19
Designs

In this chapter we give an introduction to a large and important area of combinatorial theory which is known as *design theory*. The most general object that is studied in this theory is a so-called *incidence structure*. This is a triple $\mathbf{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, where:

(1) $\mathcal{P}$ is a set, the elements of which are called *points*;
(2) $\mathcal{B}$ is a set, the elements of which are called *blocks*;
(3) $\mathbf{I}$ is an incidence relation between $\mathcal{P}$ and $\mathcal{B}$ (i.e. $\mathbf{I} \subseteq \mathcal{P} \times \mathcal{B}$). The elements of $\mathbf{I}$ are called *flags*.

If $(p, B) \in \mathbf{I}$, then we say that point p and block B are *incident*. We allow two different blocks B_1 and B_2 to be incident with the same subset of points of $\mathcal{P}$. In this case one speaks of "repeated blocks". If this does not happen, then the design is called a *simple* design and we can then consider blocks as subsets of $\mathcal{P}$. In fact, from now on we shall always do that, taking care to realize that different blocks are possibly the same subset of $\mathcal{P}$. This allows us to replace the notation $(p, B) \in \mathbf{I}$ by $p \in B$, and we shall often say that point p is "in block B" instead of incident with B.

It has become customary to denote the cardinality of $\mathcal{P}$ by v and the cardinality of $\mathcal{B}$ by b. So the incidence structure then is a set of v points and a collection of b not necessarily distinct subsets of the point set. The structure obtained by replacing each block by its complement is, of course called the *complement* of the structure. (This means that we replace $\mathbf{I}$ by its complement in $\mathcal{P} \times \mathcal{B}$.)

To obtain an interesting theory, we must impose some regularity conditions on the structure $\mathbf{S}$. As a first example, we mention incidence structures that have the confusing name "*linear spaces*". Here the blocks are usually called *lines* and the regularity conditions are that every line contains (i.e. is incident with) at least two points and any two points are on exactly one line. Example 19.6 below shows a simple but important linear space. The following theorem is due to De Bruijn and Erdős (1948). The elegant proof is due to Conway.

THEOREM 19.1. *For a linear space we have $b = 1$ or $b \geq v$, and equality implies that for any two lines there is exactly one point incident with both.*

PROOF: For $x \in \mathcal{P}$, denote by r_x the number of lines incident with x, and similarly for $B \in \mathcal{B}$, let k_B be the number of points on B. Let there be more than one line. If $x \notin L$ then $r_x \geq k_L$ because there are k_L lines "joining" x to the points on L. Suppose $b \leq v$. Then $b(v - k_L) \geq v(b - r_x)$ and hence

$$1 = \sum_{x \in \mathcal{P}} \sum_{L \not\ni x} \frac{1}{v(b - r_x)} \geq \sum_{L \in \mathcal{B}} \sum_{x \notin L} \frac{1}{b(v - k_L)} = 1$$

and this implies that in all the inequalities, equality must hold. Therefore $v = b$, and $r_x = k_L$ if $x \notin L$. □

A trivial example of equality in Theorem 19.1 is a so-called *near pencil*, a structure with one line that contains all the points but one, and all pairs containing that point as lines of size two. Much more interesting examples are the projective planes that we shall define later in this chapter.

In the rest of this chapter, we shall be interested in highly regular incidence structures called "t-designs". Let v, k, t and λ be integers with $v \geq k \geq t \geq 0$ and $\lambda \geq 1$. A t-design on v points with *blocksize* k and *index* λ is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ with:

(i) $|\mathcal{P}| = v$,
(ii) $|B| = k$ for all $B \in \mathcal{B}$,
(iii) for any set T of t points, there are exactly λ blocks incident with all points in T.

So all blocks have the same size and every t-subset of the point set is contained in the same number of blocks. Two different notations for such a design are widely used, namely t-(v, k, λ) design and $S_\lambda(t, k, v)$. We shall use both of them. A *Steiner system* $S(t, k, v)$

is a t-design with $\lambda = 1$, and we suppress the index in the notation. Most of the early theory of designs originated in statistics, where 2-designs are used in the design of experiments for statistical analysis. These designs are often called *balanced incomplete block designs* (BIBDs). Usually trivial designs are excluded from the theory: a design with one block that contains all the points or a design that has all the k-subsets of the point set as blocks is of course a t-design for $t \leq k$, but is not very interesting.

We give a few examples; more will follow further on.

EXAMPLE 19.1. Let the nonzero vectors of $\mathbb{F}_2^4$ be the points. As blocks we take all triples $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ with $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. Any pair $\mathbf{x}, \mathbf{y}$ with $\mathbf{x} \neq \mathbf{y}$ uniquely determines a third element $\mathbf{z}$, different from both, satisfying this equation. So we have constructed an $S(2, 3, 15)$. The blocks are the 2-dimensional subspaces of $\mathbb{F}_2^4$ with $\mathbf{0}$ deleted.

We construct a second design by taking all the vectors as point set and defining blocks to be 4-tuples $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}\}$ for which $\mathbf{w} + \mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. This defines an $S(3, 4, 16)$. Note that if we take the blocks that contain $\mathbf{0}$ and delete this vector, we find the blocks of the previous design.

EXAMPLE 19.2. We take the ten edges of a K_5 as point set. Each of the three kinds of 4-tuples shown in Fig. 19.1 will be a block.

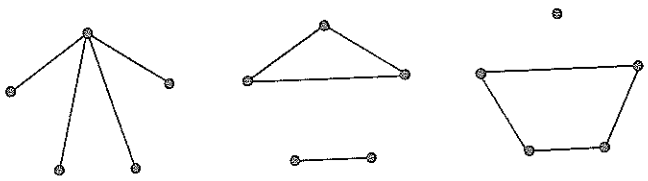

Figure 19.1

There are $5+10+15 = 30$ blocks. No triple (of edges) is contained in more than one block. Therefore the blocks contain 120 different triples, i.e. all the triples. We have constructed an $S(3, 4, 10)$.

