1 · A brief introduction to design theory

These lectures were given to an audience of design theorists; for those outside this class, the introductory chapter describes some of the concepts of design theory and examples of designs to which we shall refer.

A t-design with parameters (v, k, λ) (or a t - (v, k, λ) design) is a collection $\mathfrak{D}$ of subsets (called blocks) of a set S of v points, such that every member of $\mathfrak{D}$ contains k points, and any set of t points is contained in exactly λ members of $\mathfrak{D}$. Various conditions are usually appended to this definition to exclude degenerate cases. We assume that S and $\mathfrak{D}$ are non-empty, and that $v \geq k \geq t$ (so $\lambda > 0$). A t-design with $\lambda = 1$ is called a Steiner system. Alternatively, a t-design may be defined to consist of a set of points and a set of blocks, with a relation called incidence between points and blocks, satisfying the appropriate conditions.

Sometimes a t-design is defined so as to allow 'repeated blocks', that is, $\mathfrak{D}$ is a family rather than a set, and the same subset of S may occur more than once as a block. (This is more natural with the 'relation' definition; simply omit the condition that any k points are incident with at most one block.) In these notes, we normally do not allow repeated blocks; where they are permitted, we shall say so. There are 'non-trivial' t-designs with repeated blocks for every value of t; but the only known examples without repeated blocks with $t > 5$ are those in which every set of k points is a block. The existence of non-trivial t-designs with $t > 5$ is the most important unsolved problem in the area; even 5-designs are sufficiently rare that new constructions are interesting. Of course, for Steiner systems the question of repeated blocks does not arise. Only two Steiner systems with $t = 5$, and two with $t = 4$ are known; these will be described later.*

* Several more such systems have recently been constructed by R. H. F. Denniston.

Remark. A 0-design is simply a collection of k-element subsets of a set.

In a t-design, let λ_i denote the number of blocks containing a given set of i points, with $0 \le i \le t$. Counting in two ways the number of choices of $t - i$ further points and a block containing all t distinguished points, we obtain

$$(1.1) \quad \lambda_i \binom{k-i}{t-i} = \binom{v-i}{t-i} \lambda.$$

It follows that λ_i is independent of the i points originally chosen; that is, a t-design is also an i-design for $0 \le i \le t$. The parameters λ_0 (the total number of blocks) and λ_1 (the number of blocks containing a given point) are usually denoted by b and r respectively. With $t = 1$, $i = 0$, (1.1) shows that, in any 1-design,

$$(1.2) \quad bk = vr.$$

A 2-design is often called a block design, or simply a design; in the literature the term 'balanced incomplete block design', abbreviated to BIBD, is used in the case where not every k-subset is a block. In a 2-design we have

$$(1.3) \quad r(k - 1) = (v - 1)\lambda.$$

An incidence matrix of a design is a matrix M whose rows and columns are indexed by the blocks and points of the design respectively, the entry in row B and column p being 1 if $p \in B$, 0 otherwise. (The reader is warned that a different convention is often used, for example in the books by Dembowski [24] and Hall [33], with the result that our incidence matrix is the transpose of that appearing in these books. The present convention is adopted because we shall wish to regard the characteristic functions of blocks, or rows of M, as row vectors, and consider the subspace they span.)

The conditions that any block contains k points, any point lies in r blocks, and any pair of points lies in λ blocks, can be expressed in terms of M:

(1.4) $$MJ = kJ,$$
$$JM = rJ,$$
$$M^TM = (r - \lambda)I + \lambda J.$$

(Here, as throughout this book, I is the identity matrix, and J the matrix with every entry 1, of the appropriate size.) It is not difficult to show that

$$\det((r - \lambda)I + \lambda J) = rk(r - \lambda)^{v-1};$$

so, if $r > \lambda$, the matrix M^TM is non-singular, from which follows Fisher's inequality:

(1.5) **Theorem.** *In a* 2-*design with* $k \leq v - 1$, *we have* $b \geq v$.

