \stackrel{c}{=} I_n, \tag{7.14}$$

for any $n = 0$ (modulo 4) and any positive integer m.

(b1) Let $v = 1$ (modulo 4). Condition (7.13) can be rewritten as

$$\begin{aligned} I_{v-1} \oplus I_1 \oplus -\lambda I_1 &\stackrel{c}{=} (k-\lambda)I_{v-1} \oplus (k-\lambda)I_1 \oplus -(k-\lambda)\lambda^{-1}I_1 \\ &\stackrel{c}{=} \{\text{by (7.14)}\} \stackrel{c}{=} I_{v-1} \oplus (k-\lambda)I_1 \oplus -(k-\lambda)\lambda^{-1}I_1. \end{aligned}$$

Witt's cancellation law now gives

$$\begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix} \stackrel{c}{=} \begin{pmatrix} k-\lambda & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{pmatrix}$$

This means that there exists a nonsingular matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with *rational* entries such that

$$A' \begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix} A = \begin{pmatrix} k-\lambda & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{pmatrix}.$$

In particular we must have $a^2 - \lambda c^2 = k - \lambda$. Multiplying by a common denominator leads us to conclude that $x^2 - \lambda z^2 = (k-\lambda)y^2$ must admit a solution in integers x, y, z, not all zero.

(b2) In case $v = 3$ (modulo 4) we work with diagonal matrices of order $v+2$ by adding an additional component $(k-\lambda)I_1$ to both D and E. Then by (7.13) and (7.14)

$$\begin{aligned} I_v \oplus (k-\lambda)I_1 \oplus -\lambda I_1 &\stackrel{c}{=} (k-\lambda)I_v \oplus (k-\lambda)I_1 \oplus -(k-\lambda)\lambda^{-1}I_1 \\ &\stackrel{c}{=} \{\text{by (7.14)}\} \stackrel{c}{=} I_{v+1} \oplus -(k-\lambda)\lambda^{-1}I_1 \\ &\stackrel{c}{=} I_v \oplus I_1 \oplus -(k-\lambda)\lambda^{-1}I_1. \end{aligned}$$

Again by Witt's cancellation law it follows that

$$\begin{pmatrix} k-\lambda & 0 \\ 0 & -\lambda \end{pmatrix} \stackrel{c}{=} \begin{pmatrix} 1 & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{pmatrix}.$$

We can therefore write

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} k-\lambda & 0 \\ 0 & -\lambda \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -(k-\lambda)\lambda^{-1} \end{pmatrix},$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ nonsingular matrix with *rational* entries. Equating the entries in position (1,1) on both sides we obtain

$$1 = (k-\lambda)a^2 - \lambda c^2.$$

Multiplying, as before, by the common denominator of a^2 and c^2 we conclude that the Diophantine equation

$$x^2 = (k-\lambda)y^2 - \lambda z^2$$

must admit a solution in integers x, y, z, not all zero. This concludes our proof.

7.22

Relying on the BRC theorem we can conclude that certain (potential) symmetric 2-designs actually do not exist.

A $2-(22,7,2)$ *design, for example, cannot exist.* This follows from the fact that if such a design exists it must necessarily be symmetric and, since $v = 22$ is even, the BRC theorem requires that $k - \lambda = 7 - 2 = 5$ be a square. But 5 is not a square and consequently such a design does not exist.

The true strength of the BRC theorem is contained in the case with odd v. *Let us show that a potential* $2-(43,7,1)$ *design does not exist.* A design with these parameters (if it exists) must be symmetric, because $\lambda_0 = \binom{43}{2}\binom{7}{2}^{-1} \cdot 1 = 43 = v$. By the BRC theorem a necessary condition for its existence is that the equation

$$x^2 \;=\; 6y^2 - z^2 \tag{7.15}$$

admits a solution in integers x, y, z, not all zero. We now show that this equation does not have an integral nonzero solution.

Write (7.15) as $6y^2 = x^2 + z^2$. The prime 3 divides $6y^2$ and hence $x^2 + z^2$. Let r be the highest power of 3 that divides both x and z. Dividing equation (7.15) by 3^{2r} we obtain

$$\left(\frac{x}{3^r}\right)^2 + \left(\frac{z}{3^r}\right)^2 = \frac{6y^2}{3^{2r}} = 6\left(\frac{y}{3^r}\right)^2.$$

Observe that 3^r must necessarily divide y and denote $x/3^r = \overline{x}$, $z/3^r = \overline{z}$, and $y/3^r = \overline{y}$. Now (7.15) can be rewritten as

$$6\overline{y}^2 = \overline{x}^2 + \overline{z}^2. \tag{7.16}$$

Equation (7.15) admits a nonzero solution in integers if and only if equation (7.16) does; this is clear since the two equations are nonzero multiples of each other. By the way in which r was selected in (7.16) 3 divides $6\overline{y}^2$ but it does not divide $\overline{x}$ nor $\overline{y}$. Interpret now equation (7.16) over the field $GF(3)$, that is, look at it modulo 3. The numbers $\overline{x}$ and $\overline{y}$ are now nonzero elements of $GF(3)$ that satisfy

$$0 = \overline{x}^2 + \overline{y}^2. \tag{7.17}$$

Or, dividing out by $\overline{y}^2$, $(\overline{x}/\overline{y})^2 = \overline{x}^2/\overline{y}^2 = -1$, that is, we conclude that -1 is a square in $GF(3)$.

What we showed is that if a $2-(43,7,1)$ design exists, then -1 must be a square in $GF(3)$. But -1 is not a square in $GF(3)$ since $(-1)^2 = 1^2 = 1$ and $0^2 = 0$. We are now forced to conclude that a $2-(43,7,1)$ design cannot exist.

7.23 Nonexistence of Certain Projective Planes

A *projective plane* is a symmetric $2-(v,k,1)$ design. By letting $n = k-1$ we can write the parameters v and k in terms of n only: $v = n^2+n+1$ and $k = n+1$ (note that v is always odd, regardless of the parity of n). The number n is called the *order* of the projective plane $2-(n^2+n+1, n+1, 1)$.

If $n = 0$ or 3 (modulo 4), the BRC equation always has the solution $x = 1$, $y = 0$, $z = 1$. We therefore cannot conclude anything concerning the existence of such planes.

However, if $n = 1$ or 2 (modulo 4), the BRC equation becomes $ny^2 = x^2+z^2$. In Section 7.22 we showed that this equation has no nonzero solution if $n = 6$. We showed, in other words, that a projective plane of order 6 does not exist. Using arguments absolutely analogous to those used in Section 7.22, and working modulo 3, 7, or 11, we conclude

that projective planes of order 6, 14, 21, 22, 30, and 33 cannot exist. (It is in fact a well-known result in the theory of numbers that the equation $ny^2 = x^2 + y^2$ admits nonzero solutions in integers if and only if n is the sum of two squares. At this point it is becoming abundantly clear that knowledge about the existence of symmetric 2-designs rests fundamentally within the domain of that rich theory. We therefore direct the reader's attention to the pertinent results in the theory of numbers.)

All known projective planes have n a power of a prime. The $PG(2, n)$ are examples familiar to us (see Section 7.6). The smallest values of n for which it is not known whether a projective plane exists are: 10, 12, 15, 18, 20, 24.

7.24

A positive integer m is said to be *square free* if in the prime factorization of m all the (distinct) primes occur at power 1, that is, $m = \prod_i p_i$, with p_i distinct primes. Two positive integers a and b are called *relatively prime* [written $(a, b) = 1$] if there does not exist a prime number that divides them both. Our aim is to give a version of the BRC theorem that is easily applicable to practical situations.

Let us first consider a general Diophantine equation of the form $ax^2 + by^2 + cz^2 = 0$. Writing $a = \overline{a}A^2$, $b = \overline{b}B^2$, $c = \overline{c}C^2$ with $\overline{a}$, $\overline{b}$, and $\overline{c}$ square free, we can immediately conclude that the equation $ax^2 + by^2 + cz^2 = 0$ has nonzero integral solutions if and only if $\overline{a}x^2 + \overline{b}y^2 + \overline{c}z^2 = 0$ does.

Consider now the equation $\overline{a}x^2 + \overline{b}y^2 + \overline{c}z^2 = 0$ with $\overline{a}$, $\overline{b}$, $\overline{c}$ square free and also make the assumption that $\overline{a}$, $\overline{b}$, $\overline{c}$ are pairwise relatively prime. Let (x, y, z) be a nonzero integral solution. If p is a prime dividing $\overline{a}$, we may assume (after possibly dividing our

solution through by a power of p) that p does not divide y nor z. Modulo p the equation $\overline{a}x^2 + \overline{b}y^2 + \overline{c}z^2 = 0$ becomes

$$\overline{b}y^2 = -\overline{c}z^2$$

or, multiplying through by $\overline{b}$,

$$\overline{b}^2y^2 = -\overline{b}\overline{c}z^2.$$

The last equation informs us that $-\overline{b}\overline{c}$ $(= (\overline{b}y/z)^2)$ must necessarily be a square modulo p.

