

# Combinatorics. An Introduction

By K.H. Wehrhan

July 29, 2025

## Abstract

This is the book of K.H. Wehrhan, published by Carslaw publications 1990, retyped by Arun Ram.

**Key words**— symmetric functions, crystals, binomial theorems, and hypergeometric functions

## Contents

<b>0</b>	<b>Introduction</b>	<b>3</b>
0.1	What is combinatorics? . . . . .	3
0.2	What is combinatorics not? . . . . .	3
0.3	References . . . . .	4
<b>1</b>	<b>An introduction to counting</b>	<b>5</b>
1.1	Counting functions . . . . .	5
1.1.1	Exercises . . . . .	10
1.2	The binomial theorem and multinomial coefficients . . . . .	10
1.2.1	Exercises with Answers . . . . .	11
1.3	Binomial coefficients . . . . .	12
1.3.1	Exercises . . . . .	15
1.4	Stirling numbers . . . . .	16
1.4.1	Exercises . . . . .	17
1.5	Lattice paths . . . . .	17
1.5.1	Exercises. . . . .	19
1.6	Error correcting codes . . . . .	19
1.6.1	Exercises . . . . .	20
1.7	Problems . . . . .	21
<b>2</b>	<b>Basic combinatorial techniques</b>	<b>23</b>
2.1	Inclusion-exclusion . . . . .	23
2.2	Generating functions . . . . .	23
2.3	Binomial inversion . . . . .	24
2.4	Sieve formulas . . . . .	24
2.5	Finite integration . . . . .	24
2.5.1	Exercises with answers . . . . .	25

---

AMS Subject Classifications: Primary 05E05; Secondary 20G99.

<b>3</b>	<b>Polya theory</b>	<b>26</b>
3.1	Burnside's lemma . . . . .	26
3.2	The cycle index polynomial . . . . .	26
3.3	Polya's inventory theorem . . . . .	26
3.4	Problems . . . . .	26
<b>4</b>	<b>The Euler-Maclaurin summation formula</b>	<b>27</b>
4.1	Bernoulli numbers and polynomials . . . . .	27
4.2	The Euler-Maclaurin summation formula . . . . .	28
4.3	Problems . . . . .	28
<b>5</b>	<b>Finite operator calculus</b>	<b>29</b>
5.1	Polynomial operators . . . . .	29
5.2	Differential operators . . . . .	29
5.3	Formulas of Maclaurin type . . . . .	29
5.4	Binomial sequences . . . . .	29
5.5	The first expansion theorem . . . . .	29
5.6	Sheffer sequences . . . . .	29
<b>6</b>	<b>Möbius Inversion</b>	<b>30</b>
6.1	Partially ordered sets . . . . .	30
6.2	The incidence algebra . . . . .	30
6.2.1	Matrix representation of incidence functions . . . . .	31
6.3	Möbius inversion in partially ordered sets . . . . .	31
6.4	Applications . . . . .	32
6.4.1	Exercises with Answers . . . . .	32
<b>7</b>	<b>Combinatorial species</b>	<b>33</b>
7.1	Applications-An intuitive account . . . . .	33
7.2	The species of Graphs . . . . .	35
7.3	The definition of species . . . . .	35
7.4	Examples of species . . . . .	35
7.5	Isomorphism of species . . . . .	35
7.6	Sums and products of species . . . . .	35
7.7	Some simple species . . . . .	35
7.8	Substitution of species . . . . .	35
7.9	Derivative of a species . . . . .	35
7.10	Problems . . . . .	35
<b>8</b>	<b>Rota's method of linear functionals</b>	<b>36</b>
8.1	Linear functionals . . . . .	36
8.2	Dobinski's formula . . . . .	36
<b>9</b>	<b>More finite operator calculus</b>	<b>37</b>
9.1	The algebra of shift invariant operators . . . . .	37
9.2	The Pincherle derivative . . . . .	37
9.3	Applications . . . . .	37

## 0 Introduction

### 0.1 What is combinatorics?

Broadly, it is about combinations of objects, simple objects: like the natural numbers  $1, 2, 3, 4, \dots$ ; or subsets of a set; or points and edges.

Because we are concerned with combining separate objects, combinatorics is often called *discrete mathematics*.

Combining simple objects is very basic: to mathematics, so most mathematics has gone through a combinatorial stage. Even  $\pi$  has combinatorial nature, as we see in the beautiful product of Wallis:

$$\frac{2 \cdot 2}{3}, \frac{1 \cdot 2 \cdot 4 \cdot 4}{3 \cdot 3 \cdot 5}, \frac{1 \cdot 2 \cdot 4 \cdot 4 \cdot 6 \cdot 6}{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7}, \frac{1 \cdot 2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \cdot 8}{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdot 9}, \dots \longrightarrow \pi$$

### 0.2 What is combinatorics not?

I think that can be summed up in a famous quote of Bertrand Russell, “Mathematics, rightly viewed, possesses . . . supreme beauty, cold and austere, like that of sculpture, without appeal to any part of our weaker nature.” Combinatorics is not like that. Combinatorics is more like a mountain meadow, filled with all sorts of interesting and beautiful flowers, which appeals to every part of our nature.

But there is order within the profusion that is combinatorics, and this book attempts to show some of the underlying connections and patterns, not only within combinatorics, but between the discrete and the continuous, between the finite and the infinitesimal. Four of the nine chapters (5, 6, 8 and 9) are concerned with pioneering work of Gian-Carlo Rota, whose series of papers “*On the Foundations of Combinatorial Theory*”, have done the most to bring order out of beautiful chaos. The first of these papers resulted in the award of the 1988 Steele prize to Rota, *for a paper of lasting and fundamental importance*.

This book is based on combinatorics courses given to third year students, at both ordinary and honours level, at the University of Sydney over the last ten years. The theme of the book is the theory of counting. Chapter 1 is concerned with elementary results, including the basic facts about binomial coefficients and Stirling numbers. In Chapter 2 we give a systematic treatment of some of the main techniques used in counting. Chapter 3 is devoted to Pólya theory, which uses group theory to count collections of objects possessing some symmetry.

The combinatorial identities which arise when counting a collection in different ways lead naturally to polynomial identities and in Chapters 4 and 5 and again in Chapters 8 and 9, we explore the interplay between counting and the calculus of polynomials.

In Chapter 6 we give an introduction to Rota’s theory of Möbius inversion in partially ordered sets, which brings together the diverse theories of inclusion-exclusion, and Möbius inversion in number theory.

Finally, in Chapter 7, we introduce the notion of Species of Structure due to André Joyal which has great promise and already many achievements, in providing a conceptual interpretation to the theory of generating functions.

This book draws on the mathematics background of third year students. For example, we assume a little matrix theory, some Fourier series in some of the problems of Chapter 4, elementary group theory in Chapter 3 and, in Chapter 7, some experience with functions between finite sets.

---

“*On the foundations of combinatorial theory I. Theory of Möbius functions.*” *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 2 (1964) 340-368.

Based on the classic paper by Joyal, “*Une théorie combinatoire des séries formelles*”, *Advances in Math.* 42 (1981), 1-82.

The choice of topics reflects my interest in the subject and I have made some attempt, not enough, at telling a coherent story, at the expense of the omission of many interesting topics.

### 0.3 References

Here are some books for further reading.

M. Aigner, *Combinatorial Theory*, Springer-Verlag (1979).

C. Berge, *Principles of Combinatorics*, Academic Press (1971).

D.I.A. Cohen, *Basic Techniques of Combinatorial Theory*, Wiley (1978).

L. Comtet, *Advanced Combinatorics*, D. Reidel (1974).

W. Feller, *An Introduction to Probability Theory and its Applications*, Volume 1 2nd ed. John-Wiley (1957).

H.W. Gould, *Combinatorial Identities – A standardized table of 500 binomial coefficient summations*, Gould (1972).

R.L. Graham, D.E. Knuth, O. Patashnik, *Concrete Mathematics - A Foundation for Computer Science*, Addison-Wesley (1989).

D.E. Knuth, *The Art of Computer Programming, Volume I: Fundamental Algorithms*, 2nd ed. Addison-Wesley (1968).

C.L. Liu, *Introduction to Combinatorial Mathematics*, McGraw-Hill (1968).

J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley (1958).

S. Roman, *The Umbral Calculus*, Academic Press (1978).

G.-C. Rota, *Finite Operator Calculus*, Academic Press (1975).

R.P. Stanley, *Enumerative Combinatorics Volume I*, Wadsworth & Brooks/Cole Mathematics Series (1986).

I. Tomescu, *Introduction to Combinatorics*, Collet's (1973).

I. Tomescu, *Problems in Combinatorics and Graph Theory*, Wiley-Interscience (1985).

W.A. Whitworth, *Choice and Chance*, Bell (1901).

# 1 An introduction to counting

One of the most important ways of summarizing a collection of objects is to count the number of elements in the collection. This doesn't sound difficult, but even if the collection is very easy to describe it may be very difficult to count. Here are some of the collections we will look at in this book, and the kinds of numbers which arise when we count them.

- The subsets of a fixed size in a given set. [Binomial Coefficients]
- The onto functions between two finite sets. [Stirling Numbers]
- The total collection of partitions of a set. [Bell Numbers]
- The bracketings of a product of numbers. [Catalan Numbers]
- The set of progeny of an ancestral pair of rabbits. [Fibonacci Numbers]

We will see that complicated collections can often be expressed in terms of simple collections like the above, combined using simple rules. For example:

- (1) **The Sum Rule.** If  $A$  and  $B$  are disjoint finite sets then the number of objects in  $A \cup B$  is just the sum of the number of objects in  $A$  and the number of objects in  $B$ .
- (2) **The Product Rule.** If  $A$  and  $B$  are disjoint finite sets then the number of objects in the cartesian product  $A \times B$  (the set of all ordered pairs  $(a, b)$  with  $a \in A$  and  $b \in B$ ) is just the product of the number of objects in  $A$  and the number of objects in  $B$ .
- (3) **The One-to-One Correspondence Rule.** If the objects in  $A$  and the objects in  $B$  can be paired with one another in such a way that no objects of  $A$  or  $B$  are left over, then  $A$  and  $B$  have the same number of elements. [This is a useful way to count a collection of objects, which is analogous to the notion of congruence for comparing areas of regions. We can count a set of objects by finding another set (easier to count) which can be put in one-to-one correspondence with the first set.]

The most important of the numbers which arise in counting are the binomial coefficients. This is because, in counting a collection, we often count subsets, subsets of a given size and combinations of subsets. Thus in the first section we will introduce the binomial coefficients and at the same time gain some familiarity with partitions and Stirling numbers.

