

**MAS334 Combinatorics**  
**Autumn Semester 2011–2012**  
**Dr Sarah Whitehouse**

Lecture Notes  
(based on notes by Dr Victor Bryant)



## Contents

Chapter 1. The Binomial Coefficients	5
Chapter 2. Three Basic Principles	11
1. Parity	11
2. The Pigeon-Hole Principle	12
3. Inclusion/Exclusion	12
Chapter 3. Rook Polynomials	15
1. Definition of Rook Polynomials	15
2. Some Problems which Reduce to Rooks	16
3. Calculating Rook Polynomials	17
Chapter 4. Hall's Marriage Theorem	21
1. The Marriage Theorem	21
2. Tournaments	23
3. An Application to Matrices and Job Grids	24
Chapter 5. Latin Squares	27
1. Extending Latin Rectangles	27
2. Orthogonal Latin Squares	29
Chapter 6. Designs and Codes	31
1. Fair Experiments	31
2. Matrix Description of Designs	34
3. Error-Correcting Codes	36



## CHAPTER 1

### The Binomial Coefficients

EXAMPLE 1. If the 100 people here in this lecture theatre enter an Olympics marathon, in how many ways can the 3 medals be awarded?

EXAMPLE 2. Suppose the 100 people here are participants in a race. Sue Barker wants to interview three of the participants. In how many ways can they be chosen?

DEFINITION 3. The *binomial coefficient*  $\binom{n}{k}$ , (pronounced ‘ $n$  choose  $k$ ’), is defined by

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)(k-2)\dots 1} = \frac{n!}{k!(n-k)!}, & \text{if } 0 \leq k \leq n \text{ and } n, k \text{ are integers,} \\ 0, & \text{otherwise.} \end{cases}$$

The number of ways of choosing  $k$  items from  $n$  is  $\binom{n}{k}$ .

Of course,  $n! = n(n-1)(n-2)\dots 2 \cdot 1$  for each integer  $n \geq 1$ , and by convention  $0! = 1$ . So  $\binom{n}{0} = 1$  and  $\binom{n}{1} = n$  for all non-negative integers  $n$ .

EXAMPLE 4. How many lottery combinations are there?

EXAMPLE 5. How many  $x^3$ s are there in the expansion of  $(1+x)^7$ ?

Generalising Example 5 leads us to the following result.

---

THEOREM 6 (The Binomial Theorem).

$$\begin{aligned} (1+x)^n &= \binom{n}{0} + \binom{n}{1}x + \dots + \binom{n}{k}x^k + \dots + \binom{n}{n}x^n \\ &= \sum_{k=0}^n \binom{n}{k}x^k. \end{aligned}$$

---



So we have, for example,  $\binom{6}{1} = \binom{6}{5}$ . Here is the general statement.

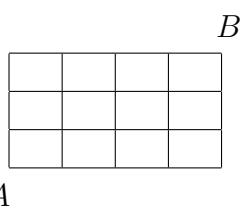
---

PROPOSITION 8. For all  $n$  and  $k$ ,

$$\binom{n}{k} = \binom{n}{n-k}.$$


---

EXAMPLE 9. Imagine that the following diagram is a grid of roads.



We want to get from  $A$  to  $B$  by as short a route as possible. How many such routes are there?

EXAMPLE 10. How many solutions are there of the equation

$$x_1 + x_2 + x_3 + x_4 = 6,$$

where each  $x_i$  is an integer and each  $x_i \geq 0$ .

Generalising Example 10 leads to:

---

PROPOSITION 11. The number of solutions involving non-negative integers  $x_i$  of the equation

$$x_1 + x_2 + \cdots + x_k = n$$

is

$$\binom{n+k-1}{k-1}.$$


---

EXAMPLE 12. How many solutions are there of the equation

$$y_1 + y_2 + \cdots + y_k = n,$$

where each  $y_i$  is an integer strictly greater than 0? (So 0 is no longer allowed.)

PROPOSITION 13. *The number of solutions involving positive integers  $y_i$  of the equation*

$$y_1 + y_2 + \cdots + y_k = n$$

*is*

$$\binom{n-1}{k-1}.$$

EXAMPLE 14. There are  $n$  seats in a row in a doctor's waiting room. There are  $k$  patients who want to choose seats with no two adjacent. In how many ways can the  $k$  seats be chosen?

EXAMPLE 15. Of the 13 983 816 lottery combinations, what proportion have at least 2 of their numbers consecutive?

EXAMPLE 16. Let  $m$  and  $n$  be integers with  $1 \leq m \leq n$ . By considering choosing  $m$  members from  $\{1, 2, 3, \dots, n\}$  and by looking at the highest choice, show that

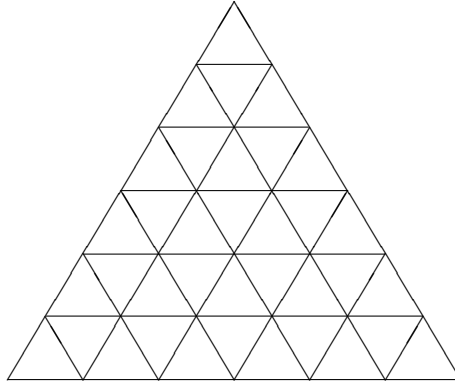
$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-2}{m-1} + \binom{n-3}{m-1} + \cdots + \binom{m-1}{m-1} = \sum_{k=m}^n \binom{k-1}{m-1}.$$

EXAMPLE 17. What is the total of all these numbers?

$$\begin{array}{cccccccc}
 & & & & & & & 1 \\
 & & & & & & & 1 & 2 \\
 & & & & & & & 1 & 2 & 3 \\
 & & & & & & & 1 & 2 & 3 & 4 \\
 & & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & & & & & & & 1 & 2 & 3 & 4 & \dots & \dots & N
 \end{array}$$

Express your answer as a single binomial coefficient.

EXAMPLE 18. How many triangles can be seen pointing upwards in this diagram?



How many when there are  $N$  rows?

