1. SYMMETRIC DESIGNS

§1.1 DEFINITIONS AND SIMPLE EXAMPLES

An incidence structure consists simply of a set $\mathcal{P}$ of points and a set $\mathcal{B}$ of blocks, with a relation of incidence between points and blocks. Being of such a general nature, incidence structures arise naturally in all branches of mathematics. The particular sort which is the subject of this monograph--symmetric designs--arose first in the statistical theory of the design of experiments, but they rapidly have become objects of great combinatorial interest in their own right.

A symmetric (v,k,λ) design (or a symmetric design with parameters (v,k,λ)) is an incidence structure satisfying the following six requirements:

(1) There are v points.

(2) There are v blocks.

(3) Any block is incident with k points.

(4) Any point is incident with k blocks.

(5) Any two blocks are incident with λ points.

(6) Any two points are incident with λ blocks.

To exclude degenerate cases, we also insist that $k > \lambda$.

These axioms are not independent, and we shall explore them further in §1.4.

Example 1. The paradigmatic example of a symmetric design is represented in Figure 1.1. This symmetric design has parameters (7,3,1). The seven points are 1,2,3,4,5,6, and 7. The seven blocks are the sets {1,2,4}, {2,3,5}, {3,4,6}, {4,5,7}, {5,6,1}, {6,7,2} and {7,1,3}. A point p is incident with a block B if $p \in B$.

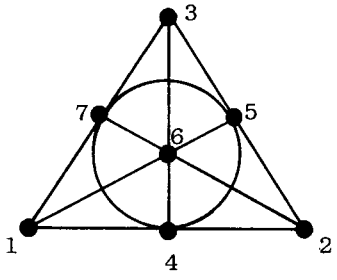

Figure 1.1 The Design Theorist's Coat of Arms

Example 2. Given any set $\mathcal{P}$ of v points, we can define a symmetric (v,v-1,v-2) design by letting $\mathcal{B}$ consist of the subsets of $\mathcal{P}$ having size v-1. A point p is defined to be incident with a block B if $p \in B$. Similarly, if $\mathcal{B}$ consists of the singleton subsets of $\mathcal{P}$ a symmetric (v,1,0) design results. Symmetric designs of these two sorts are called trivial.

The requirement that $k > \lambda$ implies that distinct blocks are incident with distinct point sets. So, we can always identify a block with the set of points with which it is incident and in general we shall not fuss over the formal distinction between them. Nevertheless, it is better not to define blocks as sets of points--for doing so would obliterate the formal duality between points and blocks (i.e., the fact that the axioms are unchanged if we reverse the role of points and blocks).

Example 3. Let $\mathcal{P}$ be the set of 11 residue classes modulo 11 and let B = {1,3,4,5,9} be the set of non-zero quadratic residues. Any two of the sets B, B+1, B+2,..., B+10 share two residue classes (where $B+i = \{x+i \mid x \in B\}$) and they may be taken as the 11 blocks of a symmetric (11,5,2) design.

Example 4. Let $\mathcal{P}$ be the set of 16 small squares in Figure 1.2. To each square there corresponds a block as in the figure--namely, the points incident with the block are

the other six squares in the same row or column. A symmetric (16,6,2) design results.

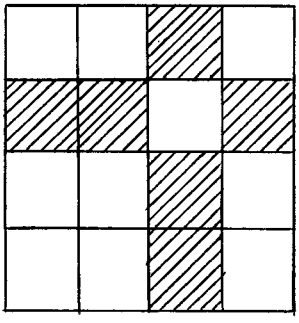

Figure 1.2

In this monograph we shall be concerned chiefly with exploring for which triples (v,k,λ) there exist symmetric designs with parameters (v,k,λ) and exposing, along the way, particularly interesting examples.

Proposition 1.1. In a symmetric (v,k,λ) design,

(1) $(v-1)\lambda = k(k-1)$,

(2) $k^2-v\lambda = k-\lambda$, and

(3) $(v-k)\lambda = (k-1)(k-\lambda)$.