## 1.1 Counting functions

Let  $N$  and  $M$  be two sets with  $n$  and  $m$  elements respectively.

**Problem.** How many mappings  $f: N \rightarrow M$  are there?

To answer this we need some notation.

**Notation.** Let  $m$  be a positive integer and  $N$  a set with  $n$  elements. We write

$$[n] = \{1, 2, \dots, n\} \quad (\text{The set containing the first } n \text{ positive integers.})$$

$$|N| = (\text{the number of elements in } N) = n.$$

There are many ways to display a function. For purposes of counting, two descriptions are particularly convenient: as a matrix or as a string. In the first we display  $N$  as the top row of a matrix and write  $f(x)$  under each element  $x \in N$ . Thus if  $N = \{1, b, c, \dots, d\}$ , we write

$$f = \begin{pmatrix} a & b & c & \cdots & d \\ f(a) & f(b) & f(c) & \cdots & f(d) \end{pmatrix} \quad (1)$$

The elements  $a, b, c, \dots, d$  could stand for anything, for example for  $1, 2, 3, \dots, n$ , if  $n = |N|$ . Hence if  $n = |N|$ , there are exactly as many functions  $f: N \rightarrow M$  as there are functions

$$f: [n] \rightarrow M. \quad (2)$$

For functions of the form (2), it's natural to display the elements of  $[n]$  in order; so functions would look like:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix} \quad (3)$$

We can shorten (3) by eliminating the bottom row and writing  $f$  as a string,

$$f(1)f(2)f(3)\cdots f(n), \quad (4)$$

or as

$$m_1m_2m_3\cdots m_n, \quad (5)$$

where  $f(i) = m_i$ .

So, by the product rule, the total number of functions  $f: [n] \rightarrow M$  is the same as the number of strings, namely

$$\underbrace{m \cdot m \cdot m \cdots m}_n = m^n.$$

Summarizing, we have

**Counting all functions between two finite sets**

Let  $N$  and  $M$  be two finite sets with  $n$  and  $m$  elements respectively.

The total number of functions  $f: N \rightarrow M$  is given by

$$|M|^{|N|} = m^n.$$

(6)

Recall that a function  $f: N \rightarrow M$  is *one-to-one* (or injective, or 1-1) if different elements have different images. In other words, if  $f(x) = f(y)$  implies that  $x = y$ . One-to-one functions  $f: N \rightarrow M$  correspond to strings of length  $n$  which contain no element of  $M$  twice. Hence we have:

**Counting one-to-one functions between two finite sets**

Let  $N$  and  $M$  be two finite sets with  $n$  and  $m$  elements respectively.

The total number of one-to-one functions  $f: N \rightarrow M$  is

$$m(m-1)(m-2)\cdots(m-n+1) = m_{(n)}.$$

The number  $m_{(n)}$  is often called the *falling factorial* of  $m$ .

(7)

For example, if  $|N| = |M| = n$ , then there are  $n!$  one-to-one functions

$$f: N \rightarrow M.$$

**Note.** The image  $f(N)$  of a one-to-one function  $f: N \rightarrow M$  between finite sets  $N$  and  $M$  has the same size (or *cardinality*) as  $N$ .

The first difficulty arises when we count *onto* functions. Recall that a function  $f: N \rightarrow M$  is *onto* (or surjective) if for any  $x \in M$  there is a  $y \in N$  for which

$$f(y) = x.$$

For example, if  $|N| = |M|$  then every one-to-one function  $f: N \rightarrow M$  is also onto. The function  $f: N \rightarrow M$  is called a *bijection* if it is both one-to-one and onto.

**Note.** Bijections are just the *one-to-one correspondences* mentioned earlier.

Before attempting to count the onto functions between two sets, let us apply the above ideas to the problem of counting the number of subsets of a set.

## Binomial coefficients

**Problem.** How many distinct subsets of size  $k$  are there in a finite set  $N$ ?

First some notation. If  $|N| = n$  and  $K$  is a subset of  $N$  with  $|K| = k$  we say that  $N$  is an  $n$ -set and that  $K$  is a  $k$ -subset of  $N$ .

The number of  $k$ -subsets of an  $n$ -set is denoted by the *binomial coefficient*  $\binom{n}{k}$ .

The above problem is just the same as calculating  $\binom{n}{k}$ . We argue as follows.

First, let  $K$  be a  $k$ -subset of  $N$ . There are  $k!$  bijections  $[k] \rightarrow K$ . Hence there are  $k!$  one-to-one functions  $[k] \rightarrow N$  whose image is  $K$ . That is

$$(\# \text{ of 1-1 functions } f: [k] \rightarrow N) = k! \cdot (\# \text{ of } k\text{-subsets of } N). \quad (8)$$

By equation (7), the total number of one-to-one functions  $[k] \rightarrow N$  is the  $n_{(k)}$ , so we must have

$$(\# \text{ of 1-1 functions } f: [k] \rightarrow N = n_{(k)} = k! \binom{n}{k}). \quad (9)$$

Equation (9) now yields,

<p><b>Counting the number of subsets of a set</b>          Let <math>N</math> be a finite set with <math>n</math> elements.          The total number of <math>k</math>-subsets of <math>N</math> is given by</p> $\binom{n}{k} = \frac{n_{(k)}}{k!} = \frac{n(n-1) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$	(10)
---	------

**Note.** This is a very indirect way of finding  $\binom{n}{k}$  and in the problems you will have a chance to learn more direct methods.

## Partitions and Onto functions

Let us now look at onto function  $f: N \rightarrow M$ . The first thing to observe is that there are none if  $|M| > |N|$ , (there are not enough elements of  $N$  to ‘cover’ the element of  $M$ ). The second observation is that each onto function  $f: N \rightarrow M$  determines a partition of  $N$  into  $|M|$  parts.

*FIGURE HERE*

**Definition.** A *partition* of a finite set  $N$  into  $k$  parts (or blocks) is a family of subsets  $N_1, N_2, \dots, N_k$ , of  $N$  with the properties:

- (1) The union of all the  $N_i$  is the whole set  $N$ , i.e.  $N_1 \cup N_2 \cup \dots \cup N_k = N$ .
- (2) the subsets are pairwise disjoint, i.e.  $N_i \cap N_j = \emptyset$  for  $i \neq j$ .

**Example 1.** The partitions of the set  $\{a, b, c, d\}$  into 3 parts can be displayed as the collection:

$$\begin{array}{lll} \{\{a\}, \{b\}, \{c\}, \{d\}\} & \{\{a\}, \{b, d\}, \{c\}\} & \{\{b\}, \{a, d\}, \{c\}\} \\ \{\{a\}, \{b, c\}, \{d\}\} & \{\{b\}, \{a, c\}, \{d\}\} & \{\{c\}, \{a, b\}, \{d\}\} \end{array}$$

Or more simply

$$\begin{array}{lll} a|b|cd & a|bd|c & b|ad|c \\ a|bc|d & b|ac|d & c|ab|d \end{array}$$

**Notation.** We write  $S(n, k)$  for the number of partitions of an  $n$ -set into  $k$  parts.  $S(n, k)$  is called a *Stirling number of the second kind*. From Example 1, we have  $S(4, 3) = 6$ .

**Example 2.** Let  $N = \{a, b, c, d\}$  and consider the onto functions  $f: N \rightarrow [3]$ . We see that each onto function is completely determined by,

- a partition of  $N$  into 3 parts,
- a one-to-one function from the *partition* (as a set) to the set  $[3]$ .

For example: the partition  $b|ac|d$  and the one-to-one function

$$\begin{pmatrix} \{b\} & \{a, c\} & \{d\} \\ 1 & 3 & 2 \end{pmatrix}$$

determine the onto function

$$\begin{pmatrix} a & b & c & d \\ 3 & 1 & 3 & 2 \end{pmatrix}$$

Conversely the onto function

$$\begin{pmatrix} a & b & c & d \\ 1 & 3 & 2 & 2 \end{pmatrix}$$

is completely determined by the partition  $a|b|cd$  and the one-to-one function  $f: \{\{a\}, \{b\}, \{c, d\}\} \rightarrow [3]$  defined by

$$\begin{pmatrix} \{a\} & \{b\} & \{c, d\} \\ 1 & 3 & 2 \end{pmatrix}.$$

The total number of onto functions  $f: N \rightarrow [3]$  is thus (writing  $K$  for an arbitrary 3-set),

$$\begin{aligned} & (\# \text{ of 1-1 functions } f: K \rightarrow [3]) \cdot (\# \text{ of partitions of } N \text{ into 3 parts}) \\ & = 2!S(4, 3) = 3! \cdot 6 = 36. \end{aligned}$$



The general case is just the same. If  $|N| = n$ , the number of  $N$  onto functions  $f: N \rightarrow [k]$  is equal to

$$\begin{aligned} & (\# \text{ of 1-1 functions } f: K \text{ to } [k]) \cdot (\# \text{ partitions of } N \text{ into } k \text{ parts}) \\ & = k!S(n, k), \end{aligned}$$

or

$$(\# \text{ of onto functions } f: N \rightarrow [k]) = k!S(n, k). \quad (11)$$

**Counting onto functions between two finite sets**

Let  $N$  and  $K$  be two finites sets with  $n$  and  $k$  elements respectively.

The total number of onto functions  $f: N \rightarrow K$  is

$$k!S(n, k).$$

(12)

The number  $S(n, k)$  is called a *Stirling number of the second kind*.

**Note.** We see in (9) and (11) that the relationship between onto functions  $f: N \rightarrow [k]$  and partitions of an  $n$ -set into  $k$  parts is similar to the relationship between one-to-one functions  $f: [k] \rightarrow N$  and  $k$ -subsets of an  $n$ -set.

**Conventions.** So far we have avoided the inconvenient possibility that  $M$ , or  $N$ , or both may be the empty set  $\emptyset$ . The following have proved with experience to be very useful conventions, and we will adopt them in this book.

- We will allow one function  $\mathbf{1}_\emptyset: \emptyset \rightarrow \emptyset$ , called the *identity function*. We will count this function as one-to-one, so  $0_{(0)} = 0! = 1$ ,  $0^0 = 1$ .
- We allow one function  $\emptyset \rightarrow M$ , for any set  $M$ . This function will also be treated as one-to-one, so  $m_{(0)} = 1$ , for  $m > 0$ . If  $N$  is non-empty then there are, of course, no function  $N \rightarrow \emptyset$ , and so no one-to-one functions, hence  $0_{(n)} = 0$ .
- There are no partitions of a non-empty set into zero parts, so  $S(n, 0) = 0$  for  $n > 0$ . But we will allow one partition of the empty set into zero parts, i.e. we define  $S(0, 0) = 1$ .

