PART III. The Existence Problem

Chapter 9

Combinatorial Designs

9.1 BLOCK DESIGNS

In the history of attempts to perform scientifically sound experiments, combinatorics has played an important role. We have already encountered problems of experimental design in Section 1.1, where we discussed the design of an experiment to study the effects of different drugs, and used this design problem to introduce the notion of Latin squares. In this chapter we study the combinatorial questions that arose originally from issues in experimental design, and discuss the role of combinatorial analysis in the theory of experimental design. In Chapter 10 we apply combinatorial designs to the theory of error-correcting codes. Other applications, some of which we will touch upon in this chapter, include topics in cryptography, design of computer and communication networks, software testing, storage in disk arrays, signal processing, sports scheduling, "group testing" for defective items, designing chips for DNA probes, and clone screening in molecular biology. Some of these applications are described in Stinson [2003] and Colbourn, Dinitz, and Stinson [1999]. For general references on combinatorial designs, see Anderson [1990], Beth, Jungnickel, and Lenz [1999], Colbourn and Dinitz [1996], Dinitz and Stinson [1992], Hughes and Piper [1988], Lindner and Rodger [1997], Street and Street [1987], and Wallis [1988].

The theory of design of experiments came into being largely through the work of R. A. Fisher, F. Yates, and others, motivated by questions of design of careful field experiments in agriculture. Although the applicability of this theory is now very widespread, much of the terminology still bears the stamp of its origin.

We shall be concerned with experiments aimed at comparing effects of different *treatments* or *varieties*, e.g., different types of fertilizers, different doses of a drug, or different brands of shoes or tires. Each treatment is applied to a number of *experimental units* or *plots*. In agriculture, the experimental unit may be an area

Table 9.1: An Experimental Design for Testing Tread Wear[a]

		Car			
		A	B	C	D
Wheel position	Left front	1	2	3	4
	Right front	1	2	3	4
	Left rear	1	2	3	4
	Right rear	1	2	3	4

[a] The i, j entry is the brand of tire used in position i on car j.

in which a crop is grown. However, the experimental unit may be a human subject on a given day, a piece of animal tissue, or the site on an animal or plant where an injection or chemical treatment is applied, or it may in other cases be a machine used in a certain location for some purpose.

Certain experimental units are grouped together in *blocks*. These are usually chosen because they have some inherent features in common: for example, because they are all on the same human subject or all in the same horizontal row in a field or all on the skin of the same animal, or all on the same machine.

To be concrete, let us consider the problem of comparing the tread wear of four different brands of tires.[1] The treatments we are comparing are the different brands of tires. Clearly, individual tires of a given brand may differ. Hence, we certainly want to try out more than one tire of each brand. A particular tire is an experimental unit. Now suppose that the tires are to be tested under real driving conditions. Then we naturally group four tires or experimental units together, since a car used to test the tires takes four of them. The test cars define the blocks.

It is natural to try to let each brand of tire or treatment be used as often as any other. Suppose that each is used r times. Then we need $4r$ experimental units in all, since there are four treatments or tire brands. Since the experimental units are split into blocks of size 4, $4r$ must be divisible by 4. In this case, r could be any positive integer. If there were five brands of tires, we would need $5r$ experimental units in all, and then r could only be chosen to be an integer so that $5r$ is divisible by 4.

If we take r to be 4, we could have a very simple experimental design. Find four cars, say A, B, C, D, and place four tires of brand 1 on car A, four tires of brand 2 on car B, four tires of brand 3 on car C, and four tires of brand 4 on car D. This design is summarized in Table 9.1. This is clearly an unsatisfactory experimental design. Different cars (and different drivers) may lead to different amounts of tire wear, and the attempt to distinguish brands of tires as to wear will be confused by extraneous factors.

Much of the theory of experimental design has been directed at eliminating the

[1] Our treatment follows Hicks [1973].

Table 9.2: A Randomized Design for Testing Tread Wear[a]

		Car			
		A	*B*	*C*	*D*
	Left front	3	4	2	2
Wheel position	Right front	1	1	4	4
	Left rear	3	4	1	3
	Right rear	2	3	2	1

[a] The i, j entry is the brand of tire used in position i on car j.

Table 9.3: A Complete Block Design for Testing Tread Wear[a]

		Car			
		A	*B*	*C*	*D*
	Left front	1	1	3	4
Wheel position	Right front	2	3	4	2
	Left rear	3	2	1	1
	Right rear	4	4	2	3

[a] The i, j entry is the brand of tire used in position i on car j.

biasing or confusing effect caused by variations in particular experimental units. One often tries to eliminate the effect by randomizing and by assigning treatments to experimental units in a random way. For instance, we could start with four tires of each brand, and assign tires to each car completely at random. This might lead to a design such as the one shown in Table 9.2. Unfortunately, as the table shows, we could end up with a tire brand such as 4 never being used on a particular car such as A, or one brand such as 3 used several times in a particular car such as A. The results might still be biased by car effects. We can avoid this situation if we require that each treatment or brand be used in each block or car, and then make the assignment of tires to wheels of the car randomly. A major question in the theory of experimental design is what we have called in Chapter 1 the existence question. Here, we ask this question as follows: Does there exist a design in which there are four brands and four cars, each brand is used four times, and it is used at least once, equivalently exactly once, in each car? The answer is yes. Table 9.3 gives such a design.

The design in Table 9.3 still has some defects. The position of a tire on a car can affect its tread life. For instance, rear tires get different wear than front tires, and even the side of a car a tire is on could affect its tread life. If we wish also to eliminate the biasing effect of wheel position, we could require that each brand

Table 9.4: A Latin Square Design for Testing Tread Wear[a]

		Car			
		A	B	C	D
Wheel position	Left front	1	2	3	4
	Right front	2	3	4	1
	Left rear	3	4	1	2
	Right rear	4	1	2	3

[a] The i, j entry is the brand of tire used in position i on car j.

or treatment be used exactly once on each car and also exactly once in each of the possible positions. Then we ask for an assignment of the numbers $1, 2, 3, 4$ in a 4×4 array with each number appearing exactly once in each row and in each column. That is, we ask for a *Latin square* (see Section 1.1). Table 9.4 shows such a design. Among all possible 4×4 Latin square designs, we might still want to pick the particular one to use randomly.

In some experiments, it may not be possible to apply all treatments to every block. For instance, if there were five brands of tires, we could use only four of them in each block. How would we design an experiment now? If each brand of tire is used r times, we have $5r$ tires in all to distribute into groups of four, so as we observed above, $5r$ must be divisible by 4. For example, r must be $4, 8, 12$, and so on. Note that we could not do the experiment with six cars; that is, there does not exist an experimental design using five brands and six cars, with each brand used the same number of times, and four (different) brands assigned to each car. For there are 24 tire locations in all, and $5r = 24$ is impossible. Suppose that we take $r = 4$. Then there are $5r = 20$ tire locations in all. If s is the number of cars, $4s$ should be 20, so s should be 5. One possible design is given in Table 9.5. Here there are four different brands of tires on each car, each brand is used exactly once in each position, and each brand is used the same number of times, 5. There are various additional requirements that we can place on such a design. We discuss some of them below.

Let us now introduce some general terminology. Suppose that P is a set of experimental units or plots, and V is a set of treatments or varieties. Certain subsets of P will be called *blocks*. Given P and V, a *block design* is defined by giving the collection of blocks and assigning to each experimental unit in P a treatment in V. Thus, corresponding to each block is a set (possibly with repetitions) of treatments. Speaking abstractly, we shall be able to disregard the experimental units and think of a block design as simply consisting of a set V of treatments and a collection of subsets of V (possibly with repetitions) called blocks. Thus, the block design corresponding to Table 9.2 has $V = \{1, 2, 3, 4\}$ and has the following blocks:

$$\{3, 1, 3, 2\}, \quad \{4, 1, 4, 3\}, \quad \{2, 4, 1, 2\}, \quad \{2, 4, 3, 1\}.$$

Table 9.5: An Incomplete Block Design for Testing Tread Wear[a]

		Car				
		A	*B*	*C*	*D*	*E*
	Left front	1	2	3	4	5
Wheel position	Right front	2	3	4	5	1
	Left rear	3	4	5	1	2
	Right rear	4	5	1	2	3

[a] The i, j entry is the brand of tire used in position i on car j.

If order counts, as in the case of Latin squares, we can think of the blocks as sequences rather than subsets. A block design is called *complete* if each block is all of V, and *incomplete* otherwise. Tables 9.3 and 9.4 define complete block designs, and Table 9.5 defines an incomplete block design. A block design is called *randomized* if elements within each block are ordered by some random device, such as a random number table or a computer program designed to pick out random permutations.

We study two types of block designs in this chapter, the complete designs that come from Latin squares and families of Latin squares, and the incomplete designs that are called balanced. We also relate experimental design to the study of the finite geometries known as finite projective planes. In Chapter 10, we apply our results about experimental design to the design of error-correcting codes.

EXERCISES FOR SECTION 9.1

1. Find a Latin square design for the tread wear experiment different from that given in Table 9.4.

2. Suppose that we wish to test the effects of six different allergy medicines. Each subject gets one medicine each day for a week.

   (a) What are the varieties, experimental units, and blocks?

   (b) What can you say about the number of subjects needed if an experiment gives each medicine to the same number of subjects?

   (c) Is there a Latin square design for this experiment?

   (d) Is there a design for this experiment in which each medicine is used the same number of times in a week? If so, what are the blocks?

   (e) Is there a design for this experiment in which each medicine is used on the same number of subjects?

   (f) Is there a design in which each subject gets each medicine the same number of times?

3. (a) Give (as subsets) the blocks of a design in which the varieties are $\{1, 2, 3, 4, 5, 6, 7\}$ and the blocks are 3-element subsets.

   (b) Repeat part (a) so that each variety appears in exactly 3 blocks.

4. Give (as subsets) the blocks of a design in which the varieties are $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, the blocks are 3-element subsets, and each variety appears in exactly 4 blocks.

5. (a) Does there exist a design in which there are 8 varieties, blocks of size 4, and each variety appears in only 1 block? If so, give (as subsets) the blocks of the design. Otherwise, explain why a design doesn't exist.

   (b) Repeat part (a) with 12 varieties, blocks of size 5, and each variety appears in only 1 block.

   (c) Repeat part (a) with 7 varieties, blocks of size 3, and each variety appears in exactly 3 blocks.

   (d) Repeat part (a) with 10 varieties, blocks of size 4, and each variety appears in exactly 2 blocks.

6. (a) For a design in which the varieties are $\{1,2,3,4,5,6,7,8\}$ and the blocks are all of the 3-element subsets, in how many different blocks does each variety appear?

   (b) In general, in how many blocks does each variety appear if there are v varieties and the blocks are all of the k-element subsets?

7. Suppose that we have a block design in which each of the v varieties appears in r blocks and the blocks are k-element subsets. Consider an associated block design in which the blocks are the complements of the original blocks. Describe this new block design in terms of the number of varieties and blocks, the size of each block, and the number of blocks in which each variety appears.

9.2 LATIN SQUARES

9.2.1 Some Examples

A Latin square design is an appropriate experimental design if there are two factors, e.g., subject and day, wheel position and car, or *row* and *column*, and we want to control for both factors. In agricultural experiments, the rows and columns are literally rows and columns in a rectangular field. Latin squares were introduced by Fisher [1926] to deal with such experiments. Suppose, for example, that there are k different row effects and k different column effects, and we wish to test k different treatments. We wish to arrange things so that each treatment appears once and only once in a given row and in a given column, for example, in a given position and on a given car. Clearly, there is such an arrangement or $k \times k$ Latin square for every k. Table 9.6 shows a $k \times k$ Latin square. Thus, for Latin squares, the existence problem is very simple. The existence problem will not be so simple for the other designs we consider in this chapter.

We now turn to a series of examples of the use of Latin square designs.

Table 9.6: A $k \times k$ Latin Square

1	2	3	$\cdots$	$k-1$	k
2	3	4	$\cdots$	k	1
3	4	5	$\cdots$	1	2
			$\vdots$		
$k-1$	k	1	$\cdots$	$k-3$	$k-2$
k	1	2	$\cdots$	$k-2$	$k-1$

Example 9.1 Prosthodontics Cox [1958][2] discusses an experiment in prosthodontics that compares seven treatments, which are commercial dentures of different materials and set at different angles. It is desirable to eliminate as much as possible of the variation due to differences between patients. Hence, each patient wears dentures of one type for a month, then dentures of another type for another month, and so on. After seven months, each patient has worn each type of denture, that is, has been subjected to each treatment.

In this experiment, it seems likely that the results in later months will be different from those in earlier months, and hence it is sensible to arrange that each treatment be used equally often in each time position. Thus, there are two types of variation: between-patient and between-time variation. The desire to balance out both types suggests the use of a Latin square. The rows correspond to the months and the columns to the patients. Each patient defines a block, and the experimental unit is the jth patient in the ith month. ■

Example 9.2 Cardiac Drugs Chen, Bliss, and Robbins [1942] tested the effects of 12 different cardiac drugs on cats. The experiment required an observer to measure carefully the effect over a period of time, so a given observer could observe only four different cats in a day. The experimenters desired to eliminate the effects of the day on which an observation was made, the observer who made the observation, and the time of day (early AM, late AM, early PM, late PM) the observation was made. Thus, there were three factors, which is inappropriate for a Latin square design. However, a Latin square design could be carried out by taking as one factor the day on which the observation was made and as a second factor the observer and the time of day of the observation. A 12×12 Latin square experiment was performed, carried out over 12 days, with each of three observers observing four cats per day, two in the morning and two in the afternoon. The design used had 12 rows, coded by observer and time of observation, and 12 columns, coded by date. The i, j entry was the drug used on date j at the time of day and by the observer encoded by i. The dates defined the blocks. ■

[2] Examples 9.2, 9.3, 9.5, 9.13, and 9.14 below are also discussed by Cox [1958]. These and other examples can also be found in Box, Hunter, and Hunter [1978], Cochran and Cox [1957], Finney [1960], or Hicks [1973].

Table 9.7: Two Latin Square Designs for the Two Parts of the Week in the Market Research Experiment[a]

		First Part of the Week					Second Part of the Week			
		Time					Time			
		Mon.	Tues.	Wed.	Thurs.		Fri. AM	Fri. PM	Sat. AM	Sat. PM
Store	A	2	1	4	3	A	2	3	1	4
	B	3	2	1	4	B	1	4	2	3
	C	4	3	2	1	C	3	2	4	1
	D	1	4	3	2	D	4	1	3	2

[a] The i, j entry gives the treatment used in store i in period j.

Example 9.3 Market Research Brunk and Federer [1953] discuss some investigations in market research. One of these studied the effect on the sale of apples of varying practices of pricing, displaying, and packaging. In each experiment of a series, four merchandising practices (treatments), $1, 2, 3$, and 4, were compared and four supermarkets took part. It was clearly desirable that each treatment should be used in each store, so it was sensible to arrange for the experiment to continue for a multiple of four time periods. The experimenters wanted to eliminate systematic differences between stores and between periods. Since there were two types of variations, a Latin square design, in particular a 4×4 Latin square, was appropriate. In fact, however, the week was divided into two parts, Monday through Thursday, and Friday and Saturday, and one 4×4 Latin square was built up for each part of the week. This was a good idea because the grocery order per customer was larger over the weekend and it was quite possible that the treatment differences would not be the same in the two parts of the experiment. For an experiment lasting one week and comparing four treatments, the design of Table 9.7 was used. ■

Example 9.4 Spinning Synthetic Yarn Box, Hunter, and Hunter [1978] discuss an experiment dealing with the breaking strength of synthetic yarn and how this is affected by changes in draw ratio, the tension applied to yarn as it is spun. The three treatments tested were (1) the usual draw ratio, (2) a 5 percent increase in draw ratio, and (3) a 10 percent increase in draw ratio. One spinning machine was used, with three different spinnerets supplying yarn to three different bobbins under different draw ratios. When all the bobbins were completely wound with yarn, they were each replaced with an empty bobbin spool and the experiment was continued. The experimenter wished to control for two factors: the effect of the three different spinnerets and the effect of the time (order) in which the spinnerets were used. This called for a 3×3 Latin square design, with columns labeled I, II, III corresponding to order of production of the yarn, and rows labeled A, B, C corresponding to which spinneret was used. The i, j entry was the treatment or draw ratio $(1, 2, \text{or } 3)$ used in producing yarn from the ith spinneret in the jth production

Table 9.8: Latin Square Designs for the Synthetic Yarn Experiment[a]

	Order of production											
Spinneret	I	II	III	I	II	III	I	II	III	I	II	III
A	1	2	3	2	1	3	3	1	2	1	2	3
B	2	3	1	3	2	1	1	2	3	2	3	1
C	3	1	2	1	3	2	2	3	1	3	1	2
	First replication			Second replication			Third replication			Fourth replication		

[a] The i, j entry is the draw ratio used with the ith spinneret in the jth production run.

run. When small Latin squares are used, it is often desirable to replicate them, so in fact the experiment was replicated four times, using different 3 × 3 Latin square designs. Table 9.8 shows the designs. ■

9.2.2 Orthogonal Latin Squares

Let us return to the example of the differing effects on tire wear of four tire brands, which we discussed in Section 9.1. Let us imagine that we are also interested in the effect of brake linings on tire wear. Suppose for simplicity that we also have four different brands of brake linings. Thus, we would like to arrange, in addition to having each brand of tire tested exactly once on each car and exactly once in each tire position, that each tire brand be tested exactly once in combination with each brand of brake lining. We can accomplish this by building a 4 × 4 array, with rows corresponding to wheel position and columns to cars, and placing in each box *both* a tire brand and a brake lining brand to be used in the corresponding position and on the corresponding car. If a_{ij} is the tire brand in entry i, j of the array and b_{ij} is the brake lining brand in this entry, we require that every possible ordered pair (a, b) of tire brands a and brake lining brands b appear if we list all ordered pairs (a_{ij}, b_{ij}). Equivalently, since there are $4 \times 4 = 16$ possible ordered pairs (a, b) and exactly 16 spots in the array, we require that all the pairs (a_{ij}, b_{ij}) be different. Can we accomplish this? We certainly can. If the brake lining brands are denoted $1, 2,$ 3,4, simply test brake lining brand i on every wheel of the ith car. Combining this design with the tire brand design of Table 9.4 gives us the array of ordered pairs of Table 9.9. All the ordered pairs in this table are different.

Unfortunately, the array of Table 9.9 is not a very satisfactory design if we consider just brake linings. For we only use brake linings of brand 1 on car A, of brand 2 on car B, and so on. It would be good to have the brake linings tested by a Latin square design, not just the tires. Thus, we would like to find two Latin square

Table 9.9: Design for Testing the Combined Effects of Tire Brand and Brake Lining Brand on Tread Wear[a]

		Car			
		A	B	C	D
Wheel position	Left front	(1, 1)	(2, 2)	(3, 3)	(4, 4)
	Right front	(2, 1)	(3, 2)	(4, 3)	(1, 4)
	Left rear	(3, 1)	(4, 2)	(1, 3)	(2, 4)
	Right rear	(4, 1)	(1, 2)	(2, 3)	(3, 4)

[a] The i, j entry is an ordered pair, giving first the tire brand used in position i on car j, and then the brake lining brand used there.

experiments, $A = (a_{ij})$ and $B = (b_{ij})$, one for tire brands and one for brake lining brands, both using the same row and column effects. Moreover, we want the ordered pairs (a_{ij}, b_{ij}) all to be different. Can this be done? In our case, it can. Table 9.10 shows a pair of Latin square designs and the corresponding array of ordered pairs, which is easily seen to have each ordered pair (a, b), with $1 \leq a \leq 4$ and $1 \leq b \leq 4$, appearing exactly once. Equivalently, the ordered pairs are all different. We shall say that two distinct $n \times n$ Latin squares $A = (a_{ij})$ and $B = (b_{ij})$ are *orthogonal* if the n^2 ordered pairs (a_{ij}, b_{ij}) are all distinct. Thus, the two 4×4 Latin squares of Table 9.10 are orthogonal. However, the two Latin squares of Table 9.7 are not, as the ordered pair $(2, 4)$ appears twice, once in the $2, 2$ position and once in the $3, 3$ position. More generally, if $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ are distinct $n \times n$ Latin squares, they are said to form an *orthogonal family* if every pair of them is orthogonal.

The main question we address in this section is the fundamental existence question: If we want to design an experiment using a pair of $n \times n$ orthogonal Latin squares, can we always be sure that such a pair exists? More generally, we shall ask: When does an orthogonal family of r different $n \times n$ Latin squares exist?

Before addressing these questions, we give several examples of the use of orthogonal Latin square designs.

Example 9.5 Fuel Economy Davies [1945] used a pair of orthogonal Latin squares in the comparison of fuel economy in miles per gallon achieved with different grades of gasoline. Seven grades of gasoline were tested. One car was used throughout. Each test involved driving the test car over a fixed route of 20 miles, including various gradients. To remove possible biases connected with the driver, seven drivers were used; and to remove possible effects connected with the traffic conditions, the experiment was run on different days and at seven different times of the day. Thus, in addition to the seven treatments under comparison, there are three classifications of the experimental units: by drivers, by days, and by times of the day. A double classification of the experimental units suggests the use of a Latin square, a triple classification a pair of orthogonal Latin squares. The latter allows for an experiment in which each grade of gasoline is used once on each day, once by

Table 9.10: Two Orthogonal Latin Square Designs for Testing the Combined Effects of Tire Brand and Brake Lining Brand on Tread Wear[a]

		Car			
		A	B	C	D
Wheel position	Left front	1	2	3	4
	Right front	2	1	4	3
	Left rear	3	4	1	2
	Right rear	4	3	2	1

	Car			
	A	B	C	D
Left front	4	1	2	3
Right front	3	2	1	4
Left rear	1	4	3	2
Right rear	2	3	4	1

		Car			
		A	B	C	D
Wheel position	Left front	(1, 4)	(2, 1)	(3, 2)	(4, 3)
	Right front	(2, 3)	(1, 2)	(4, 1)	(3, 4)
	Left rear	(3, 1)	(4, 4)	(1, 3)	(2, 2)
	Right rear	(4, 2)	(3, 3)	(2, 4)	(1, 1)

Combined Design

[a] The combined array lists in the i, j entry the ordered pair consisting of the tire brand and then the brake lining brand used in the two Latin squares in tire position i on car j.

each driver, and once at each time of day, ensuring a balanced comparison. The design assigns to each day (row) and each time of day (column) one grade of gasoline (in the first Latin square) and one driver (in the second square). (In our tire wear example of Section 9.1, we could not control for the driver in the same way, that is, it would not make sense to use a pair of orthogonal Latin square experiments, the first indicating tire brand at position i on car j and the second indicating driver at position i on car j. For the same driver must be assigned to all positions of a given car!) ■

Example 9.6 Testing Cloth for Wear Box, Hunter, and Hunter [1978] describe an experiment involving a Martindale wear tester, a machine used to test the wearing quality of materials such as cloth. In one run of a Martindale wear tester of the type considered, four pieces of cloth could be rubbed simultaneously, each against a sheet of emery paper, and then the weight loss could be measured. There were four different specimen holders, labeled A, B, C, D, and each could be used in one of four positions, P_1, P_2, P_3, P_4, on the machine. In a particular experiment, four types of cloth or treatments, labeled $1, 2, 3, 4$, were compared. The experimenters wanted to control for the effects of the four different specimen holders, the four positions of the machine, which run the cloth was tested in, and which sheet of emery paper the cloth was rubbed against. A quadruple classification of experimental units suggests an orthogonal family of three 4×4 Latin squares. It was decided to use four sheets of emery paper, labeled $\alpha, \beta, \gamma, \delta$, to cut each into four quarters, and to use each quarter in one experimental unit. There were four runs

Table 9.11: An Orthogonal Family of Three Latin Squares for Testing Cloth for Wear[a]

	Run											
Position	R_1	R_2	R_3	R_4	R_1	R_2	R_3	R_4	R_1	R_2	R_3	R_4
P_1	1	3	4	2	A	D	B	C	α	β	γ	δ
P_2	2	4	3	1	B	C	A	D	β	α	δ	γ
P_3	3	1	2	4	C	B	D	A	γ	δ	α	β
P_4	4	2	1	3	D	A	C	B	δ	γ	β	α
	Latin Square Design for Treatments				Latin Square Design for Holders				Latin Square Design for Emery Sheets			

[a]The i, j entry shows the treatment (cloth type), holder, and emery paper sheet, respectively, used in run R_j in position P_i.

in all, R_1, R_2, R_3, R_4, each testing four specimens of cloth with different holders in varying positions and with different quarter-pieces of emery paper. Table 9.11 shows the three Latin square designs used. The reader can check that these are pairwise orthogonal. (In fact, the experiment was replicated, using four more runs and four more sheets of emery paper, again in a design involving an orthogonal family of three 4 × 4 Latin squares.) ■

9.2.3 Existence Results for Orthogonal Families

Let the *order* of an $n \times n$ Latin square be n. In what follows we usually assume that the entries in a Latin square of order n are the integers $1, 2, \ldots, n$. We now discuss the question: Does there exist an orthogonal family of r Latin squares of order n? We shall assume that $n > 1$, for there is only one 1×1 Latin square. There does not exist a pair of orthogonal 2×2 Latin squares. For the only Latin squares of order 2 are shown in Table 9.12. They are not orthogonal since the pair $(1, 2)$ appears twice. We have seen in Table 9.10 that there is a pair of orthogonal Latin squares of order 4, and in Table 9.11 that there is an orthogonal family of three Latin squares of order 4. It is easy enough to give a pair of orthogonal Latin squares of order 3. (Try it.)