We can summarize this as follows: Necessary conditions for the existence of a nonzero integral solution to $\overline{a}x^2 + \overline{b}y^2 + \overline{c}z^2 = 0$ with $\overline{a}$, $\overline{b}$, $\overline{c}$ square free and pairwise relatively prime are that, for all primes p,

1. If p divides $\overline{a}$, then $-\overline{b}\overline{c}$ is a square modulo p.

2. If p divides $\overline{b}$, then $-\overline{a}\overline{c}$ is a square modulo p.

3. If p divides $\overline{c}$, then $-\overline{a}\overline{b}$ is a square modulo p.

4. The coefficients $\overline{a}$, $\overline{b}$, and $\overline{c}$ do not all have the same sign. (Condition 4 is obvious.)

With these remarks made let us study the BRC Diophantine equation $-x^2 + ny^2 + (-1)^{(v-1)/2}\lambda z^2$, where n stands for $k-\lambda$. First write the equation in the form $-x^2+\overline{n}y^2+(-1)^{(v-1)/2}\overline{\lambda}z^2$, with $\overline{n}$ and $\overline{\lambda}$ square free. For a prime p we conclude the following:

(i) If $\overline{n}$ and $\overline{\lambda}$ are relatively prime and if p divides $\overline{n}$, then $(-1)^{(v-1)/2}\overline{\lambda}$ must be a square modulo p.

(ii) If $\overline{n}$ and $\overline{\lambda}$ are relatively prime and if p divides $\overline{\lambda}$, then n must be a square modulo p.

(iii) If p divides $\overline{n}$ and $\overline{\lambda}$, then observe that the equation

$$x^2 + \overline{n}y^2 + (-1)^{(v-1)/2}\overline{\lambda}z^2 = 0$$

has a nonzero integral solution if and only if the equation

$$-px^2 + \frac{\overline{n}}{p}y^2 + (-1)^{(v-1)/2}\frac{\overline{\lambda}}{p}z^2 = 0$$

has such a solution. The coefficients $\overline{n}/p$ and $\overline{\lambda}/p$ may still not be relatively prime. But after eventually dividing a nonzero solution through by a power of p we can assume that p does not divide y nor z. Working again modulo p we conclude that

$$-\frac{\overline{n}}{p}y^2 = (-1)^{(v-1)/2}\frac{\overline{\lambda}}{p}z^2.$$

Multiplying through by $-\overline{n}/p$ we deduce that $(-\overline{n}/p)(-1)^{(v-1)/2}(\overline{\lambda}/p)$ must be a square modulo p.

We summarize as follows.

An Applicable Version of the BRC Theorem. *Suppose v, k, λ are natural numbers such that a symmetric $2-(v,k,\lambda)$ design exists $(0 \leq k+2 \leq v)$, and v is an odd number. Denote $k-\lambda$ by n and let $\overline{n}$ and $\overline{\lambda}$ be the square free parts of n and λ. Then for every prime p the following statements are true*:

(i) *If p divides $\overline{n}$ but not $\overline{\lambda}$, then $(-1)^{(v-1)/2}\overline{\lambda}$ must be a square modulo p.*

(ii) *If p divides $\overline{\lambda}$ but not $\overline{n}$, then $\overline{n}$ must be a square modulo p.*

(iii) *If p divides both $\overline{n}$ and $\overline{\lambda}$, then $(-1)^{(v+1)/2}(\overline{n}/p)(\overline{\lambda}/p)$ must be a square modulo p.*

6 AUTOMORPHISMS OF DESIGNS

7.25

Let (P, B) be a $t-(v, k, \lambda_t)$ design and g a permutation on P. Then g induces a permutation on the k-subsets of P by the "natural" action $\{x_1, \ldots, x_k\} \to \{g(x_1), \ldots, g(x_k)\}$. If g also induces a permutation on B we call g *an automorphism* of the design (P, B). More generally, a group of permutations on the points of a t-design that preserves its blocks is called an *automorphism group* of that design.

As an example, the group generated by the permutations $(1\,2\,3\,4\,5\,6\,7)$, $(2\,7\,6)(4\,3\,5)$, and $(2\,3\,4\,7)(5\,6)$ is an automorphism group of $PG(2, 2)$ as displayed in (7.2). Verify this.

The *full automorphism group* of a t-design is the group of *all* permutations on points that preserve the blocks. [It is generally difficult to find the full automorphism group of a design. Try to accomplish this for the design (7.2)!]

An automorphism group of a design has a permutation representation on the blocks of the design (in addition to its initial representation on points). It is thence natural to compare the induced action on blocks to that on points. Our first observation is the following:

$*$ *A permutation fixes all the blocks of a 2-design if and only if it fixes all the points.* (In other words the representation on blocks is faithful.)

The statement we just made is easy to justify. It is clear that the identity permutation on points fixes all the blocks; it fixes them pointwise in fact. Suppose now that a permutation on points induces the identity permutation on blocks, that is, it fixes each

individual block. If x is a point, then the intersection of all blocks containing x consists of x *alone* [else we would have $\lambda_2 \geq \lambda_1$, or $\lambda_2 \geq (v-1)(k-1)^{-1}\lambda_2$, or $k \geq v$, which is a contradiction]. Since each block containing x is fixed, the intersection of these blocks (i.e., x itself) is also fixed. The permutation therefore fixes all points, as was asserted.

Another helpful observation is the following:

$*$ *The full automorphism group of a* $2-(v,k,\lambda_2)$ *design* $(0 \leq k+2 \leq v)$ *contains the whole alternating group on the* v *points if and only if the 2-design is a complete design.*

Proof. Denote by S_v the symmetric group on the v points; $|S_v| = v!$. It is clear that any complete design on the v points has S_v as the (full) automorphism group, and S_v contains A_v, the alternating group (of even permutations) on the v points; $|A_v| = v!/2$. Conversely, if A_v is an automorphism group and α is a block in our 2-design, then by assumption the set $\{g(\alpha) : g \in A_v\}$ consists of blocks of our 2-design. But the group A_v is $(v-2)$-transitive (thus also k-transitive) on points and hence $\{g(\alpha) : g \in A_v\}$ is a complete 2-design. This concludes the proof.

7.26

We devote this section to the proof of the following result:

$*$ *An automorphism group of a* t*-design* $(t \geq 2)$ *has at least as many orbits on the blocks of the* t*-design as it has on the* $[t/2]$*-subsets of points.*

The notation $[x]$ indicates the integral part of the fraction x.

Let (P,B) be a $t-(v,k,\lambda_t)$ design and G an automorphism group of (P,B). Denote

$[t/2]$ by s. The group G acts on the $\binom{v}{s}$ s-subsets of P. The resulting orbits are called *s-orbits*. For a s-subset x of P we denote by $\overline{x}$ its s-orbit. Similarly, the orbits that G induces on B are called *block-orbits*, and we write $\overline{\alpha}$ for the block-orbit of block α. Let m be the number of s-orbits and n the number of block-orbits.

Form the $m \times n$ matrix $\overline{A} = (a_{ij})$ of s-orbits versus block-orbits with a_{ij} being the number of blocks in block-orbit j that contains a certain s-subset from s-orbit i. Observe that a_{ij} is well defined, in that it is independent of the choice of orbit representatives. Let also $\overline{B} = (b_{ij})$ be the $n \times m$ matrix of block-orbits versus s-orbits with b_{ij} being the number of s-subsets in s-orbit j contained in a block from block-orbit i; the entries b_{ij} are well defined as well.

Look now at the matrix $\overline{AB} = (c_{ij})$. This matrix is $m \times m$. We aim to prove that $\overline{AB}$ is *nonsingular*. The nonsingularity of $\overline{AB}$ implies, in particular, that $\overline{A}$ has at least as many columns as it has rows, that is, $n \geq m$, which is what our result states.

Let us investigate the matrix $\overline{AB} = (c_{ij})$ a bit more closely. The entry c_{ij} equals $\sum_{k=1}^{n} = a_{ik}b_{kj}$. We next find a simpler expression for c_{ij}.

Fix a s-subset x in s-orbit i and count the cardinality of the set

$$S_x^j = \{(y, \alpha) : \ x \in \alpha, \ \ y \in \alpha, \ \ y \in s - \text{orbit } \ j, \ \ \alpha \in B\}$$

in two different ways. Let y be fixed, initially; then there are $\lambda_{|x \cup y|}$ blocks containing both s-subsets x and y, and since y runs through s-orbit j we obtain $|S_x^j| = \sum_y \lambda_{|x \cup y|}$ (the summation is over all s-subsets y in s-orbit j). Now count differently: fix α first. Then α belongs to some block-orbit, orbit k, say; we have b_{kj} choices for y and a_{ij} choices for α

in block-orbit k. Summing over k leads to $|S_x^j| = \sum_{k=1}^n a_{ik}b_{kj}$. We therefore conclude that

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{y} \lambda_{|x\cup y|}.$$

The reader should understand that $c_{ij} = \sum_y \lambda_{|x\cup y|}$ (with y running over the s-subsets in s-orbit j and x being a fixed s-subset in s-orbit i) is a well-defined expression that does not depend on the particular choice of x in s-orbit i. It is this simpler expression of c_{ij} that we use to establish the nonsingularity of $\overline{AB}$.