Proof. To prove the first assertion, choose a particular point q and count in two different ways the number of pairs (p,B) with $p \neq q$ and B incident with both p and q (first by summing over points and second by summing over blocks). The second and third assertions are simply algebraic rearrangements of the first. Although they carry no new information, they will be useful for observing certain divisibility relations among the parameters.□

The value $k-\lambda$, which occurs in two of the equations above, is an extremely important parameter. We set $n=k-\lambda$ and call n the order of the symmetric (v,k,λ) design.

The incidence matrix A of a symmetric (v,k,λ) design is the v x v matrix whose rows are indexed by blocks and whose columns are indexed by points, with the entry in row B and column p being 1 if p and B are incident and 0 otherwise. (For our purposes, the particular order in which

blocks and points are listed is irrelevant.) The incidence requirements can be expressed in terms of A:

$$AJ = JA = KJ \quad \text{and}$$

$$AA^T = A^TA = (k-\lambda)I + \lambda J = nI + \lambda J.$$

(Here, as throughout this book, I is the identity matrix and J the matrix with every entry 1, of appropriate size.) It is not difficult to show that the v x v matrix aI + bJ has determinant $(a+vb)a^{v-1}$. Hence $\det(nI + \lambda J) = k^2n^{v-1}$.

Proposition 1.2. If A is the incidence matrix of a symmetric (v,k,λ) design then $|\det A| = kn^{\frac{1}{2}(v-1)}$

Since det A must be an integer, we obtain our first substantial restriction upon the parameters of a symmetric design.

Theorem 1.3. (Schutzenberger [120]) Suppose that there exists a symmetric (v,k,λ) design. If v is even, then n must be a square.

An isomorphism from one symmetric design to another is a one-to-one mapping of points to points and blocks to blocks which preserves both incidence and nonincidence. Isomorphic symmetric designs necessarily have the same parameters. The condition is not sufficient however, and we shall soon see examples of symmetric designs with the same parameters which are not isomorphic.

Example 5. Reversing the roles of points and blocks in a symmetric (v,k,λ) design D, we obtain the dual of D, denoted D^{dual}, which is also a symmetric (v,k,λ) design. The incidence matrices of D and D^{dual} are transpose to one another. In general, D and D^{dual} need not be isomorphic.

Example 6. By taking the complement of the incidence relation in a symmetric (v,k,λ) design D (i.e., by replacing incidence by nonincidence and vice versa), we obtain the complement of D, denoted D'. The incidence structure D' is a symmetric (v', k', λ') design where $(v', k', \lambda') = (v, v-k, v-2k+\lambda)$. In particular, D and D' both have order $n=(k-\lambda)=(k'-\lambda')=n'$. A useful identity, yet another version of the fundamental equation $(v-1)\lambda=k(k-1)$, is the equation $\lambda\lambda'=n(n-1)$.

§1.2 HADAMARD MATRICES AND DESIGNS

A Hadamard matrix of order m is an m x m matrix H with entries ± 1 satisfying $HH^T = H^TH = mI$. (It is so named because its determinant attains a bound due to Hadamard.) These matrices are closely related to symmetric designs in a number of ways. Changing the sign of all entries in any row or column does not disturb the defining equation. We may therefore assume, if we like, that all entries in the first row and column are +1; call such a Hadamard matrix normalized. If we now delete the first row and column and replace -1 by 0 throughout we obtain a matrix M which (for $m \geq 4$) is the incidence matrix of a symmetric $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ design. Such a symmetric design is called a Hadamard design.

$$\begin{pmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

A normalized Hadamard matrix

Associated Hadamard design

Figure 1.3

From any symmetric design with parameters of the form $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ we may in turn recover a normalized Hadamard matrix. (N.B. A Hadamard matrix may be modified by permuting rows and columns and subsequently renormalized; from such 'equivalent' Hadamard matrices nonisomorphic symmetric designs can result.)