EXAMPLE 19. The *Fibonacci sequence*  $(f_n)_{n \geq 1}$  is defined by

$$\begin{aligned} f_1 &= 1, & f_2 &= 2, \\ f_{n+2} &= f_{n+1} + f_n, & \text{for all } n &\geq 1. \end{aligned}$$

The first few terms of the sequence are:

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

Show that

$$f_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots$$

(Here the dots indicate that we continue the terms in the sum until they become zero. Note that we can also write

$$\sum_k \binom{n-k}{k}$$

for this sum. There is no need to specify the range of values of  $k$ , since we want all possible values of  $k$  which contribute non-zero terms to the sum.)

EXAMPLE 20. We mark  $n$  different points on the circumference of a circle. Each pair of points is joined by a straight line. This is done in such a way that no three of the lines meet at a point inside the circle.

- (1) How many lines are there?
- (2) How many internal crossing points are there?
- (3) How many regions are there?



## CHAPTER 2

### Three Basic Principles

#### 1. Parity

EXAMPLE 21. How many solutions are there of the equation

$$2x + 6y = 11 ?$$

In how many of these solutions are both  $x$  and  $y$  integers?

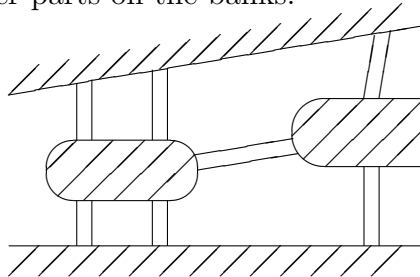
NOTE. You can prove that a situation is **impossible** by a parity mis-match. You cannot prove that something is possible by just checking the parity match.

For example, are there integer solutions of  $12x + 18y = 250$ ? No, because the LHS is divisible by 3 and the RHS is not. So there is no solution despite the odd/even parity match.

EXAMPLE 22. You are given an  $n \times n$  chessboard and some dominoes each of which can cover two adjacent squares of the board.

- (1) Show that the board can be covered completely with non-overlapping dominoes if and only if  $n$  is even.
- (2) Show that if two squares are removed from opposite corners of the board then the remaining board cannot be covered with non-overlapping dominoes.

EXAMPLE 23. Here is a schematic plan of the town of Königsburg. A river runs through the town and the parts of the town on two islands in the river are joined by bridges to the other parts on the banks.



In 1736 inhabitants of the town considered the following problem: is it possible to walk around the town using each bridge once and only once? Euler proved it was impossible by a parity argument.

## 2. The Pigeon-Hole Principle

*The Pigeon-Hole Principle* says that if you place more than  $n$  letters in  $n$  pigeon-holes then some pigeon-hole will contain more than one letter.

This is completely obvious, but it has some powerful consequences.

EXAMPLE 24. Amongst a group of people some handshaking takes place (no-one shakes their own hand, no pair shake more than once). Show that there are two people who shake the same (positive) number of hands.

EXAMPLE 25. There are (at least) two people in the world with the same number of hairs.

EXAMPLE 26. Given any 10 different positive integers less than 100, there will be two disjoint subsets with the same sum.

EXAMPLE 27. Show that, given any sequence of  $n$  integers,

$$x_1, x_2, x_3, \dots, x_n$$

some consecutive collection has a sum divisible by  $n$ .

EXAMPLE 28. Each day for 100 days I put £1 or £2 into a piggy-bank. On 50 days it's £1 and on the other 50 days it's £2. Let  $k$  be an integer with  $1 \leq k < 50$ . Show that in some consecutive period of days I will put precisely £ $k$  into the piggy-bank.

## 3. Inclusion/Exclusion

EXAMPLE 29. In a sports club

- 10 people play tennis (and maybe other games),
- 12 play squash,
- 3 play both.

How many play at least one of the games?

EXAMPLE 30. In a sports club

- 10 people play tennis,
- 15 play squash,
- 12 play badminton,
- 5 play tennis and squash,
- 4 play tennis and badminton,
- 3 play squash and badminton,
- 2 play all three.

How many play at least one of the games?

**THEOREM 31** (The Principle of Inclusion/Exclusion). *Suppose we have a finite set of items and properties  $1, 2, 3, \dots, n$ . Let  $N(i_1, i_2, \dots, i_r)$  be the number of items which have the properties  $i_1, i_2, \dots, i_r$  (and maybe others). Then the number of items with at least one of the properties is*

$$\begin{aligned} & N(1) + N(2) + N(3) + \dots + N(n) \\ & - N(1, 2) - N(1, 3) - \dots - N(n-1, n) \\ & + N(1, 2, 3) + N(1, 2, 4) + \dots \\ & - N(1, 2, 3, 4) - \dots \\ & \quad \vdots \\ & + (-1)^{n-1} N(1, 2, 3, \dots, n). \end{aligned}$$

*This sum may also be written*

$$\sum_{(i_1, i_2, \dots, i_r)} (-1)^{r-1} N(i_1, i_2, \dots, i_r).$$

**EXAMPLE 32.** A permutation of  $\{1, 2, \dots, n\}$  is called a *derangement* if  $1 \not\mapsto 1, 2 \not\mapsto 2, \dots, n \not\mapsto n$ , i.e. no number is mapped to itself.

- (1) How many derangements are there of  $\{1, 2, 3, \dots, n\}$ ?
- (2) Show that the probability of a permutation being a derangement tends to  $1/e$  as  $n$  tends to  $\infty$ .

**EXAMPLE 33.** List the numbers in  $\{1, 2, \dots, 42\}$  which are relatively prime to 42. How many are there?

**THEOREM 34** (Euler's Function). *Let  $m$  be a positive integer whose distinct prime factors are  $p_1, p_2, p_3, \dots, p_n$ . Then the number of integers from  $\{1, 2, 3, \dots, m\}$  which are relatively prime to  $m$  is*

$$m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right).$$



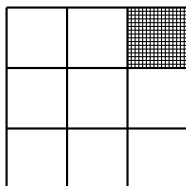
## CHAPTER 3

### Rook Polynomials

#### 1. Definition of Rook Polynomials

In chess a rook (also called a castle) challenges another piece if it is in the same row or column.

EXAMPLE 35. Look at the unshaded board in the diagram.