The first theorem gives necessary conditions for the existence of an orthogonal family of r Latin squares of order n.

Theorem 9.1 If there is an orthogonal family of r Latin squares of order n, then $r \leq n - 1$.

Proof. Suppose that $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ form an orthogonal family of $n \times n$ Latin squares. Let $a_{ij}^{(p)}$ be the i, j entry of $A^{(p)}$. Relabel the entries in the first square so that 1 comes in the 1, 1 spot, that is, so that $a_{11}^{(1)} = 1$. Do this as follows. If $a_{11}^{(1)}$

Table 9.12: The Two Latin Squares of Order 2

1	2
2	1

2	1
1	2

was k, switch 1 with k and k with 1 throughout $A^{(1)}$. This does not change $A^{(1)}$ from being a Latin square and it does not change the orthogonality, for if the pair

$$\left(a_{ij}^{(1)}, a_{ij}^{(p)}\right)$$

was (k, l), it is now $(1, l)$, and if it was $(1, l)$, it is now (k, l).

By the same reasoning, without affecting the fact that we have an orthogonal family of $n \times n$ Latin squares, we can arrange matters so that each 1, 1 entry in each square is 1, and more generally so that

$$\begin{array}{ccccccccc} a_{11}^{(1)} & = & a_{11}^{(2)} & = & \cdots & = & a_{11}^{(r)} & = & 1, \\ a_{12}^{(1)} & = & a_{12}^{(2)} & = & \cdots & = & a_{12}^{(r)} & = & 2, \\ a_{13}^{(1)} & = & a_{13}^{(2)} & = & \cdots & = & a_{13}^{(r)} & = & 3, \\ & & & & \vdots & & & & \\ a_{1n}^{(1)} & = & a_{1n}^{(2)} & = & \cdots & = & a_{1n}^{(r)} & = & n. \end{array}$$

That is, we can arrange matters so that each $A^{(p)}$ has the same first row:

$$1 \quad 2 \quad 3 \quad \cdots \quad n.$$

Let us consider the 2, 1 entry in each square. Since $A^{(p)}$ is a Latin square, and since $a_{11}^{(p)}$ is 1 and 1 can appear only once in a column, $a_{21}^{(p)}$ must be different from 1. Moreover, by orthogonality,

$$a_{21}^{(p)} \neq a_{21}^{(q)}$$

if $p \neq q$. For otherwise,

$$\left(a_{21}^{(p)}, a_{21}^{(q)}\right) = (i, i)$$

for some i, so

$$\left(a_{21}^{(p)}, a_{21}^{(q)}\right) = \left(a_{1i}^{(p)}, a_{1i}^{(q)}\right),$$

which violates orthogonality. Thus, the numbers

$$a_{21}^{(1)}, a_{21}^{(2)}, \ldots, a_{21}^{(r)}$$

are all different and all different from 1. It follows that there are at most $n - 1$ of these numbers, and $r \leq n - 1$. (Formally, this reasoning uses the pigeonhole principle of Section 2.19.) Q.E.D.

Table 9.13: The Procedure for Changing an Orthogonal Family of Latin Squares into One Where Each Square Has First Row $123\cdots n$

$A^{(1)}$	$A^{(2)}$	$A^{(3)}$
$\begin{array}{\|cccc\|}\hline 4&3&2&1\\ 3&4&1&2\\ 2&1&4&3\\ 1&2&3&4\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 2&1&4&3\\ 4&3&2&1\\ 3&4&1&2\\ 1&2&3&4\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 3&4&1&2\\ 2&1&4&3\\ 4&3&2&1\\ 1&2&3&4\\ \hline\end{array}$
$\downarrow$ Interchange 1 with 4 $\downarrow$	$\downarrow$ Interchange 1 with 2 $\downarrow$	$\downarrow$ Interchange 1 with 3 $\downarrow$
$\begin{array}{\|cccc\|}\hline 1&3&2&4\\ 3&1&4&2\\ 2&4&1&3\\ 4&2&3&1\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 1&2&4&3\\ 4&3&1&2\\ 3&4&2&1\\ 2&1&3&4\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 1&4&3&2\\ 2&3&4&1\\ 4&1&2&3\\ 3&2&1&4\\ \hline\end{array}$
$\downarrow$ Interchange 2 with 3 $\downarrow$	$\downarrow$ Interchange 3 with 4 $\downarrow$	$\downarrow$ Interchange 2 with 4 $\downarrow$
$\begin{array}{\|cccc\|}\hline 1&2&3&4\\ 2&1&4&3\\ 3&4&1&2\\ 4&3&2&1\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 1&2&3&4\\ 3&4&1&2\\ 4&3&2&1\\ 2&1&4&3\\ \hline\end{array}$	$\begin{array}{\|cccc\|}\hline 1&2&3&4\\ 4&3&2&1\\ 2&1&4&3\\ 3&4&1&2\\ \hline\end{array}$

We illustrate the proof of this theorem by starting with an orthogonal family of three Latin squares of order 4 as shown in Table 9.13. The procedure to arrange that all the first rows are 1234 is illustrated in the table. Note that the $2, 1$ entries in the three Latin squares in the last row of Table 9.13 are $2, 3$, and 4, respectively.

Theorem 9.1 says that we can never find an orthogonal family of $n \times n$ Latin squares consisting of more than $n-1$ squares. Let us say that an orthogonal family of Latin squares of order n is *complete* if it has $n-1$ Latin squares in it. Thus, the three Latin squares of order 4 shown in Table 9.13 form a complete orthogonal family. It will be convenient to think of a single 2×2 Latin square as constituting an orthogonal family.

Theorem 9.2 gives sufficient conditions for the existence of a complete orthogonal family of Latin squares.

Theorem 9.2 If $n > 1$ and $n = p^k$, where p is a prime number[3] and k is a positive integer, then there is a complete orthogonal family of Latin squares of order n.

We omit a proof of Theorem 9.2 at this point. We prove it in Sections 9.3.4 and 9.3.5 by describing a constructive procedure for finding a complete orthogonal family of Latin squares of order n if n is a power of a prime. In particular, Theorem 9.2

[3] Recall that a *prime number* n is an integer greater than 1 whose only divisors are 1 and n. See Section 7.1.3.

says that there exists a pair of orthogonal 3×3 Latin squares, since $3 = 3^1$. It also says that there exist three pairwise orthogonal 4×4 Latin squares, since $4 = 2^2$. (We have already seen three such squares in Tables 9.11 and 9.13.) There also exists a family of four pairwise orthogonal 5×5 Latin squares, since $5 = 5^1$. Since 6 is not a power of a prime, Theorem 9.2 does not tell us whether or not there is a set of five pairwise orthogonal 6×6 Latin squares, or indeed whether there is even a pair of such squares. We shall show below that there is no complete orthogonal family of Latin squares of order n, indeed, not even a pair of such squares, if $n = 6$. Thus, for $n \leq 9$, there is a complete orthogonal family of Latin squares of order n if and only if $n \neq 6$. Lam, Thiel, and Swiercz [1989], by a massive computer search, found that there is not a complete orthogonal family of Latin squares of order 10. There is one if $n = 11$. This leaves $n = 12$ as the smallest number for which we don't know if there is a complete orthogonal family. As of this writing, the best we know is that there can be 5 pairwise orthogonal Latin squares of order 12. (See Johnson, Dulmage, and Mendelsohn [1961].)

According to the Fundamental Theorem of Algebra, any integer $n > 1$ can be written *uniquely* as the product of (integer) powers of primes:

$$p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s} \tag{9.1}$$

This product is called the *prime power decomposition.* For example,

$$\begin{aligned} 6 &= 2^1 3^1, \\ 12 &= 3 \times 4 = 3^1 2^2, \\ 80 &= 16 \times 5 = 2^4 5^1, \\ 60 &= 4 \times 15 = 4 \times 3 \times 5 = 2^2 3^1 5^1. \end{aligned}$$

Theorem 9.3 Suppose that $n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ is the prime power decomposition of n, $n > 1$, and r is the smallest of the quantities

$$(p_1^{t_1} - 1), (p_2^{t_2} - 1), \ldots, (p_s^{t_s} - 1).$$

Then there is an orthogonal family of r Latin squares of order n.

We prove this theorem below. To illustrate it, we recall that $12 = 2^2 3^1$. Then

$$2^2 - 1 = 3, \quad 3^1 - 1 = 2,$$

so $r = 2$. It follows that there exist two orthogonal Latin squares of order 12. This does not say that there is not a larger orthogonal family of 12×12's. Note that Theorem 9.2 does not apply, since 12 is not a power of a prime.

Let us try to apply Theorem 9.3 to $n = 6$. We have $6 = 2^1 3^1$. Since

$$2^1 - 1 = 1, \quad 3^1 - 1 = 2,$$

$r = 1$, and we do not even know from Theorem 9.3 if there exists a pair of orthogonal 6×6 Latin squares. The famous mathematician Euler conjectured in 1782 that there was no such pair. For more than 100 years, the conjecture could neither be proved nor disproved. Around 1900, Tarry looked systematically at all possible pairs of 6×6 Latin squares. (There are 812,851,200; but by making the first row 123456, it is only necessary to consider 9408 pairs.) He succeeded in proving that Euler was right. Thus, there does not exist a pair of orthogonal Latin squares of order 6 (see Tarry [1900, 1901]; see Stinson [1984] for a modern proof that doesn't just consider all cases).

The following is a corollary of Theorem 9.3.

Corollary 9.3.1 Suppose that $n > 1$ and either 2 does not divide n or the prime power decomposition of n is

$$n = 2^{t_1} p_2^{t_2} p_3^{t_3} \cdots,$$

with $t_1 > 1$. Then there is a pair of orthogonal Latin squares.

Proof. If $t_1 > 1$,

$$2^{t_1} - 1 \geq 3.$$

Each other p_i is greater than 2, so

$$p_i^{t_i} - 1 \geq 2.$$

It follows that $r \geq 2$. Q.E.D.

Corollary 9.3.1 leaves open the question of the existence of pairs of orthogonal Latin squares of order $n = 2k$ where 2 does not divide k. Euler, also in 1782, conjectured that there does not exist a pair of orthogonal Latin squares of order n for all such n. He was right for $n = 2$ and $n = 6$. However, contrary to his usual performance, he was wrong otherwise. It was not until 1960 that he was proved wrong.

Theorem 9.4 (Bose, Shrikhande, and Parker [1960]) If $n > 6$, $n = 2k$, and 2 does not divide k, then there is a pair of orthogonal Latin squares of order n.

We can now summarize what we know about the existence of pairs of orthogonal Latin squares.

Theorem 9.5 There is a pair of orthogonal Latin squares of order n for all $n > 1$ except $n = 2$ or 6.

Thus, the existence of pairs of orthogonal Latin squares is completely settled. This is not the case for larger families of orthogonal Latin squares. For $n = 2, 3, \ldots, 9$, the size of the largest orthogonal family of $n \times n$ Latin squares is known. For by Theorems 9.2 and 9.5, it is $n - 1$ for $n = 3, 4, 5, 7, 8, 9$, and it is 1 for $n = 2, 6$. However, for $n = 10$, it is not even known if there is a family of three pairwise orthogonal $n \times n$ Latin squares.

Example 9.7 The Problem of the 36 Officers Euler encountered the notion of orthogonal Latin squares not in connection with experimental design, but in connection with the following problem. There are 36 officers, six officers of six different ranks in each of six regiments. Find an arrangement of the 36 officers in a 6×6 square formation such that each row and each column contains one and only one officer of each rank and one and only one officer from each regiment and there is only one officer from each regiment of each rank. Can this be done? The officers must be arranged so that their ranks form a Latin square and also so that their regiments form a Latin square. Moreover, the pairs of rank and regiment appear once and only once, so the two squares must be orthogonal. We now know that this cannot be done. ■

9.2.4 Proof of Theorem 9.3[4]

To prove Theorem 9.3, we first prove the following result.

Theorem 9.6 (MacNeish [1922]) Suppose that there is an orthogonal family of r Latin squares of order m and another orthogonal family of r Latin squares of order n. Then there is an orthogonal family of r Latin squares of order mn.

Proof. Let $A^{(1)}, A^{(2)}, \ldots, A^{(r)}$ be pairwise orthogonal Latin squares of order m and $B^{(1)}, B^{(2)}, \ldots, B^{(r)}$ be pairwise orthogonal Latin squares of order n. For $e = 1, 2, \ldots, r$, let $(a_{ij}^{(e)}, B^{(e)})$ represent the $n \times n$ matrix whose u, v entry is the ordered pair $(a_{ij}^{(e)}, b_{uv}^{(e)})$. For instance, suppose that $A^{(1)}, A^{(2)}, B^{(1)}$, and $B^{(2)}$ are as in Table 9.14. Then $(a_{12}^{(1)}, B^{(1)})$ and $(a_{32}^{(2)}, B^{(2)})$ are as shown in the table. Let $C^{(e)}$ be the matrix that can be represented schematically as follows:

$$C^{(e)} = \begin{bmatrix} (a_{11}^{(e)}, B^{(e)}) & (a_{12}^{(e)}, B^{(e)}) & \cdots & (a_{1m}^{(e)}, B^{(e)}) \\ (a_{21}^{(e)}, B^{(e)}) & (a_{22}^{(e)}, B^{(e)}) & \cdots & (a_{2m}^{(e)}, B^{(e)}) \\ & & \cdots & \\ (a_{m1}^{(e)}, B^{(e)}) & (a_{m2}^{(e)}, B^{(e)}) & \cdots & (a_{mm}^{(e)}, B^{(e)}) \end{bmatrix}.$$

Then $C^{(e)}$ is an $mn \times mn$ matrix. We shall show that $C^{(1)}, C^{(2)}, \ldots, C^{(r)}$ is an orthogonal family of Latin squares of order mn.

To see that $C^{(e)}$ is a Latin square, note first that in a given row, two entries in different columns are given by $(a_{ij}^{(e)}, b_{uv}^{(e)})$ and $(a_{ik}^{(e)}, b_{uw}^{(e)})$; so they are distinct since $A^{(e)}$ and $B^{(e)}$ are Latin squares. In a given column, two entries in different rows are given by $(a_{ij}^{(e)}, b_{uv}^{(e)})$ and $(a_{kj}^{(e)}, b_{wv}^{(e)})$; so again they are distinct because $A^{(e)}$ and $B^{(e)}$ are Latin squares.

To see that $C^{(e)}$ and $C^{(f)}$ are orthogonal, suppose that

$$\langle (a_{ij}^{(e)}, b_{uv}^{(e)}), (a_{ij}^{(f)}, b_{uv}^{(f)}) \rangle = \langle (a_{pq}^{(e)}, b_{st}^{(e)}), (a_{pq}^{(f)}, b_{st}^{(f)}) \rangle.$$

[4] This subsection may be omitted.

Table 9.14: Orthogonal Latin Squares $A^{(1)}$, $A^{(2)}$, $B^{(1)}$, $B^{(2)}$; Matrices $\left(a_{12}^{(1)}, B^{(1)}\right)$, $\left(a_{32}^{(2)}, B^{(2)}\right)$

$$A^{(1)} = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline\end{array}\,, \qquad A^{(2)} = \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \\ \hline\end{array}$$

$$B^{(1)} = \begin{array}{|cccc|}\hline 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \\ \hline\end{array}\,, \qquad B^{(2)} = \begin{array}{|cccc|}\hline 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ \hline\end{array}$$

$$\left(a_{12}^{(1)}, B^{(1)}\right) = \begin{bmatrix} (2,4) & (2,3) & (2,2) & (2,1) \\ (2,3) & (2,4) & (2,1) & (2,2) \\ (2,2) & (2,1) & (2,4) & (2,3) \\ (2,1) & (2,2) & (2,3) & (2,4) \end{bmatrix}, \quad \left(a_{32}^{(2)}, B^{(2)}\right) = \begin{bmatrix} (3,2) & (3,1) & (3,4) & (3,3) \\ (3,4) & (3,3) & (3,2) & (3,1) \\ (3,3) & (3,4) & (3,1) & (3,2) \\ (3,1) & (3,2) & (3,3) & (3,4) \end{bmatrix}$$

Then it follows that

$$(a_{ij}^{(e)}, a_{ij}^{(f)}) = (a_{pq}^{(e)}, a_{pq}^{(f)}),$$

so by orthogonality of $A^{(e)}$ and $A^{(f)}$, $i = p$ and $j = q$. Similarly, orthogonality of $B^{(e)}$ and $B^{(f)}$ implies that $u = s$ and $v = t$. Q.E.D.

Proof of Theorem 9.3. By Theorem 9.2, for $i = 1, 2, \ldots, s$, there is an orthogonal family of $p_i^{t_i} - 1$ Latin squares of order $p_i^{t_i}$. Thus, for $i = 1, 2, \ldots, s$, there is an orthogonal family of r Latin squares of order $p_i^{t_i}$. The result follows from Theorem 9.6 by mathematical induction on s. Q.E.D.

9.2.5 Orthogonal Arrays with Applications to Cryptography[5]

Suppose that V is a set of n elements and $k \geq 2$ is an integer. An *orthogonal array* OA(k, n) is an $n^2 \times k$ matrix A whose entries are elements of V and so that within any two columns of A, every ordered pair (a, b) with a, $b \in V$ occurs in exactly one row of A. Table 9.15 shows an OA$(4, 3)$ with $V = \{1, 2, 3\}$ and an OA$(5, 4)$ with $V = \{1, 2, 3, 4\}$.

There is a very simple relationship between orthogonal arrays and families of orthogonal Latin squares.

Theorem 9.7 There is an OA(k, n) if and only if there is a family of $k - 2$ orthogonal Latin squares of order n.

[5] This subsection depends heavily on Stinson [2003].

Table 9.15: An OA(4, 3) and an OA(5, 4)

$$\begin{bmatrix} 2 & 2 & 2 & 2 \\ 2 & 1 & 1 & 1 \\ 2 & 3 & 3 & 3 \\ 1 & 2 & 1 & 3 \\ 1 & 1 & 3 & 2 \\ 1 & 3 & 2 & 1 \\ 3 & 2 & 3 & 1 \\ 3 & 1 & 2 & 3 \\ 3 & 3 & 1 & 2 \end{bmatrix}. \quad \begin{bmatrix} 1 & 4 & 4 & 4 & 4 \\ 2 & 4 & 3 & 2 & 1 \\ 2 & 3 & 4 & 1 & 2 \\ 3 & 3 & 1 & 2 & 4 \\ 4 & 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 4 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 3 & 4 \\ 1 & 3 & 3 & 3 & 3 \\ 4 & 1 & 4 & 2 & 3 \\ 3 & 4 & 2 & 1 & 3 \\ 4 & 2 & 3 & 1 & 4 \\ 1 & 2 & 2 & 2 & 2 \\ 3 & 1 & 3 & 4 & 2 \\ 2 & 2 & 1 & 4 & 3 \\ 3 & 2 & 4 & 3 & 1 \end{bmatrix}.$$

Proof. Suppose, without loss of generality, that entries in the orthogonal arrays and Latin squares come from the set $V = \{1, 2, \ldots, n\}$. Let $A^{(1)}, A^{(2)}, \ldots, A^{(k-2)}$ denote the $k-2$ orthogonal Latin squares of order n. Form the matrix A whose rows are the n^2 sequences

$$i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(k-2)},$$

where i, $j \in \{1, 2, \ldots, n\}$ and $a_{ij}^{(l)}$ or $A^{(l)}(i, j)$ is the i, j entry of the matrix $A^{(l)}$. To see that A is an OA(k, n), consider columns u and v of A. If $u = 1$ and $v = 2$, obviously every ordered pair (i, j) from $V \times V$ occurs in these two columns, in the row corresponding to (i, j). If $u = 1$ or 2 and $v \geq 3$, every ordered pair (i, j) appears since every column of $A^{(v)}$ is a permutation of $\{1, 2, \ldots, n\}$. Finally, if u, $v \geq 3$, every ordered pair (i, j) appears since $A^{(u)}$ and $A^{(v)}$ are orthogonal.

Conversely, suppose that A is an OA(k, n) on $V = \{1, 2, \ldots, n\}$. We define $A^{(u)}$, $u \in \{1, 2, \ldots, k-2\}$, as follows. Given i and j, there is a unique r so that $i = A(r, 1)$ and $j = A(r, 2)$. Then let

$$a_{ij}^{(u)} = A(r, u+2).$$

It is not hard to show that $A^{(1)}, A^{(2)}, \ldots, A^{(k-2)}$ defined this way are orthogonal Latin squares of order n. Proof is left as an exercise (Exercise 21). Q.E.D.

Example 9.8 Authentication Codes in Cryptography In cryptography, we are concerned with checking the authenticity of messages. We use codes to help us encrypt those messages so they will be hard to modify, steal, or otherwise falsify. For more on codes, see Chapter 10. Suppose that A sends a message to B. In the theory of cryptography, we usually refer to A as Alice and B as Bob. Alice sends a message by email or fax or from her cellular telephone, all insecure channels. Bob wants to be sure that the message was really sent by Alice and, also, that no one altered the message that Alice sent. The message could be an order to purchase something, for example, so this problem is a central one in electronic commerce.