Furthermore, if $b = v$, then $MJ = JM$; thus M commutes with $(r - \lambda)I + \lambda J$, and so with $((r - \lambda)I + \lambda J)M^{-1} = M^T$. So $MM^T = (r - \lambda)I + \lambda J$, from which we see that any two blocks have λ common points.

(1.6) **Theorem.** *In a* 2-*design with* $k \leq v - 1$, *the following are equivalent:*

(i) $b = v$;

(ii) $r = k$;

(iii) *any two blocks have* λ *common points.*

A 2-design satisfying the conditions of (1.6) is called *symmetric.* Its *dual* is obtained by reversing the roles of points and blocks, identifying a point with the set of blocks containing it; the dual is a symmetric 2-design with the same parameters, having incidence matrix M^T. A *polarity* of a symmetric design $\mathfrak{D}$ is a self-inverse isomorphism between $\mathfrak{D}$ and its dual, that is, a one-to-one correspondence σ between the points and blocks of $\mathfrak{D}$ such that, for any point p and block B, $p \in B$ if and only if $B^\sigma \in p^\sigma$. A point p (resp. a block B) is *absolute* with respect to the polarity σ if $p \in p^\sigma$ (resp. $B^\sigma \in B$).

(1.5) and (1.6) follow from a more general result, which we will need in chapter 4.

(1.7) **Theorem.** *In a* 2-*design, the number of blocks not disjoint from a given block* B *is at least* $k(r-1)^2/((k-1)(\lambda-1) + (r-1))$. *Equality holds if and only if any block not disjoint from* B *meets it in a constant number of points; if this occurs, the constant is* $1 + (k-1)(\lambda-1)/(r-1)$.

Proof. Let $B_1, \ldots, B_d$ be the blocks different from but not disjoint from B, and $x_i = |B \cap B_i|$. Counting in two ways the number of choices of one or two points of B and another block containing them, we obtain (with summations running from 1 to d):

$$\sum x_i = k(r - 1),$$
$$\sum x_i(x_i - 1) = k(k - 1)(\lambda - 1).$$

So

$$\sum (x_i - x)^2 = dx^2 - 2k(r - 1)x + k((k - 1)(\lambda - 1) + (r - 1)).$$

This quadratic expression in x must be positive semi-definite, and can vanish only if all x_i are equal; the common value must then be $1 + (k - 1)(\lambda - 1)/(r - 1)$. √

Remark. Now (1.5) follows from $b-1 \geq k(r-1)^2/((k-1)(\lambda-1)+(r-1))$ on applying (1.2) and (1.3). Also, if $b = v$, then $r = k$, and $1 + (k-1)(\lambda-1)/(r-1) = \lambda$.

The *Bruck-Ryser-Chowla theorem* gives necessary conditions for the existence of symmetric designs with given parameter sets (v, k, λ) satisfying $(v - 1)\lambda = k(k - 1)$.

(1.8) **Theorem.** *Suppose there exists a symmetric* $2 - (v, k, \lambda)$ *design. Put* $n = k - \lambda$. *Then (i) if* v *is even then* n *is a square; (ii) if* v *is odd, then the equation*

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

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

The incidence equation $M^TM = nI + \lambda J$ shows that the matrices I and $nI + \lambda J$ are rationally cogredient; (1.8) can then be verified by applying the Hasse-Minkowski theorem to them, though more elementary proofs are available. The Hasse-Minkowski theorem guarantees the existence of a rational matrix M satisfying the incidence equation whenever the conditions of (1. 8) are satisfied; but this does not mean that a design exists, and indeed it is not known whether these conditions are sufficient for the existence of a design. We shall have more to say about the case $(v, k, \lambda) = (111, 11, 1)$ in chapter 11.