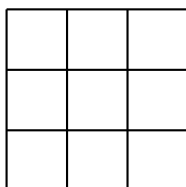
- (1) In how many ways can 1 rook be placed on the board?
- (2) In how many ways can 2 rooks be placed on the board so that neither challenges the other (i.e. in different rows and columns)?
- (3) What about 3 rooks?

DEFINITION 36. If  $B$  is part of an  $n \times n$  board, the *rook polynomial* of the board  $B$  is

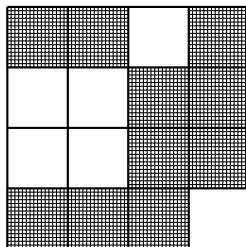
$$r_B(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + \cdots + a_nx^n,$$

where the coefficient  $a_k$  is the number of ways  $k$  rooks can be placed on the board  $B$  without challenging each other. Note that  $a_0 = 1$ , since there is just one way of placing zero rooks.

EXAMPLES 37. (Rook polynomials calculated by bare hands.)



$$1 + 9x + 18x^2 + 6x^3$$



$$1 + 6x + 11x^2 + 8x^3 + 2x^4$$

This is worth doing because

- (1) lots of problems reduce to rook-type problems,
- (2) there is a standard algorithm for calculating rook polynomials.

## 2. Some Problems which Reduce to Rooks

EXAMPLE 38. How many permutations of  $\{1, 2, 3, 4, 5\}$  are there such that

$$1 \not\mapsto 1, 1 \not\mapsto 2, 2 \not\mapsto 2, 2 \not\mapsto 3, 3 \not\mapsto 3, 3 \not\mapsto 4, 4 \not\mapsto 4, 4 \not\mapsto 5, 5 \not\mapsto 5?$$

EXAMPLE 39. Four people  $A, B, C, D$  are to be allocated a job each from jobs  $a, b, c, d$ , subject to the following conditions.

- $A$  cannot do  $b$  or  $c$ ,
- $B$  cannot do  $a$ ,
- $C$  cannot do  $a, b$  or  $d$ ,
- $D$  cannot do  $c$  or  $d$ .

In how many ways can the 4 jobs be allocated?

EXAMPLE 40 (Hostess Problem or Problème des Ménages). Five married couples want to sit round a circular table, alternating man, woman, man, woman, ... and such that no woman is sitting next to her husband. In how many ways can it be done?

EXAMPLE 41 (Snap Problem). We have two full packs of cards. The second pack is in order from top to bottom: AC, AH, AD, AS, KC, KH, KD, KS, ..., 2C, 2H, 2D, 2S. We go through the packs comparing corresponding cards. If two have the same value (not necessarily the same suit) it's a 'snap'. How many different orderings of the first pack lead to no snaps?

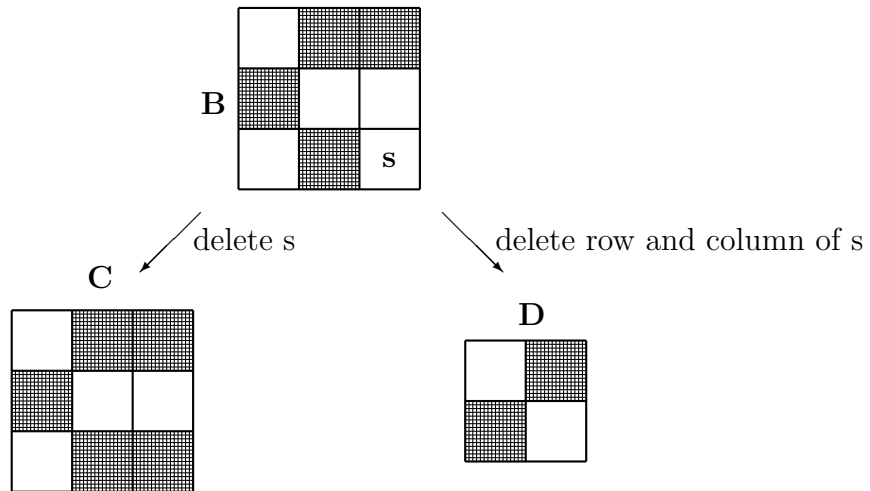
### 3. Calculating Rook Polynomials

Recall that we write  $r_B(x)$  for the rook polynomial of a board  $B$ .

**THEOREM 42.** *Let  $B$  be part of an  $n \times n$  board and let  $s$  be one specified square of  $B$ . Let  $C$  be the board  $B$  with  $s$  deleted and let  $D$  be  $B$  with the whole of  $s$ 's row and column deleted. Then*

$$r_B(x) = r_C(x) + xr_D(x).$$

**EXAMPLE 43.** We illustrate the theorem for a particular board  $B$  and square  $s$ .



Here

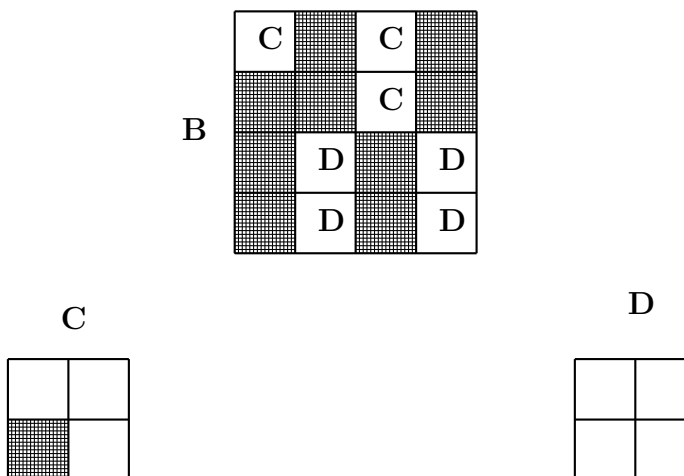
$$r_C(x) = 1 + 4x + 4x^2,$$

$$r_D(x) = 1 + 2x + x^2,$$

$$r_B(x) = 1 + 5x + 6x^2 + x^3 = r_C(x) + xr_D(x).$$

Another shortcut works in the situation when a board  $B$  can be split into two pieces,  $C$  and  $D$ , so that the two pieces do not share any row or column. We write  $B = C \cup D$  in this case.

