1. Design theory

In this chapter, we describe some concepts and results from design theory, and construct some important designs.

(1.1) DEFINITION. A *t-design* with parameters (v, k, λ) (or a t-(v, k, λ) design) is a pair $\mathcal{D} = (X, \mathcal{B})$, where X is a set of 'points' of cardinality v, and $\mathcal{B}$ a collection of k-element subsets of X called 'blocks', with the property that any t points are contained in precisely λ blocks.

Various conditions are usually appended to the definition to exclude degenerate cases. We assume that X and $\mathcal{B}$ are non-empty, and that $v \geq k \geq t$ (so that $\lambda > 0$). A t-design with $\lambda = 1$ is called a *Steiner system*. (The notation $S(t, k, v)$ is also used for Steiner systems, and is sometimes extended to $S_\lambda(t, k, v)$ for arbitrary designs.) Alternatively, a t-design can be defined to consist of a set X of points and a set $\mathcal{B}$ of blocks, with a relation of 'incidence' between points and blocks, satisfying the appropriate conditions, including the assertion that k distinct points are incident with at most one block.

Sometimes a t-design is redefined so as to allow 'repeated blocks', that is, $\mathcal{B}$ is a family rather than a set of sets, and the same k-element set of points may occur more than once as a block. (This is more natural if we adopt the 'incidence relation' definition; simply omit the condition that k points are incident with at most one block.) In this book, we normally do not allow repeated blocks; where they are permitted, we will say so. Following Hughes and Piper (1985), we often use the term *t-structure* to signify that repeated blocks are permitted.

It is worth a short digression to explain the force of the 'no repeated blocks' assumption.

The question of the existence of designs with specified parameters has very different answers depending on whether we allow repeated blocks or not. If $\mathcal{B}$ is the set of all k-subsets of X, then $(X, \mathcal{B})$ is trivially a t-design for any $t \leq k$. If repeated blocks are permitted, we have the following easy result.

(1.2) Proposition. *Suppose that $t < k < v - t$. Then there is a t-(v, k, λ) structure for some λ, in which not every k-set of points is incident with a block.*

PROOF. Let M be the $\binom{v}{k} \times \binom{v}{t}$ matrix whose rows and columns are indexed by the k-subsets and t-subsets of X respectively, in which the entry indexed by (K, T) is 1 if $T \subset K$, 0 otherwise. By hypothesis, $\binom{v}{t} < \binom{v}{k}$; so the rows of M are linearly dependent over $\mathbf{Q}$. So there is a vector $\mathbf{v} \in \mathbf{Q}^{\binom{v}{k}}$ such that $\mathbf{v}M = \mathbf{0}$. By multiplying by the least common multiple of the denominators of the entries of $\mathbf{v}$, we may assume that these entries are integers. Let $-m$ be the smallest entry of $\mathbf{v}$. If $\mathbf{1}$ denotes the all-1 vector, then $\mathbf{w} = \mathbf{v} + m\mathbf{1}$ is a non-negative integer vector with at least one component 0; and

$$\mathbf{w}M = (\mathbf{v} + m\mathbf{1})M = m\mathbf{1}M = m\binom{v-t}{k-t}\mathbf{1}.$$

The interpretation of this matrix equation is that, if $\mathcal{B}$ is the family of k-subsets of X in which the set K is repeated $\mathbf{w}_K$ times, then any t-set lies in $\lambda = m\binom{v-t}{k-t}$ members of $\mathcal{B}$ (counted with multiplicity). So $(X, \mathcal{B})$ is the required structure. □

It is possible to place some conditions on the value of λ as well: see Wilson (1973).

The situation is quite different, however, if repeated blocks are forbidden. The t-design condition becomes stronger as t increases (see (1.5)). A couple of 5-designs have been known for most of this century; but, at the time the previous version of this book was written, no non-trivial 6-design was known. Since then, first Magliveras and Leavitt (1983), and later others, found some particular 6-designs; then Teirlinck (1987), (1989) spectacularly resolved the existence question by proving the following result.

