

## Solutions to Exercises

### Chapter 6: Latin squares and SDRs

**1** Show that the number of  $n \times n$  Latin squares is 1, 2, 12, 576 for  $n = 1, 2, 3, 4$  respectively.

(b) Prove that, up to permutations of the rows, columns, and symbols in a Latin square, there are unique squares of orders 1, 2, 3, and two different squares of order 4.

(c) Show that one of the two types of Latin square of order 4 has an orthogonal 'mate' and the other does not.

(a) Build up the Latin squares row by row. Note that, once  $n - 1$  rows have been entered, there is a unique way to complete the last row. Note also that each of the  $n!$  possible first rows can be completed in the same number of ways.

For  $n = 1$ , there is only one Latin square, namely (1).

For  $n = 2$ , if the first row is (1 2), then the second is (2, 1), and *vice versa*.

For  $n = 3$ , we count the Latin squares with first row (1 2 3), and multiply the number by  $3! = 6$ . Now the first entry in the second row is either 2 or 3, and in either case, the entire square is determined. For suppose it is 2. The third entry of this row then cannot be 2, and cannot be 3 (since there is already a 3 in its column); so it must be 1, and the row is (2 3 1). So there are two squares with the given first row, and  $2 \cdot 6 = 12$  altogether.

The case  $n = 4$  is a little more complicated. Assume that the first row is (1 2 3 4). The second row (regarded as a permutation) is then a derangement. We know (Chapter 1, Question 1) that there are nine derangements, which fall into two types: six are cyclic permutations, and three consist of two transpositions. We show that a cyclic permutation can be completed in two different ways, and a permutation of the other type in four ways.

Suppose that the second row is (2 3 4 1). The first element of the third row is either 3 or 4; in each case the square can be completed uniquely (much as for  $n = 3$  above).

Suppose that the second row is (2 1 4 3). Now, in the third and fourth rows, the first two entries are 3 and 4, and the last two are 1 and 2. So the last two rows consist of two Latin squares using the symbol sets  $\{3, 4\}$  and  $\{1, 2\}$ . There are two choices for each (by the result for  $n = 2$ , so four possible completions.

So the total number of squares is  $24(6 \cdot 2 + 3 \cdot 4) = 576$ .

(b) By permuting the columns, the first row of any square can be brought to the form (1 2 ...  $n$ ). Then permuting rows other than the first brings the first column

to the same form. So at least  $n! \cdot (n-1)!$  squares can be obtained from any one by row and column permutations. Dividing the numbers obtained in part (a) by this factor, we see that there are at most 1, 1, 1, 2 squares for  $n = 1, 2, 3, 4$ , up to row and column permutations. It remains to show that there are really two different squares in the case  $n = 4$ .

To see this, we count subsquares of order 2. For the square obtained from the non-cyclic derangement, any two rows consist of two disjoint Latin squares of order 2 (using disjoint symbol sets). This property remains true if rows or columns are permuted. But for the square obtained from the cyclic derangement, the first two rows contain no Latin square of order 2. So this square is not obtained from the other by row and column permutations.

The solution to Chapter 1, Question 3 gives two orthogonal Latin squares of order 4, and by inspection, each of them is of the ‘non-cyclic type’. We have to show that the ‘cyclic’ square has no orthogonal mate. We can take the square to be

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

since the property of having an orthogonal mate is not changed by row and column permutations. Furthermore, we can assume that the first row of the orthogonal mate is (1 2 3 4). The first element of the second row is then 3 or 4, and it is easily checked that neither case can be completed.

**2** Show that, for  $n \leq 4$ , any Latin square of order  $n$  can be obtained from the multiplication table of a group by permuting rows, columns, and symbols; but this is not true for  $n = 5$ .

There is a unique group of each order 1, 2, 3, and two of order 4 (up to isomorphism); check that these give all the Latin squares.

For  $n = 5$ , the cyclic group is the only type of group, and gives a Latin square containing no subsquare of order 2. If we complete the two rows

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

to a Latin square, the resulting square contains a subsquare of order 2, and so is not equivalent to the one derived from the cyclic group.

**3** A Latin square  $A = (a_{ij})$  of order  $n$  is said to be *row-complete* if every ordered pair  $(x, y)$  of distinct symbols occurs exactly once in consecutive positions in the same row (i.e., as  $(a_{ij}, a_{i, j+1})$  for some  $i, j$ ). (Note that there are  $n(n-1)$  ordered pairs of distinct symbols, and each of the  $n$  rows contains  $n-1$  consecutive pairs of symbols.)