EXAMPLE 44. We have  $B = C \cup D$ , where  $B$ ,  $C$  and  $D$  are as in the diagram.




---

THEOREM 45. Let  $B$  be part of an  $n \times n$  board and suppose that  $B = C \cup D$ . Then

$$r_B(x) = r_C(x)r_D(x).$$


---

EXAMPLE 46. Use Theorems 42 and 45 to calculate the rook polynomial of the job allocation board from Example 39.

EXAMPLE 47. Use rook polynomials to find the number of ways of adding a 4th row of the numbers 1 to 5 to

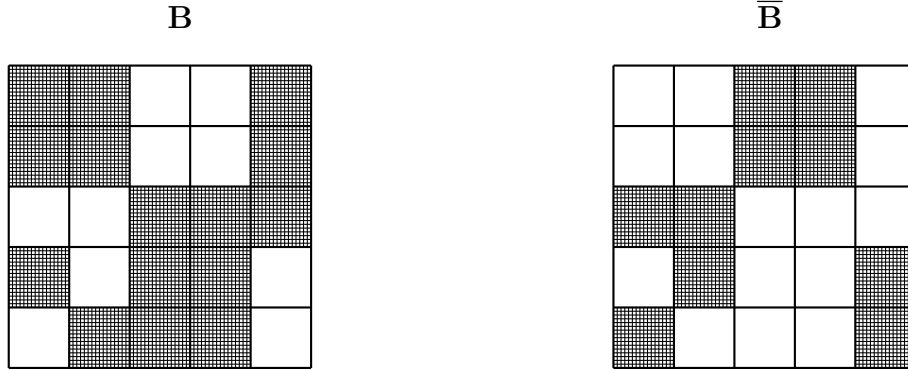
1	2	3	4	5
2	4	5	3	1
4	3	1	5	2

so that there are no repeats in any column.

Next we explain another way to get information about the rook polynomial of one board from the polynomial of a related board.

DEFINITION 48. If  $B$  is the unshaded part of an  $n \times n$  board, then the *complement* of  $B$ , written  $\overline{B}$ , is given by the shaded part of the  $n \times n$  board.

EXAMPLE 49. A board  $B$  and its complement  $\overline{B}$ .



The following theorem allows us to calculate the highest coefficient of the rook polynomial of  $\overline{B}$  from the rook polynomial of  $B$ .

THEOREM 50. Let  $B$  be part of an  $n \times n$  board and let its rook polynomial be

$$1 + r_1x + r_2x^2 + \cdots + r_nx^n.$$

Then the number of ways of placing  $n$  non-challenging rooks on  $\overline{B}$ , the complement of  $B$ , is

$$\sum_{k=0}^n (-1)^k (n-k)! r_k,$$

where  $r_0 = 1$ .

EXAMPLE 51. In Example 49, we have

$$r_B(x) = 1 + 10x + 35x^2 + 50x^3 + 26x^4 + 4x^5,$$

$$r_{\overline{B}}(x) = 1 + 15x + 75x^2 + 145x^3 + 96x^4 + 12x^5.$$

Note that

$$(5! \times 1) - (4! \times 10) + (3! \times 35) - (2! \times 50) + (1! \times 26) - (0! \times 4) = 12.$$

We will end this section by going back to Examples 40 and 41, the Hostess and Snap Problems. Earlier we showed how to reduce these to rook problems. Now we give complete solutions.



## CHAPTER 4

### Hall's Marriage Theorem

#### 1. The Marriage Theorem

EXAMPLE 52. In a group of 7 men and 6 women

woman 1 knows men 1', 2', 3',  
woman 2 knows men 2', 3',  
woman 3 knows men 3', 5', 7',  
woman 4 knows men 1', 2',  
woman 5 knows men 1', 2', 3',  
woman 6 knows men 4', 5', 6'.

Can each woman find a husband from the men she knows?

---

THEOREM 53 (Hall's Theorem - Marriage Version).

*A set of women can always find husbands from amongst the men they know.  $\iff$  For each  $r$ , any set of  $r$  of the women know at least  $r$  men between them.*

---

COROLLARY 54. *Let  $d > 0$  be fixed. Consider a group of men and women where each woman knows at least  $d$  men and each man knows at most  $d$  women. Then each woman can find a husband.*

COROLLARY 55. *In the same situation as Corollary 54, if  $P$  is the set of men who know exactly  $d$  women, then the husbands can be chosen to include  $P$ .*

COROLLARY 56 (Harem Version). *Consider a society in which a woman may have many husbands, but a man may have only one wife. In this situation, consider a group of  $n$  women and suppose that the  $i$ th woman wants to choose  $m_i$  husbands from amongst the men she knows. This is possible if and only if any set of the women,  $(i_1, i_2, \dots, i_r)$ , say, know between them at least  $m_{i_1} + m_{i_2} + \dots + m_{i_r}$  men.*

EXAMPLE 57. The sets

$$\begin{aligned} A_1 &= \{\mathbf{1}, 3\}, \\ A_2 &= \{2, \mathbf{3}\}, \\ A_3 &= \{1, 3, \mathbf{4}, 5\}, \\ A_4 &= \{2, 4, \mathbf{6}\}, \\ A_5 &= \{1, \mathbf{5}\}, \\ A_6 &= \{1, \mathbf{2}\}, \end{aligned}$$

have *distinct representatives*, (also known as a *transversal*), for example those elements indicated in bold. However, the sets

$$\begin{aligned} A_1 &= \{1, 2, 3\}, \\ A_2 &= \{2, 3\}, \\ A_3 &= \{3, 5, 7\}, \\ A_4 &= \{1, 2\}, \\ A_5 &= \{1, 2, 3\}, \\ A_6 &= \{4, 5, 6\}, \end{aligned}$$

do not have distinct representatives (since, for example, the four sets  $A_1, A_2, A_4, A_5$  contain between them only three members 1, 2, 3).

COROLLARY 58 (Hall's Theorem - Transversal Version).