(1.3) Theorem. *Given t, let*

$$\mu = \prod_{i=1}^{t} \left(\operatorname{lcm}\left\{ \binom{i}{n} : n = 1, \ldots, i \right\} \cdot \operatorname{lcm}\{1, \ldots, i+1\} \right).$$

Then, for any $v \equiv t \pmod{\mu}$, the set of all $(t+1)$-subsets of a v-set X can be partitioned into t-$(v, t+1, \mu)$ designs. In particular, a non-trivial t-$(v, t+1, \lambda)$ design exists whenever $v \equiv t \pmod{\mu}$, $\lambda \equiv 0 \pmod{\mu}$, and $v > \lambda + t$. □

However, necessary and sufficient conditions for the existence of t-designs are far from being known, even asymptotically. In particular, there are still no known examples of Steiner systems with $t \geq 6$, and only finitely many with $t \geq 4$. There are 'classical' 5-(24, 8, 1) and 5-(12, 6, 1) designs constructed by Skolem (1931), Witt (1938a,b); the other known Steiner systems with $t = 5$ can all be found in Denniston (1976) and Mills (1978). The existence of Steiner systems with large t is possibly the most important open problem in design theory.

An *isomorphism* from $(X, \mathcal{B})$ to $(X', \mathcal{B}')$ is a one-to-one map f from X to X' which carries each set in $\mathcal{B}$ to a set in $\mathcal{B}'$, and such that each set in $\mathcal{B}'$ occurs as the image of a unique set in $\mathcal{B}$. Isomorphic designs may be regarded as being structurally 'the same'. We will encounter some very nice situations in which a design $\mathcal{D}$ is 'characterized' by its parameters, in the sense that any design with the same parameters is isomorphic to $\mathcal{D}$.

(If repeated blocks are allowed, this definition of isomorphism would not suffice; we should have to define an isomorphism to be a pair of bijections, from X to X' and from $\mathcal{B}$ to $\mathcal{B}'$, preserving incidence and non-incidence. We will ignore this complication.)

The set of *automorphisms* of a design (that is, isomorphisms from the design to itself) forms a group. Moreover, this automorphism group acts in a natural way as a permutation group on the points of the design, or on its blocks. Group theory provides very powerful tools for studying permutation groups (see Wielandt (1964), Cameron (1981), for example). For the most part, we will not consider these, except for occasionally using a group in one of our constructions.

We now derive some simple necessary conditions for the existence of a design.

(1.4) Proposition. *Let $\lambda(S)$ be the number of blocks containing a given set S of s points in a t-(v, k, λ) design, where $0 \le s \le t$. Then*

$$\lambda(S)\binom{k-s}{t-s} = \lambda\binom{v-s}{t-s}.$$

PROOF. Count the number of choices of a block B containing S and $t-s$ further points of B, to obtain the result. □

Note that $\lambda(S)$ depends only on the cardinality s of S; so we will write it as λ_s. It satisfies

$$\lambda_s\binom{k-s}{t-s} = \lambda\binom{v-s}{t-s}. \tag{1.5}$$

From these remarks, two corollaries follow:

(1.6) Corollary. *A t-design is also a s-design for $0 \le s \le t$.* □

(1.7) Corollary. *If a t-(v, k, λ) design exists, then*

$$\binom{k-s}{t-s} \text{ divides } \binom{v-s}{t-s}\lambda,$$

for $s = 0, \ldots, t-1$. □

It is virtually a universal convention in design theory to denote λ_0 (the total number of blocks) by b, and (if $t \geq 1$) to denote λ_1 (the number of blocks containing a point) by r. Since any t-design for $t \geq 1$ can be regarded as a 1-design by (1.4), we can apply (1.5) to obtain:

$$bk = vr. \tag{1.8}$$

A 2-design is often called a *block design* or simply a *design*. In the literature the term 'balanced incomplete-block design' is used, abbreviated to BIBD. (Balance refers to the 2-design condition, and incompleteness to the fact that $k < v$.) An alternative term is 'pairwise balanced design', though such designs need not have constant block size. In a 2-design, we have:

$$r(k-1) = (v-1)\lambda. \tag{1.9}$$

(1.10) DEFINITION. 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 indexed by (B, p) being 1 if $p \in B$, 0 otherwise.

The incidence matrix depends on the ordering chosen for points and blocks. (The reader is warned that a different convention is often used, for example in the books by Dembowski (1968) and Hall (1986), with the result that our incidence matrices are the transposes of the ones appearing in those books. The present convention is adopted because we shall want 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:

$$\begin{aligned} MJ &= kJ, \\ JM &= rJ, \\ M^\top M &= (r-\lambda)I + \lambda J. \end{aligned} \tag{1.11}$$

(Here, as throughout this book, I is an identity matrix, and J a matrix with every entry 1, of the appropriate size.)