We shall consider the possibility that an outsider O, to be called Oscar, interferes with the message sent from Alice to Bob. Let us suppose that Oscar can simply send a message to Bob impersonating Alice, or that Oscar can modify a message sent by Alice. Bob and Alice protect against Oscar's "attacks" by sending, along with a message, an authentication code. Let M be the set of possible messages, C be a set of "authenticators," and K be a set of "keys." Alice and Bob agree on a key beforehand, when they meet in person or over a secure channel. Let us suppose that they choose the key from K at random. Associated with each key $k \in K$ is an *authentication rule* r_k that assigns an authenticator $r_k(m) \in C$ to each message $m \in M$. If Alice wants to send message m to Bob, she sends the message (m, c), where $c = r_k(m)$. When Bob receives the message (m, c), he checks that, in fact, c is $r_k(m)$. If not, Bob has reason to believe that Oscar did something and he doubts the message. Of course, it is possible that Oscar might have guessed $r_k(m)$ correctly, and thus this process will not detect all attacks by Oscar. However, Alice and Bob will be happy if the probability that this will happen is small and independent of the actual message that is sent.

Orthogonal arrays can be used to construct authentication rules. Suppose that $M = \{1, 2, \ldots, p\}$, $C = \{1, 2, \ldots, n\}$, and $K = \{1, 2, \ldots, n^2\}$. Let matrix A be an OA(p, n), with rows indexed by elements of K and columns by elements of M. Define $r_k(m) = a_{km}$.

What is the probability, if Oscar sends a message (m, c) to Bob, that in fact $c = r_k(m)$? We call this the *impersonation probability.* We can assume that Oscar knows the matrix A, but Oscar doesn't know which $k \in K$ is being used. Given m and c, there are n possible rows i of matrix A such that $a_{im} = c$, and there are n^2 rows of A. Hence, if $c = r_k(m)$, the probability that Oscar will choose a row i so that $r_i(m)$ is also equal to c is $n/n^2 = 1/n$. This code thus gives Oscar only a one in n chance of impersonating Alice.

What if Oscar simply replaces a message (m, c) that Alice sends by another message (m', c')? The *deception probability* is the probability that $c' = r_k(m')$. In other words, the deception probability is the probability that Bob will think that the message he received is authentic, thus falling for Oscar's deception. Oscar saw that Alice sent message (m, c), so he knows that $r_k(m) = c$, but he doesn't know k. He has to hope that $r_k(m') = c'$. For any two columns m, m' of A, the ordered pair (c, c') appears in those two columns in exactly one row of A. There are n rows of A in which c appears in column m. Thus, if Oscar picks one of those rows at random, the chances of his picking a row in which c' appears in column m are $1/n$. Therefore, the deception probability is $1/n$.

The authentication code Alice and Bob will choose will depend on how small they want the impersonation and deception probabilities to be. For further information about authentication codes, see Colbourn and Dinitz [1996]. ■

Example 9.9 Threshold Schemes and Secret Sharing There are situations where a decision or action is sufficiently sensitive that it must require concurrence by more than one member of a group. This is the case, for example, with the secret codes for setting off a nuclear attack, or in banks when more than one person is needed to identify the secret combination needed to open the vault.

Suppose that I is a set of p people, κ is a secret key to initiating an action (such as opening the vault or unleashing the attack), $q \geq 2$ is a fixed integer, and we want to make sure that any q of the people in the group can together determine κ, while no subgroup of fewer than q people can do so. A method for accomplishing this with high probability is called a (q,p)-*threshold scheme.* Fix a set K of keys and identify a leader not in I. The leader gives each person partial information about κ, chosen from a set P of partial information. The leader has to do this so that partial information available to any q people is enough to figure out κ, whereas that available to smaller subgroups is not. We consider the case $q = 2$.

Suppose that $K = P = \{1, 2, \ldots, n\}$, and let A be an orthogonal array OA$(p+1, n)$. Associate the first p columns of A with the participants and the last column with the keys. All people in the group are given A. Given $\kappa \in K$, let $R_\kappa = \{i : a_{i,p+1} = \kappa\}$ be the set of rows whose last entry is κ. The leader chooses a row $i \in R_\kappa$ at random and gives the partial information a_{iu} to the uth person.

Can person u and person v determine the key κ? Suppose that u gets partial information p_u and v gets partial information p_v. Since there is a unique row i with $a_{ru} = p_u$, $a_{rv} = p_v$, u and v can determine r and, therefore, can find $a_{r,p+1}$, which is the key κ they need.

Can any one person u determine κ based solely on his or her partial information p_u? For any possible value κ' of the key, there is a unique row i for which $a_{iu} = p_u$, $a_{i,p+1} = \kappa'$. Person u has no way of knowing (without sharing information with someone else) which of the n possible rows i is correct (i.e., was chosen by the leader). Thus, the probability of u correctly guessing the key based solely on his partial information is $1/n$. Therefore, we have found a $(2,p)$-threshold scheme that works with high probability.

For further information about threshold schemes and secret sharing, see Colbourn and Dinitz [1996]. ■

EXERCISES FOR SECTION 9.2

1. For each pair of Latin squares in Table 9.16, determine if it is orthogonal.
2. Check that the three Latin squares of Table 9.11 form an orthogonal family.
3. For each family of Latin squares of Table 9.17, determine if it is orthogonal.
4. Suppose that A is an $n \times n$ Latin square. For each of the following operations, determine if it results in a new Latin square.

   (a) Interchange the entries 2 and 4 whenever they occur.

   (b) Replace each row by going from last to first.

Table 9.16: Pairs of Latin Squares for Exercises of Section 9.2

1	2	3
2	3	1
3	2	1

1	2	3
3	1	2
2	3	1

(a)

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

1	2	3	4
3	4	1	2
2	3	4	1
4	1	2	3

(b)

1	2	3	4	5
2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1
1	2	3	4	5

(c)

1	2	3	4	5	6
6	1	2	3	4	5
2	3	4	5	6	1
5	6	1	2	3	4
3	4	5	6	1	2
4	5	6	1	2	3

1	2	3	4	5	6
2	3	4	5	6	1
5	6	1	2	3	4
3	4	5	6	1	2
4	5	6	1	2	3
6	1	2	3	4	5

(d)

Table 9.17: Families of Latin Squares for Exercises of Section 9.2

1	3	2	4
3	1	4	2
2	4	1	3
4	2	3	1

3	1	4	2
2	4	1	3
1	3	2	4
4	2	3	1

2	4	1	3
1	3	4	2
3	1	4	2
4	2	3	1

(a)

1	2	3	4	5
2	3	4	5	2
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4

1	2	3	4	5
3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3

1	2	3	4	5
5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1

(b)

Table 9.18: An Orthogonal Family of Latin Squares

5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1
1	2	3	4	5

4	5	1	2	3
2	3	4	5	1
5	1	2	3	4
3	4	5	1	2
1	2	3	4	5

3	4	5	1	2
5	1	2	3	4
2	3	4	5	1
4	5	1	2	3
1	2	3	4	5

2	3	4	5	1
3	4	5	1	2
4	5	1	2	3
5	1	2	3	4
1	2	3	4	5

(c) Replace A by its transpose.

5. For which of the following numbers n can you be sure that there is an orthogonal family of 3 Latin squares of order n? Why?

   (a) $n = 12$ (b) $n = 17$ (c) $n = 21$ (d) $n = 24$
   (e) $n = 33$ (f) $n = 36$ (g) $n = 55$ (h) $n = 75$
   (i) $n = 161$ (j) $n = 220$ (k) $n = 369$ (l) $n = 539$

6. If $n = 539$, show that there is a set of 10 pairwise orthogonal Latin squares of order n.

7. If $n = 130$, does there exist a pair of orthogonal Latin squares of order n? Why?

8. Does there exist a pair of orthogonal Latin squares of order 12? Why?

9. If n is divisible by 4, can you be sure (with the theorems we have stated) whether or not there is a set of three pairwise orthogonal Latin squares of order n? Give a reason for your answer.

10. For the orthogonal family of Latin squares of order 5 in Table 9.18, use the procedure in the proof of Theorem 9.1 to rearrange elements so that the first row of each Latin square is 12345.

11. Suppose that two orthogonal 8×8 Latin squares both have 87654321 as the first row.

    (a) Is it possible for them to have the same $2, 4$ entry?

    (b) What does your answer tell you about the number of possible 8×8 pairwise orthogonal Latin squares each of which has 87654321 as the first row?

12. Suppose that two orthogonal 7×7 Latin squares both have 1234567 as the last row.

    (a) Is it possible for them to have the same $1, 3$ entry?

    (b) What does your answer tell you about the number of possible 7×7 pairwise orthogonal Latin squares each of which has 1234567 as the last row?

13. Suppose that two orthogonal 4×4 Latin squares both have 1234 as the main diagonal.

    (a) Is it possible for them to have the same $2, 3$ entry?

    (b) What does your answer tell you about the number of possible 4×4 pairwise orthogonal Latin squares each of which has 1234 as the main diagonal?

14. Use the Latin squares of Table 9.14 to find a pair of orthogonal Latin squares of order 12.
15. Find a pair of orthogonal Latin squares of order 9.
16. If there exists a pair of orthogonal Latin squares of order n, and A is a Latin square of order n, A is not necessarily a member of an orthogonal pair of Latin squares. Give an example to illustrate this.
17. Given the OA$(4, 3)$ of Table 9.15, find two orthogonal Latin squares from it.
18. Given the OA$(5, 4)$ of Table 9.15, find three pairwise orthogonal Latin squares from it.
19. Given the two orthogonal Latin squares of Table 9.10, find a corresponding orthogonal array OA$(4, 4)$.
20. Given the orthogonal family of three Latin squares of Table 9.13, find a corresponding orthogonal array OA$(5, 4)$.
21. Complete the proof of Theorem 9.7.
22. For which of the following values of p and n does there exist an OA(p, n)?

    (a) $p = 3$, $n = 81$ (b) $p = 4$, $n = 6$ (c) $p = 4$, $n = 63$

23. (Stinson [2003])

    (a) If Alice and Bob deal with a set of 200 possible messages and want to be sure to limit the probability of impersonation by Oscar to less than 1/1000, explain how an orthogonal array OA$(200, 1009)$ would help them.

    (b) Show that there is such an orthogonal array.

    (c) Explain why a number smaller than 1009 in OA$(200, 1009)$ was not used.

24. In Example 9.8, assume that Oscar has information that limits the possible keys to a fixed subset of size s. How does this change the probability of impersonation?
25. (Stinson [2003])

    (a) If a group of 10 people wants to build a $(2, 10)$-threshold scheme and to be sure that the probability that any one person can guess the secret key is less than 1/100, explain how an orthogonal array OA$(11, 101)$ can accomplish this.

    (b) Show that there is such an orthogonal array.

26. (Stinson [1990, 2003]) In Example 9.8, suppose that the method of authentication rules is used, but do not assume that the rules are determined from an orthogonal array. Show that the probability of impersonation is always at least $1/|C|$ and equals $1/|C|$ if and only if $|\{k : r_k(m) = c\}| = |K|/|C|$, for all $m \in M$, $c \in C$.
27. (Stinson [1990, 2003]) In the situation of Exercise 26, suppose that the probability of impersonation is $1/|C|$. Show that the probability of deception is at least $1/|C|$ and it is equal to $1/|C|$ if and only if $|\{k : r_k(m) = c\} \cap \{k : r_k(m') = c'\}| = |K|/|C|$, for all $m, m' \in M$, $c, c' \in C$.
28. (Stinson [1990, 2003]) In the situation of Exercise 26, show that if $|M| = p$, $|C| = n$, and if the probability of impersonation and the probability of deception are both $1/n$, then $|K| \geq n^2$, with equality if and only if the authentication rules define the rows of an orthogonal array OA(p, n). (This shows that the orthogonal arrays give authentication rules that minimize the number of keys required.)

9.3 FINITE FIELDS AND COMPLETE ORTHOGONAL FAMILIES OF LATIN SQUARES[6]

In this section we aim to present a constructive proof of Theorem 9.2, namely, that if $n > 1$ and $n = p^k$ for p prime, there is a complete orthogonal family of Latin squares of order n. We begin with some mathematical preliminaries.

9.3.1 Modular Arithmetic

Arithmetics with only finitely many numbers underlie the construction of combinatorial designs. They are also vitally important in computing, where there are practical bounds on the size of the sets of integers that can be considered. In this subsection we introduce a simple example of an arithmetic with only finitely many elements, modular arithmetic. In Section 9.3.3 we introduce a general notion of an arithmetic with only finitely many elements: namely, a finite field. Then we use finite fields to construct complete orthogonal families of Latin squares. Modular arithmetic and finite fields underlie the operation of the shift registers that operate in a computer to take a bit string and produce another one. For a discussion of this application, see, for example, Fisher [1977].

Let us consider the remainders left when integers are divided by the number 3. We find that

$$\begin{array}{rclrclrcl}
0 &=& 0\cdot 3+0, & 1 &=& 0\cdot 3+1, & 2 &=& 0\cdot 3+2,\\
3 &=& 1\cdot 3+0, & 4 &=& 1\cdot 3+1, & 5 &=& 1\cdot 3+2,\\
6 &=& 2\cdot 3+0, & 7 &=& 2\cdot 3+1, & 8 &=& 2\cdot 3+2,\\
9 &=& 3\cdot 3+0, & 10 &=& 3\cdot 3+1, & 11 &=& 3\cdot 3+2.
\end{array}$$

The remainder is always one of the three integers $0, 1,$ or 2. We say that two integers a and b are *congruent modulo* 3, and write $a \equiv b \pmod 3$, if they leave the same remainder on division by 3. For instance, $2 \equiv 5 \pmod 3$ and $1 \equiv 7 \pmod 3$. In general, if $a, b,$ and n are integers, we say that a is *congruent to* b *modulo* n, and write $a \equiv b \pmod n$ if a and b leave the same remainder on division by n. For instance, $29 \equiv 17 \pmod 4$, since $29 = 7\cdot 4 + 1$ and $17 = 4 \cdot 4 + 1$. Congruence modulo 12 is used every day when we look at a clock. The hands of the clock indicate the hour modulo 12. Similarly, the mileage indicator in a car gives the mileage the car has traveled modulo 1,000,000 (depending on its make and model).

For all its beauty and functionality, a major software snafu was "created" due to modular arithmetic. The *Year 2000 problem* (Y2K) arose due to the internal workings of some computer software. Many software developers used a two-digit indicator when recording a year; the 1900s was being assumed. For example, using 2/17/59, the "59" refers to 1959. Thus, the two digits were modulo 100. The Y2K problem came to light when it was realized that in the year 2000, this same software would not be able to distinguish between the years 1900 and 2000 when using a 00 designation.

[6] This section may be omitted without loss of continuity. As an alternative, the reader might wish to read all but Section 9.3.5.

Table 9.19: The Operations + and × of Addition and Multiplication Modulo 2 on Z_2

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Table 9.20: The Operations + and × of Addition and Multiplication Modulo 3 on Z_3

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Let us now fix a number n and consider the set of integers $Z_n = \{0, 1, 2, \ldots, n-1\}$. Every integer is congruent modulo n to one of the integers in the set Z_n. If we add two integers in the set Z_n, their sum is not necessarily in the set. However, their sum is congruent to an element in Z_n. In performing *modular addition*, if a and b are in Z_n, we *define* $a + b$ to be that number in Z_n which is congruent to the ordinary sum of a and b, modulo n. For instance, suppose that $n = 3$. Then $2+2$ is 4 in ordinary arithmetic, which is congruent to 1, modulo 3. Hence, in addition modulo 3, $2+2$ is 1. Similarly, $1+2$ is 0 and $1+1$ is 2. In addition modulo 4, $3+3$ is 2 and $2+2$ is 0. Modular multiplication works similarly. If a, b are in Z_n, we define $a \times b$ to be that integer in Z_n congruent to the ordinary product of a and b, modulo n. For instance, in multiplication modulo 3, 2×2 is 1, since the ordinary product of 2 and 2 is 4, which is congruent to 1 modulo 3. Similarly, in multiplication modulo $4, 3 \times 3$ is 1 and 2×2 is 0.

We can summarize the *operations* + and × on Z_n by giving addition and multiplication tables. Tables 9.19 and 9.20 give these tables for the cases $n = 2$ and $n = 3$, respectively. In these tables, the elements of Z_n are listed in the same order along both rows and columns and the entry in the row corresponding to a and the column corresponding to b is $a + b$ or $a \times b$, depending on the table.

9.3.2 Modular Arithmetic and the RSA Cryptosystem[7]

Sending sensitive information (for example, credit card numbers) over the Internet has created much interest in cryptographic codes, codes whose goal is to conceal information. (Once information is concealed, it may be encoded to ensure correct transmission and decoding. Coding theory, in particular error-correcting and

[7] This section follows Hill [1991]. It may be omitted.

error-detecting codes, is the subject of Chapter 10.) We shall describe a "public-key cryptosystem" developed by Rivest, Shamir, and Adleman [1978], now called RSA, and based on the work of Diffie and Hellman [1976]. RSA was discussed in Section 7.1.3.

Suppose that you need to send your credit card number to a retail store over the Internet. How can you change this number (encrypt it) so that others don't have access to it if the transmission is read by someone other than at the intended store? The answer is based on prime numbers and modular arithmetic.

First, a theorem about prime numbers is needed.

Theorem 9.8 (Fermat's Little Theorem) If p is a prime, x a positive integer, and $x \not\equiv 0 \pmod{p}$, then

$$x^{p-1} \equiv 1 \pmod{p}.$$

Proof.[8] Consider the set $A = \{1x, 2x, 3x, \ldots, (p-1)x\}$. The elements of A are all distinct modulo p. (To see this, suppose not, i.e., that $ix \equiv jx \pmod{p}$ for $1 \leq i \neq j \leq p-1$. Since $x \not\equiv 0 \pmod{p}$, x^{-1} exists. Then multiplying both sides by x^{-1} results in $i \equiv j \pmod{p}$, which implies that $i = j$ since $1 \leq i, j < p$; a contradiction.) Also, since $x \not\equiv 0 \pmod{p}$, each element of A, ix, is $\not\equiv 0 \pmod{p}$ since $1 \leq i \leq p-1$. Thus, $\{1x \pmod{p}, 2x \pmod{p}, \ldots, (p-1)x \pmod{p}\} = \{1, 2, \ldots, p-1\}$. Hence,

$$(1x)(2x)\cdots((p-1)x) \equiv (1)(2)\cdots(p-1) \pmod{p}$$

or

$$(p-1)!x^{p-1} \equiv (p-1)! \pmod{p}.$$

It is clear that $(p-1)! \not\equiv 0 \pmod{p}$, so $[(p-1)!]^{-1}$ exists. Multiplying both sides by $[(p-1)!]^{-1}$ finishes the proof. Q.E.D.

To use RSA, the store chooses two distinct and extremely large prime numbers p and q. It then computes $r = pq$ and finds two positive integers s and t such that

$$st \equiv 1 \pmod{(p-1)(q-1)},$$

i.e., so that $st = j(p-1)(q-1) + 1$ for some integer j. The store then makes publicly known r and s (hence the term *public-key*). As an example, suppose the store chooses the primes $p = 37$ and $q = 23$. Thus, $r = 37 \cdot 23 = 851$, and the store can choose $s = 5$ and $t = 317$ since

$$5 \cdot 317 = 1585 = 2(36)(22) + 1 = 2(37-1)(23-1) + 1 \equiv 1 \; [\text{mod } (37-1)(23-1)].$$

(Other choices for s and t are possible. However, it is wise to avoid either of them being 1.) It is important to note that the store does not make public p, q, or t, only r and s.

[8] The proof may be omitted. It uses well-known properties of modular arithmetic that are not developed in detail here. See Exercise 9 for an alternative proof.

To encrypt your credit card number n before sending it over the Internet, you calculate and send

$$m = n^s \pmod{r}. \tag{9.2}$$

The two questions that arise are: (1) If someone steals this number m, how could they find your credit card number n? (2) When the store receives this number m, how do they calculate (*decrypt*) your credit card number n? Both questions are important.

The store computes $m^t \pmod{r}$ and, using Fermat's Little Theorem (Theorem 9.8), finds your credit card number n. Note that the store essentially only needs t for the decryption! For $m^t \equiv n^{st} \pmod{r}$ by Equation (9.2) and $n^{st} = n^{j(p-1)(q-1)+1}$. Next, if $n \not\equiv 0 \pmod{p}$, then $n^{j(p-1)(q-1)+1} = \left(n^{p-1}\right)^{j(q-1)} n \equiv n \pmod{p}$ by Fermat's Little Theorem (Theorem 9.8). And if $n \equiv 0 \pmod{p}$, then certainly $n^{j(p-1)(q-1)+1} \equiv n \pmod{p}$. In either case, p must be a factor of $n^{j(p-1)(q-1)+1} - n$. Similarly, q must be a factor of $n^{j(p-1)(q-1)+1} - n$. Since p and q are distinct primes and $r = pq$,

$$n^{j(p-1)(q-1)+1} \equiv n \pmod{r} = n,$$

which is your credit card number, as long as your credit card number is not larger than r. This will not be the case since the security of this system is based on using a very large r.

Actually, the security of the entire system is based on the unavailability of t. Since r and s are publicly known, why can't t be deduced from them by someone who wants to steal your credit card number? The answer lies in the fact that this would require knowledge of the original primes p and q, i.e., the ability to factor $r = pq$. However, prime factorization is a difficult problem. In fact, in the notation of Section 2.18, it is in the class of NP-complete problems. For our example, $r = 851$ would not take long to factor. But if the primes p and q are each 100-digit numbers then factoring r, at about 200 digits, would not be feasible using the present day (i.e., 2003) best-known algorithms and fastest computers (Stinson [2003]). So, as long as no deterministic algorithm, whose complexity is polynomial, is found for prime factorization (and credit card numbers don't exceed 200 digits), RSA cryptosystems should be secure.[9] For more on cryptographic codes and RSA, see Garrett [2001], Joye and Quisquater [1998], Kaliski [1997], Koblitz [1994], Menezes, van Oorschot, and Vanstone [1997], Salomaa [1996], and Sloane [1981].

9.3.3 The Finite Fields GF(p^k)

We turn next to a generalization of the modular arithmetic introduced in Section 9.3.1. Suppose that X is a set. A *binary operation* $\circ$ on X is a function that

[9] In Section 7.1.3 we noted that recent work has shown that the problem of testing whether or not an integer is prime can be done efficiently (i.e., in polynomial time). Although this result does not say anything about the possibility of factoring a number into primes efficiently, it certainly raises the issue as to whether or not this could be done. This is a crucial question since hardness of factoring is so critical in cryptography.

assigns to each ordered pair of elements of X another element of X, usually denoted $a \circ b$. For example, if X is the set of integers, then + and × define binary operations on X. If X is a finite set, we can define a binary operation $\circ$ by giving a table such as those in Tables 9.19 or 9.20.

A *field* $\mathcal{F}$ is a triple $(F, +, x)$, where F is a set and + and × are two binary operations on F (not necessarily the usual operations of + and ×), with certain conditions holding. These are the following:[10]

Condition **F1** (*Closure*).[11] For all a, b in F, $a + b$ is in F and $a \times b$ is in F.

Condition **F2** (*Associativity*). For all a, b, c in F,

$$\begin{aligned} a + (b + c) &= (a + b) + c, \\ a \times (b \times c) &= (a \times b) \times c. \end{aligned}$$

Condition **F3** (*Commutativity*). For all a, b in F,

$$\begin{aligned} a + b &= b + a, \\ a \times b &= b \times a. \end{aligned}$$

Condition **F4** (*Identity*).