EXAMPLE 19.3. Let H be a normalized Hadamard matrix of order $4k$. Delete the first row and the first column. We now identify points with rows of this matrix. Each column defines a subset of the rows, namely those rows for which there is a + in that column. These subsets are the blocks. From the argument in Theorem 18.1, we see that any pair of points is contained in exactly $k-1$ blocks and clearly all blocks have size $2k-1$. We have a 2-$(4k-1, 2k-1, k-1)$ design and such a design is called a *Hadamard 2-design.*

Consider the same matrix H but now delete only the first row. Each of the other rows determines two $2k$-subsets of the set of columns. This partition is unaffected if we change the sign of the row. The argument of Theorem 18.1 now shows that for any three columns, there are exactly $k-1$ of the subsets that have three elements in these columns. So these $2k$-sets are the blocks of a 3-$(4k, 2k, k-1)$ design called a *Hadamard 3-design.*

EXAMPLE 19.4. Consider a regular Hadamard matrix of order $4u^2$ (see Example 18.2). If we replace + by 1 and − by 0, we find a (0,1)-matrix with $2u^2+u$ ones in every row and column, and furthermore, any two rows or columns have inner product u^2+u. Let the columns be the characteristic functions of the blocks of a design on $4u^2$ points. The properties of the matrix show that this is a 2-$(4u^2, 2u^2+u, u^2+u)$ design. One usually prefers considering the complement of this design, i.e. a 2-$(4u^2, 2u^2-u, u^2-u)$ design.

PROBLEM 19A. Here are two more examples in the spirit of Example 19.2.

(i) Take the edges of K_6 as points of an incidence structure. The blocks are to be all sets of three edges that either are the edges of a perfect matching, or the edges of a triangle. Show that this is an $S(2,3,15)$ and show that it is isomorphic to the design in Example 19.1.

(ii) Take the edges of K_7 as points of an incidence structure. The blocks are to be all sets of five edges of these three types: (a) "claws" with five edges incident with a common vertex, (b) edge sets of pentagon subgraphs, and (c) five edges that form a triangle and two disjoint edges. Show that this is an $S_3(3,5,21)$.

We now give two elementary theorems on t-designs.

THEOREM 19.2. *The number of blocks of an $S_\lambda(t,k,v)$ is*

$$b = \lambda \binom{v}{t} \Big/ \binom{k}{t}. \tag{19.1}$$

PROOF: Count in two ways the number of pairs (T, B), where T is a t-subset of $\mathcal{P}$ and B is a block incident with all points of T. We find $\lambda\binom{v}{t} = b\binom{k}{t}$. □

THEOREM 19.3. *Given i, $0 \le i \le t$, the number of blocks incident with all the points of an i-subset I of $\mathcal{P}$ is*

$$b_i = \lambda \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i}. \tag{19.2}$$

That is, every $S_\lambda(t,k,v)$ is also an i-design for $i \le t$.

PROOF: Count in two ways the number of pairs (T, B), where T is a t-subset of $\mathcal{P}$ that contains I and B is a block that is incident with all the points of T. □

COROLLARY. *If $\mathcal{D}$ is a t-design with point set $\mathcal{P}$ and block set $\mathcal{B}$ and if I is a subset of $\mathcal{P}$ with $|I| \le t$, then the point set $\mathcal{P}\backslash I$ and the blocks $\{B\backslash I : I \subseteq B\}$ form an $S_\lambda(t-i, k-i, v-i)$. This design is called the derived design $\mathcal{D}_I$.*

In Example 19.1 we already saw an example of a derived design. If we take $I = \{\mathbf{0}\}$, the derived design for $S(3,4,16)$ is $S(2,3,15)$.

PROBLEM 19B. Show that an $S(3,6,11)$ does not exist.

The number of blocks incident with any point, i.e. b_1, is usually denoted by r (*replication number*). Two special cases of Theorem 19.3 are the following relations for the parameters of a 2-design:

$$bk = vr, \tag{19.3}$$

$$\lambda(v-1) = r(k-1). \tag{19.4}$$

THEOREM 19.4. *Let $0 \le j \le t$. The number of blocks of an $S_\lambda(t,k,v)$ that are incident with none of the points of a j-subset J of $\mathcal{P}$ is*

$$b^j = \lambda \binom{v-j}{k} \Big/ \binom{v-t}{k-t}. \tag{19.5}$$

PROOF: For $x \in \mathcal{P}$, let $\mathcal{B}_x$ be the set of blocks incident with x. We use inclusion-exclusion, Theorem 10.1. We find that

$$b^j = \sum_{i=0}^{j} (-1)^i \binom{j}{i} b_i.$$

The result follows by substitution of (19.2) and then using (10.5).

It is quicker to observe that b^j apparently does not depend on the particular set J and then count in two ways the pairs (J, B), where J is a j-subset of $\mathcal{P}$ and $J \cap B = \emptyset$. So $\binom{v}{j} b^j = b\binom{v-k}{j}$. Then the result follows from Theorem 19.2. □

COROLLARY. *If $i+j \le t$, then the number of blocks of an $S_\lambda(t,k,v)$ that are incident with all of a set of i points and none of a disjoint set of j points is a constant*

$$b_i^j = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}. \tag{19.6}$$

PROOF: The result follows upon application of Theorem 19.4 to the $(t-i)$-design $\mathcal{D}_I$, where I is the set of i points. □

COROLLARY. *If J is a j-subset of $\mathcal{P}$, $j \le t$, then the point set $\mathcal{P} \backslash J$ and the blocks B with $B \cap J = \emptyset$ form an $S_\mu(t-j, k, v-j)$ called the residual design $\mathcal{D}^J$.*

PROBLEM 19C. Prove that the complement of an $S_\lambda(t,k,v)$ is a t-design and determine its parameters.

EXAMPLE 19.5. Consider a Hadamard 3-design 3-$(4k, 2k, k-1)$ and form the residual with respect to a set with one point. We find a Hadamard 2-design 2-$(4k-1, 2k, k)$, i.e. the complement of the design of Example 19.3.

An obvious necessary condition for the existence of an $S_\lambda(t,k,v)$ is that the numbers b_i of (19.2) are integers. However, this condition is not sufficient. An $S(10, 16, 72)$ does not exist, as is demonstrated by the following theorem due to Tits (1964).

THEOREM 19.5. *In any nontrivial Steiner system $S(t, k, v)$,*

$$v \geq (t+1)(k-t+1).$$

PROOF: In a Steiner system, any two distinct blocks have at most $t-1$ points in common. Choose a set S of $t+1$ points not contained in any block. For each set $T \subseteq S$ with $|T| = t$, there is a unique block B_T containing T. Each such B_T is incident with $k-t$ points not in S, and any point not in S is incident with at most one such block B_T since two such blocks already have $t-1$ points of S in common. This shows that the union of all blocks B_T contains $(t+1)+(t+1)(k-t)$ points and the result follows. □

Given an incidence structure with $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$, the *incidence matrix* N is the v by b matrix with rows indexed by the elements p of $\mathcal{P}$, columns indexed by the elements B of $\mathcal{B}$, and with the entry $N(p, B) = 1$ if p is incident with B, $N(p, B) = 0$ otherwise. Note that the entry in row p and column q of $NN^\top$ is the sum of $N(p, B)N(q, B)$ over all blocks B, and this is the number of blocks that contain both p and q. Dually, the entry in row A and column B of $N^\top N$ is the cardinality of $A \cap B$.