(1.12) Lemma. *If I and J are the identity and all-1 matrices of order n, then*

$$\det(xI + yJ) = (x + yn)x^{n-1}.$$

PROOF. $xI + yJ$ is symmetric, and so has an orthonormal basis of eigenvectors; its determinant is the product of its eigenvalues. Now the all-1 vector $\mathbf{1}$ is an eigenvector with eigenvalue $x + yn$. Any other eigenvector $\mathbf{v}$ is orthogonal to $\mathbf{1}$, and so $\mathbf{v}J = \mathbf{0}$, and $\mathbf{v}(xI + yJ) = x\mathbf{v}$. So x is an eigenvalue with multiplicity $n - 1$. □

Suppose that $\lambda > 0$ and $k < v$. By (1.9), $\lambda(v-k) = (r-\lambda)(k-1)$, and so $r - \lambda > 0$. Now by (1.11) and (1.12),

$$\det(M^\top M) = \det\left((r-\lambda)I + \lambda J\right) = rk(r-\lambda)^{v-1}, \tag{1.13}$$

and so $M^\top M$ is non-singular. *Fisher's inequality* follows:

(1.14) Theorem. *In a 2-design with $k < v$, we have $b \geq v$.* □

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

(1.15) Theorem. *In a 2-design with $k < v$, the following conditions are equivalent:*
(a) $b = v$;
(b) $r = k$;
(c) any two blocks have λ common points;
(d) any two blocks have a constant number of common points.

PROOF. We have seen the implications (a) $\Leftrightarrow$ (b) and (b) $\Rightarrow$ (c), while (c) $\Rightarrow$ (d) is trivial.

For the last step, we need the concept of the *dual* of a design $\mathcal{D} = (X, \mathcal{B})$. This is the design $\mathcal{D}^\top = (X^\top, \mathcal{B}^\top)$, where $X^\top = \mathcal{B}$, and $\mathcal{B}^\top = \{\beta_x : x \in X\}$, where

$$\beta_x = \{B \in \mathcal{B} : x \in \mathcal{B}\}.$$

(If we had used the 'incidence relation' definition of a design, we could simply say $\mathcal{B}^\top = X$, and the incidence relation in $\mathcal{D}^\top$ is the converse of that in $\mathcal{D}$.)

The dual of a 1-design is a 1-design, and is a 2-design if and only if (1.15)(d) holds. Thus, if a 2-design satisfies (1.15)(d), then $b \geq v$ (by (1.14)) and $v \geq b$ (applying (1.14) to the dual design); so $b = v$. □

(1.16) REMARK. The notation $\mathcal{D}^\top$ is intended as an *aide-mémoire*, since the incidence matrix of $\mathcal{D}^\top$ is the transpose of that of $\mathcal{D}$.

(1.17 DEFINITION. A 2-design is called *square* if it satisfies the equivalent conditions of (1.15).

This terminology is not standard. Dembowski, in his influential book (1968), used the term 'projective', for reasons which will appear shortly. But the most common term is 'symmetric'. This is unsatisfactory, since it suggests a stronger condition, viz. isomorphism of the design with its dual, which doesn't hold in all square 2-designs. We now explore this concept.

(Note: The term 'square' has been applied to arbitrary designs or incidence structures which have equally many points and blocks.)

(1.18) DEFINITION. A *duality* of a design $\mathcal{D}$ is an isomorphism from $\mathcal{D}$ to its dual. It can be described as a pair of bijections $\sigma : X \to \mathcal{B}$ and $\tau : \mathcal{B} \to X$ such that

$$x \in \mathcal{B} \text{ if and only if } \mathcal{B}^\tau \in x^\sigma.$$

The result of applying the duality twice is the pair of maps $\sigma\tau : X \to X$ and $\tau\sigma : \mathcal{B} \to \mathcal{B}$, which give an automorphism of the design. The duality is called a *polarity* if this automorphism is trivial, that is, τ is the inverse of σ; in this case, the polarity is determined by the single map σ, which satisfies

$$x \in y^\sigma \text{ if and only if } y \in x^\sigma.$$

(1.19) Proposition. *A design admits a polarity if and only if it has a symmetric incidence matrix (relative to some ordering of points and blocks).*

PROOF. If σ is a polarity, and $X = \{x_1, \ldots, x_v\}$, then relative to this ordering of points and the ordering $\{x_1^\sigma, \ldots, x_v^\sigma\}$ for blocks, the incidence matrix is symmetric. The converse is similar. □

We return to polarities in the next chapter.