**Example 3.** Suppose  $|N| = n$ ,  $|M| = m$ . Let us count the collection of functions  $f: N \rightarrow M$  in two ways. First, as strings, as in (6), to give  $m^n$ . Secondly, classify the functions depending on the size of their images. The number of functions with image  $f(N) = K \subseteq M$  is just the number of onto functions  $f: N \rightarrow K$ , which from (12) is  $k!S(n, k)$  if  $|K| = k$ . Hence the total number of functions  $f: N \rightarrow M$  with image of size  $k$  is

$$\begin{aligned} & (\# \text{ of } k\text{-subsets } K \text{ of } M) \cdot (\# \text{ of onto functions } f: N \rightarrow K) \\ & = \binom{m}{k} k!S(n, k), \end{aligned}$$

where we have used (10) and (12).

Since the image of  $f$  may have  $0, 1, 2, \dots$ , of  $n$  elements, we obtain the following important combinatorial identity:

$$\begin{aligned} m^n &= \sum_{k=0}^n \binom{m}{k} k! S(n, k) \\ &= \sum_{k=0}^n S(n, k) m_{(k)} 13 \end{aligned} \quad (1)$$

Using the conventions above, identity (13) encompasses all possible choices for  $n$  and  $m$ .

**Note.** In classifying the objects of a collection for counting purposes, as above, it's important to remember that each object to be counted must occur in one and only one class (so that the conditions of the sum rule are satisfied).

**Example 4.** Identity (13) may be used directly to evaluate the numbers  $S(n, m)$  by solving systems of equations. For  $n = 4$ , (13) gives the system

$$\begin{aligned} 0^4 &= 0, \\ 1^4 &= S(4, 1)1_{(1)}, \\ 2^4 &= S(4, 1)2_{(1)} + S(4, 2)2_{(2)}, \\ 3^4 &= S(4, 1)3_{(1)} + S(4, 2)3_{(2)} + S(4, 3)3_{(3)}, \\ 4^4 &= S(4, 1)4_{(1)} + S(4, 2)4_{(2)} + S(4, 3)4_{(3)} + S(4, 4)4_{(4)}. \end{aligned}$$

This yields a system of four equations in four unknowns whose coefficient matrix has non-zero determinant, and so the system has a unique solution for the numbers  $S(4, 1)$ ,  $S(4, 2)$ ,  $S(4, 3)$ ,  $S(4, 4)$ . Solving we find

$$S(4, 1) = 1, \quad S(4, 2) = 7, \quad S(4, 3) = 4, \quad S(4, 4) = 1.$$

**Remark.** In later sections, we will see how to easily solve such systems of equations. We will also find simple computational formulas for the Stirling numbers, using other techniques.

### 1.1.1 Exercises

1. Find the numbers  $S(5, k)$  for  $k = 0, 1, 2, 3, 4, 5$ , directly by counting partitions, and secondly, by using the identity (15).
2. Count the number of functions from an  $n$ -set to an  $m + 1$ -set in two ways to obtain the identity.

$$(m + 1)^n = \sum_{k=0}^n \binom{n}{k} m^k.$$

## 1.2 The binomial theorem and multinomial coefficients

Let  $N$ ,  $M$  be sets,  $A$  and  $B$  subsets of  $M$  such that  $M = A \cup B$  and  $A \cap B = \emptyset$  ( $A$  or  $B$  may be empty), and  $|N| = n$ ,  $|A| = a$ ,  $|B| = b$  and  $|M| = a + b = m$ . By (6) there are  $(a + b)^n$  functions  $f: N \rightarrow M$ . We can count the functions also in of  $N$  whose image lies in  $A$ . For example, let Class 0 contain those functions mapping 0 elements of  $N$  to  $A$ . There are, by (6),  $b^n$  such functions. Let Class

---

See Example 4, Chapter 2

1 contain those functions which map one element of  $N$  to  $A$ . The element to be mapped to  $A$  can be selected in  $\binom{n}{1}$  ways and there are  $a$  possible images for it. The remaining elements can be mapped to  $B$  in  $b^{n-1}$  ways. Hence Class 1 contains  $\binom{n}{1}ab^{n-1}$  elements. Proceeding in this way we find that Class  $k$  (all functions mapping  $k$  elements of  $N$  to  $A$ ) contains  $\binom{n}{k}a^kb^{n-k}$  elements. Since functions  $f: N \rightarrow M$  may have  $0, 1, 2, \dots$ , or  $n$  elements mapping to  $A$ , we obtain the *binomial identity*,

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}. \quad (14)$$

In particular, if  $a = b = 1$  we obtain,

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = 2^n.$$

**Note..** The word ‘binomial’ refers to expressions with two terms. The name ‘*binomial coefficient*’ is due to the occurrence of these numbers in identity (14).

The argument which leads to (14) easily generalizes to more than two sets. Thus we have the *trinomial identity*

$$(a + b + c)^n = \sum_{\substack{i,j,k \\ i+j+k=n}} \binom{n}{i,j,k} a^i b^j c^k, \quad (16)$$

where summation is over all triples  $(i, j, k)$  of non-negative integers with  $n = i + j + k$ , and where the coefficients are given by

$$\binom{n}{i,j,k} = \binom{n}{i} \binom{n-i}{j} = \frac{n!}{i!j!(n-i-j)!}. \quad (17)$$

In general, we have the *multinomial identity*,

$$(a_1 + a_2 + \dots + a_p)^n = \sum_{\substack{i_1, i_2, \dots, i_p \\ i_1 + i_2 + \dots + i_p = n}} \binom{n}{i_1, i_2, \dots, i_p} a_1^{i_1} a_2^{i_2} \dots a_p^{i_p}.$$

The coefficients in (18) are called *multinomial coefficients* and, by the same argument as for binomial coefficients, are given by,

$$\begin{aligned} \binom{n}{i_1, i_2, \dots, i_p} &= \binom{i_1 + i_2 + \dots + i_p}{i_1, i_2, \dots, i_p} \\ &= \binom{n}{i_1} \binom{n-i_1}{i_2} \dots \binom{n-i_1-i_2-\dots-i_{p-1}}{i_p} \\ &= \frac{n!}{i_1! i_2! \dots i_p!} \end{aligned} \quad (19)$$

### 1.2.1 Exercises with Answers

**1.** Consider the product  $(a^2 + b^3 + c^4)^{10}$ . Find the coefficients of  $a^4 b^6 c^{24}$ ,  $a^6 b^{12} c^{12}$  and  $a^{12} b^9 c^{24}$ . [Answer:1260; 4200;0]

**2.** A *division* of a set  $N$  into  $k$  parts is a  $p$ -tuple of subsets  $(A_1, A_2, \dots, A_p)$ , some of which may be empty, satisfying the conditions,

(i)  $N = A_1 \cup A_2 \cup \dots \cup A_p$ ;

(ii)  $A_i \cap A_j = \emptyset$ , for  $i \neq j$ .

Show that the number of divisions  $(A_1, A_2, \dots, A_p)$  of  $N$  with  $|N| = n$ ,  $|A_k| = i_k$ , for  $i = 1, \dots, p$  is the multinomial coefficient  $\binom{n}{i_1, i_2, \dots, i_p}$ .

### 1.3 Binomial coefficients

In counting problems it is often useful to consider sub-collections of the collection of objects to be counted. There is an analogy here with integration. We can find the mass of a length of wire by looking at the mass of small pieces of the wire. Similarly in Example 3 we were able to count the set of functions  $f: N \rightarrow M$  in two ways to give the identity

$$m^n = \sum_{k=0}^n S(n, k) m_{(k)} \quad (20)$$

Here we have some ‘global information’ (that there are  $m^n$  functions  $f: N \rightarrow M$ ) and some ‘local information’ about the set of functions with image of a given size. Equation (20) relates these two types of information. As a biproduct we obtain a very useful information concerning the Stirling numbers. In this section we study the binomial coefficients by looking at sub-collections in different ways.

**Example 5. (Symmetry of Binomial Coefficients.)** Formula (10) for the value of the binomial coefficient  $\binom{n}{k}$  is clearly symmetric with respect to  $k$  and  $n - k$ . The identity

$$\binom{n}{k} = \binom{n}{n-k}, \quad (21)$$

expresses the fact that there is a one-to-one correspondence (pairing) between subsets of an  $n$ -set and  $n - k$ -subsets of an  $n$ -set given by the mapping  $A \mapsto \bar{A}$ , where  $\bar{A}$  is the complement of the subset  $A$  in the  $n$ -set.

**Example 6. (Product properties of Binomial Coefficients.)** Suppose again  $N$  is an  $n$ -set. Let’s count all sets of the form  $\{x, A\}$  where  $A$  is a  $k$ -subset of  $N$  and  $x \in A$ . We can do this in two ways. Since there are  $\binom{n}{k}$  ways of choosing  $A$  and then  $k$  choices for  $x$ , the total number of sets  $\{x, A\}$  must be  $k\binom{n}{k}$ .

Alternatively, we can choose  $x$  first (in  $n$  ways) and then ‘build  $A$  around  $x$ ’ by choosing a further  $k - 1$  elements from the set  $N - \{x\}$ . There are  $\binom{n-1}{k-1}$  ways of doing this so the total number of sets  $\{x, A\}$  is also  $n\binom{n-1}{k-1}$ .

Of course it is implicit in our discussion that  $k \neq 0$ , hence we have the simple product rule

$$k\binom{n}{k} = n\binom{n-1}{k-1}, \quad \text{for } k \neq 0. \quad (22)$$

You would have discovered this rule easily by manipulating formula (10). However we can generalize our counting problem to give a less obvious product rule. Let us count the collection of sets of the form  $\{B, A\}$ , where  $A$  is a  $k$ -subset of  $N$  and  $B$  is a  $l$ -subset of  $A$ . The first way of counting clearly yields  $\binom{n}{k}\binom{k}{l}$ .

In the second case we choose subset  $B$  first in  $\binom{n}{l}$  ways, then “build”  $A$  around  $B$  from the remaining  $n - l$  elements of  $N - B$ , in  $\binom{n-l}{k-l}$  ways. Hence we have an important identity,

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}, \quad \text{for } l \leq k. \quad (23)$$

**Example 7. (Vandermonde’s identity)** Is there some way to express the binomial coefficient  $\binom{m+w}{k}$  in terms of binomial coefficients of  $m$  and  $w$ ?