The problem of constructing Hadamard matrices has received a great deal of attention and we shall only touch on a few basic methods. From the connection between Hadamard matrices and symmetric designs above, it follows almost immediately that a necessary condition for the

existence of a Hadamard matrix of order m is that m=1, m=2 or m≡0 (mod 4). A longstanding conjecture states that this condition is sufficient as well. At present, no proof is known, but Hadamard matrices of order m have been found for all m divisible by 4 up through 264.

The unique normalized Hadamard matrix of order 2 is

$$H_2 = \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$$

If $H = (h_{ij})$ and K are Hadamard matrices of orders m and m', respectively, their Kronecker product

$$H \otimes K = \begin{pmatrix} h_{11}K & h_{12}K & \cdots & h_{1m}K \\ \vdots & & & \vdots \\ h_{m1}K & h_{m2}K & \cdots & h_{mm}K \end{pmatrix}$$

is a Hadamard matrix of order mm'. Starting with H_2, for example, we have the (normalized) Hadamard matrices

$$H_{2^r} = \underbrace{H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{r \text{ times}}$$

which are called the Hadamard matrices of Sylvester type, or simply, the Sylvester matrices. (The normalized Hadamard matrix of Figure 1.3 is a Sylvester matrix.) Hence,

Example 7. There exist Hadamard designs with parameters $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$ for all integers $m \geq 2$.

There are two constructions which together allow us to associate to any finite field of odd characteristic a Hadamard matrix. Let q be a power of an odd prime p, say $q=p^f$. The Legendre symbol χ of F_q is the mapping $\chi: F_q \longrightarrow \{0,1,-1\}$ given by

$\chi(0) = 0$

$\chi(a) = 1$ if a is a nonzero square in F_q and

$\chi(a) = -1$ if a is not a square in F_q.

Note that $\chi(xy) = \chi(x)\chi(y)$. The Jacobsthal matrix $R = (r_{ij})$ is a q x q matrix whose rows and columns are indexed by the

elements of F_q and in which $r_{ij} = \chi(i-j)$. The Jacobsthal matrix of order 7 is shown below.

$$\begin{pmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{pmatrix}$$

If $q \equiv 1 \pmod 4$ then -1 is a square in F_q and R is a symmetric matrix. If $q \equiv 3 \pmod 4$ then R is skew-symmetric; that is, $R^T = -R$.

Proposition 1.4. $R^TR = RR^T = qI - J$ and $RJ = JR = 0$.

Proof. The second equation reflects the fact that there are as many nonzero squares as nonsquares in F_q. For a proof of the first, see Problems 6 and 7.□

Using the Jacobsthal matrices we can give constructions for Hadamard matrices, depending on the value of $q \pmod 4$.

Example 8. Let q be a prime power congruent to 3 $\pmod 4$. Let

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & & \\ & & (R - I) & \\ 1 & & & \end{pmatrix}.$$

Then

$$HH^T = \begin{pmatrix} q+1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ & & J+(R-I)(R^T-I) & \\ 0 & & & \end{pmatrix} = H^TH.$$

From Proposition 1.4 and the skew-symmetry of R, we find that H is a Hadamard matrix of order q+1, which is said to be of Paley type. Using this Hadamard matrix we obtain a Hadamard design with parameters $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-3))$ which we denote H(q). (The incidence matrix of H(q) is of course obtained directly from R by replacing -1 by 0 throughout. That is, the blocks of H(q) are translates of the nonzero quadratic residues.)

H(11), which is Example 3 above, has incidence matrix

$$\begin{pmatrix}
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0
\end{pmatrix}.$$

This symmetric design displays a great deal of 'symmetry.' We elaborate presently on this idea.