(1.14) and (1.15) follow from a more general result, which we will need in Chapter 7. It also introduces a very useful technique, the 'variance trick'.

(1.20) Theorem. *Let B be a block of a 2-(v, k, λ) design. Then the number of blocks not disjoint from B is at least $k(r-1)^2/((k-1)(\lambda-1)+(r-1))$. Equality holds if and only if blocks which are not disjoint from B meet it in a constant number of points. If this occurs, then the constant number is $1+(k-1)(\lambda-1)/(r-1)$.*

PROOF. Let d be the number of blocks which are distinct from but not disjoint from B; suppose that n_i of these blocks meet B in i points. Count in two ways the number of choices of j points in B and a block (different from B) containing them, for $j = 0, 1, 2$. We obtain the following equations, where the summation is over i running from 1 to k.

$$\sum n_i = d,$$
$$\sum i n_i = k(r-1),$$
$$\sum i(i-1)n_i = k(k-1)(\lambda-1).$$

So

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

This quadratic form in x must be positive semi-definite, proving the inequality. It vanishes only if $d = k(r-1)^2/((k-1)(\lambda-1)+(r-1))$, in which case $n_i = 0$ for all $i \neq 1+(k-1)(\lambda-1)/(r-1)$. □

Now Fisher's inequality follows from $b-1 \geq k(r-1)^2/((k-1)(\lambda-1)+(r-1))$, using (1.8) and (1.9) and a little calculation. (A hint for the calculation: express everything in terms of the parameters r, k, λ; after clearing the denominator, the difference between these two expressions is $(r-\lambda)^2(r-k)(k-1)$.) Also, if $b = v$, then $r = k$, and $1 + (k-1)(\lambda-1)/(r-1) = k$.

The *Bruck–Ryser–Chowla theorem* gives a further necessary condition on the existence of a square 2-(v, k, λ) design, beyond the equation $k(k-1) = (v-1)\lambda$ which follows from (1.9) and (1.15).

(1.21) Theorem. *Suppose that there exists a square 2-(v, k, λ) design. Set $n = k - \lambda$. Then*
(a) if v is even then k is a square;
(b) if v is odd, then the diophantine equation

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

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

PROOF. (a) is immediate from the fact that

$$\det(M)^2 = \det(M^\top M) = k^2 n^{v-1},$$

see (1.9) and (1.11). We do not offer a proof of (b). Several different proofs are available, of which the most familiar relies on Lagrange's results on sums of squares, and others use Hasse–Minkowski theory or coding theory. We refer to Hughes and Piper (1985). □

It is now known that the condition $k(k-1) = (v-1)\lambda$ and the Bruck–Ryser–Chowla theorem are not sufficient for the existence of a square 2-design. One single parameter set, viz. 2-(111, 11, 1), is known which satisfies these conditions where no design exists. (We have more to say about this case later.) For any given value greater than 1 of λ, only finitely many square 2-(v, k, λ) designs are known to exist.

We now look at a couple of special classes of square designs.

A (finite) *projective plane* of *order* n is a 2-$(n^2+n+1, n+1, 1)$ design. Projective planes are known to exist for all prime power orders, but no plane of non prime power order is known. The most familiar projective planes are the so-called *Desarguesian* planes. These are special cases of *projective geometries*, which we now define.

(1.22) EXAMPLE. Let $\mathsf{F} = \mathbb{F}_q$, and let V be a $(n+1)$-dimensional vector space over F. The *projective space* or *projective geometry* $\mathrm{PG}(n, q)$ consists of the set of all vector subspaces of V. It can be regarded as a partially ordered set (where the ordering is set-theoretic inclusion — it is in fact a lattice with respect to this ordering), or as an 'incidence structure' in which two subspaces are incident whenever one contains the

other. An *i-flat* is a subspace of vector space dimension $i+1$; 0-flats, 1-flats, 2-flats and $(n-1)$-flats are called *points*, *lines*, *planes*, *hyperplanes* respectively.