The answer is yes, and we see why if we think of choosing  $k$  people from a group of  $m$ -men and  $n$ -women. Now we can use the classification technique. In choosing  $k$  people we can choose either  $0, 1, \dots$ , or  $k$  men and the rest women. We can choose  $k$  people  $l$  of whom are men in  $\binom{m}{l}\binom{w}{k-l}$  ways. Putting all this together, we have the identity named after the Dutch mathematician, Abnit-Theophile Vandermonde (1735-1796).

$$\binom{m}{0}\binom{n}{k} + \binom{m}{1}\binom{w}{k-1} + \dots + \binom{m}{k}\binom{w}{0} = \binom{m+w}{k}. \quad (24)$$

**Example 8. (Pascal's identity)** The special case of (24) with  $m = 1$  yields the identity,

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}. \quad (25)$$

[In other words, we can choose  $k$ -people from  $m$  men and one woman by choosing just men, or the woman together with  $k-1$  men.]

Identity (25) is course the basis of Pascal's Triangle of binomial coefficients.

$$\begin{array}{cccccccccccc} & & & & \binom{0}{0} & & & & & & & & & & & & & 1 \\ & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & & & 1 & & 1 & \\ & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & 1 & & 2 & & 1 & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & 1 & & 3 & & 3 & & 1 & & 1 & \\ & & \vdots & & \vdots & & \vdots & & & & \vdots & & \vdots & & \vdots & & & \end{array}$$

### The First Four Rows of Pascal's Triangle

The identities given in the above examples combine to yield countless further identities.

**Example 9. (Summation formulas)** Repeated application of Pascal's identity yields

$$\begin{aligned} \binom{m+1}{k} &= \binom{m}{k} + \binom{m}{k-1} \\ &= \binom{m}{k} + \binom{m-1}{k-1} + \binom{m-1}{k-2} \\ &\vdots \\ &= \binom{m}{k} + \binom{m-1}{k-1} + \dots + \binom{m-k}{0}. \end{aligned}$$

Or better, replacing  $m$  by  $n+k$  we have

$$\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \dots + \binom{n+k}{k} = \binom{n+k+1}{k}. \quad (26)$$

Alternatively, we can rewrite (25) as:

$$\begin{aligned} \binom{m+1}{k+1} &= \binom{m}{k} + \binom{m}{k+1} \\ &= \binom{m}{k} + \binom{m-1}{k} + \binom{m-1}{k+1} \\ &\vdots \\ &= \binom{m}{k} + \binom{m-1}{k} + \dots + \binom{m-(m-k)}{k} + \binom{m-(m-k)}{k+1}. \end{aligned}$$

The last term is zero, so we have the identity

$$\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{m}{k} = \binom{m+1}{k+1}. \quad (27)$$

### *Identities arising from the Binomial Theorem*

From the binomial identity (14), taking  $b = 1$ , we have

$$(1+a)^n = \sum_{k=0}^n \binom{n}{k} a^k, \quad (28)$$

which is satisfied by all positive integer values of  $a$ . This means that the polynomial

$$(1+x)^n - \sum_{k=0}^n \binom{n}{k} x^k$$

has infinitely many distinct roots, and so by the fundamental Theorem of Algebra, is the unique polynomial having that property, namely the zero polynomial. Hence we obtain from (28), the polynomial identity,

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k. \quad (29)$$

We can now perform operations on (29), like multiplication, differentiation and integration, and obtain identities by comparing coefficients, or substituting values for  $x$ .

**Example 10.** The product

$$(1+x)^n(1+x)^m = (1+x)^{m+n}$$

yields

$$\begin{aligned} & \left[ \binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n \right] \left[ \binom{m}{0} + \binom{m}{1}x + \cdots + \binom{m}{m}x^m \right] \\ &= \binom{n+m}{0} + \binom{n+m}{1}x + \cdots + \binom{n+m}{n+m}x^{m+n} \end{aligned} \quad (30)$$

Comparing coefficients of  $x^k$  on both sides of (30) now yields

$$\sum_{i=0}^k \binom{n}{i} \binom{m}{k-i} = \binom{n}{0} \binom{m}{k} + \binom{n}{1} \binom{m}{k-1} + \cdots + \binom{n}{k} \binom{m}{0} = \binom{n+m}{k} \quad (31)$$

The special case with  $k = n = m$  is just Vandermonde's identity.

**Example 11.** Differentiate (29) to obtain

$$n(1+x)^{n-1} = \sum_{k=1}^n \binom{n}{k} kx^{k-1}. \quad (32)$$

Substituting  $x = 1$  gives

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + (n-1)\binom{n}{n-1} = n2^{n-1}.$$

**Remark..** The Fundamental Theorem of Algebra generalizes to the following. Let  $N_1, N_2, \dots, N_p$  be infinite sets of rational numbers and  $f(x_1, x_2, \dots, x_p)$  and  $g(x_1, \dots, x_p)$  polynomials satisfying

$$f(a_1, a_2, \dots, a_p) = g(a_1, a_2, \dots, a_p),$$

for all  $a_i \in N_i$ ,  $1 \leq i \leq p$ . Then  $f$  and  $g$  are identically equal. Using this result, the combinatorial identity (18), becomes the multinomial identity between polynomials,

$$(x_1 + x_2 + \dots + x_p)^n = \sum_{\substack{i_1, i_2, \dots, i_p \\ i_1 + i_2 + \dots + i_p = n}} \binom{n}{i_1, i_2, \dots, i_p} x_1^{i_1} x_2^{i_2} \dots x_p^{i_p} \quad (33)$$

### Combining Simple Identities

We have seen how to obtain a number of identities involving binomial coefficients by counting collections of objects in different ways. These identities can be manipulated and combined to give an endless variety of binomial identities (usually not associated with any obvious counting problem). The binomial identities have a certain aesthetic appeal, apart from their common appearance in many parts of mathematics and their usefulness in such areas of computer science as the analysis of algorithms.

**Example 12.** Simplify  $\sum_{k=l}^n \binom{n}{k} \binom{k}{l}$ .

Applying identity (23) we get

$$\begin{aligned} \sum_{k=l}^n \binom{n}{k} \binom{k}{l} &= \sum_{k=l}^n \binom{n}{l} \binom{n-l}{k-l} \\ &= \binom{n}{l} \sum_{k=l}^n \binom{n-l}{k-l}. \end{aligned}$$

Now (14) gives the result

$$\sum_{k=l}^n \binom{n}{k} \binom{k}{l} = \binom{n}{l} 2^{n-l}. \quad (34)$$

### 1.3.1 Exercises

1. Show in two ways (first using formula (10), and second, finding an appropriate counting problem) that:

- (i)  $(n-k) \binom{n}{k} = n \binom{n-1}{k}$  for  $k \leq n$  and  $n \neq 0$ .
- (ii)  $\binom{n}{k} \binom{n-k}{l} = \binom{n}{l} \binom{n-l}{k-l}$ , for  $l \leq n-k$  and  $k \leq n$ .

2. Sum the following:

---

The proof is by induction on  $p$ . For details see for example the book by Serge Lang, “*Algebra*” Addison-Wesley (1965) p. 122.

See for example, the 1972 standardized table of 500 binomial identities, compiled by H.W. Gould, West Virginia University, Morgantown, W. Va.

See Donald E. Knuth’s, “*The Art of Computer Programming Volume 1: Fundamental Algorithms*” Addison-Wesley (1969) for a thorough account of the interrelationship between combinatorics and computer science.

- (i)  $\binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \binom{m}{2}\binom{n}{2} + \cdots + \binom{m}{n}\binom{n}{n}$ . [Answer:  $\binom{m+n}{n}$ ]
- (ii)  $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2$ . [Answer:  $\binom{2n}{n}$ ]

3.

- (i) Prove that  $\sum_{i=0}^n (-1)^i \binom{n}{i} = \begin{cases} 0, & \text{if } n \neq 0, \\ 1, & \text{if } n = 0. \end{cases}$
- (ii) Determine from (i) and identity (23) that

$$\sum_{i=m}^n (-1)^{m+i} \binom{n}{i} \binom{i}{m} = \begin{cases} 0, & \text{if } m \neq n, \\ 1, & \text{if } m = n. \end{cases}$$

4. Prove the following identities for  $n, m, r$  positive integers.

- (i)  $\binom{n}{m}\binom{r}{0} + \binom{n-1}{m-1}\binom{r+1}{1} + \cdots + \binom{n-m}{0}\binom{r+m}{m} = \binom{n+r+1}{m}$
- (ii) Show that  $\binom{x+1}{m+1} = \binom{x}{m+1} + \binom{x}{m}$  is a polynomial identity. [Note that  $\binom{x}{m} = \frac{x(m)}{m!}$ .]

## 1.4 Stirling numbers

As we have seen, a partition of a set is a family of disjoint subsets which ‘cover’ the set. Such families are important when we try to count a collection of objects. As we have seen Stirling numbers (of the *second* kind) arise when we count partitions, so these are probably the most common numbers occurring in counting problems, after binomial coefficients. They are harder to deal with than binomial coefficients (we have no simple formula like (10) for them) but we have a useful recurrence relation similar to Pascal’s identity which is satisfactory for small values of  $n$  and  $k$ .

### A Pascal-type triangle for Stirling numbers

Consider an arbitrary set with  $n+1$  elements, say  $\{x_1, x_2, \dots, x_{n+1}\}$ . Let us count the partitions of this set into  $k$  parts, or blocks. By definition, there are  $S(n+1, k)$  such partitions. But we can count them in an alternate way, by counting those partitions that have  $\{x_{n+1}\}$  as a block and those that don’t.

If  $\{x_{n+1}\}$  is a block of the partition we need to divide the set  $\{x_1, \dots, x_n\}$  into  $k-1$  blocks and there are  $S(n, k-1)$  ways of doing this.

If  $\{x_{n+1}\}$  is not a block, then  $x_{n+1}$  must be contained in a block with at least one other element of the set. There are  $S(n, k)$  ways of partitioning  $\{x_1, x_2, \dots, x_n\}$  into  $k$  blocks and  $x_{n+1}$  may lie in any one of these blocks. Hence there are a total of  $kS(n, k)$  ways in which the original set can be partitioned into  $k$  blocks without  $\{x_{n+1}\}$  being a block.