Two designs $\mathcal{D}$ and $\mathcal{D}'$ with incidence matrices N and N' are called *isomorphic* or *equivalent* if there are permutation matrices P and Q such that $N' = PNQ$.

We shall often identify N with the design, i.e. we refer to the columns as blocks instead of as characteristic functions of blocks.

Now if N is the incidence matrix of a 2-design, then $NN^\top$ has the entry r everywhere on the diagonal and entries λ in all other positions, i.e.

$$NN^\top = (r-\lambda)I + \lambda J, \tag{19.7}$$

where I and J are v by v matrices.

PROBLEM 19D. Let N be an 11 by 11 (0,1)-matrix with the following properties: (i) every row of N has six ones; (ii) the inner product of any two distinct rows of N is at most 3. Show that N is the incidence matrix of a 2-(11,6,3) design. Furthermore show that this design is unique (up to isomorphism).

The following theorem is known as *Fisher's inequality*.

THEOREM 19.6. *For a 2-(v, k, λ) design with b blocks and $v > k$ we have*

$$b \geq v.$$

PROOF: Since $v > k$, we have $r > \lambda$ by (19.4). Since J has one eigenvalue v and its other eigenvalues are 0, the matrix on the right-hand side of (19.7) has $v - 1$ eigenvalues $(r - \lambda)$ and one eigenvalue $(r - \lambda) + \lambda v = rk$. So it has determinant $rk(r - \lambda)^{v-1} \neq 0$ and hence N has rank v. This implies that $b \geq v$. □

From the argument in the preceding proof, we can make a very important conclusion, given in the next theorem.

THEOREM 19.7. *If a 2-(v, k, λ) design has $b = v$ blocks and v is even, then $k - \lambda$ must be a square.*

PROOF: Since $b = v$, we have $r = k$. Now N is a v by v matrix and by (19.7)

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

Since $\det N$ is an integer, we are done. □

Theorem 19.6 was generalized by A. Ya. Petrenjuk (1968) to $b \geq \binom{v}{2}$ for any $S_\lambda(4, k, v)$ with $v \geq k + 2$ and finally generalized to arbitrary t-designs by Ray-Chaudhuri and Wilson (1975).

THEOREM 19.8. *For an $S_\lambda(t, k, v)$ with $t \geq 2s$ and $v \geq k + s$, we have $b \geq \binom{v}{s}$.*

PROOF: We introduce the *higher incidence matrices* of the t-design $\mathcal{D} = S_\lambda(t, k, v)$. For $i = 0, 1, 2, \ldots$, let N_i denote the $\binom{v}{i}$ by b matrix with rows indexed by the i-element subsets of points, columns indexed by the blocks, and with entry 1 in row Y and column B if $Y \subseteq B$, 0 otherwise. For $0 \leq i \leq j \leq v$, we use W_{ij} to denote the i-th incidence matrix of the incidence structure whose blocks are all the j-element subsets of a v-set. Thus W_{ij} is a $\binom{v}{i}$ by $\binom{v}{j}$ matrix.

We claim that

$$N_s N_s^\top = \sum_{i=0}^{s} b_{2s-i}^{i} W_{is}^\top W_{is}.$$

To see this, note that $N_sN_s^\top$ has rows indexed by s-element subsets E and columns indexed by s-element subsets F of the points, and for given E and F, the entry in row E and column F of $N_sN_s^\top$ is the number of blocks that contain both E and F. This number is $b_{2s-\mu}$, where $\mu := |E \cap F|$. The entry in row E and column F of $W_{is}^\top W_{is}$ is the number of i-subsets of the points contained in both E and F, i.e. $\binom{\mu}{i}$. So the $(E,\ F)$-entry on the righthand side of the equation is $\sum_{i=1}^{s} b_{2s-i}^{i}\binom{\mu}{i}$, and from (19.6) it follows that this is $b_{2s-\mu}$.

The $\binom{v}{s}$ by $\binom{v}{s}$ matrices $b_{2s-i}^{i}W_{is}^\top W_{is}$ are all positive semidefinite, and $b_s^s W_{ss}^\top W_{ss} = b_s^s I$ is positive definite since $b_s^s > 0$ $(v \geq k+s)$. Therefore $N_sN_s^\top$ is positive definite and hence nonsingular. The rank of $N_sN_s^\top$ is equal to the rank of N_s, i.e. N_s has rank $\binom{v}{s}$, and this cannot exceed the number of columns of N_s, which is b. □

If equality holds in the Wilson-Petrenjuk inequality, Theorem 19.8, then the $2s$-design is called *tight*. The only known examples with $s > 1$ and $v > k + s$ are the unique Steiner system $S(4, 7, 23)$ that we treat in the next chapter and its complement.

It is useful to give some idea of the history of t-designs. Only finitely many Steiner systems $S(t, k, v)$ with $t \geq 4$ are known. The most famous are the designs $S(5, 8, 24)$ and $S(5, 6, 12)$ found by E. Witt (1938) and the derived 4-designs. These will appear in the next chapter. R. H. F. Denniston (1976) constructed $S(5, 6, 24)$, $S(5, 7, 28)$, $S(5, 6, 48)$, and $S(5, 6, 84)$. W. H. Mills (1978) constructed an $S(5, 6, 72)$. Again, the derived designs are Steiner systems. Since then, no others have been found. In 1972, W. O. Alltop constructed the first infinite sequence of 5-designs without repeated blocks. We remark that it is easy to show that t-designs with repeated blocks exist for any t, but for a long time many design theorists believed that nontrivial t-designs without repeated blocks did not exist for $t > 6$. The first simple 6-design was found by D. W. Leavitt and S. S. Magliveras in 1982, and in 1986 D. L. Kreher and S. P. Radziszowski found the smallest possible simple 6-design, an $S_4(6, 7, 14)$. The big sensation in this area was the paper by L. Teirlinck (1987) proving that nontrivial simple t-designs exist for all t. His construction produces designs with tremendously large parameters and hence the construction of small examples is still an open problem. For a number of special parameter sets, it has been shown that the corresponding designs do not exist.

For the remainder of this chapter we shall mainly be interested in 2-designs. When $t = 2$, we often omit this parameter in the "t-(v,k,λ)" notation and speak of (v,k,λ)-designs.