(a) There is an element in F, which is denoted 0 and called the *additive identity*, so that for all a in F,

$$a + 0 = a.$$

(b) There is an element in F different from 0, which is denoted 1 and called the *multiplicative identity*, so that for all a in F,

$$a \times 1 = a.$$

Condition **F5** (*Inverse*).

(a) For all a in F, there is an element b in F, called an *additive inverse* of a, so that

$$a + b = 0.$$

(b) For all a in F with $a \neq 0$, there is an element b in F, called a *multiplicative inverse* of a, so that

$$a \times b = 1.$$

[10] Our treatment of fields is necessarily brief. The reader without a background in this subject might consult such elementary treatments as Dornhoff and Hohn [1978], Durbin [1999], Fisher [1977], or Gilbert and Gilbert [1999].

[11] Condition **F1** is actually implicit in our definition of operation.

Condition **F6** (*Distributivity*). For all a, b, c in F,

$$a \times (b + c) = (a \times b) + (a \times c).$$

[Conditions **F1, F2, F4,** and **F5** say that $(F, +)$ is a group in the sense of Chapter 8. Also, if $F' = F$ less the element 0, these conditions also say that $(F', \times)$ is a group, since we can show that $a \times b$ is never 0 if $a \neq 0$ and $b \neq 0$ and we can show that the multiplicative inverse of a is never 0.] Note that it is possible to prove from conditions **F1**–**F6** that the additive and multiplicative inverses of an element a are, respectively, unique; they are denoted, respectively, as $-a$ and a^{-1}.

The following are examples of fields.

1. $(Re, +, \times)$, where Re is the set of real numbers and + and × are the usual addition and multiplication operations.

2. $(Q, +, \times)$, where Q is the set of rational numbers and + and × are the usual addition and multiplication operations.

3. $(C, +, \times)$, where C is the set of complex numbers and + and × are the usual addition and multiplication operations.

However, $(Z, +, \times)$, where Z is the set of integers and + and × are the usual addition and multiplication operations, is not a field. Conditions **F1**–**F4** and **F6** hold. However, part (b) of condition **F5** fails. There is no b in Z so that $2 \times b = 1$.

We now consider some examples of *finite fields*, fields where F is a finite set. Consider $(Z_2, +, \times)$, where + and × are modulo 2. Then this is a field, as is easy to check. Note that 0 and 1 are, respectively, the additive and multiplicative identities. The additive inverse of 1 is 1, since $1 + 1 = 0$, and the multiplicative inverse of 1 is 1, since $1 \times 1 = 1$.

Similarly, $(Z_3, +, \times)$, where + and × are modulo 3, is a field. The additive and multiplicative inverses are again 0 and 1, respectively. Note that the additive inverse of 2 is 1, since $2+1 = 0$. The multiplicative inverse of 2 is 2, since $2 \times 2 = 1$.

Is Z_n under modular addition and multiplication always a field? The answer is no. Consider Z_6. We have $3 \times 2 = 0$. If Z_6 under addition and multiplication modulo 6 is a field, let 2^{-1} denote the multiplicative inverse of 2. We have

$$(3 \times 2) \times 2^{-1} = 0 \times 2^{-1} = 0.$$

However,

$$(3 \times 2) \times 2^{-1} = 3 \times (2 \times 2^{-1}) = 3 \times 1 = 3.$$

We conclude that $0 = 3$, a contradiction.

Theorem 9.9 . For $n \geq 2$, Z_n under addition and multiplication modulo n is a field if and only if n is a prime number.

The proof of Theorem 9.9 is left as an exercise (Exercise 16).

We close this subsection by asking: For what values of n does there exist a finite field of n elements? We shall be able to give an explicit answer. Note that by

Table 9.21: Addition and Multiplication Tables for a Field GF(2^2) of Four Elements

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Theorem 9.9, Z_4 does not define a field under modular addition and multiplication. However, it is possible to define addition and multiplication operations on $\{0, 1, 2, 3\}$ which define a field. Such operations are shown in Table 9.21. Verification that these define a field is left to the reader (Exercise 17). (The reader familiar with algebra will be able to derive these tables by letting $2 = w$ and $3 = 1 + w$ and performing addition and multiplication modulo the irreducible polynomial $1 + w + w^2$ over GF[2], the finite field of 2 elements to be defined below.) The arithmetic of binary numbers which is actually used in many large computers is based on Z_{2^n} for some n. (Here, $n = 2$.) For a discussion of this particular arithmetic, see Dornhoff and Hohn [1978], Hennessy and Patterson [1998, Ch. 4], and Patterson and Hennessy [1998, Appendix A].

If $n = 6$, it is not possible to define addition and multiplication on a set of n elements, such as $\{0, 1, 2, 3, 4, 5\}$, so that we get a finite field. The situation is summarized in Theorem 9.10.

Theorem 9.10 If $(F, +, \times)$ is a finite field, there is a prime number p and a positive integer k so that F has p^k elements. Conversely, for all prime numbers p and positive integers k, there is a finite field of p^k elements.

The proof of this theorem can be found in most books on modern algebra: for instance, any of the references in footnote 10 on page 517. It turns out that there is essentially only one field of p^k elements for p a prime and k a positive integer, in the sense that any two of these fields are isomorphic.[12] The unique field of p^k elements will be denoted GF(p^k). (The letters GF stand for Galois field and are in honor of the famous mathematician Evariste Galois, who made fundamental contributions to modern algebra.)

9.3.4 Construction of a Complete Orthogonal Family of $n \times n$ Latin Squares if n Is a Power of a Prime

We now present a construction of a complete orthogonal family of $n \times n$ Latin squares that applies whenever $n = p^k$, for p prime and k a positive integer, and

[12] Two fields $\mathcal{F}$ and $\mathcal{G}$ are isomorphic if there is a one-to-one mapping from $\mathcal{F}$ onto $\mathcal{G}$ that preserves addition and multiplication.

Table 9.22: The Orthogonal Latin Squares $A^{(1)}$ and $A^{(2)}$ Defined from the Finite Field GF(3) by (9.3)

$$A^{(1)} = \begin{array}{|ccc|}\hline 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ \hline \end{array} \qquad A^{(2)} = \begin{array}{|ccc|}\hline 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \\ \hline \end{array}$$

$n > 1$. This will prove Theorem 9.2. Let $b_1, b_2, \ldots, b_n$ be elements of a finite field GF(n) of $n = p^k$ elements. Let b_1 be the multiplicative identity of this field and b_n be the additive identity. For $e = 1, 2, \ldots, n-1$, define the $n \times n$ array $A^{(e)} = (a_{ij}^{(e)})$ by taking

$$a_{ij}^{(e)} = (b_e \times b_i) + b_j, \tag{9.3}$$

where $+$ and $\times$ are the operations of the field GF(n). In Section 9.3.5 we show that $A^{(e)}$ is a Latin square and that $A^{(1)}, A^{(2)}, \ldots, A^{(n-1)}$ is an orthogonal family. Thus, if $n > 1$, we get a complete orthogonal family of $n \times n$ Latin squares. For instance, if $n = 3$, we use GF(3), whose addition and multiplication operations are addition and multiplication modulo 3, as defined by Table 9.20. We let $b_1 = 1, b_2 = 2$, and $b_3 = 0$. (Remember that b_1 is to be chosen as the multiplicative identity and b_n as the additive identity.) Then we find that $A^{(1)}$ and $A^{(2)}$ are given by Table 9.22. To see how the 1, 2 entry of $A^{(2)}$ was computed, for instance, note that

$$(b_2 \times b_1) + b_2 = (2 \times 1) + 2 = 2 + 2 = 1.$$

It is easy to check directly that $A^{(1)}$ and $A^{(2)}$ of Table 9.22 are Latin squares and that they are orthogonal.

To give another example, suppose that $n = 4$. Then we use GF$(4) = $ GF(2^2), whose addition and multiplication operations are given in Table 9.21. Taking $b_1 = 1, b_2 = 2, b_3 = 3$, and $b_4 = 0$, and using (9.3), we get the three pairwise orthogonal Latin squares of Table 9.23. To see how these entries are obtained, note, for example, that

$$\begin{aligned} a_{23}^{(3)} &= (b_3 \times b_2) + b_3 \\ &= (3 \times 2) + 3 \\ &= 1 + 3 \\ &= 2, \end{aligned}$$

where we have used the addition and multiplication rules of Table 9.21.

Table 9.23: The Orthogonal Family of 4 × 4 Latin Squares Obtained from the Finite Field GF(2^2) of Table 9.21

$$A^{(1)} = \begin{array}{|cccc|}\hline 0 & 3 & 2 & 1 \\ 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 1 & 2 & 3 & 0 \\ \hline \end{array} \qquad A^{(2)} = \begin{array}{|cccc|}\hline 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 0 & 3 & 2 & 1 \\ 1 & 2 & 3 & 0 \\ \hline \end{array} \qquad A^{(3)} = \begin{array}{|cccc|}\hline 2 & 1 & 0 & 3 \\ 0 & 3 & 2 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 \\ \hline \end{array}$$

9.3.5 Justification of the Construction of a Complete Orthogonal Family if $n = p^k$ [13]

To justify the construction of Section 9.3.4, we first show in general that if $A^{(e)}$ is defined by (9.3), then it is a Latin square. Suppose that $a_{ij}^{(e)} = a_{ik}^{(e)}$. Then

$$(b_e \times b_i) + b_j = (b_e \times b_i) + b_k. \tag{9.4}$$

By adding the additive inverse c of $(b_e \times b_i)$ to both sides of (9.4) and using associativity and commutativity of addition, we find that

$$\begin{aligned} (c + [(b_e \times b_i) + b_j]) &= (c + [(b_e \times b_i) + b_k]), \\ ([c + (b_e \times b_i)] + b_j) &= ([c + (b_e \times b_i)] + b_k), \\ 0 + b_j &= 0 + b_k, \\ b_j &= b_k, \\ j &= k. \end{aligned}$$

Thus, all elements of the same row are different.

Next, suppose that $a_{ji}^{(e)} = a_{ki}^{(e)}$. Then

$$(b_e \times b_j) + b_i = (b_e \times b_k) + b_i. \tag{9.5}$$

By adding the additive inverse of b_i to both sides of (9.5) and using associativity of addition, we obtain

$$b_e \times b_j = b_e \times b_k. \tag{9.6}$$

We now multiply (9.6) by the multiplicative inverse a of b_e, which exists since $b_e \neq 0$, and use commutativity and associativity of the × operation. We obtain

$$\begin{aligned} a \times (b_e \times b_j) &= a \times (b_e \times b_k), \\ (a \times b_e) \times b_j &= (a \times b_e) \times b_k, \\ 1 \times b_j &= 1 \times b_k, \\ b_j &= b_k, \\ j &= k. \end{aligned}$$

[13] This subsection may be omitted.

Thus, all elements of the same column are different, and we conclude that $A^{(e)}$ is a Latin square.

Finally, we verify orthogonality of $A^{(e)}$ and $A^{(f)}$, for $e \neq f$. Suppose that

$$(a_{ij}^{(e)}, a_{ij}^{(f)}) = (a_{kl}^{(e)}, a_{kl}^{(f)}).$$

Then

$$a_{ij}^{(e)} = a_{kl}^{(e)} \quad \text{and} \quad a_{ij}^{(f)} = a_{kl}^{(f)},$$

so

$$(b_e \times b_i) + b_j = (b_e \times b_k) + b_l \tag{9.7}$$

and

$$(b_f \times b_i) + b_j = (b_f \times b_k) + b_l. \tag{9.8}$$

Using the properties of fields freely, we subtract (9.8) from (9.7); that is, we add the additive inverse of both sides of (9.8) to both sides of (9.7). This yields

$$(b_e \times b_i) - (b_f \times b_i) = (b_e \times b_k) - (b_f \times b_k),$$

where $-$ means add the additive inverse. Thus, again using the properties of fields freely, we find that

$$(b_e - b_f) \times b_i = (b_e - b_f) \times b_k. \tag{9.9}$$

Finally, since $e \neq f$, it follows that $(b_e - b_f) \neq 0$, so $(b_e - b_f)$ has a multiplicative inverse. Multiplying (9.9) by this multiplicative inverse, we derive the equation

$$b_i = b_k,$$

whence

$$i = k.$$

Now (9.7) gives us

$$(b_e \times b_i) + b_j = (b_e \times b_i) + b_l,$$

from which we derive

$$b_j = b_l,$$
$$j = l.$$

Hence, $i = k$ and $j = l$, and we conclude that $A^{(e)}$ and $A^{(f)}$ are orthogonal. This completes the proof that $A^{(1)}, A^{(2)}, \ldots, A^{(n-1)}$ is an orthogonal family of $n \times n$ Latin squares.

EXERCISES FOR SECTION 9.3

1. For each of the following values of a and n, find a number b in $\{0, 1, \ldots, n-1\}$ so that $a \equiv b \pmod{n}$.

   (a) $a = 37, n = 5$ (b) $a = 42, n = 3$ (c) $a = 8, n = 10$
   (d) $a = 11, n = 9$ (e) $a = 625, n = 71$ (f) $a = 1652, n = 7$

2. For each of the following values of a, b, and n, compute $a+b$ and $a\times b$ using addition and multiplication modulo n.

   (a) $a=2, b=4, n=4$ (b) $a=4, b=5, n=12$ (c) $a=5, b=6, n=9$
   (d) $a=4, b=4, n=15$ (e) $a=3, b=11, n=2$ (f) $a=10, b=11, n=12$

3. Verify the following facts about congruence.

   (a) If $a \equiv b \pmod{n}$, then $b \equiv a (\text{mod } n)$.

   (b) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

   (c) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a+b \equiv a'+b' \pmod{n}$.

   (d) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a \times b \equiv a' \times b' \pmod{n}$.

4. Suppose that $c_1c_2\cdots c_n$ is any permutation of $0,1,2,\ldots,n-1$. Build a matrix A as follows. The first row of A is the permutation $c_1c_2\cdots c_n$. Each successive row of A is obtained from the preceding row by adding 1 to each element and using addition modulo n.

   (a) Build A for the permutation 32401.

   (b) Show that A is always a Latin square.

5. (Williams [1949]) Let $n=2m$ and let

$$0 \quad 1 \quad 2m-1 \quad 2 \quad 2m-2 \quad 3 \quad 2m-3 \quad \cdots \quad m+1 \quad m$$

   be a permutation of $\{0,1,2,...,n-1\}$. Let A be the Latin square constructed from that permutation by the method of Exercise 4.

   (a) Build A for $m=2$.

   (b) Show that for every value of $m \geq 1$, A is *horizontally complete* in the sense that whenever $1 \leq \alpha \leq n$ and $1 \leq \beta \leq n$ and $\alpha \neq \beta$, there is a row of A in which α is followed immediately by β. (Such Latin squares are important in agricultural experiments where we wish to minimize interaction of treatments applied to adjacent plots.)

   (c) For arbitrary $m \geq 1$, is A vertically complete (in the obvious sense)?

6. As opposed to a four-digit representation for the year, some computer software represents a date by the number of seconds that have elapsed since January 1, 1970. The seconds are stored in binary using 32 bits of storage. Eventually, the number of seconds since January 1, 1970 will exceed the 32 bits of storage and result in an incorrect year representation. This has been called the *Unix Time Problem.*

   (a) This representation uses congruence modulo n for what value of n?

   (b) For what date will the Unix Time Problem first occur?

7. Recall the values from Section 9.3.2: $p=37$, $q=23$, $r=851$, $s=5$, and $t=317$.

   (a) If the number $m=852$ is received by the store, find the credit card number of the customer.

   (b) Find m for the credit card number 123-45-6789.

(c) Find another possible s and t pair. That is, find positive integers s and t so that $st = j(37-1)(23-1)+1$ for some positive integer j. (Please avoid the trivial case of s or t being 1.)

8. From Section 9.3.2, suppose that the store chose the prime numbers $p = 37$ and $q = 41$. Then $r = 1517$.

   (a) Find positive integers s and t so that $st = j(37-1)(41-1)+1$ for some positive integer j. (Please avoid the trivial case of s or t being 1.)

   (b) Find m for the credit card number 123-45-6789.

   (c) Find the credit card number if the store receives the number 1163.

9. This exercise provides an alternative proof of Fermat's Little Theorem (Theorem 9.8).

   (a) Show that if p is a prime number, p divides the binomial coefficient $\binom{p}{i}$ for $1 \le i \le p-1$.

   (b) Argue by induction on positive integers x that $x^p \equiv x \pmod{p}$ by using the binomial theorem to expand $(x+1)^p$.

10. Write down the addition and multiplication tables for the following fields.

    (a) GF(5) (b) GF(7) (c) GF(9)

11. (a) Write down the tables for the binary operations of addition and multiplication modulo 4 on the set Z_4.

    (b) Find an element in Z_4 that does not have a multiplicative inverse.

12. Repeat Exercise 11 for addition and multiplication modulo 10 on the set Z_{10}.

13. Find the additive and multiplicative inverse of 8 in each of the following fields.

    (a) GF(11) (b) GF(13) (c) GF(17)

14. Repeat Exercise 13 for 6 in place of 8.

15. Which of the following triples $(F, +, \times)$ define fields?

    (a) F is the *positive* reals, $+$ and $\times$ are ordinary addition and multiplication.

    (b) F is the reals with an additional element ∞. The operations $+$ and $\times$ are the usual addition and multiplication operations on the reals, and in addition we have for all real numbers a,

$$a + \infty = a \times \infty = \infty + a = \infty \times a = \infty + \infty = \infty \times \infty = \infty$$

    (c) F is Re, $a+b$ is ordinary addition, and $a \times b = 1$ for all a, b in F.

    (d) F is Re, and $a + b = a \times b = 0$ for all a, b in F.

16. Consider Z_n under addition and multiplication modulo n and consider the conditions for a field.

    (a) Show that condition **F1** holds.

    (b) Show that condition **F2** holds.

(c) Show that condition **F3** holds.

(d) Show that condition **F4** holds by showing that 0 and 1 are the additive and multiplicative identities, respectively.

(e) Show that condition **F5**(a) holds by showing that $n - a$ is the additive inverse of a.

(f) Show that condition **F6** holds.

(g) Show that condition **F5**(b) fails if n is not a prime number.

(h) Show that condition **F5**(b) holds if n is a prime number. [*Hint:* Use Fermat's Little Theorem (Theorem 9.8) to conclude that $a^{-1} = a^{n-2}$.]

17. Verify that Table 9.21 defines a field.

18. Use the method of Section 9.3.4 to find a complete orthogonal family of Latin squares of the following orders. [Parts (c) and (d) are for the reader with knowledge of modern algebra.]

(a) 5 (b) 7 (c) 8 (d) 9

19. For a given prime number n and integer k with $3 \leq k \leq n$, build an $n^2 \times k$ matrix A as follows: Build one row corresponding to each ordered pair (i, j) for $1 \leq i, j \leq n$. If $1 \leq c \leq k$, the entry in the row corresponding to (i, j) and column c is $i + jc \pmod n$. Show that A is an orthogonal array.

9.4 BALANCED INCOMPLETE BLOCK DESIGNS

9.4.1 (b, v, r, k, λ)-Designs

In Section 9.1 we pointed out that in a block design, it is not always possible to test each treatment in each block. For instance, in testing tire wear, if there are five brands of tires, then, as we observed, only four of these can be tested in any one block. Thus, it is necessary to use an incomplete block design. The basic incomplete block design we shall study is called a balanced incomplete block design. A *balanced block design* consists of a set V of $v \geq 2$ elements called *varieties* or *treatments*, and a collection of $b > 0$ subsets of V, called *blocks*, such that the following conditions are satisfied:

$$\text{each block consists of exactly the same number } k \text{ of varieties, } k > 0; \tag{9.10}$$

$$\text{each variety appears in exactly the same number } r \text{ of blocks, } r > 0; \tag{9.11}$$

$$\begin{gathered}\text{each pair of varieties appears simultaneously in exactly the}\\ \text{same number } \lambda \text{ of blocks, } \lambda > 0.\end{gathered} \tag{9.12}$$

A balanced block design with $k < v$ is called a *balanced incomplete block design* since each block has fewer than the total number of varieties. Such a design is also called a *BIBD*, a (b, v, r, k, λ)-*design*, or a (b, v, r, k, λ)-*configuration*. The basic ideas behind BIBDs were introduced by Yates [1936]. Note that if $k = v$ and no block has repeated varieties, conditions (9.10), (9.11) and (9.12) hold trivially, with $k = v, r = b$, and $\lambda = b$. That is why we will assume that $k < v$ unless indicated otherwise.

Example 9.10 A (7, 7, 3, 3, 1)-Design If $b = 7, v = 7, r = 3, k = 3$, and $\lambda = 1$, there is a (b, v, r, k, λ)-design. It is given by taking the set of varieties V to be $\{1,2,3,4,5,6,7\}$ and using the following blocks:

$$B_1 = \{1,2,4\}, \quad B_2 = \{2,3,5\}, \quad B_3 = \{3,4,6\},$$

$$B_4 = \{4,5,7\}, \quad B_5 = \{5,6,1\}, \quad B_6 = \{6,7,2\}, \quad B_7 = \{7,1,3\}.$$

It is easy to see that each block consists of exactly 3 varieties, that each variety appears in exactly 3 blocks, and that each pair of varieties appears simultaneously in exactly 1 block (e.g., 3 and 6 appear together in B_3 and nowhere else). ■

Example 9.11 A (4, 4, 3, 3, 2)-Design If $b = 4, v = 4, r = 3, k = 3$, and $\lambda = 2$, a (b, v, r, k, λ)-design is given by

$$V = \{1,2,3,4\}$$

and the blocks

$$\{1,2,3\}, \ \{2,3,4\}, \ \{3,4,1\}, \ \{4,1,2\}.$$ ■

In the tire wear example of Section 9.1, the varieties are tire brands and the blocks are the sets of tire brands corresponding to the tires used in a given test car. The conditions (9.10), (9.11), and (9.12) correspond to the following reasonable requirements:

each car uses the same number k of tire brands;
each brand appears on the same number r of cars;
each pair of brands is tested together on the same car the same number λ of times.

It should be clear from our experience with orthogonal families of Latin squares that (b, v, r, k, λ)-designs may not exist for all combinations of the parameters b, v, r, k, and λ. Indeed, the basic combinatorial question of the subject of balanced incomplete block designs is the existence question: For what values of b, v, r, k, λ does a (b, v, r, k, λ)-design exist? We address this question below. In general, it is an unsolved problem to state complete conditions on the parameters b, v, r, k, λ necessary and sufficient for the existence of a (b, v, r, k, λ)-design. A typical reference book on practical experimental design will list, for reasonable values of the parameters, those (b, v, r, k, λ)-designs that do exist. For now, let us give some examples of the use of (b, v, r, k, λ)-designs. Then we shall study the basic existence question in some detail.

