3. Prove the rest of Theorem 7.2.4.
4. a) In the models illustrated in Figs. 7.2 and 7.3 find the maximum number of points so that no three are on the same line.
   b) In an affine plane of order n, prove there can be at most $n + 2$ points such that no three are on the same line.
   c) Repeat part (b) for a projective plane of order n.
5. Prove Theorem 7.2.5.
6. Prove Theorem 7.2.6. [*Hint:* Modify the proof of Theorem 7.2.3 and use duality.]
7. Prove Theorem 7.2.7. [*Hint:* Modify the proof of Theorem 7.2.4 and use duality.]
8. a) For which axiom of affine planes is its dual provable? Prove it.
   b) For the other axioms, show that their duals must be false.
   c) For which parts of theorems of affine planes are the duals provable? Prove them.
9. A *weak projective plane* satisfies Projective Axioms (i) and (iii) and the following replacements for Axiom (ii).
   ii′) There exist a point and a line not on that point.
   ii″) Every line has at least two points on it.
   a) Find a model of a weak projective plane of order 1.
   b) Prove that duality holds in this revised axiomatic system.
   c) Find a model of a weak projective plane with two lines having different numbers of points on them.
   d) Suppose that we replace Axiom (ii) for affine planes with the Axioms (ii′) and (ii″). Show that every such "weak affine plane" actually is an affine plane.

7.3 Design Theory

Design theory encompasses many notions besides affine and projective geometries. Design theory developed from mathematicians' natural inclination to generalize and explore and to meet the needs of applications, especially designs for statistical experiments. We concentrate on balanced incomplete block designs.

Some sampling trials require comparison of each of a number of varieties of something with all the other varieties available. Often one individual can't be expected to judge fairly among a large number of varieties. For example, taste comparisons by one person need to be done in a relatively short session. The organizer of the trials must guard against biases caused by which varieties are tasted together. Fisher and others developed designs in which each individual tests the same number of varieties (called the *size of the block*) and all pairs of varieties are compared the same number of times. Such designs are called balanced incomplete block designs (BIBD). *Balanced* refers to the uniformity of the arrangement, and *incomplete* refers to the fact that no block includes every variety. Fisher proved a number of results about BIBD. (See Anderson [1, Chapter 6].)

Remark Solutions to the n^2-officer problem are not BIBDs, although they are related, as in Example 2 of Section 7.2

Definition 7.3.1 A *balanced incomplete block design* (BIBD) is an arrangement of v varieties in b blocks (subsets), each of size k, so that each pair of varieties appear in λ blocks. We write (v, k, λ) to describe the numerical type of a BIBD.

Example 1 An affine plane of order n is a BIBD, with the lines as the blocks: $v = n^2$, $b = n^2 + n$, $k = n$, and $\lambda = 1$. Note that each point (variety) is on the same number, $r = n + 1$, of lines (blocks). ●

SIR RONALD A. FISHER

Sir Ronald A. Fisher (1890–1962) was one of the key people in establishing statistics as a mathematical discipline. Throughout his career he blended his interests in biology and statistics, building on his strong mathematical ability and insight. In 1911, as an undergraduate at Cambridge University, he gave a talk marking him as one of the first to see how to combine Darwin's theory of natural selection with Mendel's recently rediscovered ideas in genetics. He strongly advocated eugenics, the movement to improve people's genetic inheritance. (His involvement was innocent of and prior to the use of eugenics ideas for political and racist ends in various countries, most notoriously Nazi Germany.)

From an early age his eyesight was poor, which required active compensation. For example, in high school he studied spherical trigonometry entirely orally. His extraordinary visualization skills enabled him to perform all the three-dimensional thinking and computing without either a text or paper and pencil. His geometric intuition also characterized his statistical thinking. His first result, as well as many others, depended on considering a statistical sample of n points as a vector in n-dimensional Euclidean space. Many other statisticians, lacking Fisher's geometric abilities, found his reasoning difficult to follow and felt he depended too much on intuition. He made fundamental contributions in many areas of statistics, including tests of hypotheses and analysis of variance.

He combined his statistical, mathematical, and biological interests throughout his career. In 1919, he became the statistician at Rothamsted Experimental Station, where daily practical problems led him to a wide variety of theoretical discoveries in statistics. It was here that he realized the need both for randomized sampling and the careful design of experiments to study the interaction of variables. His biological experiments led to development of statistical design theory.