A class of designs of special interest are the 2-designs with $b = v$. In this case the incidence matrix N of the design is a square matrix and these designs should be called *square designs*. However, the confusing name *symmetric designs* is standard terminology. (Note that N is *not* necessarily symmetric.) For a symmetric 2-(v,k,λ) design (19.4) becomes

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

Some authors use the name *projective design*, a name derived from the fact that a 2-$(v,k,1)$ design with $b = v$ is called a projective plane (see Example 19.7). Despite the fact that we are not happy with the name, we shall use the terminology *symmetric designs* for these designs.

PROBLEM 19E. Let $\mathcal{D}$ be a 2-(v,k,λ) design with b blocks and r blocks through every point. Let B be any block. Show that the number of blocks that meet B is at least

$$k(r-1)^2/[(k-1)(\lambda-1)+(r-1)].$$

Show that equality holds if and only if any block not disjoint from B meets it in a constant number of points.

EXAMPLE 19.6. Take as points the elements of $\mathbb{Z}_7$ and as blocks all triples $B_x := \{x, x+1, x+3\}$ with $x \in \mathbb{Z}_7$. It is easy to check that this yields an $S(2,3,7)$. The following Fig. 19.2 is often drawn. The lines repesent blocks, but one block must be represented by the circle.

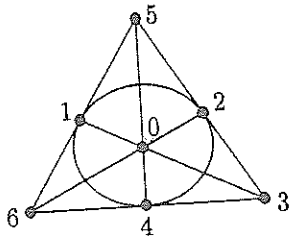

Figure 19.2

This design is known as the *Fano plane.* The idea of the construction will be extended in Chapter 27. It is based on the fact that the six differences among the elements of $\{0,1,3\}$ are exactly all the nonzero elements of $\mathbb{Z}_7$. If we wish to find the block containing say $\{1,6\}$, we observe that $6-1=1-3$ and we therefore take $x=5$ and find $x+1=6$, $x+3=1$, i.e. the pair is indeed in B_5. The reader should have no difficulty finding an $S(2,4,13)$ in the same way, using $\mathbb{Z}_{13}$.

A symmetric design with $\lambda=1$ is called a *projective plane.* If k is the size of the blocks, then $n=k-1$ is called the *order* of the plane (why this is done will become clear in Example 19.7). Expressed in n, the parameters of a projective plane of order n are:

$$v=n^2+n+1, \qquad k=n+1, \qquad \lambda=1.$$

The blocks are usually called *lines.* The Fano plane is the (unique) projective plane of order 2.

EXAMPLE 19.7. Consider the vector space $\mathbb{F}_q^3$. This vector space contains $(q^3-1)/(q-1)=q^2+q+1$ 1-dimensional subspaces and the same number of 2-dimensional subspaces. We now construct an incidence structure $(\mathcal{P},\mathcal{B},\mathrm{I})$, where $\mathcal{P}$ and $\mathcal{B}$ are these two classes of subspaces of $\mathbb{F}_q^3$. If a 1-dimensional subspace is contained in a 2-dimensional subspace, we say they are incident. It is immediately clear that we have thus defined a projective plane of order q, i.e. a 2-$(q^2+q+1,q+1,1)$ design. This design is usually denoted by $PG(2,q)$ or $PG_2(q)$, which stands for projective geometry of dimension 2 and order q.

The construction defined above can also be applied if we replace $\mathbb{F}_q$ by $\mathbb{R}$. We then obtain the classical real projective plane, where points are the 1-dimensional subspaces and lines are the 2-dimensional subspaces. This geometry contrasts with classical affine geometry in the fact that no two lines are parallel. When speaking about the designs defined above, we use terminology from geometry.

PROBLEM 19F. Find a subset $S = \{s_1, \dots, s_5\}$ of $\mathbb{Z}_{21}$ such that the elements of $\mathbb{Z}_{21}$ as points and the 21 blocks $S + x$ $(x \in \mathbb{Z}_{21})$ form a projective plane of order 4. (Hint: there is a solution S for which $2S = S$.)

PROBLEM 19G. Let $(R, C, S; L)$ be a Latin square of order 6. Define $\mathcal{P} := R \times C$. Let $\mathcal{B}$ be the set of blocks

$$B_{ij} := \\ \{(x,y) \in R \times C : x = i \text{ or } y = j \text{ or } L(x,y) = L(i,j)\} \setminus \{(i,j)\}$$

for $(i,j) \in R \times C$.

(1) Show that this defines a 2-(36,15,6) design.
(2) Show that a regular Hadamard matrix of order 36 exists.

PROBLEM 19H. Let $\mathcal{D}$ be a 3-(v, k, λ) design. Suppose that the derived design of $\mathcal{D}$ with respect to a point p (i.e. the case $i = 1$ in the Corollary to Theorem 19.3) is a symmetric design.

(1) Show that $\lambda(v-2) = (k-1)(k-2)$.
(2) Show that any two blocks of $\mathcal{D}$ meet in 0 or $\lambda + 1$ points.
(3) Show that the set of points not on a block B together with the blocks disjoint from B form a 2-design $\mathcal{D}^B$.
(4) Apply Fisher's inequality to the design $\mathcal{D}^B$ and deduce that $v = 2k$ or otherwise $k = (\lambda+1)(\lambda+2)$ or $k = 2(\lambda+1)(\lambda+2)$.

What are the possibilities for the design $\mathcal{D}$? Do we know any designs with these properties?

PROBLEM 19I. Let O be a subset of the points of a projective plane of order n such that no three points of O are on one line. Show that $|O| \le n + 1$ if n is odd and that $|O| \le n + 2$ if n is even. A set of $n + 1$ points, no three on a line, is called an *oval*; a set of

$n+2$ points, no three on a line, is a *hyperoval.* Two constructions of $PG_2(4)$ were given in Example 19.7 and Problem 19F. In each case, construct a hyperoval.

PROBLEM 19J. Let O be a hyperoval (with $q+2$ points) in $PG_2(q)$, $q=2^m$. Any of the q^2-1 points $p \notin O$ has the property that there are exactly $\frac{1}{2}(q+2)$ secants of O through p. Take five points on O and split them into

$$\{\{p_1,p_2\},\{p_3,p_4\},\{p_5\}\}.$$

This can be done in 15 ways. The two pairs determine two secants that meet in a point $p \notin O$. The line through p and p_5 meets O in a point, that we call p_6. This defines 15 (not necessarily distinct) 6-tuples of points on O, containing the given five points. This defines an $S_\lambda(5,6,q+2)$ (a construction due to D. Jungnickel and S. A. Vanstone). Construct a hyperoval O in $PG_2(q)$ and then show that the 5-design is not a simple design. (Hint: use coordinates, cf. Example 19.7.)