Define $N_S = (n_{ij})$, the $\binom{v}{s} \times \lambda_0$ incidence matrix of s-subsets versus blocks, with $n_{ij} = 1$ if the ith s-subset is contained in block j, and $n_{ij} = 0$ otherwise. Line up, moreover, the rows of N_S such that the s-subsets in s-orbit 1 come first, then those in s-orbit 2,..., and lastly those in s-orbit m.

The matrix $N_S N_S'$ is $\binom{v}{s} \times \binom{v}{s}$ with (x, y)th entry equal to $\lambda_{|x\cup y|}$. It is a positive definite matrix and thus nonsingular (the positive definiteness is established immediately following the proof). Write $N_S N_S' = (C_{ij})$ as a partitioned matrix with C_{ij} the submatrix of $N_S N_S'$ of the ith s-orbit versus the jth s-orbit.

Observe that the row sums of C_{ij} equal $\sum_y \lambda_{|x\cup y|}$, where x is in s-orbit i and y runs over the s-subsets of s-orbit j. This common value for the row sums of C_{ij} is well defined (in the sense that it does not depend upon the choice of x in s-orbit i). We thus conclude that $\overline{AB} = (c_{ij})$, where $c_{ij} = \sum_y \lambda_{|x\cup y|}$ = common value of the row sums of C_{ij}.

We end the proof by showing that the eigenvalues of $\overline{AB}$ are necessarily among those of $N_S N_S'$. And since the eigenvalues of $N_S N_S'$ are positive we conclude that $\overline{AB}$ is nonsingular.

Indeed, let

$$\overline{AB}w = (c_{ij}) \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = \mu \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} = \mu w.$$

Then

$$N_S N_S' \begin{pmatrix} w_1\mathbf{1} \\ \vdots \\ w_m\mathbf{1} \end{pmatrix} = (C_{ij}) \begin{pmatrix} w_1\mathbf{1} \\ \vdots \\ w_m\mathbf{1} \end{pmatrix} = \mu \begin{pmatrix} w_1\mathbf{1} \\ \vdots \\ w_m\mathbf{1} \end{pmatrix},$$

which shows that if μ is an eigenvalue of $\overline{AB}$, then μ is also an eigenvalue of $N_S N_S'$. The $\mathbf{1}$ in $w_j\mathbf{1}$ is the vector with all its entries equal to 1 and of length equal to the number of columns of C_{ij}.

Proof of the Positive Definiteness of $N_S N_S'$. This proof is due to Wilson [4]. Denote by W_{ij} the $\binom{v}{i} \times \binom{v}{j}$ incidence matrix between the i-subsets and j-subsets of P. Then

$$N_S N_S' = \sum_{i=0}^{S} \lambda_{2S-i}^{i} W_{iS}' W_{iS},$$

with λ_m^l signifying the number of blocks containing m points and omitting l [see Proposition 7.1, part (b)]. Matrices $\lambda_{2S-i}^{i} W_{iS}' W_{iS}$ are nonnegative definite with one of them, $\lambda_S^S W_{SS}' W_{SS} = \lambda_S^S I$, being positive definite. Thus $N_S N_S'$ is itself positive definite as their sum. This ends the proof.

(To see that $N_S N_S'$ is indeed expressible as the sum above the reader should check that the corresponding entries on both sides are equal. This involves verification of an identity of the familiar Vandermonde type.)

7.27

By the duality between points and blocks that exists in a symmetric design result (7.18) allows us to draw the following conclusion:

∗ *An automorphism group of asymmetric design has as many point-orbits as it has block-orbits.*

In this special situation a little more can in fact be said, as was observed by Baer:

∗ *An automorphism of a symmetric design fixes precisely as many points as it does blocks.*

Indeed, an automorphism g corresponds to two permutation matrices P and Q which satisfy

$$PNQ = N,$$

where N is the (square) incidence matrix between points and blocks. Recalling that $P^{-1} = P'$ and solving for Q we obtain

$$Q = N^{-1}P'N.$$

Being conjugates of each other P' and Q have the same trace. But the traces of P and Q count the number of fixed points and fixed blocks, respectively. This ends the proof.

7.28

The relationship between the design and its automorphism group is an interesting (and sporadically a fascinating) one. If the automorphism group is large, then it usually reflects

much of the structural properties of the design. Quite a number of structural characterizations through the automorphism groups are known.

The symmetric designs $PG(n, q)$ admit large automorphism groups. The blocks of $PG(n, q)$ are, by definition, the n-dimensional (vector space) subspaces of a $(n + 1)$-dimensional vector space V over $GF(q)$. The group of nonsingular linear transformations of V acts on the n-dimensional subspaces; call this group $GL(V)$. But it does not act faithfully on the projective points. We can quickly fix this small annoyance by working modulo the subgroup of scalar multiples of the identity transformation. This quotient group [which we denote by $PGL(V)$] is indeed an automorphism group of $PG(n, q)$. Up to automorphisms of the field this is the full automorphism group. We refer the reader to [7] for further reading on this classical subject.

The full automorphism group of the Mathieu $5 - (12, 6, 1)$ design displayed in Section 7.9 is the Mathieu group M_{12} which acts 5-transitively on points and is one of the sporadic simple groups. The other 5-transitive Mathieu group, M_{24}, is the automorphism group of the Mathieu $5 - (24, 8, 1)$ design. For more information we refer to [13].

EXERCISES

1. Go over the proof of the BRC theorem with the special case of a (potential) projective plane of order six and conclude that it cannot exist.

2. Examine what the BRC theorem tells us about a Hadamard 2-design. Do the same for a symmetric $2 - (v, k, 2)$ design.

3. Show that a $2 - (21, 5, 1)$ design is necessarily $PG(2, 4)$.

4. Show that a (symmetric) $2-(11,5,2)$ design must necessarily be the Paley design (7.4). In addition, prove that the full automorphism group of the Paley design (7.4) has 660 elements. What is this group?

5. (Alltop.) For any positive integer k a (nontrivial) 2-design with block size k exists. [*Hint*: Find a subgraph S with k edges (a cycle, maybe) in the complete graph K_n such that $\{g(S) : g \in \mathrm{Aut}(K_n)\}$ are the blocks of the nontrivial 2-design; by $\mathrm{Aut}(K_n)$ we understand the group of all the $n!$ permutations on the n vertices of K_n.]

6. Show that the full automorphism group of $PG(2,2)$ is a simple group of order 168. (A simple group is a group with no proper normal subgroups, i.e., it is like a prime number.) Find this group both as a group of 3×3 matrices and as a group of permutations on 7 points.

7. (The fundamental theorem of projective geometry.) Find the full automorphism group of $PG(n,q)$ and show that it acts transitively on noncolinear triples of points.

8. (Alltop.) Let (P,B) be a $t-(v,k,\lambda_t)$ design; suppose $a \notin P$. Define

$$\begin{aligned} P_a &= P \cup \{a\} \\ B' &= \{\alpha \cup \{a\} : \alpha \in B\} \\ B'' &= \{P - \alpha : \alpha \in B\} \\ B''' &= \{P - \sigma_k : \sigma_k \in \sum_k (P) - B\}. \end{aligned}$$

For certain sets of parameters $(t+1)$-designs can be constructed from various combinations of B, B', B'' or B'''. Prove the following:

(a) Let (P, B) be a $t-(2k, k, \lambda_t)$ design with t even and $B'' \cap B = \emptyset$. Then $(P, B \cup B'')$ is a $(t+1)-(2k, k, \lambda''_{t+1})$ design; $\lambda''_{t+1} = 2\lambda_t(k-t)(2k-t)^{-1}$.

(b) Let (P, B) be a $t-(2k, k, \lambda_t)$ design with t even and $B'' = B$. Then (P, B) is a $(t+1)-(2k, k, \lambda_{t+1})$ design; $\lambda_{t+1} = \lambda_t(k-t)(2k-t)^{-1}$.

(c) Let (P, B) be a $t-(2k+1, k, \lambda_t)$ design with t even. Then $(P_a, B' \cup B'')$ is a $(t+1)-(2k+2, k+1, \lambda_t)$ design.

(d) Let (P, B) be a $t-(2k+1, k, \lambda_t)$ design with t odd and $\lambda_0 = \frac{1}{2}\binom{2k+1}{k}$. Then $(P_a, B' \cup B''')$ is a $(t+1)-(2k+2, k+1, \lambda_t)$ design.

7 ASSOCIATION SCHEMES

7.29

An association scheme (or scheme for short) is a set with several binary relations defined on it, which satisfy certain properties of compatibility. The association schemes were introduced by Bose in connection with the design of experiments. Over the years they turned out to be useful in the study of other combinatorial structures such as permutation groups, coding theory, and designs. Good codes and designs often arise as maximal subsets of certain association schemes.