Example 2 A projective plane of order n is a BIBD, with the lines as the blocks: $v = n^2 + n + 1$, $b = n^2 + n + 1$, $k = n + 1$, and $\lambda = 1$. Again, each point is on the same number, $r = n + 1$, of lines. ●

Example 3 Given a BIBD $(v, k, 1)$ we can make a BIBD (v, k, λ) simply by repeating each block of the original BIBD λ times. However, experimenters often need to place a pair of varieties with different varieties in different blocks to gain additional information. The following list gives blocks for a BIBD (7, 3, 2) with no repetitions of blocks. Note that each line is a BIBD (7, 3, 1), so there are other ways to form a (7, 3, 2) BIBD by using repetition.

124	235	346	457	156	267	137
126	237	134	245	356	467	157 ●

Checking even the short list in Example 3 to verify that it is a (7, 3, 2) BIBD is tedious. It would be much worse with a larger design and harder still to find such a design by trial and error. Indeed, not every set of values (v, k, λ)—even those values that satisfy the combinatorial relations of Theorem 7.3.1—has a BIBD.

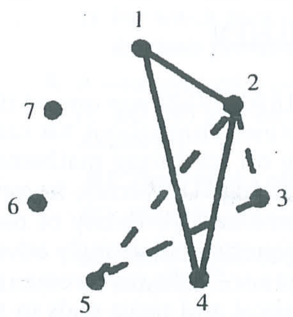

Figure 7.6 A cyclic way to represent a projective plane with seven points.

Exercise 1 Explain why there can be no BIBD (6, 3, 1).

Mathematicians and statisticians have found efficient ways to construct BIBDs and other designs. In Section 7.4 we use finite analytic geometries to construct many affine and projective spaces in any number of dimensions. Although other designs don't have such representations, symmetry often aids their construction.

Example 4 Figure 7.6 and symmetry provide the key to the BIBD of Example 3. In a regular seven-sided polygon, there are three different distances between vertices. Note that $\triangle 124$ has each of these three distances. When we rotate $\triangle 124$ to each of the seven possible positions, we get seven different blocks that satisfy a (7, 3, 1) BIBD. In fact, this design is a projective plane of order 2. Now $\triangle 157$ is the mirror image of $\triangle 124$, so the same reasoning applies to it. The 14 blocks of Example 3 are simply the rotations and mirror reflections of $\triangle 124$. Because of the different lengths of the sides, we can be sure that a given edge (pair of vertices) appears in exactly two triangles. ●

Before attempting to construct a BIBD with certain values, you should determine whether the given values are compatible with the conditions of a BIBD. Theorem 7.3.1 gives the necessary relations among the values for a BIBD. However, there is no guarantee, as Exercise 2 indicates, that values satisfying these relations always have a corresponding BIBD.

Theorem 7.3.1 In a BIBD (v, k, λ), each variety is in the same number r of blocks, $r(k-1) = \lambda(v-1)$ and $v \cdot r = b \cdot k$.

Exercise 2 Verify that the values in Example 1 for an affine plane of order n satisfy Theorem 7.3.1. However, there is no affine plane of order 6.

Proof. Let V be any variety of a BIBD and r_V be the number of blocks containing V. Each such block has $k-1$ other varieties. So $r_V(k-1)$ counts all appearances of these other varieties in blocks containing V. The value λ counts the number of times each of these other varieties appears with V. Thus $\lambda(v-1)$ also counts all appearances of other varieties in blocks containing V. Hence $r_V(k-1) = \lambda(v-1)$ for every V. As v, k and λ are constant, all varieties must be in the same number $r_V = r$ of blocks, and the first equation of the theorem holds. Similarly, $vr = bk$ counts the number of times that any variety appears in any block in two ways: Each of the v varieties appears r times, and each of the b blocks contains k varieties. ■

If we think of varieties as points and blocks as lines, a BIBD with $\lambda = 1$ satisfies the geometric axiom "two distinct points are on a unique line." In the 1840s and 1850s, Rev. Thomas Kirkman and Jacob Steiner (1796–1863) investigated such systems, with the added restriction that each line had three points on it, years before the more general notion of a BIBD was defined. A *Steiner triple system* is a BIBD with $k = 3$ and $\lambda = 1$. (See Anderson [1], Berman and Fryer [3] and Karteszi [7] for more on BIBD and Steiner systems.)

Theorem 7.3.2 There is a Steiner triple system $(v, 3, 1)$ iff $v = 6n+1$ or $v = 6n+3$.