Any 2-$(n^2,n,1)$ design is called an *affine plane.* The points and lines of the plane (= 2-dimensional vector space) $\mathbb{F}_q^2$ form an affine plane of order q. For such a design we use the notation $AG_2(n)$ (2-dimensional affine geometry of order n).

EXAMPLE 19.8. Let $\mathcal{D}$ be a projective plane of order n. If we delete one line and all the points on that line, we find an affine plane of order n.

PROBLEM 19K. Let $\mathcal{D}$ be any affine plane of order n. If B_1 and B_2 are two blocks, then we write $B_1 \sim B_2$ if the two blocks are the same or if they have no points in common. Show that $\sim$ is an equivalence relation. A class of this relation is called a *parallel class.* Show that there exists a projective plane of order n such that $\mathcal{D}$ can be obtained from that plane by the construction of Example 19.8.

We shall now show that if N is the incidence matrix of a symmetric design $\mathcal{D}$, then $N^\top$ is also the incidence matrix of a symmetric design $\mathcal{D}^\top$, called the *dual* of $\mathcal{D}$.

THEOREM 19.9. *Let N be the incidence matrix of a symmetric 2-(v,k,λ) design. Then $N^\top$ is also the incidence matrix of a design.*

PROOF: Consider any block B of the design. For $0 \le i \le k$ let a_i be the number of blocks ($\neq B$) that have i points in common with B. Then counting blocks, pairs (p, B') with $p \in B \cap B'$ and triples (p, q, B') with $p \neq q$ and $\{p, q\} \subseteq B \cap B'$ we find:

$$\sum_{i=0}^{k} a_i = v - 1, \quad \sum_{i=0}^{k} i a_i = k(k-1), \quad \sum_{i=0}^{k} \binom{i}{2} a_i = \binom{k}{2}(\lambda - 1),$$

from which we find $\sum_{i=0}^{k}(i-\lambda)^2 a_i = 0$. Hence, any block $B' \neq B$ has λ points in common with B, i.e. $N^\top N = (k-\lambda)I + \lambda J$. □

Note that in Example 19.7, we did not need to specify whether the set $\mathcal{P}$ was the 1-dimensional subspaces or the 2-dimensional subspaces. In the latter situation, we have the dual of the former.

In many cases the designs $\mathcal{D}$ and $\mathcal{D}^\top$ are not isomorphic.

Let $\mathcal{D}$ be a symmetric 2-(v,k,λ) design. There are two other ways to obtain a design from $\mathcal{D}$. These two designs are called the *derived* design and *residual* design of $\mathcal{D}$. This could be somewhat confusing since we have already introduced that terminology. We shall always indicate which of the two we mean. Take any block B of $\mathcal{D}$. The residual of $\mathcal{D}$ with respect to B has $\mathcal{P}\backslash B$ as point set and as blocks all $B'\backslash B$ with $B' \neq B$. It is a 2-$(v-k, k-\lambda, \lambda)$ design. The derived design has B as point set and as blocks all $B' \cap B$ with $B' \neq B$. It is a 2-$(k, \lambda, \lambda - 1)$ design. If a design with parameters v, k, b, r, λ is the residual of a symmetric design, then $r = k + \lambda$. Any 2-design for which this equation holds is called a *quasiresidual* design. If such a design is not the residual of a symmetric design, then we say that it is *nonembeddable.* The assertion of Problem 19K is that every affine plane is embeddable in a projective plane. A theorem due to W. S. Connor (1952), that we shall leave until Chapter 21, states that every quasiresidual design with $\lambda = 2$ is embeddable.

EXAMPLE 19.9. Let $C := \begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix}$ and let E_i denote a 3 by 3 matrix with ones in column i and zeros elsewhere. Then

$$N := \begin{pmatrix} E_1 & I & I & I \\ E_2 & I & C & C^2 \\ E_3 & I & C^2 & C \end{pmatrix}$$

is the 9 by 12 incidence matrix of $AG_2(3)$. Define

$$A := \begin{pmatrix} 1&1&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&1&1&1&0&0&0 \\ 1&1&1&0&0&0&0&0&0&1&1&1 \\ 0&0&0&1&1&1&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0&0&1&1&1 \\ 0&0&0&0&0&0&1&1&1&1&1&1 \end{pmatrix}, \quad B := \begin{pmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&0&1&0 \\ 1&0&1&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 1&0&0&1 \\ 1&0&0&1 \end{pmatrix}.$$

Form the 24 by 16 matrix

$$D := \begin{pmatrix} A & O \\ N & B \\ N & J - B \end{pmatrix}.$$

One easily checks that $D^\top$ is the 16 by 24 incidence matrix of a 2-(16,6,3) design. This is a quasiresidual design. However, it cannot be the residual of a 2-(25,9,3) symmetric design because the inner product of row $i+6$ and row $i+15$ of D, $1 \leq i \leq 9$, equals 4 and, by Theorem 19.9, the inner product of the columns of the incidence matrix of a 2-(25,9,3) design is 3. This shows that nonembeddable designs with $\lambda = 3$ exist.

The combination of a counting argument and a suitable quadratic form that we used to prove Theorem 19.9 is widely used in combinatorics. However, sometimes it is easier to use algebraic methods as we shall demonstrate in the following theorem, due to Ryser. (The reader can try to prove the theorem by using counting arguments.)

Theorem 19.10. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be an incidence structure with $|\mathcal{P}| = |\mathcal{B}| = v$, blocksize k, such that any two blocks meet in λ points. Then $\mathcal{D}$ is a symmetric 2-design.*

Proof: Let N be the incidence matrix of $\mathcal{D}$. Then

$$N^\top N = (k - \lambda)I + \lambda J, \tag{19.8}$$

and

$$JN = kJ. \tag{19.9}$$

By Theorem 19.9, we are done if we can show that $NJ = kJ$. From (19.8) we see that N is nonsingular and hence (19.9) can be read as $J = kJN^{-1}$. From (19.8) we find $JN^{\top}N = (k - \lambda + \lambda v)J$ and therefore

$$JN^{\top} = (k - \lambda + \lambda v)JN^{-1} = (k - \lambda + \lambda v)k^{-1}J,$$

i.e. N has constant rowsums. Then these rowsums must be k. This proves the theorem and yields $(k - \lambda + \lambda v)k^{-1} = k$ as was to be expected from (19.3) and (19.4). □

As a preparation for the best known nonexistence theorem for designs, we need two results, both due to Lagrange. For the first, consider the matrix H of (18.6) with $n = 1$, i.e. $A_i = (a_i)$. Define $\mathbf{y} = (y_1, y_2, y_3, y_4)$ by $\mathbf{y} := \mathbf{x}H$, where $\mathbf{x} = (x_1, x_2, x_3, x_4)$. Then from (18.7) we find

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = (y_1^2 + y_2^2 + y_3^2 + y_4^2). \tag{19.10}$$

Using this identity, Lagrange proved that every integer is the sum of four squares. Clearly the identity shows that it is sufficient to prove this for primes. For an elegant proof that a prime is the sum of four squares we refer to Chandrasekharan (1968).