*Sets  $A_1, A_2, \dots, A_n$  have distinct representatives.*  $\iff$  *For each  $r$ , any collection of  $r$  of the sets contains at least  $r$  elements.*

$$\iff \left| \bigcup_{i \in I} A_i \right| \geq |I| \quad \text{for all } I \subseteq \{1, 2, \dots, n\}.$$

COROLLARY 59. *Let  $A_1, A_2, \dots, A_n$  be subsets of  $\{1, 2, \dots, n\}$  with*

$$|A_1| = |A_2| = \dots = |A_n| = d > 0$$

*and such that for  $1 \leq i \leq n$ , each  $i$  is in precisely  $d$  of the sets. Then  $A_1, A_2, \dots, A_n$  have distinct representatives.*

COROLLARY 60 (Harem Transversal Version). *Given sets  $A_1, A_2, \dots, A_n$ , the following conditions are equivalent.*

- (1) *We can find, for  $1 \leq i \leq n$ ,  $w_i$  representatives of  $A_i$ , (with the  $w_1, w_2, \dots, w_n$  all different representatives).*

- (2) Given any collection of the sets,  $A_{i_1}, A_{i_2}, \dots, A_{i_r}$ , say, they contain between them at least  $w_{i_1} + w_{i_2} + \dots + w_{i_r}$  elements.
- (3)  $\left| \bigcup_{i \in I} A_i \right| \geq \sum_{i \in I} w_i$  for all  $I \subseteq \{1, 2, \dots, n\}$ .

EXAMPLE 61. In the matrix

$$\begin{pmatrix} 5 & 3 & 0 & \mathbf{0} \\ \mathbf{0} & 1 & 1 & 0 \\ 2 & 4 & \mathbf{0} & 1 \end{pmatrix}$$

there is a zero in every row with no two in the same column, as shown in bold for example.

COROLLARY 62 (Hall's Theorem - Matrix Version). *Let  $M$  be a matrix. The following conditions are equivalent.*

- (1) *There exists a 0 in each row of  $M$  with no two 0s in the same column.*
- (2) *For any  $r$  rows of  $M$ , those rows between them contain 0s in at least  $r$  columns.*

## 2. Tournaments

DEFINITION 63. A *tournament* of  $n$  players consists of  $\binom{n}{2}$  games where each player plays each of the others once, each game resulting in a win for one of the players.

EXAMPLE 64. Players  $A, B, C, D, E$  play in a tournament. Here are the games played, with the winners in bold:

$$\mathbf{AB}, \quad \mathbf{AC}, \quad \mathbf{AD}, \quad \mathbf{AE}, \quad BC, \quad \mathbf{BD}, \quad \mathbf{BE}, \quad CD, \quad \mathbf{CE}, \quad \mathbf{DE}.$$

Thus  $A$  won three games,  $B, C, D$  all won two and  $E$  only won one. We say that the scores are: 3, 2, 2, 2, 1. Note that

$$A \text{ beat } B \text{ beat } D \text{ beat } E \text{ beat } C.$$

THEOREM 65. *In any tournament of  $n$  players, they can be put in order  $p_1, \dots, p_n$ , so that*

$$p_1 \text{ beat } p_2 \text{ beat } p_3 \text{ beat } \dots \text{ beat } p_n.$$

EXAMPLE 66. Which of the following are possible sets of scores for a tournament of 6 players?

- (1) 5, 3, 2, 2, 2, 1.
- (2) 4, 4, 4, 2, 1, 1.
- (3) 5, 4, 4, 1, 1, 0.

THEOREM 67 (Landau). *Let  $w_1, w_2, w_3, \dots, w_n$  be non-negative integers with  $w_1 + w_2 + w_3 + \dots + w_n = \binom{n}{2}$ . Then the following conditions are equivalent.*

- (1) *There is a tournament with scores  $w_1, w_2, w_3, \dots, w_n$ .*
- (2) *Any  $r$  of the  $w_i$ s add to at least  $\binom{r}{2}$ .*
- (3) *Any  $r$  of the  $w_i$ s add to at most  $(n-1) + (n-2) + \dots + (n-r)$ .*

Note that  $(n-1) + (n-2) + \dots + (n-r) = rn - \binom{r+1}{2}$ .

### 3. An Application to Matrices and Job Grids

In a matrix we will use the word *line* to mean a row or a column.

EXAMPLE 68. In the matrix

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 2 & 2 & 2 \end{pmatrix}$$

- (1) how many 0s can you see with no two in the same line?
- (2) what is the minimum number of lines which include all the 0s?

THEOREM 69 (König-Egerváry). *In any matrix:*

*The minimum number of lines to include all the 0s. = The maximum number of 0s with no two on the same line.*

EXAMPLE 70 (Hungarian Algorithm). (This example requires the algorithm only once. In general the algorithm increases the number of 0s by 1 and it may have to be reapplied several times.)

Four people  $A, B, C, D$  have to be allocated one job each from  $a, b, c, d$ . The table shows their ‘unsuitability’ for the jobs - the *lower* numbers meaning they are *better* suited for the job. (Think of ‘time taken’ to complete the task.)

	$a$	$b$	$c$	$d$
$A$	1	0	1	0
$B$	1	3	0	2
$C$	0	4	0	2
$D$	0	3	1	4

Allocate the jobs so that total unsuitability is least.



## CHAPTER 5

### Latin Squares

#### 1. Extending Latin Rectangles

EXAMPLES 71.

$$\begin{pmatrix} 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \text{is a } 4 \times 4 \text{ Latin square.}$$

$$\begin{pmatrix} 1 & 4 & 3 \\ 5 & 2 & 1 \end{pmatrix} \quad \text{is a } 2 \times 3 \text{ Latin rectangle.}$$

DEFINITION 72. An  $n \times n$  *Latin square* is an  $n \times n$  matrix in which every one of the numbers  $1, 2, \dots, n$  appears in each row and each column.

A  $p \times q$  *Latin rectangle* with entries in  $\{1, 2, \dots, n\}$  is a  $p \times q$  matrix whose entries are from  $\{1, 2, \dots, n\}$  with no repeat in any row or column.

NOTE. An  $n \times n$  Latin rectangle with entries in  $\{1, 2, \dots, n\}$  is an  $n \times n$  Latin square.