Proof. Problem 3 shows v must equal either $6n+1$ or $6n+3$. (See Anderson [1,112] for the existence of such systems.) ■

Example 5 Is there a finite "hyperbolic" plane with three points on a line?

Solution. The key axiom of hyperbolic geometry is that every point P not on a line m has at least two lines on it that do not intersect m. Such a plane with three points per line would be a Steiner triple system in which each point (variety) has at least two more lines than there are points on a line. That is $r \geq k+2$. Note that a projective plane of order 2 gives a Steiner triple system with $v = 7$ and that an affine plane of order 3 gives a Steiner triple system with $v = 9$. By Theorem 7.3.2 the smallest possible hyperbolic plane with three points on a line would have $v = 13$ points. Theorem 7.3.1 implies that there must be $r = 6$ lines on every point and a total of $b = 26$ lines. However, combinatorics give no clue about how to construct such a design. Consider the vertices of a regular 13-gon (Fig. 7.7). Thirteen rotations of this polygon are symmetries of it. We could rotate two candidates for lines to find all 26 lines. Note the six different distances between vertices of the polygon. We can think of each line of three points as a triangle and look

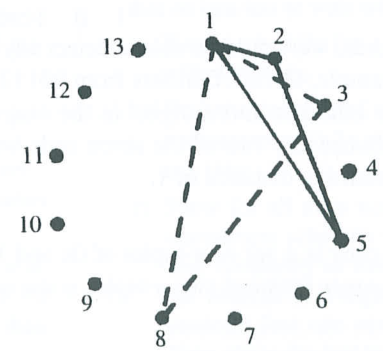

Figure 7.7 A cyclic way to represent a hyperbolic plane with 13 points.

for two triangles whose six sides include all the different lengths. After a reasonably short application of trial and error, we find that $\triangle 125$ and $\triangle 138$ satisfy this relationship. Hence their rotated images give the lines for a finite hyperbolic plane. •

7.3.1 Error-correcting codes

The advances in computers and their availability have vastly increased the amount of data transmitted as strings of 1s and 0s. Although computers are far more precise than human beings, errors in these transmissions occasionally occur because of static or for other reasons. With the use of words in real language, we can often correct errors because the context of the message or the word itself helps us recognize where the error must be and what the correction should be. However, a string such as 0010110111 provides no clue by itself about possible errors. Hence we need to build into the transmission a code to aid in finding and correcting errors; BIBD have important connections with such codes.

One way to obtain error correction is to send each individual 0 or 1 three times. The preceding message then would be sent as 000000111000111111000111111111. If just one of the three repetitions is accidentally altered, the receiving computer can correct the error by majority rule. If we assume that two or three errors in a triple are extremely unlikely, compared to none or one, this code allows us to correct most errors. However, the price of error correcting with this code is utilization of three times as much data as the actual message requires.

We can convert a BIBD into a matrix of 0s and 1s to construct a list of code words. The columns of the matrix, called an *incidence matrix*, are the varieties of the BIBD and the rows are the blocks. We put a 1 in an entry if the corresponding variety is in the corresponding block. Otherwise we put in a 0. For example, the top row of Example 3 has the incidence matrix

$$\begin{matrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{matrix}$$

. If we used the seven rows as code words, we would be able to detect any single error among the seven digits received. For example, 0010010 differs from 0011010 only in the fourth digit, but it differs from all the others in more digits. In the language of Definition 7.3.2, the Hamming distance between any two of the seven code words is 4, whereas 0010010 and 0011010 have a Hamming distance of 1.

Definition 7.3.2 A *code* is a set of n-tuples of 0s and 1s, each of which is a *code word*. The *Hamming distance* between two n-tuples is the number of places in which they differ.

Theorem 7.3.3 A code can detect as many as k errors if the Hamming distance between any two code words is at least $k+1$. A code can correct as many as k errors if the Hamming distance between any two code words is at least $2k+1$.

Proof. Suppose that all the code words are n-tuples. The number of errors in a received n-tuple is the number of places that this n-tuple differs from the code word sent, or the Hamming distance between them. Suppose that the Hamming distance between any two code words is at least $k+1$. If between 1 and k errors occur, then the received n-tuple is not a code word and so will be detected as an error. Similarly, suppose that the Hamming distance between code words is at least $2k+1$. Then a received n-tuple with between 1 and k errors will have a smaller Hamming distance from the original code word than from any other code word, enabling us to correct it. ■

Coding theory combines abstract algebra with design theory to develop more efficient codes than the incidence matrices of BIBDs. However, many of these codes are related to BIBDs. (See Anderson [1, Chapters 6 and 7] and Gallian [6, Chapter 31] for more information.)