The following nonexistence theorem is known as the Bruck-Ryser-Chowla theorem.

THEOREM 19.11. *If v, k, λ are integers such that $\lambda(v-1) = k(k-1)$, then for the existence of a symmetric 2-(v, k, λ) design it is necessary that:*

(i) *if v is even then $k - \lambda$ is a square;*
(ii) *if v is odd, then the equation $z^2 = (k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2$ has a solution in integers x, y, z, not all zero.*

PROOF: Assertion (i) was proved in Theorem 19.7. So assume that v is odd. Let $\mathcal{D}$ be a symmetric 2-(v, k, λ) design with incidence matrix $N = (n_{ij})$ and write $n := k - \lambda$. We now introduce v linear forms L_i in the variables $x_1, \ldots, x_v$ by

$$L_i := \sum_{j=1}^{v} n_{ij} x_j, \qquad 1 \le i \le v.$$

Then the equation $N^\top N = (k-\lambda)I + \lambda J$ implies that

$$(19.11) \qquad L_1^2 + \cdots + L_v^2 = n(x_1^2 + \cdots + x_v^2) + \lambda(x_1 + \cdots + x_v)^2.$$

By Lagrange's theorem, n can be written as $n = a_1^2 + \cdots + a_4^2$. This and (19.10) allow us to take four of the variables x_j and write

$$(19.12) \qquad n(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = (y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2),$$

where each y_j is a linear form in the four variables $x_i, \ldots, x_{i+3}$.

We now first assume that $v \equiv 1 \pmod 4$. By applying this to (19.11) four variables at a time and introducing w for $x_1 + \cdots + x_v$, we reduce (19.11) to

$$(19.13) \qquad L_1^2 + \cdots + L_v^2 = y_1^2 + \cdots + y_{v-1}^2 + n x_v^2 + \lambda w^2.$$

Since H in (18.6) is invertible, we can express the variables x_j for $1 \le j \le v-1$ as linear forms in the corresponding y_j and hence w is a linear form in these variables and x_v. Next, we reduce the number of variables in the following way. If the linear form L_1, expressed in $y_1, \ldots, y_{v-1}, x_v$, does not have coefficient $+1$ for y_1, then we set $L_1 = y_1$, and if the coefficient is $+1$, we set $L_1 = -y_1$, and in both cases, we subsequently solve this equation for y_1 as a linear expression in the remaining variables y_j and x_v. This is substituted in the expression w. So (19.11) has been reduced to

$$L_2^2 + \cdots + L_v^2 = y_2^2 + \cdots + y_{v-1}^2 + n x_v^2 + \lambda w^2.$$

We proceed in this way for $y_2, \ldots, y_{v-1}$. In each step, w is replaced by another linear form in the remaining variables, and hence we end up with

$$L_v^2 = n x_v^2 + \lambda w^2,$$

in which both L_v and w are rational multiples of the variable x_v. If we multiply this by the common denominator of the factors, we find an equation

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

in integers. This proves the assertion that if $v \equiv 1 \pmod 4$. If $v \equiv 3 \pmod 4$, the same procedure is applied to (19.13) after adding nx_{v+1}^2 to both sides, where x_{v+1} is a new variable. The equation is then finally reduced to $nx_{v+1}^2 = y_{v+1}^2 + \lambda w^2$ and again we multiply by a common denominator to find an equation of type

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

in accordance with assertion (ii). □

Example 19.10. From Example 19.7, we know that a projective plane of order n exists for $2 \le n \le 9$, except possibly for $n = 6$. By Theorem 19.11, a necessary condition for the existence of a projective plane of order 6 is that the equation $z^2 = 6x^2 - y^2$ has a nontrivial solution. If such a solution exists, then also one for which x, y, and z have no prime factor in common, i.e. z and y are both odd. Then z^2 and y^2 are both $\equiv 1 \pmod 8$. Since $6x^2 \pmod 8$ is either 0 or 6, we see that the equation has only the trivial solution (0,0,0). Therefore a projective plane of order 6 does not exist.

If we try the same thing for a plane of order 10, we find the equation $z^2 = 10x^2 - y^2$, which has the solution $x = 1$, $y = 1$, $z = 3$. In this case Theorem 19.11 tells us nothing. A few years ago it was announced that a computer search involving several hundred hours on a Cray 1, had excluded the existence of a projective plane of order 10. This is the only case where the nonexistence of a symmetric 2-design has been shown using something other than Theorem 19.11.

Corollary. *If there exists a projective plane of order $n \equiv 1$ or $2 \pmod 4$, then n is the sum of two integral squares.*

Proof: The condition $n \equiv 1$ or $2 \pmod 4$ implies that $v = n^2 + n + 1 \equiv 3 \pmod 4$. Theorem 19.11 asserts that n is the sum of two rational squares. It is well known that n is the sum of two rational squares if and only if n is the sum of two integral squares. (This follows from the condition that n is the sum of two integral squares if and only if no prime divisor of the square free part of n is $\equiv 3 \pmod 4$.) □

PROBLEM 19L. Show that a symmetric 2-(29,8,2) design does not exist.

PROBLEM 19M. Suppose M is a rational square matrix of order v and that $MM^\top = mI$. Show that if v is odd, then m is a square. Show that if $v \equiv 2 \pmod 4$, then m is the sum of two rational squares.

(Note that one consequence of this latter result is that the existence of a conference matrix of order $n \equiv 2 \pmod 4$ implies that $n - 1$ is the sum of two squares.)

