Square 2-designs

Square 2-designs are variously known as symmetric designs, symmetric BIBDs, and projective designs. The definition does not imply any symmetry of the design, and the term ‘projective designs’, chosen by Dembowski by analogy with ‘affine designs’, has not caught on. We call these designs square because their incidence matrices are.

1 Definition

Suppose that v,k,λ are positive integers with $v > k > \lambda > 0$. A *square* 2-(v,k,λ) *design* is a block design satisfying

(A) There are v points.

(A′) There are v blocks.

(B) Any block is incident with k points.

(B′) Any point is incident with k blocks.

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

(C′) Any two points are incident with λ blocks.

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

Of course these conditions are not all independent. If (A), (B) and (C′) hold, then we have a 2-design (a BIBD), and the number of blocks is $v(v-1)\lambda/k(k-1)$. So, if (D) also holds, then the number of blocks is also equal to v, and so (A′) holds (and indeed, all the remaining conditions do).

In this context, note that *Fisher’s Inequality* shows that a 2-design has at least as many blocks as points, and that equality implies that any two blocks meet in a constant number of points. Also, if (C) and (C′) both hold, then the dual is also a 2-design, and so Fisher’s inequality and its dual imply that the numbers of points and blocks are equal. So (A), (B), (C′) and any one of the other conditions imply all the rest.

Another characterisation is as follows.

Proposition 1 *Suppose that an incidence structure D has more than one point and more than one block. Suppose that any two points are incident with λ blocks, and any two blocks with λ' points. Then $\lambda = \lambda'$, and one of the following occurs:*

(a) D is a square 2*-design;*

(b) $\lambda > 1$*, and D has* λ *points and* λ *blocks, any point and block being incident;*

(c) $\lambda = 1$*, and D has one block incident with every point, any other block being incident with just one point, and dually;*

(d) $\lambda = 1$*, and D has one block incident with every point except one, any other block being incident with just two points, and dually.*

2 Properties

The *adjacency matrix* of a square 2-design is the $v \times v$ matrix with rows indexed by blocks and columns by points, the (b,x) entry being 1 if x is incident with b and 0 otherwise. It satisfies

$$\begin{aligned} AJ = JA &= kJ, \\ AA^\top = A^\top A &= (k-\lambda)I + \lambda J, \end{aligned}$$

where I and J are the identity and all-1 matrices of size $v \times v$.

It follows from these equations that A is invertible; its determinant is $\pm v(k-\lambda)^{(v-1)/2}$.

A square 2-design with $\lambda = 1$ is called a *projective plane*. The integer $n = k-1$ is its *order*. The parameters of a projective plane of order n are given by $v = n^2+n+1$, $k = n+1$. The blocks of a projective plane are often called *lines*; two points lie on a unique line and two lines meet in a unique point.

The *dual* of a square 2-design (obtained by interchanging the labels 'point' and 'block') is again a square 2-design with the same parameters. This holds because the duals of (A)–(C) above are (A′)–(C′). Its incidence matrix is the transpose of that of the original design.

The *complement* of a square 2-design is the design on the same point set whose blocks are the complements of the blocks of the original design. In other words, we interchange 'incidence' and 'non-incidence' between points and blocks. An inclusion-exclusion argument shows that the complement of a square 2-(v,k,λ)

design is a square 2-$(v, v-k, v-2k+\lambda)$. If the original design has incidence matrix A, then the incidence matrix of the complement is $J-A$. (Actually this is not quite true. The sets containing all but one point are the blocks of a square 2-$(v, v-1, v-2)$ design. The complement is formally a 2-$(v, 1, 0)$ design, but this does not satisfy our requirement that $\lambda > 0$. These are the only exceptions.)

3 Existence and non-existence

The parameters (v, k, λ) of a square 2-design satisfy equation (D) above:

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

Not every parameter triple with $v > k > \lambda > 0$ is realised by a square 2-design. The *Bruck–Ryser–Chowla Theorem* gives a further necessary condition:

Proposition 2 *Suppose that a square* 2-(v, k, λ) *design exists.*

(a) If v is even, then $k-\lambda$ is a square.