PROBLEMS FOR SECTION 7.3

1. a) Find a formula for the number of blocks b in terms of v, k, and λ in a BIBD (v, k, λ).

b) Verify that all the conditions of Theorem 7.3.1 are satisfied with a BIBD $(v, k, 1)$ when r is any multiple of k.

2. Fisher showed that $b \geq v$ in any BIBD, with $v > k$. (See Anderson [1, 85].)

a) If you assume that $b \geq v$, what else does Theorem 7.3.1 tell you?

b) If $b = v$ and $\lambda = 1$, find v, b, and r in terms of k. Now set $n + 1 = k$ and find v in terms of n. Relate this result to projective planes. (BIBD with $b = v$ are called *symmetric*.)

c) Prove Axioms (i) and (ii) of a projective plane for a symmetric BIBD $(v, k, 1)$, with $k \geq 3$. [*Hint:* For Axiom (ii), given two varieties (points), count the number of varieties not on the block (line) they determine. Do the same when you add the third point.]

d) Prove Axiom (iii) of a projective plane for a symmetric BIBD $(v, k, 1)$, with $k \geq 3$. [*Hint:* Count the number of blocks that meet a given block in one of its varieties and the total number of blocks that meet it.]

3. a) In Theorem 7.3.2 prove that $v = 6n + 1$ or $v = 6n + 3$. [*Hint:* Use factoring and Theorem 7.3.1 twice, first to show that v must be odd and then to eliminate $v = 6n + 5$.]

b) Show that $v = 6n + 1$ and $v = 6n + 3$ are compatible with all conditions of Theorem 7.3.1.

4. Define a *Steiner double system* and prove that, for every $v \geq 2$, there is a Steiner double system.

5. a) Find a design for a projective plane of order 3 by using symmetries of the vertices of a regular 13-gon.

b) Program a computer to search for a projective plane of order 4 using symmetries of the vertices of a regular 21-gon.

6. Modify Example 5 to find a Steiner triple system for $v = 19$.

7. In a round-robin tournament each player (or team) plays every other player (or team). The organizer of such a tournament wants to schedule as many matches at once as possible. If the number of players is even, say, $2n$, conceivably n matches at a time can be scheduled and thus the tournament arranged so that no one has to wait while others play.

a) Find a schedule for a round-robin tournament with 4 players.

b) Find the number of rounds in a round-robin tournament with $2n$ players if there are n matches at a time.

c) Show for all even numbers $2n$ that there is a tournament schedule with no waiting as follows. Use symmetry to find a "near" schedule for the vertices of a regular polygon with $2n - 1$ vertices: Just one vertex sits out each round. Then place the last team (the $2n$th) at the center of the polygon and convert the near schedule to a schedule for all $2n$ teams.

8. A *Steiner quadruple system* is a BIBD (v, k, λ), with $k = 4$ and $\lambda = 1$. Show that $v = 12n + 1$ or $12n + 4$. Generalize. [*Hint:* See Problem 3.]

9. a) Write the code words in the code based on the (7, 3, 2) BIBD of Example 3. How many errors can this code detect? How many can it correct?

   b) Repeat part (a) for the code based on the affine plane of order 3, a BIBD (9, 3, 1).

10. You can add rows to the incidence matrix given in the text in a way that doesn't give a BIBD. For example, you can add rows that have four or more 1s. By Theorem 7.3.3, if the Hamming distance between any two (new and old) code words is at least 3, you will still be able to correct a single error while having more code words.

    a) Explain why, if you want to be able to correct single errors, there is no point in adding code words with one, two, or three 1s.

    b) Find all seven code words with four 1s that have a Hamming distance of at least 4 from each other and from the seven code words in the original matrix. How do these new code words relate to the code words?

    c) Find the two other code words that are a Hamming distance of at least 3 from each other and the 14 already found.

    d) Suppose that you have a set of n code words, each a seven-dimensional vector of 0s and 1s, and that each code word is a Hamming distance of at least 3 from every other code word. Find the total number of vectors possible (including code words and noncode words). Explain why every code word has seven vectors at a Hamming distance of 1 from it. Explain why n can be no larger than 16.