A great deal of work has been done on the construction of 2-designs. We shall only treat a number of examples that will give some idea of the kind of methods that have been used. The smallest nontrivial pair (k, λ) to consider is $(3, 1)$. A 2-$(v, 3, 1)$ design is called a *Steiner triple system*. One uses the notation $STS(v)$ for such a design. By (19.3) and (19.4) a necessary condition for the existence of such a design is that $v \equiv 1 \pmod 6$ or $v \equiv 3 \pmod 6$. We shall show that this condition is also sufficient. This will be done by direct construction in Examples 19.11 and 19.15. However, it is useful to see a number of examples of a more complicated approach. The methods that we demonstrate can be used for the construction of other designs than Steiner triple systems. Furthermore, they can be used to produce designs with certain subdesigns (see Problem 19N) or prescribed automorphism group. The idea of this approach is to find direct constructions for small examples and some recursive constructions, and subsequently show that, for any v that satisfies the necessary conditions, an $STS(v)$ can be constructed by the recursive methods, using the list of known small examples. We shall see below that this in fact reduces to a (not very difficult) problem in number theory. As stated above, we restrict ourselves to a number of examples. The reader may wish to try to show that our examples suffice to find an $STS(v)$ for all possible values of v, without using Examples 19.11 and 19.15.

We consider the trivial design with only one block of size 3 as $STS(3)$. We have already seen constructions of $STS(7) = PG_2(2)$ and $STS(9) = AG_2(3)$. In Example 19.1, we constructed an $STS(15)$.

EXAMPLE 19.11. Let $n = 2t+1$. We define $\mathcal{P} := \mathbb{Z}_n \times \mathbb{Z}_3$. As blocks we take all triples $\{(x,0),(x,1),(x,2)\}$ with $x \in \mathbb{Z}_n$ and all triples $\{(x,i),(y,i),(\frac{1}{2}(x+y),i+1)\}$ with $x \neq y$ in $\mathbb{Z}_n$ and $i \in \mathbb{Z}_3$. This simple construction provides an $STS(6t+3)$ for every t.

EXAMPLE 19.12. Let $q = 6t+1$ be a prime power and let α be a primitive element in $\mathbb{F}_q$, i.e. $\mathbb{F}_q^*$ is a cyclic group generated by α. We define

$$(19.14)\quad B_{i,\xi} := \{\alpha^i+\xi, \alpha^{2t+i}+\xi, \alpha^{4t+i}+\xi\}, \qquad 0 \le i < t, \quad \xi \in \mathbb{F}_q.$$

We claim that the elements of $\mathbb{F}_q$ as points and the blocks $B_{i,\xi}$ form an $STS(q)$. The idea of the proof is the same as in Example 19.6. Note that $\alpha^{6t} = 1$, $\alpha^{3t} = -1$ and define s by $\alpha^s = (\alpha^{2t} - 1)$. We consider the six differences of pairs from $B_{0,0}$. These are:

$$\begin{aligned} \alpha^{2t} - 1 &= \alpha^s, & -(\alpha^{2t} - 1) &= \alpha^{s+3t}, \\ \alpha^{4t} - \alpha^{2t} &= \alpha^{s+2t}, & -(\alpha^{4t} - \alpha^{2t}) &= \alpha^{s+5t}, \\ \alpha^{6t} - \alpha^{4t} &= \alpha^{s+4t}, & -(1 - \alpha^{4t}) &= \alpha^{s+t}. \end{aligned}$$

It follows that for any $\eta \neq 0$ in $\mathbb{F}_q$, there is a unique i, $0 \le i < t$, such that η occurs as the difference of two elements of $B_{i,0}$. Hence for any x and y in $\mathbb{F}_q$, there is a unique i and a unique $\xi \in \mathbb{F}_q$ such that the pair x, y occurs in the block $B_{i,\xi}$. □

The method of Examples 19.6 and 19.12 is known as the *method of differences.* Example 19.15 will show a more complicated use of the same idea.

We now know that an $STS(v)$ exists for $v = 13, 19, 25, 31, 37, 43$ and 49 as well as the values mentioned above. This includes all $v \equiv 1 \pmod 6$ less than 50. In fact, we now know at least one $STS(v)$ for each feasible value of v less than 100, except $v = 55$, $v = 85$, $v = 91$.

EXAMPLE 19.13. Let there be an $STS(v_i)$ on the point set V_i ($i = 1, 2$). We take $V_1 \times V_2$ as a new point set and define as blocks all triples: $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ for which

(1) $x_1 = x_2 = x_3$ and $\{y_1, y_2, y_3\}$ is a block of $STS(v_2)$;
(2) $\{x_1, x_2, x_3\}$ is a block of $STS(v_1)$ and $y_1 = y_2 = y_3$;
(3) $\{x_1, x_2, x_3\}$ is a block of $STS(v_1)$ and $\{y_1, y_2, y_3\}$ is a block of $STS(v_2)$.

It is practically obvious that this defines an $STS(v_1 v_2)$. The reader should check that we have defined the correct number of blocks.

This construction provides us with an $STS(91)$.

EXAMPLE 19.14. We show a slightly more complicated construction. Suppose that we have an $STS(v_1)$ on the point set $V_1 = \{1, 2, \ldots, v_1\}$ with block set S_1, and furthermore suppose that the blocks that are completely contained in $V = \{s + 1, \ldots, v_1\}$, where $s = v_1 - v$, form an $STS(v)$. Let S_2 be the set of triples of an $STS(v_2)$ on the point set $V_2 = \{1, 2, \ldots, v_2\}$.

We consider a new point set

$$\mathcal{P} := V \cup \{(x, y) : 1 \leq x \leq s,\ 1 \leq y \leq v_2\}.$$

This set has $v + v_2(v_1 - v)$ points. We introduce a set $\mathcal{B}$ of four kinds of blocks:

(1) those of the subsystem $STS(v)$;
(2) $\{(a, y), (b, y), c\}$ with $c \in V$, $\{a, b, c\} \in S_1$ and $y \in V_2$;
(3) $\{(a, y), (b, y), (c, y)\}$ with $\{a, b, c\}$ a block in S_1 with no point in V, and $y \in V_2$;
(4) $\{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$, where $\{y_1, y_2, y_3\}$ is a block in S_2 and the integers x_1, x_2, x_3 satisfy

$$x_1 + x_2 + x_3 \equiv 0 \pmod{s}.$$

Again, one easily checks that any two points of $\mathcal{P}$ uniquely determine a block in $\mathcal{B}$. Hence $\mathcal{P}$ and $\mathcal{B}$ are the points and blocks of a Steiner triple system on $v + v_2(v_1 - v)$ points. A simple example is obtained by letting the subsystem be just one block, i.e. $v = 3$. Taking $v_1 = 7$, $v_2 = 13$, we find an $STS(55)$.

We have thus constructed an $STS(v)$ for every feasible value of v less than 100, except $v = 85$.