REMARK 73. A correctly completed sudoku grid is a  $9 \times 9$  Latin square satisfying the extra condition that each of the numbers  $1, \dots, 9$  appears exactly once in each  $3 \times 3$  box. Their study is not part of this course, but if you are interested, see Dr. Frazer Jarvis' sudoku pages at [www.afjarvis.staff.shef.ac.uk/sudoku](http://www.afjarvis.staff.shef.ac.uk/sudoku).

EXAMPLE 74. Can the Latin rectangle  $\begin{pmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$  be extended to a  $5 \times 5$  Latin square?

For convenience, we recall here a result (Corollary 59) from the previous chapter. We will use it in the proof of the next theorem.

Let  $A_1, A_2, \dots, A_n$  be subsets of  $\{1, 2, \dots, n\}$  with

$$|A_1| = |A_2| = \dots = |A_n| = d > 0$$

and such that for  $1 \leq i \leq n$ , each  $i$  is in precisely  $d$  of the sets. Then  $A_1, A_2, \dots, A_n$  have distinct representatives.

**THEOREM 75.** *Let  $p < n$  and let  $L$  be a  $p \times n$  Latin rectangle with entries in  $\{1, 2, \dots, n\}$ . Then  $L$  can be extended to an  $n \times n$  Latin square.*

**EXAMPLE 76.** Show that  $\begin{pmatrix} 6 & 1 & 2 & 3 \\ 5 & 6 & 3 & 1 \\ 1 & 3 & 6 & 2 \\ 3 & 2 & 4 & 6 \end{pmatrix}$  cannot be extended to a  $6 \times 6$  Latin square.

So, although  $p \times n$  rectangles can be extended to  $n \times n$  squares, in general  $p \times q$  rectangles cannot.

In a sense, the extension failed in the previous example because 5 does not appear enough times in the original rectangle. We make precise the condition needed in the next theorem. Again the proof will need a result (Corollary 55) from the previous chapter. The following lemma just restates this result in different language.

**LEMMA 77.** *Let  $A_1, A_2, \dots, A_p$  be subsets of  $\{1, 2, \dots, n\}$  and let*

$$P = \{i \mid 1 \leq i \leq n \text{ and } i \text{ is in precisely } d \text{ of the sets}\}.$$

*If*

- (1)  $|A_1| = |A_2| = \dots = |A_p| = d (> 0)$ , and
- (2) for  $1 \leq i \leq n$ , each  $i$  is in at most  $d$  of the sets,

*then  $A_1, A_2, \dots, A_p$  have distinct representatives and those representatives can be chosen to include  $P$ .*

**THEOREM 78.** *Let  $L$  be a  $p \times q$  Latin rectangle with entries in  $\{1, 2, \dots, n\}$ . For  $1 \leq i \leq n$ , let  $L(i)$  be the number of occurrences of  $i$  in  $L$ . Then  $L$  can be extended to an  $n \times n$  Latin square if and only if  $L(i) \geq p + q - n$  for each  $i$ .*

**EXAMPLE 79.** Use the process described in the proof of Theorem 78 to extend

$$\begin{pmatrix} 5 & 6 & 1 & 4 \\ 6 & 5 & 4 & 7 \\ 1 & 2 & 3 & 5 \\ 3 & 4 & 5 & 6 \\ 2 & 7 & 6 & 1 \end{pmatrix}$$

to a  $7 \times 7$  Latin square.

## 2. Orthogonal Latin Squares

EXAMPLE 80 (Sixteen Officers). There are 16 soldiers, 4 from each regiment 1, 2, 3, 4 and in each regiment they are of rank 1, 2, 3, 4. Write  $(i, j)$  to denote the soldier in regiment  $i$  of rank  $j$ . Arrange the soldiers in a  $4 \times 4$  array so that each row and each column contains a member of each regiment and with one of each rank in every row and column.

DEFINITION 81. Two  $n \times n$  Latin squares  $L = (l_{ij}), M = (m_{ij})$  are called *orthogonal* if the pairs  $(l_{ij}, m_{ij})$  include all the possibilities  $(1, 1), (1, 2), \dots, (n, n)$ .

When is it possible to construct two such orthogonal Latin squares? We have seen that we can do it for  $n = 4$ . On the other hand, it is easy to see that it is impossible for  $n = 2$ .

In 1782 Euler considered the  $6 \times 6$  case of thirty-six officers. He conjectured that it was impossible to construct two orthogonal Latin squares in this case. It took over 100 years before this was proved, by Tarry in 1900.

After Euler's work it was also conjectured that it would be impossible for all  $n$  of the form  $4m + 2$ , but this turned out to be wrong. It took until around 1960 before it was shown that in fact,  $n = 2$  and  $n = 6$  are the *only* impossible cases.

THEOREM 82. *If  $n$  is a prime (or a power of a prime) then there exist  $n - 1$   $n \times n$  Latin squares,  $L_1, \dots, L_{n-1}$ , which are mutually orthogonal (i.e. each pair is orthogonal).*

EXAMPLE 83. Here's how it works for  $n = 5$ ; four mutually orthogonal  $5 \times 5$  Latin squares are shown. The same process works for any prime. You should think about why this fails for composite numbers.

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

Each row shifts ...

by 1

by 2

by 3

by 4.

---

THEOREM 84. *There are at most  $n - 1$  mutually orthogonal  $n \times n$  Latin squares.*

---

CONJECTURE 85. There exist  $n - 1$  mutually orthogonal  $n \times n$  Latin squares if and only if  $n$  is a prime or a power of a prime.

Progress so far on this conjecture is shown in the table.

$n$	$n$ prime power?	$n-1$ orthog. Latin squares exist?	Comment
3	$Y$	$Y$	By Theorem 82.
4	$Y$	$Y$	By Theorem 82.
5	$Y$	$Y$	By Theorem 82.
$6 = 2 \cdot 3$	$N$	$N$	Conjectured by Euler that there aren't 2 orthogonal squares, proved by Tarry in 1900.
7	$Y$	$Y$	By Theorem 82.
$8 = 2^3$	$Y$	$Y$	By Theorem 82.
$9 = 3^2$	$Y$	$Y$	By Theorem 82.
$10 = 2 \cdot 5$	$N$	$N$	Proved in the 1980's. There <i>are</i> 2 orthogonal squares, it's not known if there are 3.
11	$Y$	$Y$	By Theorem 82.
$12 = 2^2 \cdot 3$	$N$	Not known.	It is known that 5 exist, but not if 6 do.