A Hadamard matrix is an $n \times n$ matrix H with entries ±1 satisfying $HH^T = H^TH = nI$. (It is so called because its determinant attains a bound due to Hadamard.) Changing the signs of rows and columns leaves the defining property unaltered, so we may assume that all entries in the first row and column are +1. If we then delete this row and column and replace -1 by 0 throughout, we obtain a matrix M which (if $n > 4$) is the incidence matrix of a symmetric $2 - (n-1, \frac{1}{2}n-1, \frac{1}{4}n-1)$ design. Such a design is called a Hadamard 2-design. From a design with these parameters, we can recover a Hadamard matrix by reversing the construction. However, a Hadamard matrix can be modified by permuting rows and columns, so from 'equivalent' Hadamard matrices it is possible to obtain different Hadamard 2-designs.

Let H be a Hadamard matrix with $n > 4$, in which every entry in the first row is +1. Any row other than the first has $\frac{1}{2}n$ entries +1 and $\frac{1}{2}n$ entries -1, thus determining two sets of $\frac{1}{2}n$ columns. (This partition is unaffected by changing the sign of the row.) If we take columns as points, and the sets determined in this way as blocks, we obtain a $3 - (n, \frac{1}{2}n, \frac{1}{4}n-1)$ design called a Hadamard 3-design. Any design with these parameters arises from a Hadamard matrix in this way.

It should be pointed out that Hadamard matrices are very plentiful. Examples are known for many orders n divisible by 4 (the smallest unsettled case at present is $n = 188$), and for moderately small n there are many inequivalent matrices.

A projective geometry over a (skew) field F is, loosely speaking, the collection of subspaces of a vector space of finite rank over F. The points of the geometry are the subspaces of rank 1. A projective geometry is often regarded as a lattice, in which points are atoms and every element is a join of atoms. We shall identify a subspace with the set of points it contains, regarded as a subset of the point set. The *dimension* of a subspace is one less than its vector-space rank (so points have dimension 0); the *dimension* of the geometry is that of the whole space. *Lines* and *planes* are subspaces of dimension 1 and 2 respectively; *hyperplanes* are subspaces of codimension 1. Thus, familiar geometric statements hold: two points lie in a unique line, a non-incident point-line pair lies in a unique plane, etc.

If F is finite, the subspaces of given positive dimension are the blocks of a 2-design. The hyperplanes form a symmetric 2-design, which we shall denote by $PG(m, q)$, where m is the dimension and $q = |F|$; its parameters are $((q^{m+1} - 1)/(q - 1), (q^m - 1)/(q - 1), (q^{m-1} - 1)/(q-1))$. These facts can be verified by counting arguments, or by using the transitivity properties of the general linear group. Note that $PG(m, 2)$ is a Hadamard 2-design for all $m \geq 2$.

A projective plane is a symmetric 2-design with $\lambda = 1$. This agrees with the previous terminology, in that $PG(2, q)$ is a projective plane; by analogy, the blocks of a projective plane are called lines. We will modify our notation and use $PG(2, q)$ to represent any projective plane with $k = q + 1$; q is not even restricted to be a prime power (though it is in all known examples). Thus $PG(2, q)$ may denote several different designs; however, the symbol $PG(m, q)$ is unambiguous for $m > 2$. This is motivated by various characterisations; we mention one due to Veblen and Young [69]:

(1.9) **Theorem.** *A collection of subsets (called 'lines') of a finite set of points is the set of lines of a projective geometry or projective plane if the following conditions hold:*

(i) *any line contains at least three points, and no line contains every point*;

(ii) *any two points lie on a unique line*;

(iii) *any three non-collinear points lie in a subset which, together with the lines it contains, forms a projective plane.*

Projective planes can be axiomatised in a way which permits the extension of the definition (and of (1.9)) to infinite planes; the requirements are that any two points lie on a unique line, any two lines have a unique common point, and there exist four points of which no three are collinear. Projective planes over fields are called Desarguesian, since they are characterised by the theorem of Desargues.