PROBLEM 19N. (a) Show that if an $STS(v_1)$ and an $STS(v_2)$ both exist, then there is an $STS(v_1v_2 - v_2 + 1)$. Use this construction to find an $STS(85)$.

(b) Construct an $STS(15)$ on the set $\{0, 1, \dots, 14\}$ such that it contains a Fano plane on $\{0, 1, \dots, 6\}$ as a subsystem.

EXAMPLE 19.15. Consider as point set $\mathbb{Z}_{2t} \times \mathbb{Z}_3 \cup \{\infty\}$. Addition of elements is coordinatewise with the extra convention $\infty + (x, i) = \infty$. For notational convenience we sometimes write the second coordinate as an index, i.e. x_i instead of (x, i). We now define four types of "*base blocks*":

(1) $\{0_0, 0_1, 0_2\}$;
(2) $\{\infty, 0_0, t_1\}$, $\{\infty, 0_1, t_2\}$, $\{\infty, 0_2, t_0\}$;
(3) $\{0_0, i_1, (-i)_1\}$, $\{0_1, i_2, (-i)_2\}$, $\{0_2, i_0, (-i)_0\}$, $i = 1, \dots, t-1$;
(4) $\{t_0, i_1, (1-i)_1\}$, $\{t_1, i_2, (1-i)_2\}$, $\{t_2, i_0, (1-i)_0\}$, $i = 1, \dots, t$.

We have $6t + 1$ base blocks. For $a = 0, 1, \dots, t-1$ we add the element $(a, 0)$ (i.e. a_0) to each of the elements of every base block, thus producing $t(6t+1)$ blocks. We claim that these are the triples of an $STS(6t+1)$. It is trivial that the base blocks of type 2 yield a set of blocks in which every pair of points, one of which is ∞, occurs exactly once. The cyclic nature of the definition of the base blocks shows that it is sufficient for us to check that all pairs $\{a_0, b_0\}$ with $a \neq b$ and all pairs $\{a_0, b_1\}$ occur in the triples we have defined. If $a < b$ and $b - a = 2s$, then the pair $\{a_0, b_0\}$ occurs in the triple obtained from $\{0_2, s_0, (-s)_0\}$ "translated" by the element $(b - s, 0)$. Similarly, if $b - a$ is odd, we find the required pair by translating a base block of type 4. Now consider a pair $\{a_0, b_1\}$. If $a = b \leq t - 1$, we find the pair by translating the base block of type 1 by $(a, 0)$. If $a \neq b$ and $a < t$, we have to look for the pair in a translate of a base block of type 2 or of type 3. We must search for a base block in which the difference $b - a$ occurs as $y - x$ for two elements y_1, x_0. For type 2, this difference is t and in the blocks $\{0_0, i_1, (-i)_1\}$ we find the differences i, $1 \leq i \leq t - 1$, and $-i = 2t - i$, $1 \leq i \leq t - 1$, indeed every difference once! Now, the rest of the details can be left as an exercise.

This example shows that if $v = 6t + 1$, then an $STS(v)$ exists. Combined with Example 19.11 we have a construction for every feasible value of v.

We end this chapter with an amusing application of the Fano plane. At present the idea is not used in practice but the problem itself has a practical origin, and maybe some day generalizations of the following method will be used. Suppose one wishes to store one of the integers 1 to 7 in a so-called "*write-once memory*". This is a binary memory, originally filled with zeros, for which it is possible to change certain bits to ones but not back again, i.e. the state 1 is permanent. This happens in practice with paper tape, into which holes are punched, or compact discs, where a laser creates pits in certain positions. In both cases, we cannot erase what was written in the memory. To store the integers 1 to 7, we need a memory of three bits. What if one wishes to use the memory four consecutive times? The simplest solution is to have a 12-bit memory that is partitioned into four 3-bit sections, one for each consecutive usage. We assume that the memory is very expensive and we would like to be able to use a shorter memory for the same purpose. We shall now show that seven bits suffice, a saving of more than 40%.

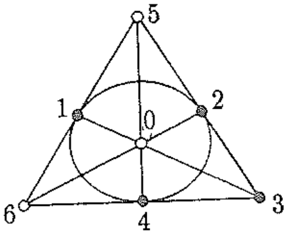

Figure 19.3

Let $\mathcal{P} = \{1, 2, \ldots, 7\}$ be the set of points of $PG_2(2)$ and let $\mathcal{L}$ denote the set of lines. To store one of the integers 1 to 7 in a memory with positions numbered 1 to 7, we use the following rules. As a general rule: if we wish to store i and the memory is in a state corresponding to i (from a previous usage), then we do nothing. Otherwise the rules are:

(1) if the memory is empty, store i by putting a 1 in position i;
(2) to store j when the memory is in state i, put a 1 in position k, where $\{i, j, k\} \in \mathcal{L}$;
(3) to store i when the memory contains two 1's, not correspond-

ing to i, put in two more 1's, such that i is one of the four 1's and the other three form a line in $\mathcal{L}$. No matter what the two original 1's were, this is possible (sometimes in two ways);

(4) if the memory contains four 1's, we may assume that we are in the situation of Fig. 19.3. To store 3, we do nothing (by the general rule); to store one of the missing numbers, we put 1's in the other two positions; to store 1, 2, or 4, store a 1 in the empty position on the line through 3 and the number we wish to store.

We leave it as an exercise for the reader to formulate the rules for reading the memory. Note that the memory uniquely reads the integer presently stored in the memory but it cannot see how often an integer has been stored or what was stored on the previous usage.

Notes.

The first occurrence of a 2-design may be $AG_2(3)$ in a paper by Plücker (1839). One usually attributes the introduction of Steiner systems to Woolhouse (1844); of course *not* to Steiner! Quite often they are said to originate with a problem of T. P. Kirkman (1847). T. P. Kirkman (1806–1895), a self-educated man, was a minister of the Church of England. He was an amateur mathematician with many contributions to the subject. Probably the best known is his *15 schoolgirls problem.* The problem is to arrange 15 schoolgirls in parties of three for seven days' walks such that every two of them walk together exactly once. This amounts to constructing an $STS(15)$ for which the set of triples can be partitioned into seven "parallel classes".

Jakob Steiner (1796–1863) was an important geometer of his time. He became interested in what we now call Steiner systems in 1853 when he studied the configuration of 28 double tangents of a plane quartic curve.

Sir Ronald A. Fisher (1890–1962) is considered to be one of the most prominent statisticians. Besides important contributions to statistics (multivariate analysis) and genetics, he is known for his work on the application of statistical theory to agriculture and the