(a) Prove that there is no row-complete Latin square of order 3 or 5, and construct one of order 4.

(b) Define analogously a *column-complete* Latin square.

(c) Suppose that the elements of  $\mathbf{Z}/(n)$  are written in a sequence  $(x_1, x_2, \dots, x_n)$  with the property that every non-zero element of  $\mathbf{Z}/(n)$  can be written uniquely in the form  $x_{i+1} - x_i$  for some  $i = 1, \dots, n-1$ . Let  $A$  be the Latin square (with rows, columns and entries indexed by  $0, \dots, n-1$  instead of  $1, \dots, n$ ) whose  $(i, j)$  entry is  $a_{ij} = x_i + x_j$ . (This is the addition table of the integers mod  $n$ , written in a strange order.) Prove that  $A$  is both row-complete and column-complete.

(d) If  $n$  is even, show that the sequence

$$(0, 1, n-1, 2, n-2, \dots, \frac{1}{2}n-1, \frac{1}{2}n+1, \frac{1}{2}n)$$

has the property described in (c).

(a) Since the property of row-completeness is unaffected if we rename the symbols, or if we permute the columns, for  $n = 3$  we need only check that the square

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

is not row-complete: indeed, the pair  $(1, 2)$  occurs twice and the pair  $(2, 1)$  not at all.

For  $n = 5$ , we may assume that the first row is  $(1 \dots 5)$  and that the 1s occur on the main diagonal of the square. The 1s in rows 2, 3, 4 must be followed by 3, 4, 5 in some order; the Latin property gives the possibilities 4, 5, 3 or 5, 3, 4 only. In each case the square can be completed uniquely, and is not row-complete.

For  $n = 4$ , trial and error (or the construction in parts (c) and (d)) gives

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

(b) A Latin square  $A = (a_{ij})$  of order  $n$  is *column-complete* if every ordered pair  $(x, y)$  of distinct symbols occurs exactly once in consecutive positions in the same column (that is, as  $(a_{ij}, a_{i+1j})$  for some  $i, j$ ).

(c) Suppose that the sequence  $(x_1, \dots, x_n)$  has the property specified in the question, and let  $A = (a_{ij})$ , where  $a_{ij} = x_i + x_j$ .

*A is a Latin square:* If  $a_{ij} = a_{ik}$ , then  $x_i + x_j = x_i + x_k$ , whence  $x_j = x_k$  and  $j = k$  (since  $x_1, \dots, x_n$  are all distinct). So the entries in any row are distinct. The argument for columns is similar.

*A is row-complete:* Let  $(x, y)$  be given, with  $x \neq y$ . We seek values  $i$  and  $j$  such that  $a_{ij} = x$ ,  $a_{i+1j} = y$ . This gives  $x_i + x_j = x$ ,  $x_i + x_{j+1} = y$ , whence  $x_{j+1} - x_j = y - x$ . By the property of the sequence, the non-zero element  $y - x$  occurs just once as the difference of consecutive elements; so from this equation we determine a unique value of  $j$ . Now  $x_i = x - x_j$  is determined, and hence there is a unique value of  $i$  also.

*A is column-complete:* Either argue similarly, or use the fact that  $A$  is symmetric.

(d) The differences  $x_{2i+1} - x_{2i}$ , for  $i = 0, 1, 2, \dots, \frac{1}{2}n - 1$ , are  $1 - 0 = 1, 2 - (n - 1) = 3, 3 - (n - 2) = 5, \dots$ : that is, all the odd numbers less than  $n$ . The differences  $x_{2i} - x_{2i-1}$ , for  $i = 1, 2, \dots, \frac{1}{2}n - 1$ , are  $(n - 1) - 1 = n - 2, (n - 2) - 2 = n - 4, \dots$ : that is, all the even numbers.

**4** (a) Find a family of three subsets of a 3-set having exactly three SDRs.

(b) How many SDRs does the family

$$\{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}$$

have?

(a) Take  $A_1 = \{1, 2\}$ ,  $A_2 = \{1, 3\}$ ,  $A_3 = \{1, 2, 3\}$ . The representatives for  $A_1$  and  $A_2$  must be  $(1, 3)$ ,  $(2, 1)$  or  $(2, 3)$ , and the unused element must be the representative for  $A_3$ .