An affine (or Euclidean) geometry of dimension m is the collection of cosets of subspaces of a vector space of rank m over a field F. Here, the geometric dimension of a coset is equal to the vector-space dimension of the underlying subspace; points are just vectors (or cosets of the zero subspace). Again, we identify a subspace with the set of points it contains. If F is finite, the subspaces of given positive dimension form a 2-design. If $|F| = 2$, then any line has two points (and any set of two points is a line), while the subspaces of given dimension $d > 1$ form a 3-design. We denote the design of points and hyperplanes by $AG(m, q)$, where $q = |F|$. $AG(m, 2)$ is a Hadamard 3-design.

An affine plane $AG(2, q)$ can be defined to be a $2 - (q^2, q, 1)$ design. (It is also possible to give an axiomatic definition of an affine plane, in terms of the concept of 'parallelism'.) Again our notation is ambiguous. The exact analogue of the Veblen-Young theorem has been proved by Buekenhout [15] under the restriction that each line has at least four points; Hall [33] has given a counterexample with three points on any line. Again, affine planes over fields are characterised by Desargues' theorem.

Finally, we note that an affine geometry can be obtained from the corresponding projective geometry by deleting a hyperplane (the 'hyperplane at infinity') together with all of its subspaces, while the projective geometry can be recovered from the affine geometry. The same is true for projective and affine planes.

We shall consider briefly in chapter 4 the affine symplectic geometry of dimension 4 over $GF(2)$. Here the vector space carries a symplectic bilinear form, and the blocks of the design are the cosets of those subspaces of rank 2 which are totally isotropic with respect to the form.

Given a t-design $\mathfrak{D}$, the derived design $\mathfrak{D}_p$ with respect to a point p is the $(t-1)$-design whose points are the points of $\mathfrak{D}$ different from p, and whose blocks are the sets $B - \{p\}$ for each block B of

CAMBRIDGE

Cambridge University Press
978-0-521-20742-3 - Graph Theory Coding Theory and Block Designs
P.J. Cameron and J.H. Van Lint
Excerpt
More information

$\mathfrak{D}$ which contains p. The *residual design* $\mathfrak{D}^p$ with respect to p has the same point set as $\mathfrak{D}_p$, but its blocks are the blocks of $\mathfrak{D}$ not containing p; it is also a (t-1)-design.

A converse question, which is very important in design theory and permutation groups, is that of *extendability*:

given a t-design, is it isomorphic to $\mathfrak{D}_p$ for some (t+1)-design $\mathfrak{D}$? $\mathfrak{D}$ is called an *extension* of the given design. An extension may not exist, or there may be more than one. (To construct the extension, we must find a suitable design $\mathfrak{D}^p$.) By applying (1.2) to the extension, we obtain a simple necessary condition for extendability:

(1.10) **Proposition.** *If a* t - (v, k, λ) *design with* b *blocks is extendable, then* k + 1 *divides* b(v + 1).

The 2-design PG(2, q) has $v = q^2 + q + 1 = b$, $k = q + 1$. Applying (1.10), we obtain a result of Hughes [39]:

(1.11) **Theorem.** *If* PG(2, q) *is extendable, then* q = 2, 4, *or* 10.

Much effort has been devoted to these projective planes and their extensions. Further application of (1.10) shows that PG(2, 2) and PG(2, 10) can be extended at most once, and PG(2, 4) at most three times. In fact, PG(2, 2) is unique, and has a unique extension, namely AG(3, 2). PG(2, 4) is also unique, and can be extended three times, each successive extension being unique (up to isomorphism). The existence of PG(2, 10) is still undecided (we will discuss this further in chapter 11) and its extendability appears rather remote at present.

Hughes showed further that there are only finitely many extendable symmetric 2 - (v, k, λ) designs with any given value of λ. The strongest result in this direction is due to Cameron [17]. We will use it (and indicate the proof) in chapter 4.