Putting all this together we obtain the recurrence relation for the Stirling numbers of the second kind.

$$S(n+1, k) = S(n, k-1) + kS(n, k). \quad (35)$$



In addition we have the obvious initial conditions,

$$\begin{aligned} S(n, 1) &= 1, \\ S(n, n) &= 1, \quad \text{for } n \geq 1, \end{aligned} \tag{36}$$

This yields the following triangle for the Stirling numbers of the second kind.

$$\begin{array}{cccccccc} & & & & S(1, 1) & & & \\ & & & & S(2, 1) & & S(2, 2) & \\ & & S(3, 1) & & S(3, 2) & & S(3, 3) & \\ & S(4, 1) & & S(4, 2) & & S(4, 3) & & S(4, 4) \\ S(5, 1) & & S(5, 2) & & S(5, 3) & & S(5, 4) & S(5, 5) \\ & \vdots & & \vdots & & \vdots & & \vdots \end{array}$$
  

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & & 1 & & 1 & & \\ & & 1 & & 3 & & 1 & & \\ & 1 & & 7 & & 6 & & 1 & \\ 1 & & 15 & & 25 & & 10 & & 1 \\ & \vdots & & \vdots & & \vdots & & \vdots & \end{array}$$

**The First Five Rows of Stirling Numbers**

### 1.4.1 Exercises

1. Show that  $S(n, k)m_{(k)}$  is the number of ways of placing  $n$  balls in  $m$  boxes so that exactly  $m - k$  boxes remain empty.

2. Prove the recurrence relation

$$S(n + 1, k) = \sum_{j=0}^n \binom{n}{j} S(j, k - 1).$$

3. The  $n$ th *Bell number*,  $B_n$  is the number of partitions of a set with  $n$  elements. Establish the recurrence formula

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k.$$

## 1.5 Lattice paths

In this section we give a different interpretation of binomial coefficients, in terms of counting paths in the lattice of integer lines. This will yield quite different “combinatorial proofs” of many binomial identities.

Consider the lattice of integer lines on the cartesian plane as shown in the diagram. Let  $(m, n)$  be a fixed point on this lattice.

*PICTURE*

We define an *increasing path* from  $(0, 0)$  to  $(m, n)$  to be an ordered set of edges  $(e_1, e_2, \dots, e_k)$  from the lattice which have the following properties:

- (i)  $e_i$  has a vertex in common with both  $e_{i-1}$  and  $e_{i+1}$  for  $i = 2, 3, \dots, k-1$ ; i.e. the edges make a connected path from  $(0, 0)$  to  $(m, n)$ .
- (ii) In going from one vertex to another, the path either increases in  $x$  or increases in  $y$ .

The path shown in the diagram could be represented by the sequence:

$$x \ y \ y \ x \ x \ y \ x \ y \ x \ x \ y.$$

**Problem..** How many increasing paths are there from  $(0, 0)$  to  $(m, n)$ ?

To answer this, notice first that each path must increase in  $x$  exactly  $m$  times and in  $y$  exactly  $n$  times, so each sequence will have a total of  $m + n$   $x$ 's and  $y$ 's. The total number of sequences is thus the number of ways of assigning  $x$ 's and the  $y$ 's to the  $m + n$  possible places in the sequence, i.e.

**The Number of Increasing Lattice Paths.**

The number of increasing lattice paths from the point  $(0, 0)$  to the point  $(m, n)$  is

$$\binom{n+m}{m} = \binom{n+m}{n}$$

(37)

**Remark.** We content ourselves with the lattice path proof of identity (26) and leave the interpretation of several other identities as problems.

**Example 13.** Consider the point  $(m, n+1)$ . The total number of increasing paths from  $(0, 0)$  to  $(m, n+1)$  is, by (37),  $\binom{n+m+1}{m}$ .

However, we can count the paths in another way. Consider the points  $(0, n+1), (1, n+1), \dots, (m, n+1)$ . As soon as a path reaches one of those points, its route to  $(m, n+1)$  is then completely determined. So the paths can be classified according to which of the points  $(0, n), (1, n), \dots, (m, n)$  *precedes* the entry of the path to the line  $y = n+1$ .

*PICTURE*

There are

- $\binom{n}{0}$  paths with enter at  $(0, n)$ ,
- $\binom{n+1}{1}$  paths with enter at  $(1, n)$ ,
- $\binom{n+2}{2}$  paths with enter at  $(2, n)$ ,

and so on. Hence we obtain the identity,

$$\binom{n}{0} + \binom{n+1}{1} + \dots + \binom{n+m}{m} = \binom{n+m+1}{m}, \quad (38)$$

which is of course just the same as (26).

### 1.5.1 Exercises.

1. Give lattice path interpretations of the following identities:

(i)  $\binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}.$

[Hint: Consider the increasing lattice paths from  $(0, 0)$  to  $(m - k, k + 1)$  for  $m \geq k$ .]

(ii)  $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$

(iii) Vandermonde's identity.

## 1.6 Error correcting codes

We finish this introductory chapter by looking at one important application in which binomial coefficients occur: to finding bounds on the maximal number of codewords that can occur in an *error-correcting code*.

A *binary block code* is a set of “words” (*codewords*) made up of 0's and 1's and all having the same length, say  $n$ . The *distance* between codewords is defined to be the number of places in which the codewords differ.

For example, the distance between the codewords 0110101 and 1010111 is 3.

A codeword may become garbled in transmission. In this case how should the receiver interpret the incoming string? A good strategy would be for the receiver to find the codeword closest to the string received. If there is a *unique* codeword closest to the string received then it would be reasonable to assume that this was the intended codeword.

The aim of constructing codes is to keep the codewords far enough apart so that garbled words can be interpreted.

Suppose we have a binary block code with words of length  $n$ . Let the minimum distance between any two codewords be  $2r + 1$ , for a positive integer  $r$ . Then if we consider the circles of radius  $r$  about the codewords, these do not intersect and hence if a codeword is transmitted with at most  $r$  errors the transmitted string is nearest the correct codeword. We call such a code an  *$r$ -error correcting code*. On the other hand, spacing the words far apart will allow only a few codewords of a given length  $n$ .

### PICTURE

Let  $M(n, r)$  denote the maximum number of codewords in an  $r$ -error correcting code.

For each codeword, there are many other strings which cannot be codewords. For example, none of the strings having distance 1, 2,  $\dots$ , or  $r$  from the codeword can themselves be codewords. Let's count the number of strings that are excluded from the code by a given codeword.

- There are those which differ by 1 digit. Since each digit can be only 0 or 1, there are  $n = \binom{n}{1}$  of these.
- There are those which differ by 2 digits. There are many of these as there are ways of choosing the 2 digits from a set of  $n$ , namely  $\binom{n}{2}$  such strings.

- There are those which differ by 3 digits and so on. In general there are  $\binom{n}{k}$  strings which differ from a given codeword by  $k$  digits.

We conclude that each codeword in an  $r$ -error correcting binary block code accounts for a total of (including the codeword itself)

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$$

strings of length  $n$ . In §1 we saw that there were  $2^n$  binary strings of length  $n$ . Hence we must have

$$M(n, r) \left[ 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r} \right] \leq 2^n. \quad (39)$$

Alternatively, we can rewrite (39) as

$$M(n, r) \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}. \quad (40)$$

Inequality (40) is called the *Hamming bound* on the maximum number of codewords in an  $r$ -error correcting code.

**Example 14.** If  $N = 6$  and  $r = 1$ , (40) tells us that the maximum number of codewords of length 6 which could correct one error is

$$M(6, 1) \leq \frac{2^6}{1 + \binom{6}{1}} = \frac{64}{7} \approx 9.14.$$

In fact the best we can do is eight codewords, for example

000000	100110	001111	101001
010011	110101	011100	111010

### 1.6.1 Exercises

**1.** Suppose  $n$  different letters can be transmitted through a communication channel. How many different messages consisting of  $m$  letters are possible if

- (i) letters can be used repeatedly in each message;
- (ii) each letter can appear at most once in a message;
- (iii)  $k$  of the letters can be used only for the beginning or end of the message (but not both), all other letters can be used, with possible repetition, inside the message.

**2.** Proteins are constructed from amino acids which are coded in the RNA molecule by triplets of the four bases  $A, U, G, C$  (adenine, uracil, guanine and cytosine). Determine the number of

- (i) unordered triplets;
- (ii) ordered triplets;
- (iii) ordered triplets in which the middle base is significant but the end bases may occur in either order (e.g.  $ACG = GCA$  but  $ACG \neq AGC$ ).

**3.** Establish the *Gilbert lower bound*,

$$M(n, r) \geq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{2r}}. \quad (41)$$

## 1.7 Problems

1. In how many ways can the letters  $x, y, z, w, w, w, w$  be ordered so that no two  $w$ 's are adjacent?
2. Show that the number of different ways in which  $m$  distinct numbers from  $[n]$  can be arranged in a circle is

$$\frac{n!}{m(n-m)!},$$

if arrangements which differ by rotations are considered the same.

3. A bijection  $N \rightarrow N$  is called a *permutation* of the set  $N$ . Find the number of permutations of  $[2n]$  in which even numbers are mapped to even numbers.
4. A partition of  $[n]$  is said to be of type  $(k_1, k_2, \dots, k_n)$  if it has  $k_i$  blocks of size  $i$ . If  $k_1, k_2, \dots, k_n$  are non-negative integers, show that the total number of partitions of type  $(k_1, k_2, \dots, k_n)$  is

$$\frac{n!}{k_1!(1!)^{k_1} \cdot k_2!(2!)^{k_2} \cdots k_n!(n!)^{k_n}}.$$

5. Suppose that  $a_1 \leq a_2 \leq \dots \leq a_k$  is a sequence of  $k$  elements from the set  $[m]$  and consider the associated subset  $\{a_1, a_2 + 1, \dots, a_k + (k - 1)\}$  of  $[m + k - 1]$ .

- (i) Show that this correspondence between sequences and subsets is one-to-one and onto.
- (ii) Deduce that the number of ways of choosing  $k$  things from  $m$  things (allowing repetitions) is  $\binom{m+k-1}{k}$ .

6. Given a set  $N$  of size  $n$ , show that the number of ways to choose  $k$  things from  $N$ , allowing repetition is the number of  $n$ -tuples of natural numbers  $(x_1, x_2, \dots, x_n)$  such that

$$x_1 + x_2 + \dots + x_n = k.$$

7. Consider a set of  $2n$  objects,  $n$  of which are identical. How many ways are there of choosing  $n$  objects from the set?
8. A flag is divided into  $n$  vertical stripes which are to be colored so that adjacent stripes have different colors. In how many ways can this be done?
9. In how many ways can three distinct integers be selected from  $[600]$  so that their sum is divisible by 3?
10. Consider a polygon with  $n$  sides (an  $n$ -gon), in which no three diagonals (lines joining non-adjacent vertices) intersect at a common point. If all possible diagonals are drawn in such an  $n$ -gon, how many intersection points will there be?
11. Show that the number of ways of arranging  $m$  one's and  $n$  zero's in a row such that no two one's are adjacent is  $\binom{n+1}{m}$ .
12. Show that  $\binom{n}{k-1} < \binom{n}{k}$  for  $1 \leq k \leq n/2$  and that  $\binom{n}{k} < \binom{n+1}{k}$  for  $1 \leq k \leq n$ .