In case you are tempted to start tackling the  $n = 12$  case, it is perhaps worth noting that the total number of  $12 \times 12$  Latin squares is of the order of  $10^{60}$ .

## CHAPTER 6

### Designs and Codes

#### 1. Fair Experiments

A *design* is a mathematical object invented with a view to designing fair experiments.

EXAMPLE 86. Nine types of coffee are to be tested. Each of twelve families is asked to compare three of the types. Overall we want each pair from the nine to be compared by the same number of families. (In fact, in this example, we'll ask for each to be compared by just one family). Here is one way to do it.

Family	'Block' of varieties to be tested
1	{1, 2, 3}
2	{4, 5, 6}
3	{7, 8, 9}
4	{1, 4, 7}
5	{1, 5, 9}
6	{2, 5, 8}
7	{3, 6, 9}
8	{2, 6, 7}
9	{3, 4, 8}
10	{1, 6, 8}
11	{2, 4, 9}
12	{3, 5, 7}

DEFINITION 87. A *design* consists of  $v$  varieties and  $b$  blocks, each block consisting of  $k$  varieties and with each pair of varieties in precisely  $\lambda$  blocks. It will follow, by the next theorem, that each variety is then in the same number of blocks, called  $r$ . The design is then called a  $(v, b, r, k, \lambda)$  *design*.

We will assume throughout our work on designs that  $1 < k < v$ . (The cases  $k = 1$  and  $k = v$  are trivial.)

---

THEOREM 88. *Given a design of  $v$  varieties,  $b$  blocks,  $k$  varieties per block and every pair of varieties appearing in  $\lambda$  blocks, then each variety is in  $r$  blocks, where*

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

---

In the coffee example,  $\frac{bk}{v} = \frac{12 \cdot 3}{9} = 4$  and  $\frac{\lambda(v-1)}{k-1} = \frac{1 \cdot (9-1)}{3-1} = 4$ . This is a  $(9, 12, 4, 3, 1)$  design.

NOTE. Not every collection of numbers satisfying the theorem necessarily corresponds to a design.

Designs are hard to construct, but sometimes modular arithmetic works.

EXAMPLE 89. We use arithmetic mod 11 to construct a design with 11 varieties and 5 varieties per block,  $v = 11, k = 5$ . The blocks are listed below. Each one is constructed from the previous one by adding one to the entries and working mod 11 (with the slight variation that we write 11 rather than 0).

block number	block
1	$\{1, 3, 4, 5, 9\}$
2	$\{2, 4, 5, 6, 10\}$
3	$\{3, 5, 6, 7, 11\}$
4	$\{4, 6, 7, 8, 1\} = \{1, 4, 6, 7, 8\}$
5	$\{2, 5, 7, 8, 9\}$
6	$\{3, 6, 8, 9, 10\}$
7	$\{4, 7, 9, 10, 11\}$
8	$\{1, 5, 8, 10, 11\}$
9	$\{1, 2, 6, 9, 11\}$
10	$\{1, 2, 3, 7, 10\}$
11	$\{2, 3, 4, 8, 11\}$

This is a design because each pair is in 2 blocks,  $\lambda = 2$ . In fact, it's an  $(11, 11, 5, 5, 2)$  design.

This process only rarely works. For example, with 11 varieties, if you start with the first block  $\{1, 2, 3, 4, 5\}$  then you will find that the pair  $(4, 5)$  appears in 4 blocks, but the pair  $(1, 6)$  appears in none. So this is not a design.

So how did we choose the first block in the previous example? This is answered by the next theorem.

---

**THEOREM 90.** *Let  $p$  be a prime of the form  $4n+3$ . Calculate  $1^2, 2^2, \dots, (2n+1)^2 \pmod p$ . Then these  $2n+1$  numbers (called the quadratic residues of  $p$ ) will form the first block of a  $(4n+3, 4n+3, 2n+1, 2n+1, n)$  design.*

---

We will not prove this theorem in the course, but see ‘Aspects of Combinatorics’ by V.W. Bryant, pp184–192.

**DEFINITION 91.** Designs generated by repeatedly adding 1 to all the numbers in the previous block are called *cyclic*. Ones of the form  $(v, v, k, k, \lambda)$  are called *symmetric*.

**EXAMPLES 92.** (1) Let  $p = 11 = 4n + 3$ , where  $n = 2$ . Working mod 11 we have:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9, \quad 4^2 = 16 \equiv 5, \quad 5^2 = 25 \equiv 3.$$

(With  $6^2 = 36 \equiv 3$  we begin to get repeats.) So the quadratic residues of 11 are 1, 3, 4, 5, 9 and this is how we chose the first block in Example 89.

(2) Let  $p = 7 = 4n + 3$ , with  $n = 1$ . Working mod 7,

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2.$$

Thus the quadratic residues of 7 are 1, 2, 4. By Theorem 90 there is a  $(7, 7, 3, 3, 1)$  design with starter block  $\{1, 2, 4\}$ . Here is the list of all seven blocks.

$$\{1, 2, 4\}$$

$$\{2, 3, 5\}$$

$$\{3, 4, 6\}$$

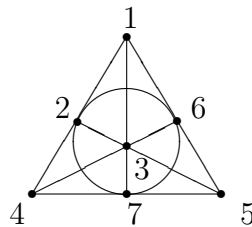
$$\{4, 5, 7\}$$

$$\{1, 5, 6\}$$

$$\{2, 6, 7\}$$

$$\{1, 3, 7\}$$

This design can be illustrated geometrically:



In the diagram the points correspond to the seven varieties and the lines (the six straight lines and the circle) correspond to the seven blocks. Any two points determine a line. This is a picture of something called a *finite projective plane*.

Although finite projective planes have been studied for over a century and designs only recently, it turns out that finite projective planes correspond precisely to  $(n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1)$  designs. (See ‘Aspects of Combinatorics’, by V.W. Bryant, p191.)