We present the basic theory of association schemes, which centers around the Bose-Mesner algebra. Examples are then given focusing mostly on the Hamming and Johnson (or triangular) schemes. Finally, we interpret t-designs as special subsets of the Johnson scheme.

7.30 The Definition of an Association Scheme

An *association scheme with n classes* (or relations, or colors) consists of a finite set P of v points together with $n+1$ binary relations $R_0, R_1, \ldots, R_n$ that satisfy:

(i) R_0 is the identity relation, that is, $R_0 = \{(x,x) : x \in P\}$.

(ii) For every x, y in P, $(x,y) \in R_i$; for exactly one i.

(iii) Each R_i is symmetric, that is, $(x,y) \in R_i$ implies $(y,x) \in R_i$.

(iv) If $(x,y) \in R_k$, then the number of z in P such that $(x,z) \in R_i$ and $(y,z) \in R_j$, is a constant c_{ijk} depending on i,j,k but not on the particular choice of x and y in R_k.

It is often helpful to think of an association scheme as a complete graph on v points with colored edges. (Relation R_i corresponds to color i; R_0 has a somewhat degenerate meaning – it informs us that each point has color 0. Instead of coloring points one may prefer to draw a loop on top of a point; think of it as an edge and color that 0.) An edge $\{x,y\}$ is colored with color i if $(x,y) \in R_i$, and such x, y we call ith *associates*. Condition (i) states that points have color 0; (ii) tells us that each edge has a unique color; (iii) informs us that the edges are not oriented. And finally, condition (iv) is equivalent to saying that the number of triangles with a fixed base $\{x,y\}$ of color k having the edge incident with x colored i and the edge incident with y colored j is a constant c_{ijk} depending on i,j,k but not on the specific choice of the base of color k. In particular each vertex is incident with c_{ii0} edges of color i. We denote c_{ii0} by v_i. Observe that the subgraph with edges of color i (i.e., the subgraph corresponding to R_i) is regular of degree v_i. (We remind the reader that a graph is called regular of degree d if all its vertices have degree

d.)

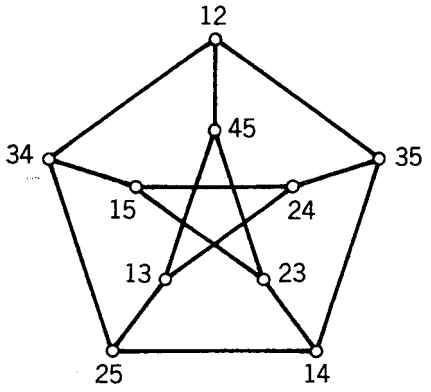
7.31 An Example – The Johnson Scheme

We give an example of a triangular scheme with two associate classes on ten points. Let the points of the scheme be the 2-subsets of $\{1, 2, 3, 4, 5\}$. Call two points $\{i, j\}$ and $\{k, l\}$ first associates if they have precisely one symbol in common, and second associates if they are disjoint.

If we place the ten points in a (symmetric) triangular array $J(5, 2)$ with diagonal entries filled by $*$ as displayed below, two points are first associated if they are in the same row or column of $J(5, 2)$; they are second associates if they are not in the same row or column.

$$J(5,2) = \begin{array}{ccccc} * & \{1,2\} & \{1,3\} & \{1,4\} & \{1,5\} \\ \{l,2\} & * & \{2,3\} & \{2,4\} & \{2,5\} \\ \{1,3\} & \{2,3\} & * & \{3,4\} & \{3,5\} \\ \{1,4\} & \{2,4\} & \{3,4\} & * & \{4,5\} \\ \{1,5\} & \{2,5\} & \{3,5\} & \{4,5\} & * \end{array}$$

We color the pairs of first associates red and those of second associates blue. The subgraph of blue edges that results is known as the Petersen graph (we write ij instead of $\{i, j\}$ for simplicity):



The complementary graph to this graph (in K_{10}, the complete graph on the ten points) is the subgraph of red edges.

The reader can check that $J(5,2)$ is indeed an association scheme with two associate classes. Its parameters are

$$\begin{pmatrix} c_{000} & c_{010} & c_{020} \\ & c_{110} & c_{120} \\ & & c_{220} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ & 6 & 0 \\ & & 3 \end{pmatrix}$$
$$\begin{pmatrix} c_{001} & c_{011} & c_{021} \\ & c_{111} & c_{121} \\ & & c_{221} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ & 3 & 2 \\ & & 1 \end{pmatrix} \tag{7.19}$$
$$\begin{pmatrix} c_{002} & c_{012} & c_{022} \\ & c_{112} & c_{122} \\ & & c_{222} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ & 4 & 2 \\ & & 0 \end{pmatrix}$$

The matrices of parameters displayed above are all symmetric.

There is a general scheme of which the above example is a special case. This general scheme we denote by $J(m,n)$ and define as follows: The points of the scheme are the $\binom{m}{n}$ subsets of size n of a set with m elements; two subsets of size n are said to be ith

associates if they intersect in precisely $n-i$ elements, $0 \leq i \leq n$. The scheme $J(m,n)$ has n associate classes. (By definition we do not count the 0th associates as an association class.) We call $J(m,n)$ the *Johnson (or triangular) scheme.*

The parameters of the scheme $J(m,n)$ are

$$c_{n-i,n-j,n-k} = \sum_l \binom{k}{l}\binom{n-k}{i-l}\binom{n-k}{j-l}\binom{m-2n+k}{n-i-j+l},$$

with $0 \leq i,\ j,k \leq n$. (This expression is derived by counting the number of n-subsets that intersect x in i elements and y in j elements, where x and y are a pair of n-subsets that intersect in k elements. The n-subsets in question are sorted by l, the number of elements that they have in common with $x \cap y$.)

7.32 Other Examples of Association Schemes

The association schemes are combinatorial objects of great mathematical richness and elegance. Fundamental questions of classification were addressed and partly answered by Bose and his students. Complete classification re- mains, however, a formidable undertaking. It has been actively researched only in the last decade or so.

We mention several examples of association schemes, the selection being motivated chiefly by the immediate connections between these schemes and other parts of combinatorics such as graph theory, finite groups, coding theory, and finite geometries.

A The Hamming Scheme $H(n)$

The points of the scheme are the 2^n vertices of a n-dimensional cube. The relations of association are defined as follows: Think of each vertex of the cube being a vector of n components with 0 and 1 as entries. Two vertices are called ith associates if the

corresponding vectors differ in precisely i coordinates. The scheme $H(n)$ has n associate classes. It is the fundamental object of coding theory.

B The Projective Schemes

Let V be a vector space of dimension $n+1$ over $GF(q)$. Denote by PV the associated projective geometry (see the introductory passages to Section 7.6 for the exact definition).

The points of the scheme are the m-subsets of (projective) points of PV. Two m-subsets are called ith associates if the projective points in their union span a projective subspace of PV of (projective) dimension i.

C Metric Schemes

Let G be a connected simple graph with P the set of vertices. The *distance* $d(x,y)$ between two vertices x and y is defined as the length of the shortest path joining them. The maximal distance between any two vertices is called the *diameter* of G.

The graph G is called *distance regular* if for any x and y in P with $d(x,y) = k$, the number of vertices z in P such that $d(z,x) = i$ and $d(z,y) = j$ is a constant c_{ijk} independent of the choice of x and y (so long as they are at distance k of each other).

We obtain an association scheme from a distance regular graph by calling two vertices x and y ith associates if $d(x,y) = i$. The schemes thus obtained from distance regular graphs are called *metric schemes*. (To recover the graph from the metric scheme define x and y to be adjacent if they are first associates.)

Distance regular graphs of diameter 2 are called *strongly regular*. It is easy to see that any scheme with two associate classes is metric and is obtained from a strongly regular

graph.

D The Schemes Arising from Permutation Groups

Let G be a permutation group acting transitively on a set of points P. We can make G act on $P \times P$ by defining $g(x, y) = (g(x), g(y))$, for g in G and x, y in P. Let the orbits of this latter action on $P \times P$ be $R_0 = \{(x, x) : x \in P\}$, $R_1, \ldots, R_n$. The R_i's are binary relations that need not be symmetric. If they are symmetric they define an association scheme with n classes.

The Johnson and Hamming schemes correspond to special choices of the group: the symmetric group, and the symmetry group of the n-cube (of order $2^n n!$), respectively.

7.33 Relations Among the Parameters

Let c_{ijk} be the parameters of an association scheme with n classes. The reader may have already observed certain relations among the c_{ijk}'s in (7.19). In general we can say the following:

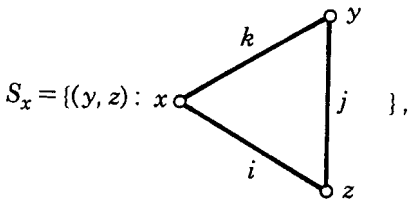
** The parameters Cijk of an association scheme with n classes satisfy*

$$\begin{aligned} c_{ijk} &= c_{jik}, \quad c_{0jk} = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{otherwise} \end{cases} \\ v_k c_{ijk} &= v_i c_{kji} \\ \sum_{j=0}^{n} c_{ijk} &= v_i \\ \sum_{m=0}^{n} c_{ijm} c_{mkl} &= \sum_{h=0}^{n} c_{ihl} c_{jkh}. \end{aligned}$$

(We denote c_{ii0} by v_i.)