(b) There are 24 SDRs. This can be proved by laboriously listing them all. The argument can be shortened by using the symmetry of the family, though it is

necessary to use some care in justifying the symmetry arguments. Whenever it is claimed that ‘by symmetry, we may assume that the representative of  $A_i$  is  $j$ ’, say, the justification consists of permutations which preserve the family and fix all the choices already made while permuting the possible choices at the next stage among themselves. I will not list all these permutations: see Section 14.6.

By symmetry, we can assume that the representative of  $\{1, 2, 3\}$  is 1 (and we must multiply the number of SDRs we find by 3 to allow for the other possible choices here). We may further assume that the representatives of the other sets containing 1, namely  $\{1, 4, 5\}$  and  $\{1, 6, 7\}$ , are 4 and 6, and must multiply the number of SDRs also by  $2 \cdot 2 = 4$ . Now we must represent  $\{2, 4, 6\}$  by 2. If we remove these points from the remaining sets, we are left with  $\{3, 5\}$ ,  $\{3, 7\}$  and  $\{5, 7\}$ , which have two SDRs. So there are 24 altogether.

**5** Let  $(A_1, \dots, A_n)$  be a family of subsets of  $\{1, \dots, n\}$ . Suppose that the incidence matrix of the family is invertible. Prove that the family possesses a SDR.

Let  $M = (m_{ij})$  be the incidence matrix of the family: that is,

$$m_{ij} = \begin{cases} 1 & \text{if } j \in A_i, \\ 0 & \text{otherwise.} \end{cases}$$

Since  $M$  is invertible, we have  $\det(M) \neq 0$ . Using the formula for the determinant as a sum over permutations, we see that there is a permutation  $\pi$  of  $\{1, 2, \dots, n\}$  such that  $m_{i i\pi} \neq 0$  for all  $i$ . This means that  $i\pi \in A_i$  for all  $i$ . Since  $\pi$  is a permutation,  $(1\pi, \dots, n\pi)$  is a SDR.

Note: Each SDR corresponds to a non-zero term in the expansion of the determinant; and the value of the term is  $\pm 1$  (the sign is the sign of the corresponding permutation). So we can say more: the number of SDRs is not less than  $|\det(M)|$ , and is congruent to  $\det(M) \pmod{2}$ .

**6** Use the truth of the van der Waerden permanent conjecture to prove that the number  $d(n)$  of derangements of  $\{1, \dots, n\}$  satisfies

$$d(n) \geq n! \left(1 - \frac{1}{n}\right)^n.$$

How does this estimate compare with the truth?

In the language of SDRs, a derangement of  $\{1, \dots, n\}$  is precisely a SDR for the family of sets  $(A_1, A_2, \dots, A_n)$ , where  $A_i = \{1, \dots, n\} \setminus \{i\}$ . Then (6.5.2) applies, with  $r = n - 1$ ; so the number of SDRs is at least  $n!((n - 1)/n)^n$ .

Since  $(1 - 1/n)^n \rightarrow e$  as  $n \rightarrow \infty$ , the formula is asymptotically correct. However, it does not give the correct value as the nearest integer. For  $n = 3, 4, 5$ , the lower bound is approximately 1.778, 7.594, 39.322, whereas the actual value is 2, 9, 44.

**7** Prove the following generalisation of Hall's Theorem:

*If a family  $(A_1, \dots, A_n)$  of subsets of  $X$  satisfies  $|A(J)| \geq |J| - r$  for all  $J \subseteq \{1, \dots, n\}$ , then there is a subfamily of size  $n - r$  which has a SDR.*

Let  $y_1, \dots, y_r$  be  $r$  new elements not in  $X$ . Define  $A'_i = A_i \cup \{y_1, \dots, y_r\}$  for  $i = 1, \dots, n$ . Then, for any  $J \subseteq \{1, \dots, n\}$ , we have

$$|A'(J)| = |A(J)| + r \geq |J| - r + r = |J|.$$

So the family  $(A'_1, \dots, A'_n)$  satisfies Hall's condition, and has an SDR. Now at most  $r$  of the elements of the SDR are  $y$ s; the remainder (at least  $n - r$  of them) belong to  $X$ , and so are representatives of the corresponding  $A_i$ s.