(b) If v is odd, then the equation

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

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

See, for example, [4] for a proof.

A consequence of this theorem is that, if the order n of a projective plane is congruent to 1 or 2 mod 4, then n is the sum of two integer squares. So there is no projective plane of order 6.

Equation (D) and the Bruck–Ryser–Chowla Theorem are not sufficient for the existence of a design. However, only a single instance (up to complementation) is known of a parameter set satisfying the BRC Theorem for which no design exists. This is the result of a massive computation by Lam *et al.*, which showed the following:

Proposition 3 *There is no projective plane of order* 10.

There are many constructions of square 2-designs. What follows is by no means a complete survey, but mentions some of the most important types.

Projective spaces. The projective space $\mathrm{PG}(n,q)$ is constructed from an $(n+1)$-dimensional vector space V over the finite field $\mathrm{GF}(q)$, where q is a prime power. The objects or varieties of the projective space are all the subspaces of V apart from $\{0\}$ and V; two subspaces are incident if one contains the other. A *point* is a 1-dimensional subspace, and a *hyperplane* is a subspace of codimension 1. Now the points and hyperplanes form a square 2-$(q^{n+1}-1)/(q-1),(q^n-1)/(q-1),(q^{n-1}-1)/(q-1)$ design. In particular, if $n=2$, this design is a projective plane of order q.

Difference sets. Let G be a group of order v, and D a subset of G of cardinality k. D is called a (v,k,λ) *difference set* if, for every son-zero element $g \in G$, the number of pairs $x,y \in D$ with $yx^{-1} = g$ is equal to λ. The name arises because, if the group is Abelian and written additively, the condition refers to pairs x,y with $y-x = g$: the differences of distinct elements in D cover the non-zero elements of G uniformly.

If D is a (v,k,λ) difference set, then the subsets of G of the form $Da = \{xa : x \in D\}$ are the blocks of a square 2-(v,k,λ) design on the point set G. This design is obtained by *developing D*. Conversely, any square design admitting an automorphism group acting transitively can be constructed by developing a difference set.

See Lander [6] for more on difference sets. Examples of difference set designs include:

Paley designs: if q is a prime power congruent to 3 mod 4, then the non-zero squares in $\mathrm{GF}(q)$ form a $(q,(q-1)/2,(q-3)/4)$ difference set. The corresponding design is the *Paley design* $P(q)$.

Symplectic designs: if Q is a non-singular quadratic form in $2n$ variables over $\mathrm{GF}(2)$, then the set $\{v : Q(v) = 1\}$ is a $(2^{2n}, 2^{2n-1} \pm 2^{n-1}, 2^{2n-2} \pm 2^{n-1})$ difference set in the additive group of the $2n$-dimensional vector space. The sign depends on the quadratic form chosen, but all quadratic forms for given n produce isomorphic or complementary designs. The design with block size $2^{2n-1} + \varepsilon 2^{n-1}$ is denoted by $S^{\varepsilon}(2n)$.

Hadamard designs. A *Hadamard matrix* is an $n \times n$ matrix H with entries ± 1 satisfying $HH^{\top} = nI$. If such a matrix exists with $n > 2$, then n must be a multiple of 4; it is conjectured that Hadamard matrices of all orders divisible by 4 exist.

There are many constructions for such matrices. The simplest is recursive: if H_1 and H_2 are Hadamard matrices, then so is their *Kronecker product* $H_1 \otimes H_2$. The Kronecker product of n copies of the Hadamard matrix $\begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$ is said to be of *Sylvester type*.

Given a Hadamard matrix of order $n = 4m$, we can change signs of rows and columns without affecting the Hadamard property. So we can *normalise* the matrix so that all entries so that the first row and column consist of $+1$s. If we now delete the first row and column, and replace -1 by 0 throughout the remaining matrix, we obtain the incidence matrix of a square 2-$(4m-1, 2m-1, m-1)$ design, called a *Hadamard* 2-*design*. Any design with these parameters arises in this way: we go back by replacing 0 by -1 and bordering with $+1$s.