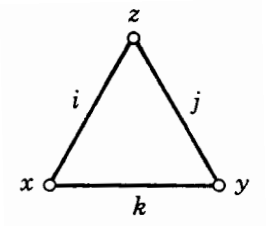
Proof. That $c_{ijk} = c_{jik}$ follows directly from the fact that the relation R_k is symmetric. For x and y a pair of kth associates c_{0jk} equals the number of 0th associates of x and jth associates of y. Since the only 0th associate of x is x itself, $c_{0jk} = 0$, unless $j = k$, in which case $c_{0jk} = 1$.

To see that $v_k c_{ijk} = v_i c_{kji}$ count in two ways the cardinality of the set



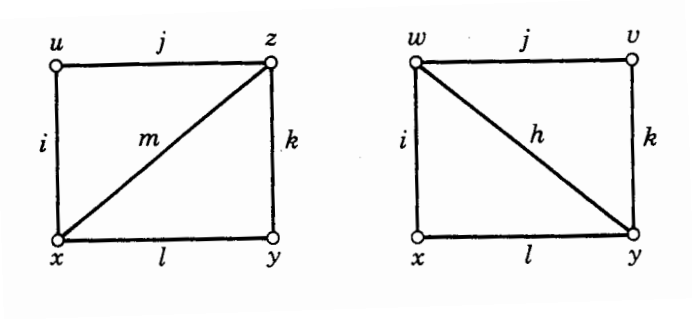
that is, S_x consists of ordered pairs (y, z) of jth associates such that (x, y) are kth associates and (x, z) are ith associates, with x a point fixed a priori.

Proving that $v_i = \sum_{j=0}^{n} c_{ijk}$ amounts to sorting out the triangles



by the values of j, with x and y a fixed pair of kth associates.

The last identity follows from counting in two ways (as indicated in the figures below) the number of paths with color sequence (i, j, k) joining x and y.
In the first of the two figures fix z. For this fixed z there are c_{ijm} possible choices for u; and there actually exist c_{mkl} possibilities for z. Summing over m



leads to $\sum_{m=0}^{n} c_{ijm}c_{mkl}$. Similar counting in the second figure gives $\sum_{h=0}^{n} c_{ihl}c_{jkh}$. We conclude that

$$\sum_{m=0}^{n} c_{ijm}c_{mkl} = \sum_{h=0}^{n} c_{ihl}c_{jkh},$$

and this ends our proof.

7.34 The Bose-Mesner Algebra

To an association scheme with n classes on a set of v points we attach an algebra of $v \times v$ matrices. Think of the association scheme as a complete graph K_v on the v vertices with edges colored with n colors. Let A_i be the $v \times v$ (points versus points) adjacency matrix of the subgraph of K_v with edges of color i, $0 \leq i \leq n$. To be exact, the (x, y)th entry of A_i is 1 if the edge $\{x, y\}$ is colored i, and 0 otherwise.

The defining properties of the association scheme can be readily rewritten in terms of the matrices A_i as follows:

(i) $A_0 = I$ (the identity matrix).

(ii) $\sum_{i=0}^{n} A_i = J$ (the matrix with all entries 1).

(iii) A_i is symmetric.

(iv) $A_iA_j = \sum_{k=0}^{n} c_{ijk}A_k = A_jA_i$; $0 \leq i, j \leq n$.

[Indeed, the (x, y)th entry of A_iA_j equals the number of paths

$$x \circ\!\!-\!\!-\!\overset{i}{\circ}\!\!-\!\!-\!\overset{j}{\circ}\!\!-\!\!-\circ\ y$$

in K_v. This number is c_{ijk} for some k, which is what $\sum_{k=0}^{n} c_{ijk}A_k$ has for its (x, y)th entry. This explains (iv) above.]

Observe also that $A_iJ = JA_i = v_iJ$. In words this means that A_i has row and column sums equal to v_i (recall that $v_i = c_{ii0}$).

Let us consider the vector space $\mathcal{B}$ of all matrices of the form $\sum_{i=0}^{n} a_iA_i$, with a_i real numbers. From (iii) these matrices are symmetric. Condition (ii) tells us that $A_0, A_1, \ldots, A_n$ are linearly independent. We thus conclude that the A_i's form a basis for $\mathcal{B}$, and that the dimension of $\mathcal{B}$ is $n + 1$. Most importantly, (iv) informs us that $\mathcal{B}$ is closed under matrix multiplication, and that the multiplication in $\mathcal{B}$ is in fact commutative; the multiplication of $\mathcal{B}$ is, of course, associative as well (matrix multiplication is always associative). A vector space with a rule of multiplication that is associative, commutative (distributive with respect to addition and "polite" to scalar multiplication) is called an *algebra*. We thus call $\mathcal{B}$ the *Bose-Mesner algebra* of the association scheme.

The matrices in $\mathcal{B}$ are symmetric and commute with each other. A well-known result in matrix theory tells us then that they can be simultaneously diagonalized, that is, there exists a nonsingular matrix S such that

$$S^{-1}AS = D_A$$

with D_A diagonal, for all A in $\mathcal{B}$.

The algebra $\mathcal{B}$ is now seen to be semisimple and thus admits a unique basis $J_0, J_1, \ldots, J_n$ of primitive idempotents (see [18]). These are matrices in $\mathcal{B}$ satisfying

$$\begin{aligned} J_i^2 &= J_i, \quad 0 \leq i \leq n \\ J_i J_k &= 0, \quad i \neq k \\ \sum_{i=0}^{n} J_i &= I. \end{aligned} \tag{7.20}$$

[The matrix J (of all 1's) is in $\mathcal{B}$ and $(1/v)J$ is idempotent. *We shall therefore always choose* $J_0 = (1/v)J$.]

We now have two bases for $\mathcal{B}$: the A_i's and the J_i's. Let us relate these two bases by writing

$$A_k = \sum_{i=0}^{n} p(k,i) J_i, \quad 0 \leq k \leq n$$

and

$$J_k = \sum_{i=0}^{n} v^{-1} q(k,i) A_i, \quad 0 \leq k \leq n. \tag{7.21}$$

The $p(k,i)$ and $v^{-1}q(k,i)$ are real numbers. Observe, in fact, that $p(k,i)$ is an eigenvalue of A_k, in that it satisfies

$$A_k J_i = \left(\sum_{j=0}^{n} p(k,j) J_j \right) J_i = p(k,i) J_i. \tag{7.22}$$

[The first equality sign holds by (7.21) while the second by (7.20).] Equation (7.22) also shows that (the columns of) J_i are eigenvectors of A_k, $0 \leq k \leq n$.

Denote by P the $(n+1) \times (n+1)$ matrix $(p(k,i))$ and by Q the matrix $(q(k,i))$. By (7.21) P and $v^{-1}Q$ are inverses of each other. Further, let μ_i denote the rank of J_i, that is, the multiplicity of the eigenvalue $p(k,i)$, as written in (7.22).

The following result holds:

∗ *The eigenmatrices P and Q satisfy the orthogonality conditions*

$$P' \begin{pmatrix} \mu_0 & & 0 \\ & \ddots & \\ 0 & & \mu_n \end{pmatrix} P = v \begin{pmatrix} v_0 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix}$$

and

$$Q' \begin{pmatrix} v_0 & & 0 \\ & \ddots & \\ 0 & & v_n \end{pmatrix} Q = v \begin{pmatrix} \mu_0 & & 0 \\ & \ddots & \\ 0 & & \mu_n \end{pmatrix} \tag{7.23}$$

Moreover, $p(i,m)p(j,m) = \sum_{k=0}^{n} c_{ijk}p(k,m)$. [Recall that $P = (p(k,i))$ and $Q = (q(k,i)) = vP^{-1}$.]

Proof. The eigenvalues of A_iA_j are $p(i,m)p(j,m)$ with multiplicity μ_m, $0 \le m \le n$. Thus the trace of A_iA_j is $\sum_{m=0}^{n} \mu_m p(i,m)p(j,m)$. But we know that

$$A_iA_j = \sum_{k=0}^{n} c_{ijk}A_k$$

and hence the trace of A_iA_j is

$$\begin{aligned} \operatorname{trace} A_iA_j &= \operatorname{trace} \sum_{k=0}^{n} c_{ijk}A_k = \sum_{k=0}^{n} c_{ijk} \operatorname{trace} A_k \\ &= c_{ij0}\operatorname{trace}A_0 = c_{ij0}v = \begin{cases} v_iv & \text{if } i = j \\ 0 & \text{if } i \ne j \end{cases}. \end{aligned}$$

This proves $P'\operatorname{diag}(\mu_0, \ldots, \mu_n)P = v \operatorname{diag}(v_0, \ldots, v_n)$. Replacing P^{-1} by $v^{-1}Q$ gives the second equation.