It is clear that two subspaces are equal if and only if they contain the same points. So we can regard the set of points as basic, and identify any flat with the set of points it contains. The design theorist's interest in this procedure is that, for any fixed i with $1 \leq i \leq n-1$, the points and i-flats form a 2-design. In particular, the points and lines form a Steiner system (a 2-$((q^{n+1}-1)/(q-1), q+1, 1)$ design); while the points and hyperplanes form a square 2-design (which is a 2-$((q^{n+1}-1)/(q-1), (q^n-1)/(q-1), (q^{n-1}-1)/(q-1))$ design). We sometimes use the notation $\mathrm{PG}(n,q)$ to denote the point-hyperplane design.

The intersection of these two cases is the design of points and lines in $\mathrm{PG}(2,q)$, which is a 2-$(q^2+q+1, q+1, 1)$ design, that is, a projective plane of order q.

We now give some characterizations of projective spaces as designs. For undefined terms such as 'Desargues' Theorem', we refer to Hughes and Piper (1973).

(1.23) Theorem. *For a projective plane $\mathcal{D}$, the following conditions are equivalent:*
(a) $\mathcal{D}$ is the point-line design of $\mathrm{PG}(2,q)$ for some prime power q;
(b) $\mathcal{D}$ satisfies Desargues' Theorem;
(c) $\mathcal{D}$ satisfies Pappus' Theorem;
(d) $\mathrm{Aut}(\mathcal{D})$ is 2-transitive on the points of $\mathcal{D}$. □

(The last condition means that any two distinct points can be mapped to any other two distinct points by an automorphism of $\mathcal{D}$.)

(1.24) Theorem. *For a 2-$(v,k,1)$ design $\mathcal{D}$ with $v > k > 2$, which is not a projective plane, the following conditions are equivalent:*
(a) $\mathcal{D}$ is the point-line design of $\mathrm{PG}(n,q)$ for some prime power q and some integer $n \geq 3$;
(b) if a, b, c, d are four points such that the lines ab and cd are concurrent, then the lines ac and bd are concurrent. □

(The *line* ab here means the unique block containing a and b; two lines are *concurrent* if they meet in a point. This result is due to Veblen and Young (1916).)

Point-hyperplane designs of projective geometries may be recognized by the *Dembowski–Wagner theorem* (1960). In any 2-design, the *line* joining two distinct points p, q is defined to be the intersection of all blocks containing p and q. It is straightforward to show that two points lie on a unique line.

(1.25) Theorem. *Let $\mathcal{D}$ be a square 2-design with $\lambda > 1$. Then the following are equivalent:*
(a) $\mathcal{D}$ is a projective geometry;

(b) every line meets every block;
(c) the number of blocks containing three non-collinear points is constant. □

The Bruck–Ryser–Chowla theorem shows that if a projective plane of order $n \equiv 1$ or $2 \pmod 4$ exists, then n is the sum of two squares. (In this case, $v = n^2+n+1 \equiv 3 \pmod 4$, and so the diophantine equation is $y^2+z^2 = nx^2$. Standard reduction arguments, as in Hardy and Wright (1981), p. 301, show that, if this equation has a non-zero solution, then it has one with $x = 1$.) Thus there is no projective plane of order 6. As noted above, this theorem does not preclude the existence of a projective plane of order 10. The non-existence of such a plane was shown by several massive computations by Lam *et al.* (1983), (1986), (1989), using a coding-theoretic approach due to MacWilliams, Sloane and Thompson (1972). In Chapter 13, we describe the method used.

A *subplane* of a projective plane $(X, \mathcal{B})$ of order n consists of a proper subset X' of the point set X, and a subset $\mathcal{B}'$ of the line set $\mathcal{B}$, such that $(X', \mathcal{B}')$ is itself a projective plane (of order m, say). In this situation, $n \geq m^2$ holds (see Exercise 16); equality holds if and only if every line in $\mathcal{B}$ contains a point of X' (and dually). In the situation of equality, $(X', \mathcal{B}')$ is called a *Baer subplane* of $(X, \mathcal{B})$; and X' is a set of m^2+m+1 points which intersects every line in 1 or $m+1$ points.

Another class of symmetric designs arises from Hadamard matrices, so-called because of their relationship to a theorem of Hadamard (1893).