Example 9.12 Testing Cloth for Wear (Example 9.6 Revisited) Suppose that we have a Martindale wear tester as described in Example 9.6, and we wish to

Table 9.24: A Youden Square for the Wear Testing Experiment[a]

		Block (run)						
		B_1	B_2	B_3	B_4	B_5	B_6	B_7
Variety (cloth type)	1		p		q		r	s
	2	p			s	r		q
	3		q	p		s		r
	4	q		r			s	p
	5			s	r	q	p	
	6	r	s			q	p	
	7	s	r	q	p			

[a]The i, j entry gives the position of variety i in block B_j.

use it to compare seven different types of cloth. Since only four pieces of cloth can be tested in one run of the machine, an incomplete block design must be used. The number v of varieties is 7 and the blocks will all be of size $k = 4$. Box, Hunter, and Hunter [1978] describe a (b, v, r, k, λ)-design for this situation in which there are 7 blocks ($b = 7$), each type of cloth is run $r = 4$ times, and each pair of cloth types is used together in a run $\lambda = 2$ times. If the cloth types are labeled $1, 2, 3, 4, 5, 6, 7$, the blocks used can be described as

$$B_1 = \{2,4,6,7\}, \quad B_2 = \{1,3,6,7\}, \quad B_3 = \{3,4,5,7\},$$

$$B_4 = \{1,2,5,7\}, \quad B_5 = \{2,3,5,6\}, \quad B_6 = \{1,4,5,6\}, \quad B_7 = \{1,2,3,4\}.$$

Since there were four positions in which to place the cloth, and since the design could be chosen so that each cloth type was used in 4 runs, it was also possible to arrange to place each type of cloth exactly once in each position. Thus, it was possible to control for differences due to machine position. Such an incomplete block design which is balanced for 2 different sources of block variation is called a *Youden square*, after its inventor W. J. Youden (see Youden [1937]). In this case, the Youden square can be summarized in Table 9.24, where p, q, r, and s represent the 4 positions, and the i, j entry gives the position of variety i in block B_j. ■

Example 9.13 Tuberculosis in Cattle Wadley [1948] used balanced incomplete block designs in work on diagnosing tuberculosis in cattle. The disease can be diagnosed by injecting the skin of a cow with an appropriate allergen and observing the thickening produced. In an experiment to compare allergens, the observation for each allergen was the log concentration required to produce a 3-millimeter thickening. This concentration was being estimated by observing the thickenings at four different concentrations and interpolating. Thus, each test of an allergen required a number of injections of the allergen at different concentrations.

In Wadley's experiment, 16 allergens were under comparison. Thus, $v = 16$. On each cow there were four main regions, and in each region about 16 injections could be made. This suggests using each region as a block, with four allergen preparations in each block, each used four times at different concentrations, making 16 injections in all. Thus, $k = 4$. There is a design with $k = 4, v = 16, b = 20$, and $r = 5$. This information is available from a typical reference book. Since there are 20 blocks and four blocks per cow, this calls for five cows (or, by repeating the experiment, some multiple of five cows; Wadley's experiment used 10 cows). If no suitable design had been available with $k = 4$ and $v = 16$, it would have been natural to have considered whether five preparations could have been included in each region (20 injections per region). ■

Example 9.14 Comparing Dishwashing Detergents In experiments such as that by Pugh [1953] to compare detergents used for domestic dishwashing, the following procedure has been used. To obtain a series of homogeneous experimental units, a pile of plates from one course in a canteen is divided into groups. Each group of plates is then washed with water at a standard temperature and with a controlled amount of one detergent. The experimenter records the (logarithm of the) number of plates washed before the foam is reduced to a thin surface layer. The detergents form the varieties. Each group of plates from the one course forms an experimental unit and the different groups of plates from the same course form a block. The washing for one block is done by one person. Each group of plates within a course is assigned to a variety. The experimental conditions are as constant as possible within one block. Different blocks consist of plates soiled in different ways and washed by different people.

Now the number of plates available in one block is limited. It frequently allows only four tests to be completed; that is, there is a restriction to four experimental units and hence varieties per block. If eight varieties are to be compared, not every variety can be tried out in every block. This calls for an incomplete block design, with $v = 8, k = 4$. There is such a design with $r = 7$ and $b = 14$.

In sum, the experimenter takes a set of dishes from a given course, divides it into four groups, and applies a different detergent to each of the groups. The experiment is repeated 14 times, each time with a collection of four detergents chosen to make up the four varieties in the corresponding block. ■

9.4.2 Necessary Conditions for the Existence of (b, v, r, k, λ)-Designs

Our first theorem states some necessary conditions that the parameters for a balanced incomplete block design must satisfy.

Theorem 9.11 In a (b, v, r, k, λ)-design,

$$bk = vr \tag{9.13}$$

and

$$r(k-1) = \lambda(v-1). \tag{9.14}$$

To illustrate this theorem, we note that no $(12, 9, 4, 3, 2)$-design exists, for $bk = 36, vr = 36, r(k-1) = 8$, and $\lambda(v-1) = 16$. Hence, although (9.13) is satisfied, (9.14) is not. If $b = 12, v = 9, r = 4, k = 3$, and $\lambda = 1$, $bk = vr = 36$, and $r(k-1) = \lambda(v-1) = 8$, so (9.13) and (9.14) are satisfied. This says that a $(12, 9, 4, 3, 1)$-design *could* exist; it does not guarantee that such a design *does* exist. [Conditions (9.13) and (9.14) are necessary, but not sufficient.]

Proof of Theorem 9.11. The product bk is the product of the number of blocks (b) by the number of varieties in each block (k), and hence gives the total number of elements that are listed if the blocks are written out as

$$B_1 : \quad \ldots \quad B_2 : \quad \ldots \quad \cdots \quad B_b : \quad \ldots$$

The product vr is the product of the number of varieties (v) by the number of replications of each variety (r) and hence also gives the number of elements listed above. Hence, $bk = vr$, and (9.13) holds.

The product $r(k-1)$ is the product of the number of blocks in which a variety i appears (r) by the number of other varieties in each block in which i appears, and hence gives the number of pairs $\{i, j\}$ appearing in a common block (counting a pair once for each time it occurs). The product $\lambda(v-1)$ is the product of the number of times each pair $\{i, j\}$ appears in a block (λ) by the number of possible j's $(v-1)$, and hence gives the number of pairs $\{i, j\}$ appearing in a common block (counting a pair once for each time it occurs). Thus, $r(k-1) = \lambda(v-1)$, and (9.14) holds. Q.E.D.

Corollary 9.11.1 Suppose that in an incomplete block design with $v \geq 2$ varieties and b blocks,

1. each block consists of the same number k of varieties, and
2. each pair of varieties appears simultaneously in exactly the same number λ of blocks, $\lambda > 0$.

Then each variety appears in the same number r of blocks, r is given by $\lambda(v-1)/(k-1)$, and the block design is balanced.

Proof. The proof of (9.14) above actually shows this. For suppose that a given variety i appears in r_i blocks. The proof above shows that

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

Note that since $v \geq 2$ and $\lambda > 0, k$ could not be 1. Thus,

$$r_i = \frac{\lambda(v-1)}{k-1}.$$

This is the same number r_i for each i. Q.E.D.

Corollary 9.11.1 shows that the definition of balanced incomplete block design is redundant: One of the conditions in the definition, namely the condition (9.11) that every variety appears in the same number of blocks, follows from the other conditions, (9.10) and (9.12).

Theorem 9.12 (Fisher's Inequality[14]) In a (b, v, r, k, λ)-design, $b \geq v$.

We shall prove this result in Section 9.4.3. To prove it, it will be helpful to introduce a concept that will also be very useful in our study of error-correcting codes in Chapter 10. This is the notion of an *incidence matrix* A of a block design. If the design has varieties $x_1, x_2, \ldots, x_v$, and blocks $B_1, B_2, \ldots, B_b$, then A is a $v \times b$ matrix of 0's and 1's, with the i, j entry of A being 1 if x_i is in B_j and 0 otherwise. (This is the point-set incidence matrix of Section 3.7.) For example, in the (b, v, r, k, λ)-design of Example 9.10, we have the following incidence matrix:

$$A = \begin{array}{c|ccccccc} & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 3 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 4 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 7 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Designs can be defined by giving $v \times b$ matrices of 0's and 1's. An arbitrary $v \times b$ matrix of 0's and 1's with $v \geq 2$ is the incidence matrix of a (b, v, r, k, λ)-design, $b, v, r, k, \lambda > 0$, if and only if the following conditions hold:

$$\text{each column has the same number of 1's, } k \text{ of them, } k > 0; \tag{9.15}$$

$$\text{each row has the same number of 1's, } r \text{ of them, } r > 0; \tag{9.16}$$

$$\begin{gathered}\text{each pair of rows has the same number of columns} \\ \text{with a common 1, } \lambda \text{ of them, } \lambda > 0.\end{gathered} \tag{9.17}$$

We have seen (in Corollary 9.11.1) that (9.15) and (9.17) imply (9.16). A natural analog of (9.17) is the following:

$$\text{each pair of columns has the same number of rows with a common 1.} \tag{9.18}$$

Exercise 48 investigates the relations among conditions (9.15)–(9.18).

9.4.3 Proof of Fisher's Inequality[15]

To prove Fisher's Inequality, we shall first prove a result about incidence matrices of (b, v, r, k, λ)-designs.

[14] This theorem is due to Fisher [1940].

[15] This subsection may be omitted.

Theorem 9.13 If $\mathbf{A}$ is the incidence matrix of a (b, v, r, k, λ)-design, then

$$\mathbf{A}\mathbf{A}^T = (r-\lambda)\mathbf{I} + \lambda\mathbf{J}, \tag{9.19}$$

where $\mathbf{A}^T$ is the transpose of $\mathbf{A}$, $\mathbf{I}$ is a $v \times v$ identity matrix, and $\mathbf{J}$ is the $v \times v$ matrix of all 1's.

Proof. Let b_{ij} be the i, j entry of $\mathbf{A}\mathbf{A}^T$. Then b_{ij} is the *inner product* of the ith row of $\mathbf{A}$ with the jth row of $\mathbf{A}$, that is,

$$b_{ij} = \sum_{k=1}^{b} a_{ik}a_{jk}.$$

If $i = j$, we see that $a_{ik}a_{jk}$ is 1 if the ith variety belongs to the kth block, and it is 0 otherwise. Thus, b_{ii} counts the number of blocks that i belongs to, that is, r. If $i \neq j$, then $a_{ik}a_{jk}$ is 1 if the ith and jth varieties both belong to the kth block, and it is 0 otherwise. Thus, b_{ij} counts the number of blocks that the ith and jth varieties both belong to, that is, λ. Translating these conclusions into matrix language gives us (9.19). Q.E.D.

Proof of Fisher's Inequality (Theorem 9.12). We shall suppose that $b < v$ and reach a contradiction. Let $\mathbf{A}$ be the incidence matrix. Since $b < v$, we can add $v - b$ columns of 0's to $\mathbf{A}$, giving us a square $v \times v$ matrix $\mathbf{B}$. Now $\mathbf{A}\mathbf{A}^T = \mathbf{B}\mathbf{B}^T$, since the inner product of two rows of $\mathbf{A}$ is the same as the inner product of two rows of $\mathbf{B}$. Taking determinants, we conclude that

$$\det(\mathbf{A}\mathbf{A}^T) = \det(\mathbf{B}\mathbf{B}^T) = (\det \mathbf{B})(\det \mathbf{B}^T).$$

But $\det \mathbf{B} = 0$ since $\mathbf{B}$ has a column of 0's. Thus, $\det(\mathbf{A}\mathbf{A}^T) = 0$. Now by Theorem 9.13,

$$\det(\mathbf{A}\mathbf{A}^T) = \det \begin{bmatrix} r & \lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda & \lambda & \lambda & \lambda & \cdots & r \end{bmatrix}. \tag{9.20}$$

Subtracting the first column from each of the others in the matrix in the right-hand side of (9.20) does not change the determinant. Hence,

$$\det(\mathbf{A}\mathbf{A}^T) = \det \begin{bmatrix} r & \lambda - r & \lambda - r & \lambda - r & \cdots & \lambda - r \\ \lambda & r-\lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & 0 & 0 & 0 & \cdots & r-\lambda \end{bmatrix}. \tag{9.21}$$

Adding to the first row of the matrix on the right-hand side of (9.21) all the other rows does not change the determinant. Hence,

$$\det(\mathbf{A}\mathbf{A}^T) = \det \begin{bmatrix} r+(v-1)\lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & r-\lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & 0 & 0 & 0 & \cdots & r-\lambda \end{bmatrix}. \qquad (9.22)$$

Since the matrix in the right-hand side of (9.22) has all 0's above the diagonal, its determinant is the product of the diagonal elements, so

$$\det(\mathbf{A}\mathbf{A}^T) = [r+(v-1)\lambda](r-\lambda)^{v-1}.$$

Since we have concluded that $\det(\mathbf{A}\mathbf{A}^T) = 0$, we have

$$[r+(v-1)\lambda](r-\lambda)^{v-1} = 0. \qquad (9.23)$$

But since r, v, and λ are all assumed positive,

$$[r+(v-1)\lambda] > 0.$$

Also, by Equation (9.14) of Theorem 9.11, since $k < v$, it follows that $r > \lambda$. Hence,

$$(r-\lambda)^{v-1} > 0$$

We conclude that the left-hand side of (9.23) is positive, which is a contradiction. Q.E.D.

9.4.4 Resolvable Designs

We say that a (b, v, r, k, λ)-design is *resolvable* if the blocks can be partitioned into groups, called *parallel classes*, so that the blocks in each parallel class in turn partition the set of varieties. For example, Table 9.25 shows a $(12, 9, 4, 3, 1)$-design that consists of four parallel classes. Note that in each parallel class, the three blocks are disjoint and their union is $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Example 9.15 Anonymous Threshold Schemes and Secret Sharing[16] In Example 9.9 we introduced (q, p)-threshold schemes for secret sharing. In an *anonymous (q, p)-threshold scheme*, the p persons receive p distinct partial pieces of information and the secret key can be computed from any q of the partial pieces without knowing which person holds which piece. The threshold schemes we have constructed from orthogonal arrays in Example 9.9 are not anonymous (see Exercise 13). We shall see how resolvable (b, v, r, k, λ)-designs can help us find anonymous (q, p)-threshold schemes, in particular anonymous $(2, p)$-threshold schemes.

[16] This example is due to Stinson [2003].

Table 9.25: A $(12, 9, 4, 3, 1)$-Design with Parallel Classes C_1, C_2, C_3, C_4

$$\begin{aligned} C_1 &: \{1,2,3\},\{4,5,6\},\{7,8,9\} \\ C_2 &: \{1,4,7\},\{2,5,8\},\{3,6,9\} \\ C_3 &: \{1,5,9\},\{2,6,7\},\{3,4,8\} \\ C_4 &: \{1,6,8\},\{2,4,9\},\{3,5,7\} \end{aligned}$$

Suppose that we have a resolvable (b, v, r, k, λ)-design with $\lambda = 1$ and $k = p$ varieties per block. Let C_1, C_2, $\ldots$, C_r be the parallel classes. Thus, each parallel class has v/p blocks. Each variety appears once per parallel class, so the number of parallel classes can be computed from Equation (9.14):

$$r = \frac{\lambda(v-1)}{p-1} = \frac{(v-1)}{p-1}.$$

Suppose that the parallel classes are made known to all p persons in the group. Let us take the set K of possible keys to be $\{1, 2, \ldots, r\}$ and the set P of pieces of partial information to be V, the set of varieties. Suppose that the leader wants to share the secret key $\kappa \in K$. Then he chooses a block from parallel class C_κ at random and gives the p pieces of partial information from this block to the p persons, one per participant. Note that any two persons can now identify the secret key κ. For if p_u is the partial information given to person u and p_v is the partial information given to person v, then since $\lambda = 1$, there is a unique block in the design that contains the varieties p_u and p_v. Persons u and v can find that block and know that the secret key is κ if the block containing p_u and p_v is in parallel class C_κ. Note that this is anonymous since it does not matter which person holds which key, just which keys are held by the pair of persons.

What is the probability that any one person u can determine the secret key given his or her partial information p_u? Every parallel class has exactly one block containing p_u. Thus, the probability of correctly guessing which secret key/parallel class the leader had in mind is $1/r$, where r is the number of parallel classes. This is exactly the same as the probability of guessing right given no partial information. If r is large, we have a very secure anonymous $(2, p)$-threshold scheme.

For example, the resolvable $(12, 9, 4, 3, 1)$-design of Table 9.25 can be used to build an anonymous $(2, 3)$-threshold scheme. If the leader wants to share secret key 3, he or she picks a random block in C_3, say $\{3, 4, 8\}$. These pieces of partial information are given to the three persons in the group. Those getting 3 and 8, for example, know that the only block that the leader could have had in mind is $\{3, 4, 8\}$, which is in C_3, and so know that the secret key is 3. ■

9.4.5 Steiner Triple Systems

So far our results have given necessary conditions for the existence of (b, v, r, k, λ)-designs, but have not given us sufficient conditions for their existence, or constructive procedures for finding them. We shall describe several such procedures. We begin by considering special cases of (b, v, r, k, λ)-designs.

In particular, suppose that $k = 2$ and $\lambda = 1$. In this case, each block consists of two varieties and each pair of varieties appears in exactly one block. Equation (9.14) implies that $r = v - 1$, so (9.13) implies that

$$2b = v(v-1)$$

or

$$b = \frac{v(v-1)}{2}.$$

Now

$$\frac{v(v-1)}{2} = \binom{v}{2}$$

is the number of two-element subsets of a set of v elements. Hence, the number of blocks is the number of two-element subsets of the set of varieties. If, for example, $v = 3$, such a design with $V = \{1, 2, 3\}$ has as blocks the subsets

$$\{1, 2\}, \{1, 3\}, \{2, 3\}.$$

In this subsection we concentrate on another special case of (b, v, r, k, λ)-designs, that where $k = 3$ and $\lambda = 1$. Such a design is a set of triples in which each pair of varieties appears in exactly one triple. These designs are called *Steiner triple systems*. Some authors define Steiner triple systems as block designs in which the blocks are triples from a set V and each pair of varieties appears in exactly one triple. This definition allows inclusion of the complete block design where $k = v$. This is the trivial design where $V = \{1, 2, 3\}$ and there is only one block, $\{1, 2, 3\}$. For the purposes of this subsection, we shall include this design as a Steiner triple system. A more interesting example of a Steiner triple system occurs when $v = 7$. Example 9.10, a $(7, 7, 3, 3, 1)$-design, is such an example.

We shall now discuss the existence problem for Steiner triple systems. Note that in a Steiner triple system, (9.14) implies that

$$r(2) = v - 1, \tag{9.24}$$

so

$$r = \frac{v-1}{2}. \tag{9.25}$$

Equation (9.13) now implies that

$$3b = \frac{v(v-1)}{2},$$

so

$$b = \frac{v(v-1)}{6}. \tag{9.26}$$

Equation (9.25) implies that $v - 1$ is even and v is odd. Also, $v \geq 2$ implies that v is at least 3. Equation (9.26) implies that $v(v-1) = 6b$, so $v(v-1)$ is a multiple of

6. These are necessary conditions. Let us begin to tabulate what values of v satisfy the two necessary conditions: v odd and at least 3, $v(v-1)$ a multiple of 6. If $v = 3$, then $v(v-1) = 6$, so there could be a Steiner triple system with $v = 3$; that is, the necessary conditions are satisfied. However, with $v = 5$, $v(v-1) = 20$, which is not divisible by 6, so there is no Steiner triple system with $v = 5$. In general, Steiner triple systems are possible for $v = 3, 7, 9, 13, 15, 19, 21, \ldots$, that is, for $v = 6n+1$ or $6n+3, n \geq 1$, and $v = 3$. In fact, these systems do exist for all of these values of v.

Theorem 9.14 (Kirkman [1847]) There is a Steiner triple system of v varieties if and only if $v = 3$ or $v = 6n+1$ or $v = 6n+3, n \geq 1$.

We have already proved the necessity of the conditions in Theorem 9.14. Rather than prove sufficiency, we shall prove a simpler theorem, which gives us the existence of some of these Steiner triple systems: for instance, those with $3 \cdot 3 = 9$ varieties, $3 \cdot 7 = 21$ varieties, $7 \cdot 7 = 49$ varieties, $9 \cdot 7 = 63$ varieties, and so on. For a number of proofs of sufficiency, see, for instance, Lindner and Rodger [1997].

Theorem 9.15 If there is a Steiner triple system S_1 of v_1 varieties and a Steiner triple system S_2 of v_2 varieties, then there is a Steiner triple system S of $v_1 v_2$ varieties.

Proof.[17] The proof provides a construction for building a Steiner triple system S given Steiner triple systems S_1 and S_2. Suppose that the varieties of S_1 are $a_1, a_2, \ldots, a_{v_1}$ and those of S_2 are $b_1, b_2, \ldots, b_{v_2}$. Let S consist of the $v_1 v_2$ elements $C_{ij}, i = 1, 2, \ldots, v_1, j = 1, 2, \ldots, v_2$. A triple $\{c_{ir}, c_{js}, c_{kt}\}$ is in S if and only if one of the following conditions holds:

(1) $r = s = t$ and $\{a_i, a_j, a_k\} \in S_1$,
(2) $i = j = k$ and $\{b_r, b_s, b_t\} \in S_2$,

or

(3) $\{a_i, a_j, a_k\} \in S_1$ and $\{b_r, b_s, b_t\} \in S_2$.

Then it is easy to prove that S forms a Steiner triple system. Q.E.D.

Let us illustrate the construction in the proof of Theorem 9.15. Suppose that $v_1 = v_2 = 3$, S_1 has the one triple $\{a_1, a_2, a_3\}$ and S_2 has the one triple $\{b_1, b_2, b_3\}$. Then S has the triples shown in Table 9.26 and forms a Steiner triple system of 9 varieties and 12 blocks.

If an experimental design is to be a Steiner triple system on v varieties, the specific choice of design is simple if $v = 3, 7$, or 9, for there is (up to relabeling of varieties) only one Steiner triple system of v varieties in these cases. However, for $v = 13$ there are two essentially different Steiner triple systems, for $v = 15$ there are 80, and for $v = 19$ there are 11,084,874,829 (Kaski and Östergård [2004]). Presumably, one of these will be chosen at random if a Steiner triple system of 13, 15, or 19 varieties is required. In general, when there exist Steiner triple systems for $v > 19$, the number of such distinct Steiner triple systems is unknown.

[17] The proof and the illustration of it may be omitted.

Table 9.26: Construction of a Steiner Triple System S of $v_1 v_2 = 9$ Varieties from S_1, S_2 If S_1 Has Only the Triple $\{a_1, a_2, a_3\}$ and S_2 Only the Triple $\{b_1, b_2, b_3\}$

Condition (1) from the proof of Theorem 9.15:	$r = s = t = 1$ $\{c_{11}, c_{21}, c_{31}\}$	$r = s = t = 2$ $\{c_{12}, c_{22}, c_{32}\}$	$r = s = t = 3$ $\{c_{13}, c_{23}, c_{33}\}$
Condition (2) from the proof of Theorem 9.15:	$i = j = k = 1$ $\{c_{11}, c_{12}, c_{13}\}$	$i = j = k = 2$ $\{c_{21}, c_{22}, c_{23}\}$	$i = j = k = 3$ $\{c_{31}, c_{32}, c_{33}\}$
Condition (3) from the proof of Theorem 9.15:	$\{c_{11}, c_{22}, c_{33}\}$ $\{c_{11}, c_{23}, c_{32}\}$	$\{c_{12}, c_{23}, c_{31}\}$ $\{c_{12}, c_{21}, c_{33}\}$	$\{c_{13}, c_{21}, c_{32}\}$ $\{c_{13}, c_{22}, c_{31}\}$

9.4.6 Symmetric Balanced Incomplete Block Designs

A balanced incomplete block design or (b, v, r, k, λ)-design is called *symmetric* if $b = v$ (the number of blocks is the same as the number of varieties) and if $r = k$ (the number of times a variety occurs is the same as the number of varieties in a block). A symmetric BIBD is sometimes called a (v, k, λ)-*design* or a (v, k, λ)-*configuration*. By Equation (9.13) of Theorem 9.11,

$$b = v \quad \text{iff} \quad k = r.$$

Hence, the two conditions in the definition are redundant. Example 9.11 is an example of a symmetric BIBD: We have $b = v = 4$ and $r = k = 3$. So is Example 9.10: We have $b = v = 7$ and $r = k = 3$. The Steiner triple system of Table 9.26 is an example of a BIBD that is not symmetric.