To explain the last relation write

$$\begin{aligned} p(i,m)p(j,m)J_m &= A_i p(j,m)J_m = A_i A_j J_m = \left(\sum_{k=0}^{n} c_{ijk}A_k\right) J_m \\ &= \sum_{k=0}^{n} c_{ijk}A_k J_m = \left(\sum_{k=0}^{n} c_{ijk}p(k,m)\right) J_m. \end{aligned}$$

This ends our proof.

An Algebra of Dimension $n+1$ Isomorphic to $\mathcal{B}$

In an association scheme the number of relations (or colors), n, is in general much less than v. As it turns out, we can facilitate the spectral analysis of $\mathcal{B}$ by working with an algebra $\overline{\mathcal{B}}$ of $(n+1)\times(n+1)$ matrices, rather than with the $v \times v$ matrices of the original algebra $\mathcal{B}$.

Indeed, let $B_i = (c_{ijk})$, that is, the (j,k)th entry of B_i is c_{ijk}. Then

$$B_i B_j = \sum_{k=0}^{n} c_{ijk} B_k. \tag{7.24}$$

[That this is true can be seen as follows. The (l,m)th entry of $\sum_{k=0}^{n} c_{ijk}B_k$ is $\sum_{k=0}^{n} c_{ijk}c_{klm}$; on the other hand, the (l,m)th entry of B_iB_j is $\sum_{k=0}^{n} c_{ilk}c_{jkm}$. The last of the relations among the parameters, listed in Section 7.33, allows us to write $\sum_{k=0}^{n} c_{ilk}c_{jkm} = \sum_{k=0}^{n} c_{jkm}c_{ilk} = \sum_{k=0}^{n} c_{jik}c_{klm} = \sum_{k=0}^{n} c_{ijk}c_{klm}$ This proves (7.24).]

Display (7.24) shows that the matrices B_i multiply in the same manner as the matrices A_i. Furthermore, the B_i's are linearly independent since c_{ij0} equals 0, unless $i = j$, in which case $c_{ii0} = v_i$.

Define $\overline{\mathcal{B}}$ to be the algebra of matrices $\sum_{i=0}^{n} a_i B_i$, with a_i real numbers. Note that, unlike the A_i's, the matrices B_i need not necessarily be symmetric.

Under the mapping $A_i \to B_i$, the algebras $\mathcal{B}$ and $\overline{\mathcal{B}}$ are isomorphic. (This is true since, as we said, the B_i's multiply in the same way as the A_i's). In particular A_k and B_k have the same set of eigenvalues (not with the same multiplicities, of course). Indeed, let $p(k,i)$ be an eigenvalue of A_k. Then $A_k J_i = p(k,i)J_i$, and since the isomorphic image of this equation is $B_k \overline{J}_i = p(k,i)\overline{J}_i$ we conclude that $p(k,i)$ is also an eigenvalue of B_k (we denoted by $\overline{J}_i$ the isomorphic image of J_i). In particular, this allows us to conclude that any matrix in the Bose-Mesner algebra $\mathcal{B}$ has at most $n+1$ distinct eigenvalues.

Another happy consequence of the fact that A_k and B_k have the same set of eigenvalues is the actual computation of these; the dimension of the matrices B_k is quite small (relative to that of the A_k's) and thus the $p(k,i)$'s are easier to find as eigenvalues of the B_k's.

In the case of the Johnson scheme $J(m,n)$, for example, one finds: $p(k,i) = E(k,i)$, $q(k,i) = vi^{-1}\mu_k E(i,k)$, where $v_i = \binom{n}{i}\binom{m-n}{i}$, $\mu_k = (m-2k+1)(m-k+1)^{-1}\binom{m}{k}$ and

$$E(k,x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{n-x}{k-j}\binom{m-n-x}{k-j}, 0 \le k \le n.$$

The $E(k,x)$ are called *Eberlein* polynomials.

7.35 t-Designs as Subsets of Association Schemes

In this section we present a result of P. Delsarte concerning the existence of t-designs as subsets of association schemes. The language of association schemes brings into common perspective many results from coding theory, designs, and finite geometry. The reader is referred to [15] for a better understanding of this important point of view.

We work in an association scheme with point set $P = \{1, 2, \ldots, v\}$ and relations $R_0, R_1, \ldots, R_n$. Let S be a subset of P. Define

$$s_i = |R_i \cap (S \times S)|.$$

The constant s_i counts the number of ordered pairs in $S \times S$ that belong to relation R_i. Since the subsets $R_i \cap (S \times S)$ partition $S \times S$ it is clear that $\sum_{i=0}^{n} s_i = |S|^2$. We call the vector $(s_0, s_1, \ldots, s_n)$ the *weight distribution* of S.

We wish to interpret the weights s_i in terms of operations with the adjacency matrices A_i of the scheme. Recall that A_i is the adjacency matrix of relation R_i. To accomplish this, denote by x the $v \times 1$ indicator vector of the subset S; that is, $x' = (x_1, \ldots, x_v)$ with $x_k = 1$ if the point k belongs to S, and 0 otherwise. It then follows immediately that $s_i = x' A_i x$.

Define

$$d_i(S) = \sum_{j=0}^{n} q(i,j) s_j,$$

where $q(i,j)$ is the (i,j)th entry of the matrix Q whose inverse is $v^{-1}P$, with $P = (p(i,j))$ being the $(n+1) \times (n+1)$ matrix of the eigenvalues of the scheme.

A crucial observation made by Delsarte is that

$$d_i(S) = v x' J_i x, \tag{7.25}$$

where x is the indicator vector of S and J_i is the ith idempotent in the Bose-Mesner algebra $\mathcal{B}$ of the scheme. [Statement (7.25) is proved as follows: $d_i(S) = \sum_{j=0}^{n} q(i,j) s_j = \sum_{j=0}^{n} q(i,j) x' A_j x = x' (\sum_{j=0}^{n} \cdot q(i,j) A_j) x = v x' J_i x$. The last sign of equality is explained by (7.21).]

The idempotent J_i is a symmetric matrix that satisfies $J_i^2 - J_i = 0$. Its eigenvalues are therefore 0 or 1. We thus conclude that J_i is a nonnegative definite matrix, that is, it satisfies $y' J_i y \geq 0$ for all vectors y. With this in mind (7.25) informs us that

$$d_i(S) \geq 0, \quad 0 \leq i \leq n.$$

Subsets S of an association scheme for which $d_i(S) = 0$, for a large number of indices i, are in a sense "extreme" and possess interesting combinatorial properties. Delsarte proved the following:

$*$ *A nonempty subset S of the Johnson scheme $J(m,k)$ consists of the blocks of a $t-(m,k,\lambda_t)$ design if and only if the vector $(d_1(S), d_2(S), \ldots, d_k(S))$ has at least t components equal to 0.*

Proof. Points of the scheme are k-subsets of a set M; $|M| = m$. For an i-subset z of M, denote by $\lambda_i(z)$ the cardinality of the set $\{\alpha : z \subset \alpha;\ \alpha \in S\}$. A two-way counting of $|\{(z,\alpha) : z \subset \alpha;\ \alpha \in S\}|$ gives

$$\sum_z \lambda_i(z) = \binom{k}{i}|S|$$

Yet another two-way counting, this time of the cardinality of the set $\{(z,(\alpha,\beta)) : z \subset \alpha,\ z \subset \beta;\ \alpha,\beta \in S\}$, leads us to the following equation:

$$\sum_z \lambda_i^2(z) = \sum_{j=0}^{k} s_j \binom{j}{i}.$$

Denote by λ_i the average $\binom{m}{i}^{-1}\sum_z \lambda_i(z)$. The two equations we just derived allow us to write

$$\sum_z (\lambda_i(z) - \lambda_i)^2 = \left(\sum_{j=0}^{k} s_j \binom{j}{i}\right) - |S|\binom{k}{i}\lambda_i. \tag{7.26}$$

In this notation we can say that the subset S consists of the blocks of a $t-(m,k,\lambda_t)$ design if and only if $\lambda_i(z) = \lambda_i$ for all $z \in \sum_i(M)$ and all $1 \le i \le t$ (see Proposition 7.1, part (a)). Equation (7.26) allows us now to conclude that S is a $t-(m,k,\lambda_t)$ design if

and only if the weights s_j satisfy the system:

$$\sum_{j=0}^{k} \binom{j}{i} s_j = |S| \binom{k}{i} \lambda_i, \quad \text{for } 1 \leq i \leq t. \tag{7.27}$$

For a fixed i $(1 \leq i \leq t)$ observe, however, that

$$\begin{aligned} |S|^{-2} \sum_{j=0}^{k} \binom{j}{i} s_j &= |S|^{-2} |S| \binom{k}{i} \lambda_i \\ &= |S|^{-1} \binom{k}{i} \binom{m}{i}^{-1} \binom{k}{i} |S| = \binom{m}{i}^{-1} \binom{k}{i}^2. \end{aligned} \tag{7.28}$$