If instead, we merely normalise the first row to consist of $+1$s and delete it, and take blocks $B_i^{\varepsilon} = \{j : H_{ji} = \varepsilon\}$ for $j = 2, \ldots, 4m$ and $\varepsilon = \pm 1$, we obtain a 3-$(4m, 2m, m-1)$ design called a *Hadamard* 3-*design*. It is an extension of the Hadamard 2-design just discussed (see later).

The designs $\mathrm{PG}(n, 2)$ and $P(q)$ are Hadamard 2-designs. They are isomorphic for $n = 2$, $q = 7$, but not in any other case. The projective space comes from a Hadamard matrix of Sylvester type.

4 Automorphisms

An automorphism of a square 2-design can be defined to be a permutation of the point set which maps any block to a block. Thus, an automorphism induces a permutation on the block set; there is no ambiguity, as the block permutation is uniquely determined by the point permutation (since there are no repeated blocks).

There is a close relation between the point and block permutations: *they have the same cycle structure* (the same number of cycles of each length).

To prove this, one shows first that the numbers of fixed points and blocks are equal. The simplest proof involves counting triples (x, xg, b), where $x, x^g \in b$: this is the same as the number of triples (x, b, bg^{-1}), where $x \in b, bg^{-1}$. Now apply this to powers of g, observing that knowledge of the number of fixed points of g^n for all n determines the cycle structure of g.

The simplest case of this result is an automorphism with a single cycle on points (and also on blocks). If we have such an automorphism, then we can index the points by integers mod v: fix a basepoint x_0 indexed by 0, and let $x_0 g^i$ be indexed by i mod v. Now if b is a block, then the set of indices of the points in b

is a (v,k,λ) difference set in the cyclic group of order v. Conversely, the design obtained by developing a difference set mod v admits a cyclic automorphism.

A consequence of the equality of fixed point and block numbers of an automorphism is that any group of automorphisms has equally many orbits on the point and block sets; moreover, it is 2-transitive on points if and only if it is 2-transitive on blocks. Using results about finite permutation groups, it is known that (up to complementation) there are just two infinite families and two sporadic examples of square 2-designs admitting 2-transitive groups:

- the point-hyperplane design of a projective space $\mathrm{PG}(n,q)$, where $n \geq 2$ and q is a prime power, with $v = (q^{n+1}-1)/(q-1)$, $k = (q^n-1)/(q-1)$, $\lambda = (q^{n-1}-1)/(q-1)$;

- a symplectic design $S^{\varepsilon}(2n)$, with $v = 2^{2n}$, $k = 2^{2n-1} + \varepsilon 2^{n-1}$, $\lambda = 2^{2n-2} + \varepsilon 2^{n-1}$;

- The Paley design $P(11)$, with $v = 11$, $k = 5$, $\lambda = 2$;

- A design with $v = 176$, $k = 50$, $\lambda = 14$, associated with the Higman–Sims simple group.

The detailed theory of automorphisms is best developed in the case of projective planes ($\lambda = 1$). One of the reasons for this is the following. Let g be an automorphism of prime order $p > \lambda$. Then any two fixed points of g are incident with λ fixed blocks, and any two fixed blocks with λ fixed points. By Proposition 1, for $\lambda > 1$ this implies that the fixed points and blocks form a square 2-(v',k',λ) design (possibly degenerate, that is, with $v' = k' = \lambda$). For $\lambda = 1$, there are other possibilities: all, or all but one, of the points lie on a single block.

Involutions (automorphisms of order 2) of a projective plane have the further property that every non-fixed point x lies on a fixed block (the unique block containing x andxg), and dually. Thus the structure of the fixed points and lines is restricted to one of the following:

- all the points on a line b, and all the lines through a point x;

- a *Baer subplane*, whose order is the square root of that of the whole plane.