For which  $n$  does such a design exist? This problem is equivalent to one we have already discussed.

**THEOREM 93.** *There exists an  $(n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1)$  design if and only if there exist  $n - 1$  mutually orthogonal  $n \times n$  Latin squares.*

## 2. Matrix Description of Designs

The sets of a design are tedious to list, so we represent designs by matrices. In general, given sets  $A_1, A_2, \dots, A_m \subseteq \{x_1, x_2, \dots, x_n\}$  we can represent them by an  $m \times n$  *incidence matrix* whose  $(i, j)$ th entry is

$$\begin{cases} 1, & \text{if } x_j \in A_i, \\ 0, & \text{if } x_j \notin A_i. \end{cases}$$

**EXAMPLE 94.** The  $(9, 12, 4, 3, 1)$  coffee design of Example 86 is represented by the  $12 \times 9$  matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ & & & & \vdots & & & & \\ & & & & \vdots & & & & \\ & & & & \vdots & & & & \end{pmatrix}$$

In general, a  $(v, b, r, k, \lambda)$  design is represented by a  $b \times v$  matrix, with  $k$  1s in each row and  $r$  1s in each column. The  $\lambda$  is a bit harder to spot in the matrix: any pair of columns has 1s appearing together  $\lambda$  times.

We now see how to test this property using matrix algebra.

---

**THEOREM 95.** *Let  $M$  be a  $b \times v$  matrix of 0s and 1s with  $k$  1s in each row. Then  $M$  is the matrix of a  $(v, b, r, k, \lambda)$  design if and only if*

$$M^T M = \begin{pmatrix} r & \lambda & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \lambda & \lambda & \lambda & \lambda & \dots & r \end{pmatrix}$$


---

Using this theorem, we can prove a result that helps establish a basic inequality.

**LEMMA 96.** *Let  $M$  be the matrix of a  $(v, b, r, k, \lambda)$  design. Then  $\det(M^T M) > 0$ .*

---

**THEOREM 97 (Fisher's Inequality).** *In a  $(v, b, r, k, \lambda)$  design,  $b \geq v$ .*

---

So to construct a design with  $v$  varieties you need at least  $v$  blocks. Thus, in a sense, the most efficient designs have  $b = v$ . Note that if  $b = v$  then  $r = \frac{bk}{v} = k$ . So we have a symmetric design  $(v, v, k, k, \lambda)$ .

**EXAMPLE 98.** Consider the (symmetric)  $(7, 7, 3, 3, 1)$  design with blocks:

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

Here is the matrix  $M$  of the design and its transpose.

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \quad M^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$M^T$  represents the blocks  $\{1, 3, 4\}$ ,  $\{1, 5, 7\}$ ,  $\{1, 2, 6\}$ , ... and these give another  $(7, 7, 3, 3, 1)$  design.

**THEOREM 99.** *Let  $M$  be a matrix of a symmetric design. Then  $M^T$  is also the matrix of a symmetric design.*

**COROLLARY 100.** *If  $M$  is the matrix of a  $(v, v, k, k, \lambda)$  design then any two rows of  $M$  differ in  $2(k - \lambda)$  places.*

### 3. Error-Correcting Codes

Suppose you want to send messages in binary code.

**EXAMPLE 101.** Suppose you only want to send  $N, S, E$  or  $W$ . You could use the code

$$N : 00, \quad S : 01, \quad E : 10, \quad W : 11.$$

However if a single error occurs in transmission the message is changed.

One way to improve this is to add a ‘check’ digit.

$$N : 000, \quad S : 011, \quad E : 101, \quad W : 110.$$

The final digit was chosen so that they all have an even number of 1s. If a single error occurs the received message will not have this property. Thus it will not be an acceptable codeword and the error will be detected. The sender can be asked to repeat the message. (This principle is used in bar-codes and supermarket tills.)

Here’s a bigger improvement:

$$N : 000111, \quad S : 011010, \quad E : 101100, \quad W : 110001.$$

These have been chosen so that each differs from all the others in 4 places. If up to 3 errors occur the received message will not be an acceptable codeword. So 3 errors per code word can be detected. Better still, we have a good chance of correcting an error. Suppose that at most two errors occur in transmission and the message 111001 is received. We compare it with the acceptable codewords:

$$\begin{aligned} N : 000111 &\rightarrow 111001 && 5 \text{ changes,} \\ S : 011010 &\rightarrow 111001 && 3 \text{ changes,} \\ E : 101100 &\rightarrow 111001 && 3 \text{ changes,} \\ W : 110001 &\rightarrow 111001 && 1 \text{ change.} \end{aligned}$$

By using the nearest word we recover the correct message  $W$ .

---

THEOREM 102. *Let the code words of a binary code all differ in at least  $d$  places. Then*

- (1) *if less than  $d$  errors per word occur in transmission, errors can be detected;*
- (2) *if less than  $\frac{d}{2}$  errors per word occur in transmission then errors can be corrected.*

---

COROLLARY 103. *Let  $M$  be the matrix of a  $(v, v, k, k, \lambda)$  design. Use the rows of  $M$  as the codewords of a binary code. Then*

- (1) *if less than  $2(k - \lambda)$  errors occur per word, errors can be detected;*
- (2) *if less than  $k - \lambda$  errors occur per word, errors can be corrected.*

EXAMPLE 104. Let  $p = 19 = 4n + 3$ , where  $n = 4$ . We know how to construct a cyclic  $(19, 19, 9, 9, 4)$  design. For this design  $k - \lambda = 9 - 4 = 5$ . So, using the rows of this design's matrix as codewords gives a binary code with 19 codewords each of 19 digits, which will detect up to 9 errors per word and will correct up to 4 errors per word.

Of course, having only 19 words is very limiting, but this may be extended by clever tricks. For example, use  $M^*$  as well as  $M$ , where  $M^*$  means replace all 1s by 0s and all 0s by 1s in  $M$ . This produces a code with 38 words and good error-correcting properties.

If you find this material interesting, consider taking MAS345 Codes and Cryptography next semester!

**The End**