The far right-hand side, that is, $\binom{m}{i}^{-1}\binom{k}{i}^2$, is seen to depend on m, k, and i only and not on the specific choice of the t-design. Select in particular the complete design consisting of all $\binom{m}{k}$ subsets of size k of M. The weight distribution of this complete design is $(v_0, v_1, \ldots, v_n)$ and thus (7.28) becomes

$$\binom{m}{k}^{-2} \sum_{j=0}^{k} \binom{j}{i} v_j = \binom{m}{i}^{-1} \binom{k}{i}^2. \tag{7.29}$$

In view of (7.28) and (7.29), system (7.27) can be written as follows:

$$|S|^{-2} \sum_{j=0}^{k} \binom{j}{i} s_j = \binom{m}{k}^{-2} \sum_{j=0}^{k} \binom{j}{i} v_j, \quad 1 \leq i \leq t. \tag{7.30}$$

Let $s' = |S|^{-2}(s_0, s_1, \ldots, s_n)$, $v' = \binom{m}{k}^{-2}(v_0, v_1, \ldots, v_n)$ and let $\overline{T}$ be the $t \times (k+1)$ matrix with (i,j)th entry equal to $\binom{j}{i}$ if $i \leq j$ and 0 otherwise. System (7.30) can be rewritten as

$$\overline{T}s = \overline{T}v. \tag{7.31}$$

Think of the binomial coefficient $\binom{j}{i}$ as the polynomial $\binom{x}{i}$ $(= [x]_i/i!)$ evaluated at j (by x we understand an indeterminate ready and willing to take numerical values at all times). The polynomials $\binom{x}{i}$, for $1 \leq i \leq t$, form a basis for the subspace of polynomials

of degree at least 1 and at most t over the real numbers. The numbers $q(i,j)$ turn out also to be values of polynomials $F(i,x)$ evaluated at j. (This is a *most important* fact; the polynomials $F(i,x)$ are related to the Eberlein polynomials.) The polynomial $F(i,x)$ is of degree i and hence the $F(i,x)$, $1 \le i \le t$, also span the subspace of polynomials of degree at least 1 and at most t. Perform a change of basis by writing

$$\binom{x}{i} = \sum_{j=1}^{t} w_{ij} F(j,x), \quad 1 \le i \le t, \tag{7.32}$$

for a $t \times t$ nonsingular matrix $W = (w_{ij})$.

Let $\overline{Q}$ be the $t \times (k+1)$ matrix with (i,j)th entry equal to $q(i,j)$. [Note that $\overline{Q}$ consists of the first t rows of the $(k+1) \times (k+1)$ matrix $Q = (q(i,j))$.] We can use the matrix W to write $\overline{T} = W\overline{Q}$ [this follows directly from (7.32)].

Observe now that $\overline{T}s = \overline{T}v$ if and only if $W\overline{Q}s = W\overline{Q}v$ if and only if $\overline{Q}s = \overline{Q}v$ (since W is nonsingular). But $\overline{Q}v = 0$ by the orthogonality relations (7.23) proved in Section 7.34. To be more exact, the ith equation of the system $\overline{Q}v = 0$ is

$$\sum_{j=0}^{k} q(i,j) v_j = 0, \quad 1 \le i \le t.$$

Read this last equation as $\sum_{j=0}^{k} v_j q(i,j) q(0,j) = 0$ by recalling that $q(0,j) = 1$, for $0 \le j \le k$. Since $i \neq 0$ the equation is explained by the aforementioned orthogonality conditions.

To summarize, we showed that S is a t-design if and only if $\overline{T}s = \overline{T}v$ if and only if $\overline{Q}s = \overline{Q}v$ $(= 0)$ if and only if $\overline{Q}s = 0$ if and only if

$$\sum_{j=0}^{k} q(i,j) s_j = 0, \quad 1 \le i \le t$$

if and only if

$$d_i(S) = 0, \quad 1 \leq i \leq t.$$

This ends the proof.

7.36 Partial Designs

Let a set P of v points with relations $R_0, R_1, \ldots, R_n$ be an association scheme with n classes. We define the notion of a partial design, a concept less restrictive combinatonally than a 2-design. It was originally introduced by Bose in connection with statistical design of experiments.

The pair (P, B) is called a *partial design with n classes* if B is a collection of k-subsets of P (called blocks) such that points x and y appear in p_i blocks whenever $(x, y) \in R_i$, $0 \leq i \leq n$. [Observe, in particular, that each point occurs in p_0 blocks since $(x, x) \in R_0$.]

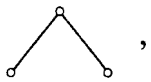
In case $p_1 = p_2 = \cdots = p_n \ (= \lambda_2)$ we obtain a $2 - (v, k, \lambda_2)$ design. This, however, does not happen frequently.

We can construct partial designs with two classes as follows: Let P be a set of v points. Let also G be a group that acts transitively on P and has three symmetric orbits $R_0 = \{(x, x) : x \in P\}$, R_1 and R_2 on $P \times P$. This action generates an association scheme with two associate classes on P; two points x and y are first associates if $(x, y) \in R_1$ and second associates if $(x, y) \in R_2$. Let S be *any* k-subset of P ($k \geq 2$). We define the blocks of our partial design as

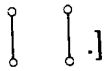
$$B = \{g(S) : g \in G\}.$$

The pair (P, B) is indeed a partial design with two classes. Suppose a point x is in blocks $\{S_i : 1 \leq i \leq p_0\}$. Then any other point y will be in blocks $\{g(S_i) : 1 \leq i \leq p_0\}$, where g

is an element of G that sends x to y (we use here the transitivity of G on P). Moreover, if $(x, y) \in R_i$ and $(z, w) \in R_i$, then there exists an element g_i of G that sends (x, y) into (z, w), $i = 1, 2$. Consequently, if $\{x, y\}$ occurs in blocks $\{S_j : 1 \leq j \leq p_i\}$, then $\{z, w\}$ occurs in blocks $\{g_i(S_j) : 1 \leq j \leq p_i\}$, $i = 1, 2$. This proves that (P, B) is a partial design with two classes. [This construction can easily be remembered by a special case: Take P to be the *edges* of a complete graph on m vertices and let the group G be the whole symmetric group S_m on the m vertices. The group S_m acts transitively on edges and has three orbits on $P \times P$. One orbit is just the diagonal $R_0 = \{(x, x) : x \in P\}$; R_1 consists of all pairs of edges like



and R_2 consists of all pairs of parallel edges

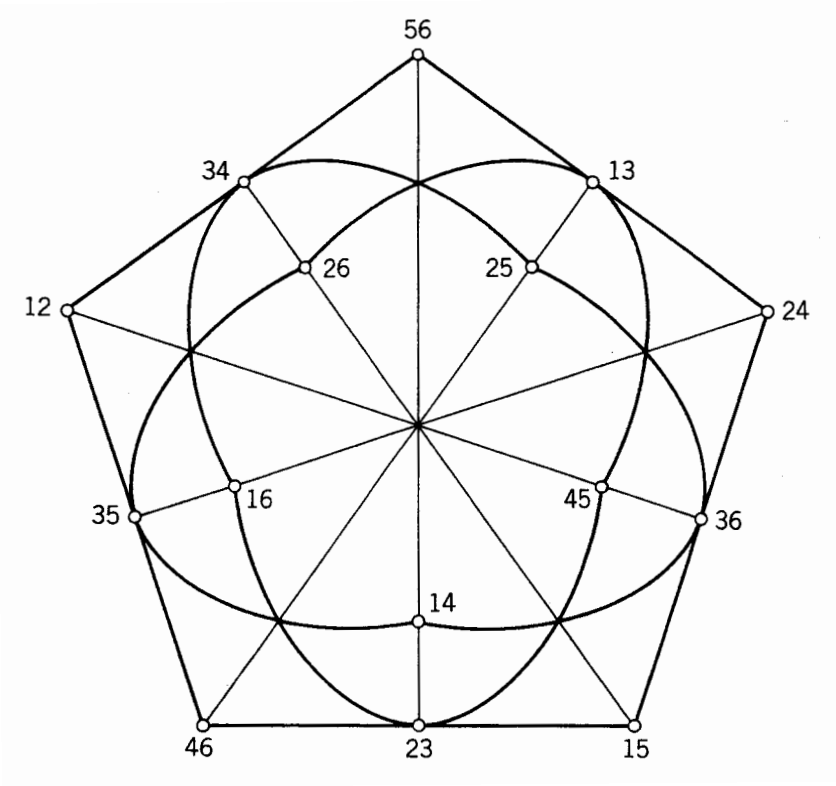


Let us now introduce another concept (still due to Bose [1]). A *partial geometry* (r, k, t) is a collection of subsets (called *lines*) with the following properties: each line contains k points; each point is on r lines; two distinct points are on at most one line; given a line and a point not on it, there exist precisely t lines passing through that point and intersecting the original line.

We mention without proof a result of Bose [1]:

$*$ *A partial geometry is a partial design with two classes. A partial design with two classes, strictly fewer blocks than points, and in which two distinct points occur in at most one block must necessarily be a partial geometry.*

We conclude our discussion on the subject of partial designs with a graphical display of a partial geometry $(r, k, t) = (3, 3, 1)$:



The points are labeled by the 2-subsets of the set $\{1, 2, 3, 4, 5, 6\}$. There are 15 points and 15 lines in all. Graphically we have lines of the form $\{12, 34, 56\}$, $\{13, 25, 46\}$, and "curved lines" such as $\{34, 16, 25\}$, five of each kind. To be exact, a line consists of three disjoint pairs.