**13.** Show that the number of subsets of  $[n]$  consisting of  $k$  elements, no two of which are consecutive integers, is

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

**14.** Find closed forms for  $\sum_{j=0}^n j^k \binom{n}{j}$  for  $k = 2$  and  $k = 3$ .

**15.** Define the polynomial  $x^{(n)}$  (the  $n$ th rising factorial of  $x$ ) by

$$x^{(n)} = x(x+1)(x+2)\cdots(x+n-1).$$

Establish the polynomial identity

$$\frac{(x+1)^{(n)}}{n!} = \sum_{k=0}^n \frac{x^{(k)}}{k!}.$$

(i) Show that  $m^{(n)}$  is the number of ways of arranging  $n$  objects in  $m$  stacks, where the order within each stack is important and it is allowable for some stacks to be empty.

(ii) Show that the number of ways of arranging  $n$  objects in  $m$  non-empty stacks is

$$n! \binom{n-1}{m-1}.$$

(iii) Deduce from (i) and (ii) that

$$(a) \quad x^{(n)} = \sum_{k=1}^n \frac{n!}{k!} \binom{n-1}{k-1} x^{(k)}.$$

$$(b) \quad x_{(n)} = \sum_{k=1}^n (-1)^{n+k} \frac{n!}{k!} \binom{n-1}{k-1} x^{(k)}.$$

The integers  $(-1)^n \frac{n!}{k!} \binom{n-1}{k-1}$  are called *Lah numbers*.

**16.** Show that

$$k!S(n, k) = \sum \binom{n}{i_1, i_2, \dots, i_k},$$

where the sum is over all the  $k$ -tuples of positive integers  $(i_1, i_2, \dots, i_k)$  such that  $i_1 + \dots + i_k = n$ .

**17.** The *Stirling numbers of the first kind*  $s(n, m)$  are defined as the connection coefficients in the polynomial identities,

$$x_{(n)} = \sum_{k=0}^n s(n, k) x^k,$$

where  $x_{(n)} = x(x-1)(x-2)\cdots(x-n+1)$ . Establish the following formulas for the Stirling numbers of the first kind:

$$(i) \quad s(n, 1) = (-1)^{n-1} (n-1)!.$$

$$(ii) \quad s(n, n-1) = \binom{n}{2}.$$

$$(iii) \quad s(n+1, 2) = (-1)^{n+1} \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}\right) n!.$$

## 2 Basic combinatorial techniques

In this chapter we bring together some systematic methods for solving counting problems.

### 2.1 Inclusion-exclusion

Let  $X$  be a set and  $A$  and  $B$  subsets of  $X$ . Our starting point is the obvious numerical identity,

$$|A \cup B| = |A| + |B| - |A \cap B|. \quad (1)$$

In other words, to count the elements in  $A \cup B$ , it suffices to count the elements of  $A$  and  $B$  separately, and then subtract elements in the intersection (which have been counted twice).

If  $A, B, C$  are subsets of  $X$  then (1) generalizes to,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \quad (2)$$

In this case, to get the count right, we subtract the elements counted by any two subsets then add on the elements in all three subsets (which have been added three times, but also subtracted three times). This process is called the inclusion-Exclusion principle, and it generalizes to  $n$  subsets  $A_1, A_2, \dots, A_n$  of the set  $X$ . That is

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= |A_1| + |A_2| + \dots + |A_n| \\ &\quad - |A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_{n-1} \cap A_n| \\ &\quad + |A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| - \dots \\ &\quad (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned} \quad (3)$$

**Note.** Identity (3) follows easily from (1) by induction.

MORE HERE

### 2.2 Generating functions

In this section we introduce one of the most successful devices for studying a sequence of numbers, by treating them as coefficients in a *formal power series*. If  $a_0, a_1, \dots, = \{a_n\}_{n=0}^\infty$  is a sequence, we call,

$$G(t) = a_0 + a_1 t + a_2 t^2 + \dots,$$

the *generating function* for the sequence. [The indeterminate  $t$  may be replaced by any other symbol.]

Generating functions may be replaced by scalars (usually real numbers), added together and multiplied just like infinite series. [In short, the set of all generating functions of sequences of real numbers form an algebra over the real numbers.] These operations are often sufficient for us to deduce the essential properties of sequences of numbers which arise in counting. On the other hand, most students will be familiar with the basic properties of infinite series and convergences of these, so it is a good idea to think of generating functions as if they were functions (almost all of these we consider will have a non-zero radius of convergence, and so are functions on a non-zero interval). This will allow us to freely use the operations that hold for infinite series.

---

See the paper by Ivan Niven, *Formal Power Series*, American Math. Monthly (1969), 871-889, for a systematic and self contained-account of the theory of generating functions.

## 2.3 Binomial inversion

## 2.4 Sieve formulas

In §1 we were able to use the Inclusion-Exclusion Principle to find the number of elements in a union of sets, or the complement of such a union. In this section we apply the inversion methods of §3 to obtain some important refinements. The results of this section and §1 are examples of “sieve methods” which work to count the number of elements of a set by subtracting unwanted elements of some larger set.

Let  $X$  be a finite set and  $A_1, A_2, \dots, A_n$  subsets of  $X$ .

## 2.5 Finite integration

Combinatorial identities often involve finite sums, expressed in closed form. In this section we will find a relatively simple method which will allow us, in principle, to sum many finite series. The method is based on the fact that, just as integration and differentiation are inverse processes involving the derivative operator  $D$ , summing finite series and taking differences are inverse processes involving the *forward difference operator*,  $\Delta$ . This process is called *Finite Integration*.

**Definition.** The *forward difference operator*,  $\Delta$ , maps functions to functions, just as  $D$  does. It is defined by,

$$\Delta f: x \mapsto f(x+1) - f(x), \quad (37)$$

for any function  $f$  whose domain contains  $x+1$  whenever it contains  $x$ . [We will consider mainly functions with domain the positive integers.]

### Summation by parts

We now take a brief look at sums like

$$1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \dots + n \cdot 2^n.$$

The terms of this sum are products of terms of two simpler series which we can sum. We need a rule for handling such products.

Observe first that for functions  $f(x)$  and  $g(x)$ ,

$$\begin{aligned} \Delta(f(x)g(x)) &= f(x+1)g(x+1) - f(x)g(x) \\ &= f(x+1)g(x+1) - f(x+1)g(x) + f(x+1)g(x) - f(x)g(x) \\ &= f(x+1)\Delta g(x) + (\Delta f(x))g(x). \end{aligned}$$

Hence we have the important rule:

### The rule for summation by parts

$$\Delta^{-1}[g(x)\Delta f(x)] = f(x)g(x) - \Delta^{-1}[f(x+1)\Delta g(x)]$$

**Remark.** This rule is analogous to the familiar integration by parts rule of the integral calculus.

**Example 16..** PUT THIS IN. In particular, setting  $n = 2$  we find that the sum (??) is

$$\begin{aligned} 1 \cdot 2 + 2 \cdot 2^2 + 3 \cdot 2^3 + \dots + n \cdot 2^n &= (n+1)2^{n+1} - 2^{n+1} + 2 \\ &= (n-1)2^{n+1} + 2. \end{aligned}$$

---

See Stanley, Richard P., *Enumerative Combinatorics Volume I*, Wadsworth & Brooks/Cole Mathematics Series 1986, Chapter 2, for a comprehensive treatment of sieve methods.



### 2.5.1 Exercises with answers

1. Show that  $x(x+2)(x+3) = (x+3)_{(3)} - (x+2)_{(2)}$  and hence sum the series,

$$1 \cdot 3 \cdot 4 + 2 \cdot 4 \cdot 5 + 3 \cdot 5 \cdot 6 + \cdots + n(n+2)(n+3).$$

2. Sum the following series

$$1^2 \cdot 2 + 2^2 \cdot 2^2 + 3^2 \cdot 2^2 + 4^2 \cdot 2^3 + 4^2 \cdot 2^4 + \cdots + n^2 \cdot 2^n.$$

3. Use finite integration to sum the following series:

$$\begin{aligned} \text{(i)} \quad & \binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{n}{m} \\ \text{(ii)} \quad & m \binom{m}{m} + (m+1) \binom{m+1}{m} + \cdots + n \binom{n}{m} \end{aligned}$$

### **3 Polyá theory**

#### **3.1 Burnside's lemma**

#### **3.2 The cycle index polynomial**

#### **3.3 Polyá's inventory theorem**

#### **3.4 Problems**

## 4 The Euler-Maclaurin summation formula

In this chapter we will find a precise relationship between summation and integration. A study of the Bernoulli polynomials and numbers that arise here will allow us to prove such famous formulas as,

$$1^p + 2^p + 3^p + \cdots + (n-1)^p = \frac{1}{p+1} ((n+B)^{p+1} - B^{p+1}),$$

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6},$$

and see how Stirling's formula,

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n,$$

may be derived.

### 4.1 Bernoulli numbers and polynomials

Recall first a common characterization for the standard polynomials  $\{x^n\}$ .

Define  $\{P_n(x)\}$  by:

$$(i)^* \quad P_0(x) = 1,$$

$$(ii)^* \quad P'_n(x) = nP_{n-1}(x), \text{ for } n \geq 1,$$

$$\text{or equivalently, } P_n(x) = \int nP_{n-1}(x)dx,$$

$$(iii)^* \quad P_n(0) = 0, \text{ for } n \geq 1.$$

It is easy to check that  $P_n(x) = x^n$  for  $n = 0, 1, 2, \dots$

**Remark.** Condition (iii)\* is necessary to uniquely determine the polynomials. It says that each of the polynomials, except for  $P_0(x)$ , passes through the origin.

**Defintiion.** The *Bernoulli polynomials*  $\{B_n(x)\}$  are characterized by the conditions

$$(i) \quad B_0(x) = 1,$$

$$(ii) \quad B'_n(x) = nB_{n-1}(x), \text{ for } n \geq 1,$$

$$\text{or equivalently, } B_n(x) = \int nB_{n-1}(x)dx,$$

$$(iii) \quad \int_0^1 B_n(x)dx = 0, \text{ for } n \geq 1.$$

**Note.** Condition (iii) now forces the  $B_n(x)$ , for  $n \geq 1$  to have an average value of 0 over the interval  $[0, 1]$ .