An automorphism of a symmetric design is an isomorphism of the symmetric design onto itself. To describe an automorphism then, we must give a permutation of the points and a permutation of the blocks which preserve the incidence structure. (So, in terms of the incidence matrix A, an automorphism specifies matrices P and Q such that PAQ = A.) The collection of all automorphisms forms a group under composition, called the full automorphism group of the symmetric design. Any subgroup is called an automorphism group of the symmetric design.

In practice, it is unnecessary to specify the action of an automorphism on both points and blocks. Once we know how it acts on points its action on blocks is determined--for blocks are completely specified by the points incident

with them. Accordingly, we abuse terminology and frequently call a permutation π of the points of a symmetric design an automorphism if π induces an automorphism--that is, if for all blocks B, the set $\{\pi(p) \mid p \text{ is incident with } B\}$ is also a block.

Consider the Paley designs H(q). The permutation of the points given by $x \longmapsto x + b$, where b is any element of GF(q), induces an automorphism of H(q). The collection of all such automorphisms forms a group which acts regularly on the points (and blocks) of H(q). (The definitions and results which we shall require concerning permutation groups are summarized in Appendix A.) We can find an even larger automorphism group. Let $\Sigma(q)$ denote the group of all permutations π of the points given by

$$\pi: x \longrightarrow a\sigma(x) + b$$

where a is a nonzero square in F_q and σ is an automorphism of the field F_q. Since $\chi(\pi(i) - \pi(j)) = \chi(a)\chi(\sigma(i-j)) = \chi(i-j)$, every element of $\Sigma(q)$ induces an automorphism of H(q) and we may regard $\Sigma(q)$ as an automorphism group of H(q).

It is sometimes useful to work with the subgroup S(q) of $\Sigma(q)$ consisting of all the permutations π in which σ is the identity field automorphism. Note that S(q) has order $\frac{1}{2}q(q-1)$ and that when q is a prime, $S(q)=\Sigma(q)$.

The reader should check that both S(q) and $\Sigma(q)$ act 2-homogeneously (although not 2-transitively) and are thus rather large as permutation groups go.

Todd [130] first posed the question: Is $\Sigma(q)$ the full automorphism group of H(q)? Kantor [72] finally supplied the complete answer.

Theorem 1.5. (Kantor) For $q > 19$, the full automorphism group of H(q) is $\Sigma(q)$.

The proof goes beyond the scope of this book. For $q < 19$, it turns out that the full automorphism group of H(q) is even larger. When q=3, of course, the full symmetric group on three letters acts on H(3), which is a symmetric (3,2,1) design. In the other two cases, q=7 and q=11 we can

find a 2-transitive automorphism group of H(q) properly containing $\Sigma(q)$. We explore this in Problems 3 and 4.

Having now constructed Hadamard matrices and designs corresponding to F_q when $q \equiv 3 \pmod 4$, we turn to the case $q \equiv 1 \pmod 4$.

Example 9. Suppose that q is a prime power congruent to 1 (mod 4). Let

$$M = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & R & \\ 1 & & & \end{pmatrix}$$

where R is the Jacobsthal matrix of F_q. Construct a Hadamard matrix of order 2(q+1) as follows. Define auxiliary matrices

$$U = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

Replace each 0 in M by V, each +1 in M by U and each -1 in M by -U. Using the relations

$$UU^T = VV^T = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

and

$$UV^T = -VU^T = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$$

we can verify that a Hadamard matrix results (Problem 8). From the Hadamard matrix, we obtain a symmetric $(2q+1, q, \frac{1}{2}(q-1))$ design which we denote by H'(2q+1).

There is an entirely different construction of symmetric designs which relies not on normalized Hadamard matrices but on Hadamard matrices with constant row and column sums. Suppose that H is a Hadamard matrix of order v having constant row and column sums. We shall see that the positions of the +1 entries describe a symmetric design. For, let k be the number of +1 entries in each row (column). Select any pair of rows (columns) and let λ be the number