(1.12) **Theorem.** *If a symmetric* 2 - (v, k, λ) *design* $\mathfrak{D}$ *is extendable, then one of the following occurs:*

(i) $\mathfrak{D}$ *is a Hadamard* 2-*design;*

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

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

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

Regarding case (i) of this result, a Hadamard 2-design is uniquely extendable. For it is not hard to show that, in a Hadamard 3-design, the complement of a block is a block; then the unique extension of the Hadamard 2-design $\mathfrak{D}$ is obtained by adding the 'extra point' to each block of $\mathfrak{D}$ and then defining the complement of each such block to be also a block in the extension. Apart from Hadamard designs, the only known extendable symmetric 2-design is PG(2, 4) (case (ii) with $\lambda = 1$); it is also the only twice-extendable symmetric 2-design.

For affine planes, the situation is a little different, since the necessary condition (1.10) is always satisfied. An extension of an affine plane (that is, a $3 - (q^2 + 1, q + 1, 1)$ design) is called an <u>inversive plane</u> or <u>Möbius plane</u>. Many examples are known; the affine planes over finite fields are all extendable, sometimes in more than one way. However, Dembowski [22], [23] has shown that an inversive plane with even q can be embedded in PG(3, q) in a natural way (so q is a power of 2). Using this and a further embedding technique in conjunction with (1.10), Kantor [42] showed that if AG(2, q) is twice extendable (with $q > 2$), then $q = 3$ or 13. In fact, AG(2, 3) is three times extendable; the extensions are 'embedded' in the corresponding extensions of PG(2, 4), as well as in the projective geometries over GF(3). It is not known whether any AG(2, 13) is twice extendable.

The extensions of PG(2, 4) and AG(2, 3) are so important that we shall give a brief outline of their construction. See also Witt [73], [74], Lüneberg [46], Todd [68], Jónsson [41], etc.

Starting from PG(2, 4), the $5 - (24, 8, 1)$ design is constructed by adding three points p, q, r; the blocks containing all three of these points are the sets $\{p, q, r\} \cup L$, where L is a line of PG(2, 4). We must specify the blocks which do not contain all three of these points, as subsets of PG(2, 4). They turn out to be natural geometric objects: hyperovals, subplanes PG(2, 2), and symmetric differences of pairs of lines. Indeed, these are the only possible candidates; in this way the uniqueness of the designs can be shown. (Important for this is the fact, proved by simple counting, that two blocks of a $5 - (24, 8, 1)$ design

Cambridge University Press
978-0-521-20742-3 - Graph Theory Coding Theory and Block Designs
P.J. Cameron and J.H. Van Lint
Excerpt
More information

have 0, 2 or 4 common points.) Also, if U is a unital in PG(2, 4) (the set of absolute points of a polarity of unitary type), then $\{p, q, r\} \cup U$ is the point set of a 5 - (12, 6, 1) design. Alternatively, the latter design can be obtained by extending AG(2, 3) three times, identifying the added blocks with geometric objects in the plane as before.

Another construction for the 5 - (12, 6, 1) design uses the fact that the symmetric group S_6 has an outer automorphism. Taking two sets of six elements on which S_6 acts in the two possible ways, the blocks of the 5 - (12, 6, 1) design can be defined in terms of the permutations. This method also gives a uniqueness proof. The process can be continued: the automorphism group M_{12} of the design itself has an outer automorphism, and a similar construction produces the 5 - (24, 8, 1) design.

It is possible to construct the 5-fold transitive Mathieu groups M_{12} and M_{24} directly, and to deduce properties of the designs from them.

The techniques of coding theory can be used to construct the design in a purely algebraic way. We shall describe this in chapters 11 and 12.

In higher dimensions, the situation is simpler. PG(m, 2) (with $m > 2$) has an extension only if $q = 2$, when the Hadamard 3-design AG(m + 1, 2) is the unique extension; AG(m, q) is not extendable for $m > 2$.

For further reading, see Dembowski [24], chapter 2 for designs, section 1.4 for projective and affine geometries, chapters 3-5 for projective planes, and chapter 6 for inversive planes. Block designs are also discussed in the books by Hall [33] and Ryser [56].