**Defintiion.** The  $n$ th *Bernoulli number*  $B_n$  is defined by

$$B_n = B_n(0), \quad \text{for } n = 0, 1, 2, \dots$$

**Example 1.** MORE

A more efficient formula can be obtained by studying the *Maclaurin series* for  $B_n(x)$ , namely,

$$B_n(x) = \sum_{k=0}^{\infty} B_n^{(k)}(0) \frac{x^k}{k!}.$$

Then  $k$ th derivative of  $B_n(x)$  is

$$\begin{aligned} B_n^{(k)}(x) &= n(n-1)(n-2) \cdots (n-k+1) B_{n-k}(x) \\ &= n_{(k)} B_{n-k}(x), \quad \text{for } k = 0, 1, 2, \dots, \quad \text{by condition (ii).} \end{aligned}$$

Hence,

$$\begin{aligned} B_n(x) &= \sum_{k=0}^n n_{(k)} B_{n-k}(0) \frac{x^k}{k!} = \sum_{k=0}^n \binom{n}{k} B_{n-k} x^k \\ &= \sum_{k=0}^n \binom{n}{k} B_k x^{n-k}. \end{aligned} \tag{2}$$

[We have replaced the index of summation,  $k$ , by  $n-k$  in the last sum.]

**General formula for the Bernoulli polynomials.**

$$B_n(x) = \sum_{k=0}^n \binom{n}{k} B_k x^{n-k}. \tag{3}$$

**Remark..** The problem of uniqueness of the Bernoulli polynomials now depends only on whether or not the Bernoulli numbers are uniquely determined. We can establish this by using condition (iii).

For  $n \geq 1$  we have

$$\int_0^1 B_n(x) dx = 0.$$

And so,

$$\begin{aligned} &\sum_{k=0}^n \binom{n}{k} B_k \frac{x^{n-k+1}}{n-k+1} \Big|_0^1 \\ &= \sum_{k=0}^n \binom{n}{k} \frac{B_k}{n-k+1} = \frac{1}{n+1} \sum_{k=0}^n \binom{n+1}{k} B_k \\ &= 0, \quad \text{for } n \geq 1. \end{aligned} \tag{4}$$

Condition (i) and equation (4) now define a recurrence relation for the Bernoulli numbers, proving that they are uniquely determined.

**Recurrence Formula for the Bernoulli numbers.**

$$\begin{aligned} &B_0 = 1, \\ &\sum_{k=0}^n \binom{n+1}{k} B_k = 0, \quad \text{for } n = 1, 2, 3, \dots \end{aligned} \tag{5}$$

## 4.2 The Euler-Maclaurin summation formula

## 4.3 Problems

## 5 Finite operator calculus

We have seen in Chapter 4 §1 the close connection between the polynomial sequences,  $\{x^{\downarrow}\}$  and  $B_n(x)$ , of standard and Bernoulli polynomials respectively and the derivative operator  $D$ . In Chapter 2 §5 we saw a similar relationship between the sequence  $\{x_{(n)}\}$  and the forward difference operator  $\Delta$ . In this chapter we will see that this is part of a general pattern. That, for example, many polynomial sequences satisfy a binomial identity, like,

$$(x + y)_{(n)} = \sum_{k \geq 0} \binom{n}{k} x_{(k)} y_{(n-k)}.$$

Many other combinatorial identities arise from the interrelationship between operators and polynomial sequences, for example, we will be able to prove Abel's famous generalization of the binomial theorem,

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x(x_k \alpha)^{k-1} (y + k\alpha)^{n-k}.$$

The formulation we give here was developed mainly by Gian-Carlo Rota and collaborators, in a sequence of articles entitled *The Foundations of Combinatorics*.

### 5.1 Polynomial operators

### 5.2 Differential operators

Because of their special relationship with the sequences  $\{x^n\}$  and  $\{x_{(n)}\}$ , respectively, the derivative and forward difference operators are not typical of polynomial operators. In this section we will look at other operators associated with polynomial sequences.

**Definition..** Given a sequence  $\{p_n(x)\}$  the unique operator  $Q$  defined by,

$$Qp_0(x) = 0, \tag{i}$$

$$Qp_n(x) = np_{n-1}(x), \tag{ii}$$

is called the *basis operator* for the sequence  $\{p_n(x)\}$ . Conversely, given a polynomial operator  $Q$ , any sequence  $\{p_n(x)\}$  satisfying conditions (i) and (ii) is called a *basis sequence* for  $Q$ .

**Note.** Basis operators reduce the degree of each polynomial by exactly one. The same basis operator has many basis sequences associated with it. For example,

### 5.3 Formulas of Maclaurin type

### 5.4 Binomial sequences

### 5.5 The first expansion theorem

### 5.6 Sheffer sequences

---

Specifically, see III, *The Theory of Binomial Enumeration*, Ronald Mullin and Rota, Graph Theory and Applications, 167-213, 1970; and VIII, *Finite Operator Calculus*, D. Kahaner, A. Odlyzko, and Rota, Journal of Mathematical Analysis and Applications, 684-760, 1973.

## 6 Möbius Inversion

Our aim in this chapter is to look at the valuable idea of inclusion-exclusion which we studied in §1 and §4 of Chapter 2. We will show how this notion may be generalized to the setting of *partially ordered sets*. Our account is based on the first of the *Foundations of Combinatorics* papers by Gian-Carlo Rota, “On the foundations of combinatorial theory I. Theory of Möbius functions”, *Z. Wahrscheinlichkeitstheorie* 2 (1964) 340-368.

### 6.1 Partially ordered sets

**Definition.** Let  $P$  be a set (not necessarily finite). A *partial order* on  $P$  is a binary relation  $\leq$  which is

(i) reflexive, i.e.,

$$x \leq x, \quad \text{for all } x \in P;$$

(ii) transitive, i.e.,

$$x \leq y \quad \text{and} \quad y \leq z \quad \Rightarrow \quad x \leq z, \quad \text{for all } x, y, z \in P;$$

(iii) antisymmetric, i.e.,

*MORE*

We say that  $P$  is a *partially ordered set*, or *poset*, if it has a partial order.

We say that  $x$  and  $y$  are *comparable* if  $x \leq y$  or  $y \leq x$ .

### 6.2 The incidence algebra

Let  $P$  be a locally finite poset and  $\mathcal{A}(P)$  the set of all functions

$$f: P \times P \rightarrow \mathbb{R},$$

which satisfy the condition

$$f(x, y) = 0, \quad \text{whenever } x \not\leq y.$$

[That is,  $f(x, y) \neq 0$  only when  $[x, y]$  is a *non-empty* interval.]

The element of  $\mathcal{A}(P)$  can be multiplied by real numbers,

$$(\alpha f): (x, y) \mapsto \alpha(f(x, y));$$

added together,

$$(f + g): (x, y) \mapsto f(x, y) + g(x, y);$$

and multiplied (by the convolution product),

$$(f * g): (x, y) \mapsto \sum_{z \in [x, y]} f(x, z)g(z, y).$$

**Comment.** With respect to these three operations,  $\mathcal{A}(P)$  is an associative algebra over  $\mathbb{R}$ , called the *incidence algebra* of the poset  $P$ . The elements of  $\mathcal{A}(P)$  are called *incidence functions*.

---

Rota won the Steele prize “for a paper of lasting and fundamental importance” for this paper. See Stanley, Richard P., “*Enumerative combinatorics Volume I*”, Wadsworth & Brooks/Cole Mathematics Series 1986, Chapter 3, for a thorough account.

### 6.2.1 Matrix representation of incidence functions

If  $P$  is a finite poset we can identify the elements of  $\mathcal{A}(P)$  with upper triangular matrices. To do this we need first a linear ordering of the elements of  $P$ , say  $x_1, x_2, \dots, x_n$ . The only restriction on this ordering will be that it preserves the partial order, i.e.,  $x_i \leq x_j \Rightarrow i \leq j$ .

Once the linear ordering has been decided, we associate  $f \in \mathcal{A}(P)$  (with respect to the chosen ordering), the  $n \times n$  matrix  $(f(x_i, x_j))$ , whose  $(i, j)$ th entry is  $f(x_i, x_j)$ .

MORE HERE

### Two important functions

(1) The *zeta function*  $\zeta$  is defined by

$$\zeta(x, y) = \begin{cases} 1, & \text{if } x \leq y, \\ 0, & \text{otherwise.} \end{cases}$$

(2) The *Möbius functions*  $\mu$  is the inverse of the zeta function  $\zeta$ . That is,  $\mu$  satisfies the conditions,

$$\mu * \zeta = \zeta * \mu = \delta. \tag{1}$$

### 6.3 Möbius inversion in partially ordered sets

In this section we give the most general of our inversion formulas. First some definitions.

**Definition..** An *order ideal* of  $P$  is a subset  $I$  of  $P$  such that whenever  $x \in I$  and  $y \leq x$  then  $y \in I$ . The *principal order ideal* generated by  $x \in P$  is  $\{y \mid y \leq x\}$ .

A *dual order ideal* (also called a *filter*) of  $P$  is a subset  $\tilde{I}$  of  $P$  such that whenever  $x \in \tilde{I}$  and  $x \leq y$  then  $y \in \tilde{I}$ . The *principal dual order ideal* generated by  $x \in P$  is the set  $\{y \mid x \leq y\}$ .

#### Theorem 6.1.

(1) Let  $P$  be a poset in which each principal order ideal is finite. Then

$$t(x) = \sum_{y \leq x} e(y)$$

if and only if

$$e(x) = \sum_{y \leq x} t(y) \mu(y, x).$$

(2) Let  $P$  be a poset in which each principal dual order ideal is finite. Then

$$s(x) = \sum_{x \leq y} e(y)$$

if and only if

$$e(x) = \sum_{x \leq y} \mu(x, y) s(y).$$

---

The algebra  $\mathcal{A}(P)$  is isomorphic to the algebra  $\mathcal{M} = (m_{i,j})$ , of upper triangular matrices having  $m_{i,j} = 0$  if  $x_i \leq x_j$ .

## 6.4 Applications

### 6.4.1 Exercises with Answers

1. Consider the circular arrangements of sixteen beads, in which beads can be colored red, blue or green.
  - (i) Write out the distinct arrangements of 1, 2 and 4.
  - (ii) Determine the total number of such arrangements.
2. Find the number of non-equivalent 4-compositions of 6 and 8.



## 7 Combinatorial species

Combinatorial species were invented by the Canadian mathematician André Joyal ( $\sim 1980$ ). They provide a conceptual interpretation to relations between generating functions. In a way, they restore the combinatorial meaning that is often lost when we pass to generating functions. As motivation we give first two problems which lend themselves naturally to a species analysis.

### 7.1 Applications-An intuitive account

#### Derangements

As we have seen in Chapter 2 §1, derangements are permutations without fixed points. Their exponential generating function is,

$$D(t) = D_0 + D_1 t + D_2 \frac{t^2}{2!} + D_3 \frac{t^3}{3!} + \cdots,$$

where  $D_n$  is the number of derangements of  $[n] = \{1, 2, 3, \dots, n\}$ .