Theorem 9.16 (Bruck-Ryser-Chowla Theorem[18]) The following conditions are necessary for the existence of a (v, k, λ)-design:

1. If v is even, then $k - \lambda$ is the square of an integer.
2. If v is odd, the following equation has a solution in integers x, y, z, not all of which are 0:

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2. \tag{9.27}$$

We omit the proof of Theorem 9.16. For a proof, see Ryser [1963] or Hall [1967]. To illustrate the theorem, suppose that $v = 16, k = 6$, and $\lambda = 2$. Then v is even and $k - \lambda = 4$ is a square, so condition 1 says that a $(16, 6, 2)$-design *could* exist. However, it also implies that a $(22, 7, 2)$-design *could not* exist, since $k - \lambda = 5$ is not a square. Suppose that $v = 111, k = 11$, and $\lambda = 1$. Then v is odd and (9.27) becomes

$$x^2 = 10y^2 - z^2.$$

This has a solution $x = y = 1, z = 3$. Hence, a $(111, 11, 1)$-design *could* exist.

[18] This theorem was proved for $\lambda = 1$ by Bruck and Ryser [1949] and in generality by Chowla and Ryser [1950].

The conditions for existence of a symmetric BIBD given in Theorem 9.16 are not sufficient. Even though we have shown that a $(111, 11, 1)$-design could exist, Lam, Thiel, and Swiercz [1989] proved that one does not. Some specific sufficient conditions are given by the following theorem, whose proof we leave to Section 10.5.2.[19]

Theorem 9.17 For arbitrarily large values of m, and in particular for $m = 2^k, k \geq 1$, there is a $(4m-1, 2m-1, m-1)$-design.

A $(4m-1, 2m-1, m-1)$-design is called a *Hadamard design of dimension m*. The case $m = 2$ gives a $(7, 3, 1)$-design, an example of which is given in Example 9.10. That Hadamard designs of dimension m *could* exist for all $m \geq 2$ follows from Theorem 9.16. For $v = 4m - 1$ is odd and (9.27) becomes

$$x^2 = my^2 - (m-1)z^2,$$

which has the solution $x = y = z = 1$. Hadamard designs will be very important in the theory of error-correcting codes in Section 10.5.

A second theorem giving sufficient conditions for the existence of symmetric BIBDs is the following, which is proved in Section 9.5.2 in our study of projective planes.

Theorem 9.18 If $m \geq 1$ is a power of a prime, there is an $(m^2+m+1, m+1, 1)$-design.

To illustrate this theorem, note that taking $m = 1$ gives us a $(3, 2, 1)$-design. We have seen such a design at the beginning of Section 9.4.5. Taking $m = 2$ gives us a $(7, 3, 1)$-design. We have seen such a design in Example 9.10. Taking $m = 3$ gives us a $(13, 4, 1)$-design, which is something new.

Still a third way to construct symmetric BIBDs is to use difference sets. This method is described in Exercises 31 and 32.

9.4.7 Building New (b, v, r, k, λ)-Designs from Existing Ones

Theorem 9.15 gives us a way of building new (b, v, r, k, λ)-designs from old ones. Here we shall present other such ways. The most trivial way to get one design from another is simply to repeat blocks. If we take p copies of each block in a (b, v, r, k, λ)-design, we get a $(pb, v, pr, k, p\lambda)$-design. For example, from the $(4, 4, 3, 3, 2)$-design of Example 9.11, we get an $(8, 4, 6, 3, 4)$-design by repeating each block twice. To describe more interesting methods of obtaining new designs from old ones, we need one preliminary result.

Theorem 9.19 In a (v, k, λ)-design, any two blocks have exactly λ elements in common.

Proof. Exercise 48. Q.E.D.

[19] That section may be read at this point.

If U and V are sets, $U - V$ will denote the set $U \cap V^c$.

Theorem 9.20 Suppose that $B_1, B_2, \ldots, B_v$ are the blocks of a (v, k, λ)-design with $V = \{x_1, x_2, \ldots, x_v\}$ the set of varieties. Then for any i,

$$B_1 - B_i, B_2 - B_i, \ldots, B_{i-1} - B_i, B_{i+1} - B_i, \ldots, B_v - B_i$$

are the blocks of a $(v-1, v-k, k, k-\lambda, \lambda)$-design on the set of varieties $V - B_i$.

Proof. There are clearly $v-1$ blocks and $v-k$ varieties. By Theorem 9.19, each block $B_j - B_i$ has $k - \lambda$ elements. Each variety in $V - B_i$ appears in k blocks of the original design and hence in k blocks of the new design. Similarly, each pair of varieties in $V - B_i$ appear in common in λ blocks of the original design and hence in λ blocks of the new design. Q.E.D.

To illustrate this construction, suppose that we start with the $(7, 3, 1)$-design of Example 9.10 and let $B_i = \{3, 4, 6\}$. Then the following blocks form a $(6, 4, 3, 2, 1)$-design on the set of varieties $\{1, 2, 5, 7\}$:

$$\{1, 2\}, \{2, 5\}, \{5, 7\}, \{1, 5\}, \{2, 7\}, \{1, 7\}.$$

Theorem 9.21 Suppose that $B_1, B_2, \ldots, B_v$ are the blocks of a (v, k, λ)-design with $V = \{x_1, x_2, \ldots, x_v\}$ the set of varieties. Then for any i,

$$B_1 \cap B_i, B_2 \cap B_i, \ldots, B_{i-1} \cap B_i, B_{i+1} \cap B_i, \ldots, B_v \cap B_i$$

are the blocks of a $(v-1, k, k-1, \lambda, \lambda-1)$-design on the set of varieties B_i.

Proof. There are clearly $v - 1$ blocks and k varieties. By Theorem 9.19, each block $B_j \cap B_i$ has λ elements. Moreover, a given variety in B_i appears in the original design in blocks

$$B_{j_1}, \quad B_{j_2}, \quad \ldots, \quad B_{j_{k-1}}, \quad B_i.$$

Then it appears in the new design in $k-1$ blocks,

$$B_{j_1} \cap B_i, \quad B_{j_2} \cap B_i, \quad \ldots, \quad B_{j_{k-1}} \cap B_i.$$

Moreover, any pair of varieties in B_i appear in common in the original design in λ blocks,

$$B_{j_1}, \quad B_{j_2}, \quad \ldots, \quad B_{j_{\lambda-1}}, \quad B_i,$$

and hence appear in common in the new design in $\lambda - 1$ blocks,

$$B_{j_1} \cap B_i, \quad B_{j_2} \cap B_i, \quad \ldots, \quad B_{j_{\lambda-1}} \cap B_i.$$

Q.E.D.

To illustrate this theorem, we note that by Theorem 9.17, there is a $(15, 7, 3)$-design. Hence, Theorem 9.21 implies that there is a $(14, 7, 6, 3, 2)$-design. To exhibit such a design, we note that the blocks in Table 9.27 define a $(15, 7, 3)$-design on $V = \{1, 2, \ldots, 15\}$. We show how to construct this design in Section 10.5.2. Taking $B_i = \{1, 2, 3, 8, 9, 10, 11\}$, we get the $(14, 7, 6, 3, 2)$-design of Table 9.28 on the set of varieties B_i. Note that this design has repeated blocks. If we take only one copy of each of these blocks, we get a $(7, 3, 1)$-design.

Table 9.27: The Blocks of a $(15, 7, 3)$-Design on the Set of Varieties $V = \{1, 2, \ldots, 15\}$

{2, 4, 6, 8, 10, 12, 14},	{1, 4, 5, 8, 9, 12, 13},	{3, 4, 7, 8, 11, 12, 15},
{1, 2, 3, 8, 9, 10, 11},	{2, 5, 7, 8, 10, 13, 15},	{1, 6, 7, 8, 9, 14, 15},
{3, 5, 6, 8, 11, 13, 14},	{1, 2, 3, 4, 5, 6, 7},	{2, 4, 6, 9, 11, 13, 15},
{1, 4, 5, 10, 11, 14, 15},	{3, 4, 7, 9, 10, 13, 14},	{1, 2, 3, 12, 13, 14, 15}
{2, 5, 7, 9, 11, 12, 14}	{1, 6, 7, 10, 11, 12, 13},	{3, 5, 6, 9, 10, 12, 15}

Table 9.28: The Blocks of a $(14, 7, 6, 3, 2)$-Design Obtained from the Design of Table 9.27 by Intersecting Blocks with $B_i = \{1, 2, 3, 8, 9, 10, 11\}$

{2, 8, 10},	{1, 8, 9},	{3, 8, 11},	{2, 8, 10},	{1, 8, 9},	{3, 8, 11},	{1, 2, 3}
{2, 9, 11},	{1, 10, 11},	{3, 9, 10},	{1, 2, 3},	{2, 9, 11},	{1, 10, 11},	{3, 9, 10}

9.4.8 Group Testing and Its Applications

Suppose that a large population U of items is partitioned into two classes, positive and negative. We wish to locate positive items, but to examine each item in U is prohibitively expensive. However, we can group the items into subsets of U and can test if a subset contains at least one positive item. We would like to identify all positive items through a number of group tests. If we have to identify all groups to test and then carry out the group tests without being able to use the results of these tests to select new groups to test, we talk about *nonadaptive group testing*. Otherwise, we talk about *adaptive group testing*. The modern theory of group testing is heavily influenced by combinatorial methods, in particular by the methods of combinatorial designs.

Here are some examples of the uses of group testing.

(1) Defective Products. We want to pick out those items manufactured in a given plant that are defective before shipping them. (Here, defective items are "positive.")

(2) Screening for Diseases. We want to determine which persons in a group have a certain disease. It was this problem (in connection with testing millions of military draftees for syphilis) that gave rise to the study of group testing by Dorfman [1943]. The subject has become very important with the possibility of large-scale HIV screening. (Here, having the disease is "positive.")

(3) Mapping Genomes. We have a long molecular sequence S, e.g., DNA. We form a library of substrings known as *clones*. We test whether or not a particular sequence, known as a *probe*, appears in S by testing to see in which clones it appears. We do this by pooling the clones into groups, since a clone library can have thousands, even hundreds of thousands, of clones.

(4) **Satellite Communications.** Many ground stations are potential users of a satellite communications link. In scheduling requests for time slots in the satellite link, one doesn't contact all of the ground stations individually, but instead, pools of ground stations are contacted to see if a station in the pool wishes to reserve satellite time.

(5) **Scientific or Industrial Experiments.** We want to determine which of a large number of possible variables are important. If we can assume that the effect of an important variable is strong enough not to be masked by other variables, we can study them first in groups to identify the important ones.

Information about these and other applications of group testing, the theory of group testing, as well as references to the literature, can be found in the book by Du and Hwang [2000]. See also Colbourn, Dinitz, and Stinson [1999].

In this section we illustrate the connection between nonadaptive group testing and (b, v, r, k, λ)-designs. A *nonadaptive group testing algorithm* or *NAGTA* starts with a population U of u elements. It seeks to identify those items in U that belong to a subset of positive items. The algorithm uses a collection G of g subsets of U called *groups*. We order the subsets in G. The data of our group testing can be reported as a vector v of 0's and 1's whose ith entry is 1 if and only if the ith group tests positive. For each group $X \subseteq U$ in G and each subset $P \subseteq U$, let $f_X(P)$ give the outcome 1 if $X \cap P \neq \emptyset$ and 0 otherwise. The bit string $(f_{X_1}(P), f_{X_2}(P), \ldots, f_{X_g}(P))$ corresponding to all the groups X in G is denoted by $f_G(P)$. Suppose we can find the collection G so that for all subsets $Q \neq P$ of U of size at most t, $f_G(Q) \neq f_G(P)$. If this is the case, then, as long as the number of positive items is at most t, we can tell from our g group tests exactly which items in U are positive by seeing for which subset P the vector $f_G(P)$ matches the observed vector v. To give an example, suppose that $U = \{1, 2, 3, 4\}$ and G is given by the ordered sequence

$$G = (\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}). \tag{9.28}$$

Then

$$f_G(\{2\}) = (1, 0, 0, 1, 1, 0)$$

and

$$f_G(\{1,2\}) = (1, 1, 1, 1, 1, 0).$$

In Table 9.29, the vectors $f_G(P)$ are given for all P with $|P| \leq 2$. So $f_G(\{2\}) \neq f_G(\{1,2\})$, and, clearly, $f_G(Q) \neq f_G(P)$ for all $Q \neq P$ with $|P| \leq 2$, $|Q| \leq 2$. Thus, the result of the six group tests in G uniquely identifies the subset P of positive items. Suppose again that $U = \{1, 2, 3, 4\}$. The collection

$$G' = (\{1,2\}, \{1,3\}, \{1,4\})$$

Table 9.29: $f_G(P)$ for All P with $|P| \leq 2$, $U = \{1, 2, 3, 4\}$, and G from (9.28)

P	$f_G(P)$
$\{1\}$	$(1, 1, 1, 0, 0, 0)$
$\{2\}$	$(1, 0, 0, 1, 1, 0)$
$\{3\}$	$(0, 1, 0, 1, 0, 1)$
$\{4\}$	$(0, 0, 1, 0, 1, 1)$
$\{1, 2\}$	$(1, 1, 1, 1, 1, 0)$
$\{1, 3\}$	$(1, 1, 1, 1, 0, 1)$
$\{1, 4\}$	$(1, 1, 1, 0, 1, 1)$
$\{2, 3\}$	$(1, 1, 0, 1, 1, 1)$
$\{2, 4\}$	$(1, 0, 1, 1, 1, 1)$
$\{3, 4\}$	$(0, 1, 1, 1, 1, 1)$

has $f_{G'}(\{1\}) = f_{G'}(\{1, 2\}) = (1, 1, 1)$, but it has $f_{G'}(\{i\}) \neq f_{G'}(\{j\})$ for all $i \neq j$. We say that G defines a *successful NAGTA with threshold* t if $f_G(Q) \neq f_G(P)$ for all Q and P with at most t elements (and $P \neq Q$). Thus, G' is a successful NAGTA with threshold 1, but not with threshold 2. In other words, the collection of groups G' can be used to determine the positive items if there is exactly one but not if there are two or more.

We now show how to construct successful NAGTAs with given threshold t if we have a population U of size u.[20] Start with a (b, v, r, k, λ)-design with $b = u$, $k = t + 1$, and $\lambda = 1$. Let the b blocks correspond to the elements of the population U. Let $V = \{1, 2, \ldots, v\}$ be the set of varieties and define the ith group X_i in G to be the set of blocks containing variety i. Then:

- Each element of U (block of the design) is in exactly k groups.
- Each group has exactly r items from U.
- Each pair of distinct items in U is contained in at most one group (since $\lambda = 1$).

The reader may find it useful to think of the pair (U, G) as defined by the transpose of the incidence matrix of the (b, v, r, k, λ)-design.[21]

We shall prove that G has threshold $t = k - 1$. First, to illustrate the construction, suppose that we start with the $(7, 7, 3, 3, 1)$-design of Example 9.10. Then the population U is $\{B_1, B_2, B_3, B_4, B_5, B_6, B_7\}$ and the groups are given by

$$X_1 = \{B_1, B_5, B_7\},\ X_2 = \{B_1, B_2, B_6\},\ X_3 = \{B_2, B_3, B_7\},\ X_4 = \{B_1, B_3, B_4\},$$
$$X_5 = \{B_2, B_4, B_5\},\ X_6 = \{B_3, B_5, B_6\},\ X_7 = \{B_4, B_6, B_7\}.$$

[20] This construction follows Stinson [2003].

[21] The design whose incidence matrix is the transpose of the incidence matrix of a known BIBD is called the *dual* of that design.

Now, suppose that we know that $f_G(P) = (1,1,1,1,0,1,0)$. The reader can check that $f_G(\{B_1, B_3\}) = (1,1,1,1,0,1,0)$. Since we have a threshold of $k-1=2$, we know that P must be $\{B_1, B_3\}$.

We conclude by proving that the threshold of G is $k-1$. Suppose that $|P| \leq k-1$, $|Q| \leq k-1$, and $P \neq Q$. We show that $f_{X_j}(P) \neq f_{X_j}(Q)$ for some j. Without loss of generality, there is a block B in Q but not in P. Now B is in exactly k groups $X_{j_1}, X_{j_2}, \ldots, X_{j_k}$. If $X_{j_i} \cap P \neq \emptyset$ for all $i = 1, 2, \ldots, k$, then for every i there is a block $B(i) \in X_{j_i} \cap P$. Now $B(i) \neq B(i')$ if $i \neq i'$ since B and $B(i)$ are in at most one group. But then P has at least k elements, $B(1), B(2), \ldots, B(k)$, contradicting $|P| \leq k-1$. Thus, for some i with $1 \leq i \leq k$, $X_{j_i} \cap P = \emptyset$. Hence, $f_{X_{j_i}}(P) = 0$. However, B is in Q and X_{j_i} so $f_{X_{j_i}}(Q) = 1$.

9.4.9 Steiner Systems and the National Lottery[22]

The National Lottery in the United Kingdom involves buying a ticket with six of the integers from 1 to 49. Twice a week, six "winning" numbers are randomly drawn. A ticket with three or more of the winning numbers wins at least £10. Our question is: What is the fewest number of tickets that must be bought to ensure a winning ticket? To address this question, we consider a variant of block designs called Steiner systems.

An $S(t,k,v)$ *Steiner system* is a set V of v elements and a collection of subsets of V of size k called blocks such that any t elements of V are in exactly one of the blocks. Any Steiner triple system (Section 9.4.5) is an $S(2,3,v)$ Steiner system.

Steiner systems do not exist for many t, k, and v. In fact, we do not know if any exist for $t \geq 6$.

Theorem 9.22 If an $S(t,k,v)$ Steiner system exists, $\binom{k}{t}$ divides $\binom{v}{t}$ and the number of blocks is given by $\binom{v}{t} \Big/ \binom{k}{t}$.

Proof. Consider an $S(t,k,v)$ Steiner system on the set V. There are $\binom{v}{t}$ t-element subsets of V. Each occurs in exactly one block of V. And each block, being a k-element subset, contains $\binom{k}{t}$ t-element subsets of V. Therefore,

$$\binom{v}{t} \Big/ \binom{k}{t} = \text{the number of blocks of } S(t,k,v).$$

If this is not an integer, $S(t,k,v)$ cannot exist. Q.E.D.

An $S(3,6,49)$ Steiner system would yield a method to ensure that every possible triple appeared on exactly one of our tickets. (Why?) Unfortunately, an $S(3,6,49)$

[22] This subsection is based on Brinkman, Hodgkinson, and Humphreys [2001].

Steiner system doesn't exist, since

$$\binom{49}{3} \Big/ \binom{6}{3} = 18{,}424/20 = 921.2.$$

A method that modifies this idea (with perhaps some triple of numbers appearing in more than one block) would therefore need at least 922 blocks or tickets (921.2 rounded up). We describe a much more efficient method.

What if the lottery only used numbers between 1 and 26 and required that of the six winning numbers drawn, a winning ticket had to have at least three of them? An $S(3,6,26)$ Steiner system exists (Chen [1972]). By Theorem 9.22, it contains $\binom{26}{3} \Big/ \binom{6}{3} = 130$ blocks, so there is a method that can be used to guarantee a winning ticket if 130 tickets are purchased.

We now show how to modify this idea to guarantee a winning ticket in the UK National Lottery with numbers 1 to 49 used if one purchases 260 tickets. Note that any six winning numbers must contain either three even numbers or three odd ones. Thus, the idea is to buy enough tickets to be sure that every even triple and every odd triple is represented. If $V = \{2,4,\ldots,48\} \cup \{1,3\}$, then $|V| = 26$. Using an $S(3,6,26)$ Steiner system on V, we find 130 tickets that guarantee that every even triple of integers from 2 through 48 is included in one of these tickets. Similarly, using an $S(3,6,26)$ Steiner system on $V = \{1,3,\ldots,49\} \cup \{2\}$, we find 130 other tickets that guarantee that every odd triple of integers from 1 through 49 is included in one of these tickets. Thus, 260 tickets in all suffice to guarantee that one of them will have three numbers among the six chosen from 1 to 49. For a recent paper that summarizes all so-called "lotto designs," see Li and van Rees [2002].

EXERCISES FOR SECTION 9.4

1. For each of the following block designs, determine if the design is a BIBD, and if so, determine its parameters b, v, r, k, and λ.

(a) Varieties: $\{1,2,3,4\}$
Blocks: $\{1,2\}, \{1,3\}, \{2,4\}, \{1,2,3\}, \{2,3,4\}$

(b) Varieties: $\{1,2,3,4,5\}$
Blocks: $\{1,2,3\}, \{2,3,4\}, \{3,4,5\}, \{1,4,5\}, \{1,2,5\}$

(c) Varieties: $\{1,2,3,4,5\}$
Blocks: $\{1,2,3,4\}, \{1,3,4,5\}, \{1,2,4,5\}, \{1,2,3,5\}, \{2,3,4,5\}$

(d) Varieties: $\{1,2,3,4,5,6,7\}$
Blocks: $\{1,2,3\}, \{1,2,4\}, \{1,3,5\}, \{1,4,6\}, \{1,5,7\}, \{1,6,7\}, \{3,5,6\}, \{2,3,7\}, \{2,4,5\}, \{2,5,6\}, \{2,6,7\}, \{3,4,6\}, \{3,4,7\}, \{4,5,7\}$

(e) Varieties: $\{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p\}$
Blocks: $\{a,b,c,d,e,f\}, \{a,b,g,h,i,j\}, \{a,c,g,k,l,m\}, \{a,d,h,k,n,o\}, \{a,e,i,l,n,p\}, \{a,f,j,m,o,p\}, \{b,c,g,n,o,p\}, \{b,d,h,l,m,p\}, \{b,e,i,k,m,o\}, \{b,f,j,k,l,n\}, \{c,d,i,j,m,n\}, \{c,e,h,j,k,p\}, \{c,f,h,i,l,o\}, \{d,e,g,j,l,o\}, \{d,f,g,i,k,p\}, \{e,f,g,h,m,n\}$

2. (a) A BIBD has parameters $v = 6, k = 3$, and $\lambda = 10$. Find b and r.
   (b) A BIBD has parameters $v = 13, b = 78$, and $r = 24$. Find k and λ.
   (c) A BIBD has parameters $b = 85, k = 21$, and $\lambda = 5$. Find v and r.
3. Show that there is no (b, v, r, k, λ)-design with the following parameters.

   (a) $b = 6, v = 9, r = 2, k = 3, \lambda = 1$; (b) $b = 22, v = 22, r = 7, k = 7, \lambda = 2$.
4. Show that there is no (b, v, r, k, λ)-design with the following parameters: $b = 4, v = 9, r = 4, k = 9, \lambda = 4$.
5. Could there be a $(12, 6, 8, 7, 1)$-design?
6. Could there be a $(13, 3, 26, 6, 1)$-design?
7. Could there be a $(6, 8, 6, 8, 6)$-design?
8. In Wadley's experiment (Example 9.13), in the case where there are five cows, find λ.
9. For each of the block designs of Exercise 1, find its incidence matrix.
10. For each of the following block designs, compute $\mathbf{AA}^T$ for $\mathbf{A}$ the incidence matrix of the design.