In the first case, the involution is called an *elation* or a *homology* according as x is on b or not. In the second, it is a *Baer involution*.

5 Extensions

An *extension* of a t-design D is a $(t+1)$-design E with a point p such that $E_x \cong D$. (Here, if E has point set X and block set B, the *derived design* E_x has point set $X \setminus \{x\}$ and block set $\{b \setminus \{x\} : x \in b \in B\}$. Regarding E as an incidence structure, E_x denotes its restriction to the points different from x and the blocks incident with x.)

Which square 2-designs have extensions? Said otherwise, which 3-designs E have the property that E_x is a square 2-design for some point x? (If this holds for some point, then it holds for all, since the parameters of E_x are independent of the chosen point x.)

Hughes [3] first investigated this question for projective planes and showed that an extendable projective plane has order 2, 4 or 10. This is proved by a simple counting argument to show that the number of blocks in this extension is $(n^2+n+2)(n^2+n+1)/(n+2)$, and observing that this quantity is an integer if and only if $n+2$ divides 12, leading to the stated values.

Suppose that E is an extension of a projective plane D of order n. Any block of E has $n+2$ points, and any two blocks meet in 0 or 2 points. So, if $E_x = D$, then a block not containing x is a hyperoval in D. Now the unique plane of order 2 has 7 hyperovals, exactly the number required for an extension; and indeed it has a unique extension (a 3-$(8,4,1)$ design). The unique plane of order 4 has 168 hyperovals, three times the number required for an extension; and indeed it can be extended three times (to a 5-$(24,8,1)$ design). Proposition 3 shows the non-existence of a plane of order 10; but by a relatively early stage in the computation of Lam *et al.*, it was known that such a plane can contain no hyperoval (and so cannot be extendable).

In general we have the following result, which (apart from the non-existence of an extension of a plane of order 10) is due to Cameron [1].

Proposition 4 *Let E be a* 3-(v,k,λ) *design which is an extension of a square* 2-*design. Then one of the following occurs:*

(a) E is a Hadamard 3-*design (that is,* $v = 4(\lambda+1)$ *and* $k = 2(\lambda+1)$*);*

(b) $v = (\lambda+1)(\lambda^2+5\lambda+5)$, $k = (\lambda+1)(\lambda+2)$*;*

(c) $v = 496$, $k = 40$, $\lambda = 3$.

In case (a), it is known that any Hadamard 2-design has a unique extension to a Hadamard 3-design. The recipe is simple: if D is a Hadamard 2-design with point set X and block set B, and ∞ is a point not in X, then the extension has point set $X \cup \{\infty\}$ and block set $\{b \cup \infty, X \setminus b : b \in B\}$. Alternatively, go via the Hadamard matrix as described earlier.

In case (b), for $\lambda = 1$, the square design D is the projective plane of order 4, which (as noted above) is three times extendable. For $\lambda = 2$, D is a 2-$(56, 11, 2)$ design. Five non-isomorphic designs with these parameters are known; none is known to be extendable, and at least some are known not to be, but the question is not resolved. For larger values of λ, and in case (c), nothing is known.

6 Related designs

6.1 Affine designs

Fisher's inequality asserts that in any 2-design (BIBD), the number of blocks is at least as great as the number of points; equality holds if and only if any two blocks intersect in a constant number of points (in which case the design is square).

A design is *resolvable* if its blocks can be partitioned into *parallel classes* each of which partitions the points. Clearly a resolvable 2-design cannot be square, so the number of blocks exceeds the number of points. Bose showed that, in fact, a resolvable 2-design satisfies

$$b \geq v + r - 1,$$

where b is the number of blocks, v the number of points, and r the number of parallel classes (the number of blocks containing a point).

This bound is attained if and only if the intersection of any two non-parallel blocks has constant cardinality. Such a design is called *affine*. Examples include the point-hyperplane designs of affine spaces over finite fields.