EXERCISES

1. Find the 3×3 matrix of eigenvalues of an association scheme with two classes.

2. In any association scheme show that

$$p(0, j) = q(0, j) = 1, \quad p(i, 0) = v_i, \quad \text{and} \quad q(i, 0) = \mu_i.$$

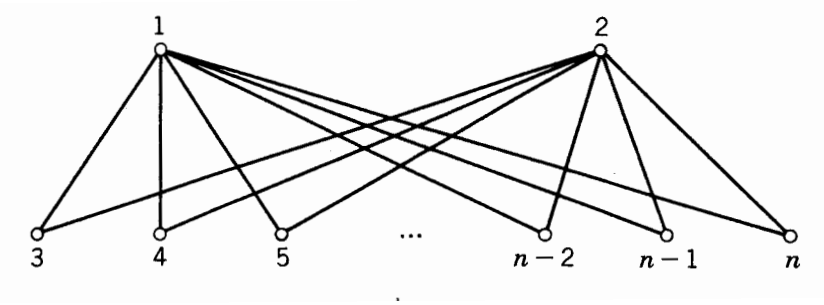
Show, in addition, that $|p(i,j)| \leq v_i$.

3. In the Hamming scheme $H(n)$ show that $v = 2^n$, $vi = \binom{n}{i}$,

$$c_{ijk} = \binom{k}{2^{-1}(i-j+k)}\binom{n-k}{2^{-1}(i+j-k)},$$

if $i+j-k$ is even, and $c_{ijk} = 0$ otherwise.

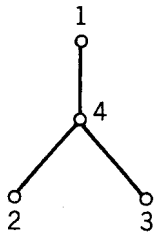
4. By looking at the images of the subgraph



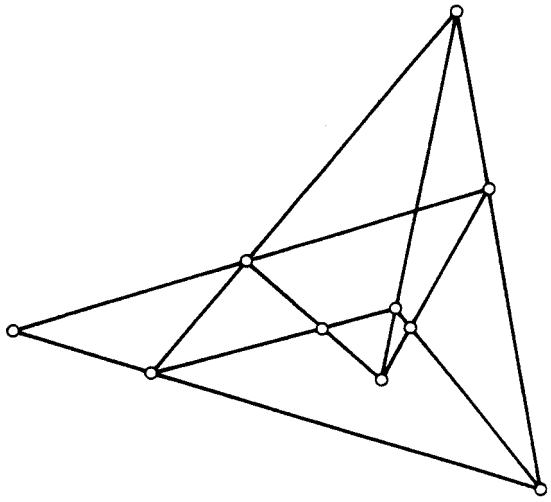
of K_n (the complete graph on n vertices) under all the $n!$ permutations on vertices we obtain a partial design. Compute its parameters.

5. (Nair.) Let N be the incidence matrix (points versus blocks) of a partial design with two classes. If the partial design has fewer blocks than points, then NN' is a singular matrix. Relying on this and looking at the algebra $\overline{\mathcal{B}}$ of 3×3 matrices (c_{ijk}) find an *explicit* relation among the parameters (c_{ijk}) of the scheme and the parameters p_i of the partial design. [*Hint*: The determinant of the 3×3 matrix (c_{ijk}) is zero.]

6. A graph like this



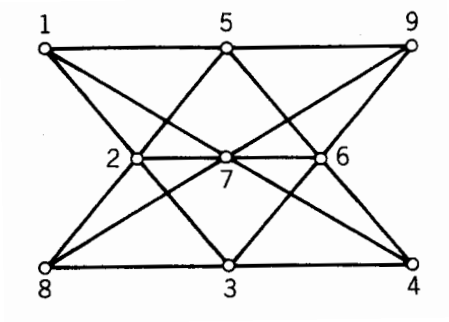
is called a 3-claw; the "missing" edges are indeed understood to be missing. Vertices 1, 2, and 3 are called the outer vertices of the 3-claw. In the Petersen graph (see Section 7.31) call three points colinear if they are the outer vertices of a 3-claw. The configuration of ten points and ten lines that results is the Desargue configuration:



Check this. (A line is a straight line, as drawn, and it contains three points.)

7. Show that the Desargue configuration displayed above is a partial design with two classes. Find its full automorphism group.

8. Prove that the Pappus configuration



is a partial design with two classes. Compute its full automorphism group. (The blocks are the nine straight lines with three points on each, as drawn.)

9. Consider the combinatorial structure whose lines are the columns below:

$$\begin{array}{cccccccccc} 2 & 4 & 1 & 1 & 4 & 7 & 1 & 2 & 3 & 3 \\ 10 & 10 & 10 & 2 & 5 & 8 & 4 & 5 & 6 & 5 \\ 6 & 8 & 9 & 3 & 6 & 9 & 7 & 8 & 9 & 7 \end{array}$$

Is this structure isomorphic to the Desargue configuration? Is it a partial design?

10. Show that a partial geometry (r, k, t) can exist only if

$$rk(r-1)(k-1)(k+r-t-1)^{-1}t^{-1}$$

is an integer. [*Hint*: This number is the multiplicity of an eigenvalue of the scheme.]

11. Prove that a partial design with fewer blocks than points in which a pair of distinct points appears in at most one block is necessarily a partial geometry.

8 NOTES

A systematic study of the subject discussed in this chapter was initiated by Fisher, Bose, and their students. The fundamental motivation stems from the planning of efficient statistical experiments.

Relatively recent contributions to t-designs of particular significance were made by Ray-Chaudhuri and Wilson [3], as well as Wilson [4]. Sections 1 and 3 are based on the results presented in these two papers. The author was exposed to this material by his former teacher, Professor Noboru Ito.

All of the methods of construction of t-designs that we present are well known and most of them are mentioned implicitly or explicitly in [5] or [6]. We highly recommend these two books, along with [7], to anyone interested in further research on the subject. The construction through hypergraphs appears to have led to the first nontrivial 6-design [16].

Section 4 consists of a result of Cameron [8]. A couple of other results on extending t-designs are found in Exercise 8 at the end of Section 6.

The well-known result of Bruck, Ryser, and Chowla is presented in Section 5. Several books contain this theorem. We recommend [9] and [6]. Much more can be said on the interplay between the design and its automorphism group than what we mention in Section 6. Except for the proof of the nonsingularity of matrix N_S, Section 7.26 is an observation due to the author. We refer to [10] for more information on the automorphism group in general, and to [7] for the automorphism groups of projective geometries in particular.

Association schemes, creations of Bose, have enjoyed a flurry of activity in recent years. Attempts at classification are vigorously pursued, influenced chiefly by Bannai and Ito [11]. Connections to designs and codes are described in Section 7.35. Recent work by Bailey et al. [12] places association schemes at the foundation of the analysis of variance.

9 REFERENCES

1. R. C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.*, **13**, 389-419 (1963).

2. R. C. Bose and D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Statist.*, **30**, 21-38 (1959).

3. D. K. Ray-Chaudhuri and R. M. Wilson, On t-designs, *Osaka J. Math.*, **12**, 737-744 (1975).

4. R. M. Wilson, Incidence matrices of t-designs, *Lin. Alg. and Applic.*, **46**, 73-82 (1982).

5. P. J. Cameron and J. H. van Lint, *Graphs, Codes and Designs*, LMS Lecture Note Series 43, Cambridge University Press, Cambridge, 1980.

6. E. S. Lander, *Symmetric Designs: An Algebraic Approach*, LMS Lecture Note Series 74, Cambridge University Press, Cambridge, 1983.

7. N. L. Biggs and A. T. White, *Permutation Groups and Combinatorial Structures*, LMS Lecture Note Series 33, Cambridge University Press, Cambridge, 1979.

8. P. J. Cameron, Expending symmetric designs, *J. Comb. Th. (A)*, **14**, 215-220 (1973).

9. H. J. Ryser, *Combinatorial Mathematics*, Carus Math. Monographs 14, 1963.

10. P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin, 1968.

11. E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin Cummings, Menlo Park, 1984.

12. R. Bailey, C. E. Praeger, T. P. Speed, and D. E. Taylor, *The Analysis of Variance*, manuscript, Rothamsted experimental station (private communication), 1985.

13. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

14. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

15. P. Delsarte, The association schemes of coding theory, *Combinatorics, Part* 1, Math. Centre Tracts 55, Amsterdam, 1974.

16. S. Magliveras and D. W. Leavitt, Simple 6-(33,8,36) designs from $P\Gamma L_2(32)$, preliminary report (private communication) (1984).

17. A. Hedayat and W. D. Wallis, Hadamard matrices and their applications, *Ann. Statist.*, **6**, 1184-1238 (1978).

18. M. Burrow, *Representation Theory of Finite Groups*, Academic Press, New York, 1965.