(1.26) Theorem. *Let A be a $n \times n$ real matrix whose entries satisfy $|a_{ij}| \leq 1$ for all i, j. Then $|\det(A)| \leq n^{\frac{n}{2}}$. Equality holds if and only if all entries of A are ± 1 and $AA^\top = nI$.*

PROOF. $|\det(A)|$ is the volume of the n-dimensional parallelepiped spanned by the rows of A. By assumption, each row vector has Euclidean length at most $n^{\frac{1}{2}}$, with equality if and only if all its entries are ± 1. Also, the volume is at most the product of the edge lengths, with equality if and only if the edges are mutually perpendicular. □

(1.27) DEFINITION. A $n \times n$ real matrix H with entries ± 1 satisfying $HH^\top = nI$ is called a *Hadamard matrix* (or *H-matrix*, for short) of *order* n.]

Apart from trivial examples of orders 1 and 2, any Hadamard matrix has order divisible by 4, as we will see. It is conjectured that Hadamard matrices exist for all orders divisible by 4. The smallest multiple of 4 for which no Hadamard matrix is known is currently 428.

The defining property of a Hadamard matrix is unaltered if some rows or columns are multiplied by -1, or if rows or columns are permuted. We call two Hadamard matrices *equivalent* if one can be transformed into the other by such operations.

Any Hadamard matrix is equivalent (by sign changes alone!) to a *normalized* Hadamard matrix, in which the first row and column consist entirely of +1s. Let M be the $(n-1) \times (n-1)$ matrix obtained from a normalized Hadamard matrix by deleting the first row and column and replacing the -1s by 0s. Then M is the incidence matrix of a square 2-$(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ design, where $v = n-1$. For any two rows of H agree in $\frac{1}{2}n$ positions, and so a row of M agrees with the all-1 vector in $\frac{1}{2}n - 1 = \frac{1}{2}(v-1)$ positions, i.e. has $\frac{1}{2}(v-1)$ entries 1. Moreover, suppose that two rows of M have x common ones. Then there are $\frac{1}{2}(v-1) - x$ positions where the entries in the two rows are 1 and 0, and the same number where they are 0 and 1; hence there are $x+1$ where both have the entry 0, and we conclude that $2x + 1 = \frac{1}{2}(v-1)$, or $x = \frac{1}{4}(v-3)$. Similar remarks apply to columns. So M is the incidence matrix of a design, as claimed. Note that $v \equiv 3 \pmod 4$, so n is divisible by 4.

Conversely, if M is the incidence matrix of a square 2-$(4\lambda+3, 2\lambda+1, \lambda)$ design, then replacing the zeros in M by -1s and bordering M with a row and column of +1s gives a Hadamard matrix of order $4\lambda + 4$. Hence:

(1.28) Proposition. *There exists a Hadamard matrix of order $n > 2$ if and only if there exists a square 2-design with parameters $(n-1, \frac{1}{2}n - 1, \frac{1}{4}n - 1)$.* □

A square 2-design with these parameters is called a *Hadamard 2-design.*

(1.29) REMARK. Isomorphic Hadamard 2-designs come from equivalent H-matrices; but the converse is not true.

(1.30) EXAMPLE. A class of examples is due to Paley (1933). Let q be a prime power congruent to 3 mod 4, and let $\mathsf{F} = \mathsf{F}_q$, and Q the set of non-zero squares in F. Then $(\mathsf{F}, \{Q + x : x \in \mathsf{F}\})$ is a Hadamard 2-design. These designs are called *Paley designs*, and the Hadamard matrices obtained from them as in (1.24) are called *Paley H-matrices.* We reserve the term *Paley matrix* for a slightly different object, defined for any odd prime power q, namely the $q \times q$ matrix $P = (p_{ij})$, where

$$p_{ij} = \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } i - j \text{ is a square in } \mathsf{F}_q, \\ -1 & \text{otherwise,} \end{cases}$$

where the indices are taken to be elements of F_q. If $q \equiv 3 \pmod 4$, the Paley H-matrix is obtained from P by putting -1 on the diagonal and bordering with a row and column of 1s.

(1.31) EXAMPLE. The point-hyperplane design of PG$(n, 2)$ is a Hadamard 2-$(2^{n+1} - 1, 2^n - 1, 2^{n-1} - 1)$ design.The corresponding Hadamard matrix is called a *Sylvester H-matrix.* Sylvester H-matrices have a number of remarkable properties. For example, the character table of an abelian group of exponent 2 is a Sylvester H-matrix. See also Exercise 2.