6.2 Quasi-symmetric 2-designs

As noted earlier, a 2-design is square if any two blocks intersect in a constant number of points, that is, if its dual is a 2-design. A 2-design is said to be *quasi-symmetric* if the cardinality of the intersection of two blocks takes just two distinct values.

The main result about such designs is a doe to Goethals and Seidel: the dual of a quasi-symmetric 2-design is partially balanced with respect to a 2-class association scheme. In other words, if we define two relations on the blocks by the cardinality of their intersections, we obtain a 2-class association scheme.

For example, any affine design is quasi-symmetric; its dual is group-divisible (the ‘groups’ being the parallel classes).

For much more about quasi-symmetric designs, see the book by Shrikhande and Sane [7].

6.3 Linked square designs

Suppose we have more than two sets, say $X_1,\ldots,X_m$, with an incidence relation between each pair (X_i,X_j) forming a square 2-design. Both mathematical and statistical considerations suggest that we should impose a further condition ‘linking’ any three of the sets. However, various inequivalent forms of the linking condition have been proposed. Let A_{ij} denote the incidence matrix of the relation between X_i and X_j, where rows are indexed by X_i and columns by X_j. Three conditions which have been proposed, in order of decreasing strength, are:

(a) $A_{ij}A_{jk} = xA_{ik} + yJ$;

(b) $A_{ij}A_{jk}A_{ki} = xI + yJ$;

(c) $A_{ij}A_{jk}A_{ki} + A_{ik}A_{kj}A_{ji} = xI + yJ$.

Here J denotes the all-1 matrix. The conditions are required to hold for all distinct indices i, j, k. The parameters x, y may depend on the indices i, j, k, and are not the same in the three conditions.

Condition (a) guarantees that the structure on the union of the sets is a coherent configuration. It was first introduced to study 2-transitive permutation groups. Examples (in which the square 2-designs are all symplectic) can be constructed from quadratic forms over $\mathrm{GF}(2)$.

Condition (c) has been considered by Preece. It is the most natural from a statistical point of view.

6.4 Youden “squares”

It follows from Hall’s marriage theorem that the edge set of any regular bipartite graph can be partitioned into 1-factors. Applying this to the incidence graph of a square 2-(v,k,λ) design gives a structure known as a *Youden ‘square’*. Each entry 1 in the incidence matrix of the design is replaced by one of the symbols $1,2,\ldots,k$, and the zeros by blanks, in such a way that each symbol occurs once in each row and once in each column. (The symbols index the 1-factors).

Another, more commonly used, representation, is as a $k \times v$ rectangle containing the symbols $1, \ldots, v$ and forming a Latin rectangle, such that the symbols contained in each column form a block of the design.

From the point of view of experimental design, we have a set of plots with treatment and block partitions forming a square 2-design (that is, each balanced with respect to the other), and one further partition orthogonal to both the treatment and block partitions.

As noted, Hall's theorem guarantees that any square design with constant block size and constant replication number can be 'Youdenised'. Sometimes, systems of linked designs can be 'Youdenised' as well: see Cameron [2].

References

[1] P. J. Cameron, Extending symmetric designs, *J. Combinatorial Theory* (A) **14** (1973), 215-220.

[2] P. J. Cameron, Multi-letter Youden rectangles, *Discrete Math.*, in press.

[3] D. R. Hughes, On *t*-designs and groups, *Amer. J. Math.* **87** (1965), 761–778.

[4] D. R. Hughes and F. C. Piper, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[5] C. W. H. Lam, S. Swiercz and L. Thiel, The nonexistence of finite projective planes of order 10, *Canad. J. Math.* **41** (1989), 1117–1123.

[6] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, London Math. Soc Lecture Note Series **74**, Cambridge Univ. Press, Cambridge, 1983.

[7] M. S. Shrikhande and S. S. Sane, *Quasi-Symmetric Designs*, London Math. Soc Lecture Note Series **164**, Cambridge Univ. Press, Cambridge, 1991.

Peter J. Cameron
May 30, 2003