    (a) The design of Example 9.11 (b) The design of Example 9.12
    (c) A $(15, 15, 7, 7, 3)$-design
11. In a Steiner triple system with $v = 9$, find b and r.
12. The following nine blocks form part of a Steiner triple system with nine varieties:

    $$\{a, b, c\}, \{d, e, f\}, \{g, h, i\}, \{a, d, g\}, \{c, e, h\}, \{b, f, i\}, \{a, e, i\}, \{c, f, g\}, \{b, d, h\}.$$

    (a) How many missing blocks are there?
    (b) Add additional blocks that will lead to a Steiner triple system.
13. Show why the threshold schemes constructed from an orthogonal array in Example 9.9 are not anonymous.
14. There is a resolvable $(35, 15, 7, 3, 1)$-design. Find the number of parallel classes and the number of blocks per parallel class.
15. Find a resolvable $(12, 9, 4, 3, 1)$-design different from the one in Table 9.25.
16. Two designs on X and X' are called *isomorphic* if there exists a one-to-one function f from X onto X' such that $f(B)$ is a block of X' whenever B is a block of X and $f(B) = \{f(x) | x \in B\}$.

    (a) Show that any two resolvable $(12, 9, 4, 3, 1)$-designs are isomorphic.
    (b) Show that any two Steiner triple systems on seven varieties are isomorphic.
17. In an anonymous threshold scheme based on the design of Table 9.25, the leader gives person u partial information 8 and person v partial information 6. What is the secret key?
18. If a Steiner triple system has 67 varieties, how many blocks does it have?
19. Compute $\mathbf{AA}^T$ for $\mathbf{A}$ the incidence matrix of a Steiner triple system of 13 varieties.

20. Given a design, the incidence matrix of the *complementary design* is obtained by interchanging 0 and 1 in the incidence matrix of the original design. In general, if one starts with a (b, v, r, k, λ)-design, the complementary design is a $(b', v', r', k', \lambda')$-design.

    (a) Find formulas for b', v', r', and k'.
    (b) Show that $\lambda' = b + \lambda - 2r$.
    (c) Find a $(16, 16, 6, 6, 2)$-design.
    (d) Find a $(12, 9, 8, 6, 5)$-design.

21. Suppose that the complementary design (Exercise 20) of a Steiner triple system with 13 varieties is a (b, v, r, k, λ)-design. Find b, v, r, k, and λ.

22. Construct a Steiner triple system of 21 varieties.

23. Complete the proof of Theorem 9.15 by showing that the set S is in fact a Steiner triple system.

24. Four of the blocks of a $(7, 3, 1)$-design are

$$\{1, 2, 3\}, \quad \{1, 5, 6\}, \quad \{2, 5, 7\}, \quad \text{and} \quad \{1, 4, 7\}.$$

    Find the remaining blocks.

25. Show by construction that there is a $(v, v - 1, v - 2)$-design.

26. Show that each of the following designs exists.

    (a) A $(31, 15, 7)$-design
    (b) A $(63, 31, 15)$-design
    (c) A $(21, 5, 1)$-design
    (d) A $(31, 6, 1)$-design

27. Compute $\mathbf{AA}^T$ for $\mathbf{A}$ the incidence matrix of a $(31, 15, 7)$-design.

28. Show that in a (v, k, λ)-design, any two blocks have exactly λ varieties in common.

29. (a) If $\mathbf{A}$ is the incidence matrix of a (b, v, r, k, λ)-design, show that $\mathbf{A}^T$ is not necessarily the incidence matrix of a (v, k, λ)-design.

    (b) Show that if $\mathbf{A}$ is the incidence matrix of a (v, k, λ)-design, then $\mathbf{A}^T$ is the incidence matrix of a (v, k, λ)-design.

30. Show that there can be no $(43, 43, 7, 7, 1)$-design.

31. Consider Z_v, the set of integers $\{0, 1, 2, \ldots, v-1\}$, with addition modulo v. A subset D of k integers in Z_v is called a (v, k, λ)-*difference set*, or just a *difference set*, if every nonzero integer in Z_v appears the exact same number λ of times if we list the differences among distinct elements x, y of D (using both $x - y$ and $y - x$) modulo v.

    (a) Show that $D = \{0, 1, 3\}$ is a difference set in Z_7.

    (b) Show that $D = \{0, 1, 4\}$ is not a difference set in Z_7.

    (c) Show that $D = \{0, 1, 6, 8, 18\}$ is a difference set in Z_{21}.

    (d) Find an $(11, 5, 2)$-difference set.

    (e) If D is a (v, k, λ)-difference set, how many elements will it have?

    (f) If D is a (v, k, λ)-difference set, find an expression for λ as a function of v and k.

32. Suppose that D is a (v, k, λ)-difference set. If $x \in Z_v$, let

$$D + x = \{y + x : y \in D\},$$

    where addition is modulo v.

(a) Prove the following theorem:

Theorem: If D is a (v, k, λ)-difference set, then $\{D+x : x \in Z_v\}$ is a (v, k, λ)-design.

(b) Illustrate the theorem by constructing a $(7, 3, 1)$-design corresponding to the difference set $D = \{0, 1, 3\}$ in Z_7.

(c) Illustrate the theorem by constructing a $(21, 5, 1)$-design corresponding to the difference set $D = \{0, 1, 6, 8, 18\}$ in Z_{21}.

(d) Illustrate the theorem by constructing an $(11, 5, 2)$-design corresponding to the difference set you found in Exercise 31(d).

33. Show that if $m \geq 1$ is a power of a prime, there is a $(2m^2+2m+2, m^2+m+1, 2m+2, m+1, 2)$-design.

34. Use the Bruck-Ryser-Chowla Theorem to show that a $(20, 5, 1)$-design could exist.

35. Which of the following (v, k, λ)-designs could possibly exist?

(a) (16, 9, 1) (b) (34, 12, 4) (c) (43, 7, 1)

36. Show that a $(46, 46, 10, 10, 2)$-design does not exist.

37. Show by construction that there is a $(14, 8, 7, 4, 3)$-design. (*Hint:* Use Theorem 9.17 and another theorem.)

38. Show by construction that there is a $(30, 16, 15, 8, 7)$-design. (*Hint:* Use Theorem 9.17 and another theorem.)

39. Show that there is a $(30, 15, 14, 7, 6)$-design.

40. Suppose that there is a (v, k, λ)-design.

(a) Show that there is a $(2v, v, 2k, k, 2\lambda)$-design.

(b) Show that for any positive integer p, there is a $(pv, v, pk, k, p\lambda)$-design.

41. Show that there is a $(62, 31, 30, 15, 14)$-design.

42. We wish to test for the presence of HIV in a group of six people whose names are encoded as A, B, C, D, E, F. Let $P \subseteq U = \{A, B, C, D, E, F\}$. We use the four groups $X_1 = \{A, B, C\}$, $X_2 = \{A, D, E\}$, $X_3 = \{B, D, F\}$, $X_4 = \{C, E, F\}$.

(a) Compute the vector $(f_{X_1}(P), f_{X_2}(P), f_{X_3}(P), f_{X_4}(P))$ for all subsets P of U.

(b) If the vector $(1, 1, 1, 1)$ is obtained as $f_G(P)$ for some P and we know that $|P| \leq 2$, can we determine P?

(c) Show that this collection of groups gives a successful NAGTA with threshold 1.

43. We wish to determine the interest in a new network on the part of 8 cable TV providers, whose names are encoded as A, B, $\ldots$, H. Let $P \subseteq \{A, B, C, D, E, F, G, H\}$. Consider the collection G of 6 groups $X_1 = \{A, B, C, D\}$, $X_2 = \{E, F, G, H\}$, $X_3 = \{A, C, E, G\}$, $X_4 = \{B, D, F, H\}$, $X_5 = \{A, B, D, G\}$, $X_6 = \{C, E, F, H\}$.

(a) If the vector $(1, 0, 1, 0, 1)$ is obtained as $f_G(P)$ for some P, can we determine P?

(b) Show that this collection G does not give a successful NAGTA with threshold 1.

44. (a) Use the $(12, 9, 4, 3, 1)$-design of Table 9.25 to construct a successful NAGTA G with threshold 3.

    (b) Use the notation $B_{i,j}$ for the jth block in parallel class C_i. If

$$f_G(P) = (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$$

and we know that $|P| \leq 3$, find P.

45. If $t \geq 2$, a t-(b, v, r, k, λ)-*design* consists of a set V of $v \geq 2$ varieties, and a collection of $b > 0$ subsets of V called blocks, such that (9.10) and (9.11) hold, such that

$$\text{every } t\text{-element subset of } V \text{ is a subset of exactly } \lambda \text{ blocks, } \lambda > 0, \tag{9.29}$$

and such that $k < v$. Obviously, a 2-(b, v, r, k, λ)-design is a (b, v, r, k, λ)-design.

(a) Suppose that $x_{i_1}, x_{i_2}, \ldots, x_{i_t}$, are t distinct varieties of a t-(b, v, r, k, λ)-design. For $1 \leq j \leq t$, let λ_j be the number of blocks containing $x_{i_1}, x_{i_2}, \ldots, x_{i_j}$. Let $\lambda_0 = b$. Show that for $0 \leq j \leq t$,

$$\lambda_j = \frac{\lambda \begin{pmatrix} v - j \\ t - j \end{pmatrix}}{\begin{pmatrix} k - j \\ t - j \end{pmatrix}}, \tag{9.30}$$

and conclude that λ_j is independent of the choice of $x_{i_1}, x_{i_2}, \ldots, x_{i_j}$. Hence, conclude that for all $1 \leq j \leq t$, a t-(b, v, r, k, λ)-design is also a j-(b, v, r, k, λ)-design.

(b) Show that for $t \geq 2$, (9.10) and (9.29) imply (9.11).

(c) Note that if a t-(b, v, r, k, λ)-design exists, the numbers λ_j defined by (9.30) are integers for all j with $0 \leq j \leq t$.

(d) The results of Section 9.5.2 will imply that there is no $(43, 7, 1)$-design. Use this result to prove that even if all λ_j are integers, this is not sufficient for the existence of a t-(b, v, r, k, λ)-design.

46. Suppose that the square matrix $\mathbf{A}$ is the incidence matrix of a BIBD. Show that $\mathbf{A}^{-1}$ exists.

47. If $\mathbf{A}$ is the incidence matrix of a (b, v, r, k, λ)-design, show that $\mathbf{AJ} = r\mathbf{J}$, where $\mathbf{J}$ is a matrix of all 1's.

48. Suppose that $\mathbf{A}$ is a $v \times v$ matrix of 0's and 1's, $v \geq 2$, and that there are $k > 0$ and $\lambda > 0$ with $k > \lambda$ and so that:

    (1) Any row of $\mathbf{A}$ contains exactly k 1's.
    (2) Any pair of rows of $\mathbf{A}$ have 1's in common in exactly λ columns.

This exercise asks the reader to prove that:

(3) Any column of $\mathbf{A}$ contains exactly k 1's.
(4) Any pair of columns of $\mathbf{A}$ have 1's in common in exactly λ rows.

[In particular, it follows that (3) and (4) hold for incidence matrices of (v, k, λ)-designs, and Theorem 9.19 follows.]

(a) Show that $\mathbf{AJ} = k\mathbf{J}$, where $\mathbf{J}$ is a square matrix of all 1's.

(b) Show that $\mathbf{AA}^T = (k - \lambda)\mathbf{I} + \lambda\mathbf{J}$.

(c) Show that $\mathbf{A}^{-1}$ exists.

(d) Show that $\mathbf{A}^{-1}\mathbf{J} = k^{-1}\mathbf{J}$.

(e) Show that $\mathbf{A}^T\mathbf{A} = (k - \lambda)\mathbf{I} + \lambda k^{-1}\mathbf{JA}$.

(f) Show that if $\mathbf{JA} = k\mathbf{J}$, then (3) and (4) follow.

(g) Show that $\mathbf{JA} = k^{-1}(k - \lambda + \lambda v)\mathbf{J}$.

(h) Show that $k - \lambda + \lambda v = k^2$.

(i) Show that $\mathbf{JA} = k\mathbf{J}$ and hence that (3) and (4) hold.

49. In an experiment, there are two kinds of treatments or varieties, the controls and the noncontrols. There are three controls and 120 blocks. Each control is used in 48 blocks. Each pair of controls is used in the same block 24 times. All three controls are used in the same block together 16 times. In how many blocks are none of the controls used?

50. (Stinson [2003]). Suppose that there is an anonymous $(2, p)$-threshold scheme that allows any two persons to find the key but no single person to find it with probability higher than $1/|K|$.

(a) Show that $|P| \geq (p - 1)|K| + 1$. (*Hint:* For $\kappa \in K$, let C_κ be the set of all possible p-element subsets of P that could be distributed, one per person, when the secret key is κ. Argue that these subsets overlap in exactly one element.)

(b) Show that if $|P| = (p-1)|K|+1 = v$, there must exist a resolvable (b, v, r, k, λ)-design with $k = p$. (*Hint:* Use the subsets defined in part (a) as blocks.)

51. Prove that an $S(5, 7, 18)$ Steiner system doesn't exist.

52. How many blocks are present in an $S(5, 6, 48)$ Steiner system?

53. Suppose that an $S(t, k, v)$ Steiner system exists on a set V.

(a) Prove that an $S(t - 1, k - 1, v - 1)$ Steiner system also exists. (*Hint:* Fix an element of V and consider only those k-element subsets that contain it.)

(b) Conclude that an $S(t - j, k - j, v - j)$ Steiner system exists for every $j < t$.

54. (Anderson [1990]) Using Exercise 53 and the fact that an $S(5, 8, 24)$ Steiner system exists on a set V, show that

(a) the number of blocks in an $S(5, 8, 24)$ Steiner system is 759,

(b) every element of V lies in 253 blocks,

(c) every pair of elements of V lies in 77 blocks,

(d) every triple of elements of V lies in 21 blocks,

(e) every quadruple of elements of V lies in 5 blocks,

(f) every quintuple of elements of V lies in exactly 1 block.

9.5 FINITE PROJECTIVE PLANES

9.5.1 Basic Properties

It is interesting that experimental designs have geometric applications, and conversely that geometry has played an important role in the analysis of experimental designs. Let us consider the design of Example 9.10. This is a Steiner triple system and a symmetric BIBD. It can be represented geometrically by letting the varieties be points and representing a block by a "line" (not necessarily straight) through the points it contains. Figure 9.1 shows this geometric representation. All but one line is straight. This representation is known as a *projective plane*, the *Fano plane*.[23] It has the following properties:

(P_1) Two distinct points lie on one and only one common line.
(P_2) Two distinct lines pass through one and only one common point.

In general, a *projective plane* consists of a set of objects called *points*, a second set of objects called *lines*, and a notion of when a *point lies on a line*, or equivalently, when a *line passes through a point*, so that conditions (P_1) and (P_2) hold. A projective plane is *finite* if the set of points is finite. Projective planes are important not only in combinatorial design but also in art, where they arise in the study of perspective. They are also important in geometry, for they define a geometry where Euclid's parallel postulate is violated: By (P_2), there is no line that passes through a given point and has no points in common with (and hence is "parallel" to) a given line. The development of projective geometry had its roots in the work of Pappas of Alexandria in the fourth century. It led in the 1840s to the algebraic theory of invariance, developed by the famous mathematicians Boole, Cayley, and Sylvester. This in turn led to the tensor calculus, and eventually to ideas of fundamental importance in physics, in particular to the work of Einstein in the theory of gravitation.

The basic existence question that dominates the theory of combinatorial design arises also for projective planes: For what values of n is there a projective plane of n points? If $n = 2$, we can take two points a and b and one line L that passes through the two points. The postulates (P_1) and (P_2) for a projective plane are trivially satisfied. They are also trivially satisfied if there are n points, any n, and just one line, which passes through all n points. Finally, they are trivially satisfied if there are three points, a, b, and c, and three lines, L_1, L_2, and L_3, with a and b lying on L_1, b and c on L_2, and a and c on L_3. To rule out these dull examples, one usually adds one additional postulate:

(P_3) There are four distinct points, no three of which lie on the same line.

A finite projective plane satisfying (P_3) is called *nondegenerate* and we shall assume (without making the assumption explicit every time) that *all finite projective*

[23] Named after a nineteenth-century mathematician, Gino Fano.

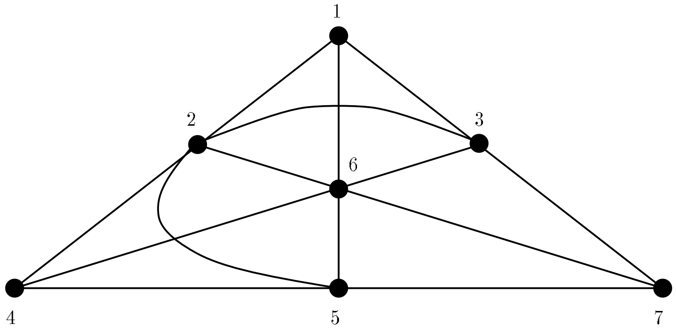

Figure 9.1: The Fano plane.

planes are nondegenerate. Any theorem about these planes will be proved using the postulates (P_1), (P_2), and (P_3).

The smallest possible projective plane would now have at least four points. Is there such a plane with exactly four points? Suppose that a, b, c, and d are four points, and that no three lie on a line. By (P_1), there must be a line L_1 passing through a and b and a line L_2 passing through c and d. Since no three of these points lie on a line, c and d are not on L_1 and a and b are not on L_2. Then if a, b, c, and d are all the points of the projective plane, L_1 and L_2 do not have a common point, which violates (P_2). Thus, there is no projective plane of four points. We shall see below that there is no projective plane of five or six points either. However, the Fano plane of Figure 9.1 is a projective plane of seven points, for (P_3) is easy to verify.

The reader will note that the postulates (P_1) and (P_2) have a certain *duality*: We obtain (P_2) from (P_1) by interchanging the words "point" and "line" and interchanging the expressions "point lying on a line" and "line passing through a point." We obtain (P_1) from (P_2) by the same interchanges. If (P) is any *statement* about finite projective planes, the *dual* of (P) is the statement obtained from (P) by making these interchanges. The dual of postulate (P_3) turns out to be true, and we formulate this result as a theorem.

Theorem 9.23 In a finite projective plane, the following holds:

(P_4) There are four distinct lines, no three of which pass through the same point.

Proof. By (P_3), there are points a, b, c, d no three of which lie on a line. By (P_1), there are lines L_1, through a and b, L_2 through b and c, L_3 through c and d, and L_4 through d and a. Now these four lines are distinct, because c and d are not in L_1, a and d are not in L_2, and so on. Moreover, no three of these lines pass through a common point. We prove this by contradiction. Suppose without loss of generality that L_1, L_2, and L_3 have the point x in common. Then x could not be b, for b is not on L_3. Now L_1 and L_2 have two distinct points in common, b and x. Since $L_1 \neq L_2$, postulate (P_2) is violated, which is a contradiction. Q.E.D.

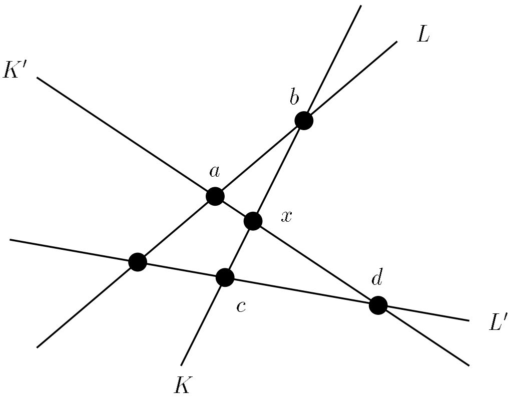

Figure 9.2: The point x is not on either line L or line L'.

Now conditions (P_1) and (P_2) are duals and conditions (P_3) and (P_4) are duals. Any theorem (provable statement) about finite projective planes must be proved from the postulates (P_1), (P_2), and (P_3). Any such theorem will have a *dual theorem*, obtained by interchanging the words "point" and "line" and interchanging the expressions "point lying on a line" with "line passing through a point." A proof of the dual theorem can be obtained from a proof of the theorem by replacing (P_1), (P_2), and (P_3) by their appropriate dual statements, which we know to be true. Thus, we have the following result.

Theorem 9.24 (Duality Principle) For every statement about finite projective planes which is a theorem, the dual statement is also a theorem.

The next basic theorem about finite projective planes is the following.

Theorem 9.25 In a finite projective plane, every point lies on the same number of lines, and every line passes through the same number of points.

To illustrate this theorem, we note that the projective plane of Figure 9.1 has three points on a line and three lines through every point.

Proof of Theorem 9.25. We first show that every line passes through the same number of points. The basic idea of the proof is to set up a one-to-one correspondence between points on two distinct lines, L and L', which shows that the two lines have the same number of points.

We first show that there is a point x not on either L or L'. By postulate (P_3), there are four points a, b, c, and d, no three of which lie on a line. If any one of these is not on either L or L', we can take that as x. If all of these are on L or L', we must have two points (say, a and b) on L and two (say, c and d) on L'. By (P_1), there are lines K through b and c and K' through a and d. By (P_2), the lines K and K' have a point x in common (see Figure 9.2). If x lies on L, then x and b lie

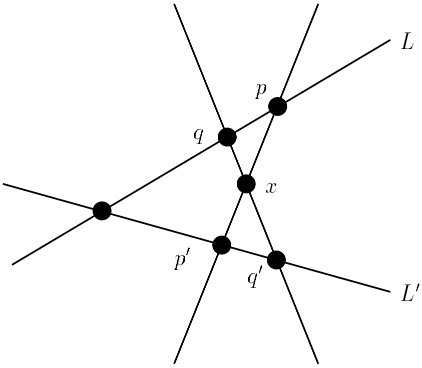

Figure 9.3: The point p' is the projection of p through x onto L'.

on two distinct lines, violating (P_1). If x lies on L', then x and c lie on two distinct lines, again violating (P_1). Thus, x is the desired point.

Now given a point p on line L, the line through p and x [which exists by (P_1)] must meet L' in exactly one point p' [by (P_2)]. We say that p' is the *projection* of p through x onto L' (see Figure 9.3). If q is any other point on L, let q' be its projection through x onto L'. Now if $q \neq p, q'$ must be different from p'. For otherwise, q' and x are on two distinct lines, violating (P_1). We conclude that projection defines a one-to-one correspondence between points of L and points of L'. We know that it is one-to-one. To see that it is a correspondence, note that every point r of L' is obtained from some point of L by this procedure. To see that, simply project back from r through x onto L. Thus, L and L' have the same number of points. This proves that every line passes through the same number of points.

By using the duality principle (Theorem 9.24), we conclude that every point lies on the same number of lines. Q.E.D.

Theorem 9.26 In a finite projective plane, the number of lines through each point is the same as the number of points on each line.

Proof. Pick an arbitrary line L. By (P_3), there is a point x not on line L. By (P_1), for any point y on L, there is one and only one line $L(y)$ passing through x and y. Moreover, any line L' through x cannot be L, and hence by (P_2) it must pass through a point y of L, so L' is $L(y)$. Thus, $L(y)$ defines a one-to-one correspondence between points of L and lines through x. Thus, there are the same number of lines through x as there are points on L. The theorem follows from Theorem 9.25. Q.E.D.

It follows from Theorem 9.26 that the projective plane with $m+1$ points on each line has $m+1$ lines through each point.

Corollary 9.26.1 A projective plane with $m+1$ points on each line and $m+1$ lines through each point has m^2+m+1 points and m^2+m+1 lines.

Table 9.30: A Projective Plane of Order 3 (Having 13 Points and 13 Lines)

Points:	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
Lines:	{1, 2, 8, 12}, {3, 9, 10, 12}, {4, 5, 11, 12}, {1, 4, 6, 9}, {3, 6, 8, 11}, {2, 5, 6, 10}, {1, 10, 11, 13}, {5, 8, 9, 13}, {2, 3, 4, 13}, {1, 3, 5, 7}, {4, 7, 8, 10}, {2, 7, 9, 11}, {6, 7, 12, 13}.

Proof. Let x be any point. There are $m+1$ lines through x. Each such line has m points other than x. Every point lies on one and only one line through x. Hence, we count all the points by counting the number of points other than x on the lines through x and adding x; we get

$$(m+1)(m)+1 = m^2+m+1$$

points. The rest of the corollary follows by a duality argument. Q.E.D.

In our example of Figure 9.1, $m+1 = 3, m = 2$, and $m^2+m+1 = 7$. We know now that projective planes of n points can only exist for n of the form m^2+m+1. In particular, no such planes can exist for $n = 4, 5$, or 6. Postulate (P_3) rules out $n = 3$ (even though $3 = 1^2+1+1$). Thus, $n = 7$ corresponds to the first possible projective plane. The next possible one is obtained by taking $m = 3$, obtaining $n = 3^2+3+1 = 13$. We will see that projective planes exist whenever m is a power of a prime. Thus, the 13-point plane ($m = 3$) will exist. (Table 9.30 shows such a plane.) The number m will be called the *order* of the projective plane. Note that the order is different from the number of points.

9.5.2 Projective Planes, Latin Squares, and (v, k, λ)-Designs

In this section we investigate the relations among projective planes and certain kinds of combinatorial designs.

Theorem 9.27 (Bose [1938]) Suppose that $m \geq 2$. A finite projective plane of order m exists if and only if a complete orthogonal family of $m \times m$ Latin squares exists.[24]

The proof of this theorem is constructive; that is, it shows how to go back and forth between finite projective planes and sets of orthogonal Latin squares. We sketch the proof in Exercises 22 and 23.

Corollary 9.27.1 If $m = p^k$ for p prime and k a positive integer, there is a projective plane of order m.

Proof. The result follows by Theorem 9.2. Q.E.D.

[24] Recall that by our convention, a single 2×2 Latin square constitutes an orthogonal family.

It follows from Theorem 9.27 and Corollary 9.27.1 that the first possible order m for which there does not exist a finite projective plane of that order (i.e., of $m^2 + m + 1$ points) is $m = 6$. In fact, for $m = 6$, we have seen in Section 9.2 that there does not exist a set of five orthogonal 6×6 Latin squares (or indeed a pair of such squares), and hence there is no finite projective plane of order 6 (i.e., of $6^2 + 6 + 1 = 43$ points). There are projective planes of orders $7, 8$, and 9, since $7 = 7^1, 8 = 2^3$, and $9 = 3^2$. However, $m = 10$ is not a power of a prime. Lam, Thiel, and Swiercz [1989] used a computer proof to show the nonexistence of a finite projective plane of order 10 (i.e., $10^2 + 10 + 1 = 111$ points). We know that there is a finite projective plane of order 11, but 12 remains an open problem.

The next theorem takes care of some other cases not covered by Corollary 9.27.1. We omit the proof.

Theorem 9.28 (Bruck and Ryser [1949]) Let $m \equiv 1$ or 2 (mod 4). Suppose that the largest square dividing into m is d and that $m = m'd$. If m' is divisible by a prime number p which is $\equiv 3$(mod 4), there does not exist a projective plane of order m.

To illustrate this theorem, suppose that $m = 6$. Note that $6 \equiv 2 \pmod{4}$. Then $d = 1$ and $m' = m$. Since m' is divisible by 3, there is no projective plane of order 6, as we observed previously. Next, suppose that $m = 54$. Note that $54 \equiv 2$ (mod 4), that $d = 9$, and that $m' = 6$. Since 3 divides m', there is no projective plane of order 54. It follows by Theorem 9.27 that there is no complete orthogonal family of Latin squares of order 54.

A projective plane gives rise to a (b, v, r, k, λ)-design by taking the varieties as the points and the blocks as the lines. Then $b = v = m^2 + m + 1, k = r = m + 1$, and $\lambda = 1$ since each pair of points lies on one and only one line. Hence, we have a symmetric balanced incomplete block design or a (v, k, λ)-design. Conversely, for every $m \geq 2$, an $(m^2 + m + 1, m + 1, 1)$-design gives rise to a projective plane by taking the varieties as the points and the blocks as the lines. To see why Axiom (P_3) holds, let a and b be any two points. There is a unique block B_1 containing a and b. Since the design is incomplete, there is a point x not in block B_1. Now there is a unique block B_2 containing a and x and there is a unique block B_3 containing b and x. Each block has $m+1$ points. Thus, other than a, b, and x, B_1, B_2, and B_3 each have at most $m - 1$ other points. In short, the number of points in B_1, B_2, or B_3 is at most $3 + 3(m - 1) = 3m$. Since $m \geq 2$, we have $m^2 + m + 1 > 3m$. Thus, there is a point y not in B_1, B_2, or B_3. No three of the points a, b, x, and y lie in a block. Thus, we have the following result.

Theorem 9.29 If $m \geq 2$, a finite projective plane of order m exists if and only if an $(m^2 + m + 1, m + 1, 1)$-design exists.

Corollary 9.29.1 There are $(m^2 + m + 1, m + 1, 1)$-designs whenever m is a power of a prime.

Corollary 9.29.2 Suppose that $m \geq 2$. Then the following are equivalent.

(a) There exists a finite projective plane of order m.
(b) There exists a complete orthogonal family of Latin squares of order m.
(c) There exists an $(m^2 + m + 1, m + 1, 1)$-design.

EXERCISES FOR SECTION 9.5

1. In each of the following, P is a set of points and Q a set of lines. A point x lies on a line L if $x \in L$ and a line L passes through a point x if $x \in L$. Determine which of axioms $(P_1), (P_2)$, and (P_3) hold.

   (a) $P =$ all points in 3-space, $Q =$ all lines in 3-space.
   (b) $P = \{1, 2, 3\}, Q = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$.
   (c) $P =$ any set, $Q =$ all ordered pairs from P.
   (d) $P =$ all lines in 3-space, $Q =$ all planes in 3-space.
   (e) $P =$ all lines through the origin in 3-space, $Q =$ all planes through the origin in 3-space.

2. State the dual of each of the following (not necessarily true) statements about finite projective planes.

   (a) There are nine distinct lines, no three of which pass through the same point.
   (b) There is a point that lies on every line.
   (c) There are four distinct lines so that every point lies on one of these lines.
   (d) There are four distinct points, no three of which lie on the same line, so that every line passes through one of these points.

3. If a projective plane has four points on every line, how many points does it have in all?
4. If a projective plane has five lines through every point, how many points does it have in all?
5. If a projective plane has 31 points, how many points lie on each line?
6. If a projective plane has 57 points, how many lines pass through each point?
7. If a projective plane has 73 lines, how many points lie on each line?
8. Is there a projective plane of:

   (a) 25 points? (b) 73 points? (c) 43 lines? (d) 91 lines?

9. Suppose that a projective plane has n points and a (v, k, λ)-design is defined from the plane with the points as the varieties and the lines as the blocks. For each of the following values of n, compute v, k, and λ.

   (a) 31 (b) 91 (c) 133

10. Could there be a finite projective plane of order (not number of points) equal to the following values? Justify your answer.

    (a) 11 (b) 49 (c) 81

11. Show that there is no finite projective plane of order 14.
12. Show that there could be no finite projective plane of order 245.
13. Show that there could be no finite projective plane of order 150.
14. Could there be a finite projective plane of order equal to the following values? Justify your answer.

    (a) 60 (b) 81 (c) 93

15. Show that there is no complete orthogonal family of Latin squares of order 378.
16. Recall the definition of *projection* in the proof of Theorem 9.25. In the Fano plane (Figure 9.1):

    (a) Find the projection of the point 6 on the line $\{3, 4, 6\}$ through the point 5 onto the line $\{1, 3, 7\}$.
    (b) Find the projection of the point 4 on the line $\{1, 2, 4\}$ through the point 3 onto the line $\{2, 6, 7\}$.
    (c) Find the projection of the point 2 on the line $\{1, 2, 4\}$ through the point 3 onto the line $\{4, 5, 7\}$.

17. Recall the definition of *projection* in the proof of Theorem 9.25. In the projective plane of Table 9.30:

    (a) Find the projection of the point 2 on the line $\{2, 3, 4, 13\}$ through the point 8 onto the line $\{1, 4, 6, 9\}$.
    (b) Find the projection of the point 11 on the line $\{2, 7, 9, 11\}$ through the point 1 onto the line $\{2, 5, 6, 10\}$.

18. (Bogart [1983]). Take the points of an $(n^2+n, n^2, n+1, n, 1)$-design as the points and the blocks of this design as the lines. Which of axioms $(P_1), (P_2), (P_3)$ are satisfied?
19. Show that in Exercise 18, the following "parallel postulate" is satisfied: Given a point x and a line L not passing through x, there is one and only one line L' passing through x that has no points in common with L.
20. An *affine plane* is related to a projective plane in that it satisfies axioms (P_1), (P_3), and the "parallel postulate" of Exercise 19. Prove the following about affine planes:

    (a) Every line contains the same number of points.
    (b) Every point is on the same number of lines.
    (c) If every line contains the same number n of points, then every point is on exactly $n + 1$ lines, there are exactly n^2 points, and there are exactly $n^2 + n$ lines.

21. In an affine plane (see Exercise 20), every line contains the same number n of points. We call n the *order* of the affine plane. Prove that if there is a projective plane of order n, there is an affine plane of order n. (*Hint:* Remove a line and all of its points.)

22. The next two exercises sketch a proof of Theorem 9.27. Let P be a finite projective plane of order m.

    (a) Pick a line L from P arbitrarily and call L the *line at infinity.* Let L have points
    $$u, v, w_1, w_2, \ldots, w_{m-1}.$$
    Through each point of L there are $m+1$ lines, hence m lines in addition to L. Let these be listed as follows:
    $$\begin{array}{rl} \text{lines through } u: & U_1, U_2, \ldots, U_m, \\ \text{lines through } v: & V_1, V_2, \ldots, V_m, \\ \text{lines through } w_j: & W_{j1}, W_{j2}, \ldots, W_{jm}. \end{array}$$
    Every point x not on line L is joined by a unique line to each point on L. Suppose that U_h is the line containing x and u, V_i the line containing x and v, and W_{jk_j} the line containing x and w_j. Thus, we can associate with the point x the $(m+1)$-tuple $(h, i, k_1, k_2, \ldots, k_{m-1})$. Show that the correspondence between points x not on L and ordered pairs (h, i) is one-to-one.

    (b) Illustrate this construction with the projective plane of Table 9.30. Write out all of the lines and the associations $x \rightarrow (h, i)$ and $x \rightarrow (h, i, k_1, k_2)$, assuming that $\{1, 2, 8, 12\}$ is the line at infinity.

    (c) Let $a_{hi}^{(j)} = k_j$ if the point x corresponding to ordered pair (h, i) gives rise to the $(m+1)$-tuple $(h, i, k_1, k_2, \ldots, k_{m-1})$, and let $A^{(j)} = (a_{hi}^{(j)}), j = 1, 2, \ldots, m-1$. Find $A^{(1)}$ and $A^{(2)}$ for the projective plane of Table 9.30.

    (d) Show that $A^{(j)}$ is a Latin square.

    (e) Show that $A^{(p)}$ and $A^{(q)}$ are orthogonal if $p \neq q$.

23. Suppose that $A^{(1)}, A^{(2)}, \ldots, A^{(m-1)}$ is a family of pairwise orthogonal Latin squares of order m.

    (a) Consider m^2 "finite" points $(h, i), h = 1, 2, \ldots, m, i = 1, 2, \ldots, m$. Given the point (h, i), associate with it the $(m+1)$-tuple
    $$(h, i, k_1, k_2, \ldots, k_{m-1}),$$
    where k_j is $a_{hi}^{(j)}$ Find these $(m+1)$-tuples given the two orthogonal Latin squares $A^{(1)}$ and $A^{(2)}$ of order 3 shown in Table 9.14. (This will be our running example.)

    (b) Form $m^2 + m = m(m+1)$ lines $W_{jk}, j = -1, 0, 1, 2, \ldots, m-1, k = 1, 2, \ldots, m$, by letting W_{jk} be the set of all finite points (h, i) where the $(j+2)$th entry in the $(m+1)$-tuple corresponding to (h, i) is k. (These lines will be extended by one point later.) Identify the lines W_{jk} in our example.

    (c) Note that for fixed j,
    $$W_{j1}, W_{j2}, \ldots, W_{jm} \tag{9.31}$$
    as we have defined them is a collection of m lines, no two of which intersect. We say that two of these are *parallel* in the sense of having no finite points in common. Show that W_{jk} has m finite points.

(d) Show that if $j \neq j'$, then W_{jk} and $W_{j'k'}$ as we have defined them have one and only one common point.

(e) We now have $m+1$ sets of m parallel lines, and any two nonparallels intersect in one point. To each set of parallels (9.31), we now add a distinct "point at infinity," w_j, lying on each line in the set. Let $w_{-1} = u$ and $w_0 = v$. We have added $m+1$ infinite points in all. We then add one more line L, the "line at infinity," defined to be the line consisting of $u, v, w_1, w_2, \ldots, w_{m-1}$. Complete and update the list of lines begun for our example in part (b). Also list all points (finite or infinite) in this example.

(f) Find in general the number of points and lines constructed.

(g) Find the number of points on each line and the number of lines passing through each point.

(h) Verify that postulates $(P_1), (P_2)$, and (P_3) hold with the collection of all points (finite or infinite) and the collection of all lines W_{jk} as augmented plus the line L at infinity. [*Hint:* Verify (P_2) first.]

REFERENCES FOR CHAPTER 9

ANDERSON, I., *Combinatorial Designs: Construction Methods*, Prentice Hall, Upper Saddle River, NJ, 1990.

BETH, T., JUNGNICKEL, D., and LENZ, H., *Design Theory*, 2nd ed., Cambridge University Press, New York, 1999.

BOGART, K. P., *Introductory Combinatorics*, Pitman, Marshfield, MA, 1983.

BOSE, R. C., "On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Graeco-Latin Squares," *Sankhyā, 3* (1938), 323–338.

BOSE, R. C., SHRIKHANDE, S. S., and PARKER, E. T., "Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler's Conjecture," *Canad. J. Math., 12* (1960), 189–203.

BOX, G. E. P., HUNTER, W. G., and HUNTER, J. S., *Statistics for Experimenters: An Introduction to Design, Data Analysis, and Model Building*, Wiley, New York, 1978.

BRINKMAN, J., HODGKINSON, D. E., and HUMPHREYS, J. F., "How to Buy a Winning Ticket on the National Lottery," *Math. Gaz., 85* (2001), 202–207.

BRUCK, R. H., and RYSER, H. J., "The Nonexistence of Certain Finite Projective Planes," *Canad. J. Math, 1* (1949), 88–93.

BRUNK, M. E., and FEDERER, W. T., "Experimental Designs and Probability Sampling in Marketing Research," *J. Am. Statist. Assoc., 48* (1953), 440–452.

CHEN, K. K., BLISS, C., and ROBBINS, E. B., "The Digitalis-like Principles of *Calotropis* Compared with Other Cardiac Substances," *J. Pharmacol. Exp. Ther., 74* (1942), 223–234.

CHEN, Y., "The Steiner System $S(3, 6, 26)$," *J. Geometry, 2* (1972), 7–28.

CHOWLA, S., and RYSER, H. J., "Combinatorial Problems," *Canad. J. Math., 2* (1950), 93–99.

COCHRAN, W. G., and COX, G. M., *Experimental Designs*, 2nd ed., Wiley, New York, 1957.

COLBOURN, C. J., and DINITZ, J. H. (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL, 1996.

Colbourn, C. J., Dinitz, J. H., and Stinson, D. R., "Applications of Combinatorial Designs to Communications, Cryptography, and Networking," in J. D. Lamb and D. A. Preece (eds.), *Surveys in Combinatorics, 1999*, London Mathematical Society Lecture Note Series, 267, Cambridge University Press, Cambridge, 1999, 37–100.

Cox, D. R., *Planning of Experiments*, Wiley, New York, 1958.

Davies, H. M., "The Application of Variance Analysis to Some Problems of Petroleum Technology," Technical paper, Institute of Petroleum, London, 1945.

Diffie, W., and Hellman, M. E., "New Directions in Cryptography," *IEEE Trans. Info. Theory, 22* (1976), 644–654.

Dinitz, J. H., and Stinson, D. R. (eds.), *Contemporary Design Theory: A Collection of Surveys*, Wiley, New York, 1992.

Dorfman, R., "The Detection of Defective Members of a Large Population," *Annals of Math. Stats., 14* (1943), 436–440.

Dornhoff, L. L., and Hohn, F. E., *Applied Modern Algebra*, Macmillan, New York, 1978.

Du, D.-Z., and Hwang, F. K., *Combinatorial Group Testing and Its Applications*, 2nd ed., World Scientific, Singapore, 2000.

Durbin, J. R., *Modern Algebra*, 4th ed., University of Chicago Press, Chicago, 1999.

Finney, D. J., *An Introduction to the Theory of Experimental Design*, University of Chicago Press, Chicago, 1960.

Fisher, J. L., *Application-Oriented Algebra*, Harper & Row, New York, 1977.

Fisher, R. A., "The Arrangement of Field Experiments," *J. Minist. Agric., 33* (1926), 503–513.

Fisher, R. A., "An Examination of the Different Possible Solutions of a Problem in Incomplete Blocks," *Ann. Eugen., 10* (1940), 52–75.

Garrett, P., *Making, Breaking Codes: Introduction to Cryptology*, Prentice Hall, Upper Saddle River, NJ, 2001.

Gilbert, J., and Gilbert, L., *Elements of Modern Algebra*, Brooks/Cole, Pacific Grove, CA, 1999.

Hall, M., *Combinatorial Theory*, Blaisdell, Waltham, MA, 1967. (Second printing, Wiley, New York, 1980.)

Hennessy, J. L., and Patterson, D. A., *Computer Architecture: A Quantitative Approach*, 2nd ed., Morgan Kaufmann Publishers, San Francisco, 1998.

Hicks, C. R., *Fundamental Concepts in the Design of Experiments*, Holt, Rinehart and Winston, New York, 1973.

Hill, R., *A First Course in Coding Theory*, Oxford University Press, New York, 1991.

Hughes, D. R., and Piper, F. C., *Design Theory*, 2nd ed., Cambridge University Press, New York, 1988.

Johnson, D. M., Dulmage, A. L., and Mendelsohn, N. S., "Orthomorphisms of Groups and Orthogonal Latin Squares. I," *Canad. J. Math., 13* (1961), 356–372.

Joye, M., and Quisquater, J.-J., "Cryptoanalysis of RSA-Type Cryptosystems: A Visit," in R. N. Wright and P. G. Neumann (eds.), *Network Threats*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 38, American Mathematical Society, Providence, RI, 1998, 21–31.

Kaliski, B. S. (ed.), *Advances in Cryptology – CRYPTO '97. Proceedings of the 17th Annual International Cryptology Conference*, Lecture Notes in Computer Science, 1294, Springer-Verlag, Berlin, 1997.

Kaski, P., and Östergård, P. R. J., "The Steiner Triple Systems of Order 19," *Math. Comp., 73*, (2004), 2075–2092.

KIRKMAN, T. A., "On a Problem in Combinatorics," *Camb. Dublin Math J., 2* (1847), 191–204.

KOBLITZ, N., *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994.

LAM, C. W. H., THIEL, L. H., and SWIERCZ, S., "The Nonexistence of Finite Projective Planes of Order 10," *Canad. J. Math., 41* (1989), 1117–1123.

LI, P. C., and VAN REES, G. H. J., "Lotto Design Tables," *J. Combin. Des., 10* (2002), 335–359.

LINDNER, C. C., and RODGER, C. A., *Design Theory*, CRC Press, Boca Raton, FL, 1997.

MACNEISH, H. F., "Euler Squares," *Ann. Math., 23* (1922), 221–227.

MENEZES, A. J., VAN OORSCHOT, P. C., and VANSTONE, S. A., *Handbook of Applied Cryptography*, CRC Press Series on Discrete Mathematics and Its Applications, CRC Press, Boca Raton, FL, 1997.

PATTERSON, D. A., and HENNESSY, J. L., *Computer Organization and Design: The Hardware/Software Interface*, 2nd ed., Morgan Kaufmann Publishers, San Francisco, 1998.

PUGH, C., "The Evaluation of Detergent Performance in Domestic Dishwashing," *Appl. Statist., 2* (1953), 172–179.

RIVEST, R. L., SHAMIR, A., and ADLEMAN, L. M., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM, 21* (1978), 120–126.

RYSER, H. J., *Combinatorial Mathematics*, Carus Mathematical Monographs, No. 14, Mathematical Association of America, Washington, DC, 1963.

SALOMAA, A., *Public-Key Cryptography*, Texts in Theoretical Computer Science—An EATCS Series, Springer-Verlag, Berlin, 1996.

SLOANE, N. J. A., "Error-Correcting Codes and Cryptography," in D. A. Klarner (ed.), *The Mathematical Gardner*, Wadsworth, Belmont, CA, 1981, 346–382.

STINSON, D. R., "A Short Proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six," *J. Combin. Theory (A), 36* (1984), 373–376.

STINSON, D. R., "The Combinatorics of Authentication and Secrecy Codes," *J. Cryptology, 2* (1990), 23–49.

STINSON, D. R., *Combinatorial Designs: Constructions and Analysis*, Springer-Verlag, New York, 2003.

STREET, A. P., and STREET, D. J., *Combinatorics of Experimental Design*, Oxford University Press, New York, 1987.

TARRY, G., "Le Problème de 36 Officieurs," *C. R. Assoc. Fr. Avance. Sci. Nat., 1* (1900), 122–123.

TARRY, G., "Le Problème de 36 Officieurs," *C. R. Assoc. Fr. Avance. Sci. Nat., 2* (1901), 170–203.

WADLEY, F. M., "Experimental Design in the Comparison of Allergens on Cattle," *Biometrics, 4* (1948), 100–108.

WALLIS, W. D., *Combinatorial Designs*, Marcel Dekker, New York, 1988.

WILLIAMS, E. J., "Experimental Designs Balanced for the Estimation of Residual Effects of Treatments," *Aust. J. Sci. Res., A2* (1949), 149–168.

YATES, F., "Incomplete Randomized Blocks," *Ann. Eugen., 7* (1936), 121–140.

YOUDEN, W. J., "Use of Incomplete Block Replications in Estimating Tobacco-Mosaic Virus," *Contrib. Boyce Thompson Inst., 9* (1937), 41–48.