On the other hand, an arbitrary permutation of  $[n]$  will have a cycle structure like,

$$(* * \cdots *) (* * \cdots *) \cdots (**) \cdots (**) (*) (*) \cdots (*),$$

where the cycles  $(*)$  correspond to points fixed by the permutation. In other words, an arbitrary permutation is a *product* of a permutation which fixes no points (a derangement), and a permutation which fixes every point (the identity permutation). For example,  $(19573)(46)(2)(8)(10)$  is the product of  $(19573)(46)$  (a derangement of the set  $\{1, 3, 4, 5, 6, 7, 9\}$ ) and  $(2)(8)(10)$  (the identity permutation on the set  $\{2, 8, 10\}$ ).

Hence, intuitively,

$$\text{Permutations} \equiv \text{Derangements} \times \text{Identity Permutations}. \quad (2)$$

Let us write the exponential generating function for permutations as

$$\begin{aligned} P(t) &= 1 + t + 2! \frac{t^2}{2!} + 3! \frac{t^3}{3!} + \cdots \\ &= 1 + t + t^2 + t^3 + \cdots \\ &= (1 - t)^{-1}, \end{aligned} \quad (3)$$

and for the identity permutations

$$\begin{aligned} U(t) &= 1 + t + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots \\ &= e^t. \end{aligned} \quad (4)$$

**Question.** Is it possible that the intuitive insight of (2) will translate over to generating functions? That is, can we say,

$$P(t) = D(t)U(t)? \quad (5)$$

We can indeed, as we can see by multiplying (5), or equivalently,

$$D(t) = P(t)U(t)^{-1} = (1 + t + t^2 + t^3 + \cdots)(1 - t + \frac{t^2}{2!} - \frac{t^3}{3!} + \cdots),$$

---

See the classic paper by Joyal, “*Une théorie combinatoire des series formelles*”, Advances in Math. 42 (1981), 1-82.

which yields

$$D_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}),$$

the formula which we found for the number of derangements (Chapter 2, (5)).

The insight of Joyal consists in the observation that relations between generating functions and combinations of generating functions (like (5)), already exist as relations between *structures* and ways of combining structures, like (2).

### Cayley's formula

Cayley's formula gives the number of *labeled trees* on a finite set. If the set has  $n$  elements (labelled), the formula says that there are  $n^{n-2}$  distinct trees that have elements of the set as vertices.

For example, if the set is  $[4]$ , the trees are,

PICTURE

and the twelve linear trees of the form

PICTURE

for a total of  $4^2 = 16$ .

A *rooted labelled tree* is a labelled tree with a distinguished element (called the root). Cayley's formula says that there are  $n^{n-1}$  rooted labelled trees, and  $n^n$  doubly rooted labelled trees.

Knowing Cayley's formula, we suspect a connection between the number of doubly rooted labelled trees, and the number of functions  $f: [n] \rightarrow [n]$  (endofunctions of  $[n]$ ), which, by Chapter 1 (6), is also  $n^n$ . Many proofs of Cayley's formula exploit this connection.

Let us see what the relationship between endofunctions and doubly labelled trees.

**Endofunctions..** Such a function can be represented by an *arrowgraph*, consisting of the elements of  $[n]$ , with an arrow from  $x$  to  $f(x)$ , for each  $x \in [n]$ . The figure shows the arrowgraph for an endofunction on the set  $[12]$ . (For this example  $f(6) = 1$ ,  $f(2) = 3$ ,  $f(11) = 11$ , etc.)

PICTURE

Notice that if we repeatedly apply  $f$  to a point  $x$  we eventually obtain a cycle (since  $[n]$  is finite). The points which lie on these cycles form what we may call the *final image* of  $f$ . Thus, the final image of  $f$  consists of the points 2, 3, 7, 8 and 11. The final image gives us a natural way of partition the set  $[n]$  into subsets. If  $x$  is an element of the final image, define the set  $U_x$  to consist of all elements  $y \in [n]$  which enter the final image first at  $x$ , under repeated applications of  $f$ .

In the above figure,

$$U_2 = \{1, 2, 6\}, U_3 = \{3, 4\}, U_7 = \{7\}, U_8 = \{8\}, U_{11} = \{5, 9, 1, 11, 12\}.$$

Then sets  $U_2, U_3, U_7, U_8, U_{11}$  give a partition of  $[n]$  into 5 parts. Moreover each set  $U_i$  has a rooted tree structure on it, the root being the unique element of  $U_i$  from the final image. To complete the description of  $f$  it remains only to know how the final image is arranged, i.e. how the parts of the partition are permuted.

To summarize: an endofunction on  $[n]$  is completely determined by the following information.

- (i) . a partition of  $[n]$ ,
- (ii) a rooted tree structure on each part of the partition,

- (iii) a permutation of the parts,  
 (in the above figure, this permutation is  $(U_2U_3U_8U_7)(U_{11})$ .)

**Doubly rooted labelled trees.** Atypical such tree is shown below (we have left off the labels).

*PICTURE*

The roots are denoted by  $\star$  and  $\square$  (in general the two roots could be the same vertex and if we interchange  $\star$  and  $\square$  we obtain a different tree).

Notice that in a doubly rooted tree there is a unique path, determined by the roots. This path allows us to partition the set of vertices into subsets of the form  $U_\alpha$  consisting of all vertices connected to the point  $x$  on the path. In the figure the partition is indicated by the dotted lines. Moreover each  $U_x$  posses the structure of a rooted tree. In fac thte doubly rooted tree on the set  $[n]$  is completely determined by the data

- (i) a partition of  $[n]$ ,
- (ii) a rooted tree structure on each part of the partition,
- (iii) a linear ordering of the parts.

**Note.** The number of linear orderings of  $[n]$  is  $n!$  and hence is the same as the number of permutations of the set. This suggests, from the above two descriptions, that Cayley's formula holds.

More precisely, Let  $E(t)$ ,  $R(t)$ ,  $R_2(t)$  be the generating functions for endofunctions, root labelled trees and doubly root labelled trees,

## 7.2 The species of Graphs

## 7.3 The definition of species

## 7.4 Examples of species

## 7.5 Isomorphism of species

## 7.6 Sums and products of species

## 7.7 Some simple species

## 7.8 Substitution of speicies

## 7.9 Derivative of a species

## 7.10 Problems

## 8 Rota's method of linear functionals

### 8.1 Linear functionals

### 8.2 Dobinski's formula

## **9 More finite operator calculus**

### **9.1 The algebra of shift invariant operators**

### **9.2 The Pincherle derivative**

### **9.3 Applications**

## References

- [Bou] N. Bourbaki, *Groupes et algèbres de Lie*, vol. 4–6, Masson 1981, MR0647314
- [CR22] L. Colmenarejo and A. Ram, *c-functions and Macdonald polynomials*, arxiv:2212.03312.
- [CR81] C.W. Curtis and I. Reiner, *Methods of Representation Theory: With Applications to Finite Groups and Orders*, Wiley Classics Lib. I and II, John Wiley & Sons, New York, 1981. MR0892316.
- [DL76] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. (2) **103** (1976) 103–161, MR0393266.
- [DRS22] P. Diaconis, A. Ram and M. Simper, *Double coset Markov chains*, Forum Math. Sigma **11** (2023), Paper No. e2, 45 pp., MR4530094, arXiv:2208.10699.
- [GH93] A. Garsia and M. Haiman, *A graded representation model for Macdonald’s polynomials*, Proc. Nat. Acad. Sci. USA **90** (1993) 3607–3610. MR1214091
- [GH96] A. Garsia and M. Haiman, *A remarkable  $q, t$ -Catalan sequence and  $q$ -Lagrange inversion*, J. Algebraic Combinatorics **5** (1996) 191–244, MR1394305.
- [GR05] A. Garsia and J.B. Remmel, *Breakthroughs in the theory of Macdonald polynomials*, Proc. Nat. Acad. Sci. USA **102** (2005) 3891–3894, MR2139721.
- [GP00] M. Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Math. Soc. Monogr. (N.S.) **21** The Clarendon Press, Oxford University Press, New York, 2000, xvi+446 pp. ISBN: 0-19-850250-8, MR1778802.
- [GMV14] E. Gorsky, M. Mazin and M. Vazirani, *Affine permutations and rational slope parking functions*, Trans. Amer. Math. Soc. **368** (2016) 8403–8445, MR3551576, arXiv:140303.
- [HR99] T. Halverson and A. Ram, *Bitraces for  $GL_n(\mathbb{F}_q)$  and the Iwahori-Hecke algebra of type  $A_{n-1}$* , Indag. Mathem. N.S. **10** (1999) 247–268, MR1816219.
- [HR04] T. Halverson and A. Ram, *Partition algebras*, European J. of Combinatorics, **26**(2005) 869–921, MR2143201, arxiv:0401314.
- [HLR] T. Halverson, R. Leduc and A. Ram, *Iwahori-Hecke algebras of type  $A$ , bitraces and symmetric functions*, Int. Math. Research Notices (1997) 401–416. MR1443319.
- [He23] X. He, *On affine Lusztig varieties*, arXiv:2302.03203.
- [Hik12] T. Hikita, *Affine Springer fibers of type  $A$  and combinatorics of diagonal coinvariants*, Adv. Math. **263** (2014) 88–122, MR3239135, arXiv:1203.5878.
- [HS79] R. Hotta, N. Shimomura, *The fixed point subvarieties of unipotent transformations on generalized flag varieties and the Green functions*, Math. Ann. **241** (1979) 193–208.
- [LLT95] A. Lascoux, B. Leclerc and J.-Y. Thibon, *Ribbon tableaux, Hall-Littlewood functions, quantum affine algebras, and unipotent varieties*, J. Math. Phys. **38** (1997) 1041–1068. MR1434225, arXiv:q-alg/9512031.
- [Lu81] G. Lusztig, *Green polynomials and singularities of unipotent classes*, Adv. Math. **42** (1981) 169–178, MR0641425.

- [Lu21] G. Lusztig, *Traces on Iwahori-Hecke algebras and counting rational points*, arXiv:2105.04061.
- [Mac] I.G. Macdonald, *Symmetric functions and Hall polynomials*, Second edition, Oxford Mathematical Monographs, Oxford University Press, New York, 1995. ISBN: 0-19-853489-2, MR1354144.
- [Mac03] I.G. Macdonald, *Affine Hecke Algebras and Orthogonal Polynomials*, Cambridge Tracts in Mathematics, vol. **157**, Cambridge University Press, Cambridge, 2003. MR1976581.
- [Me17] A. Mellit, *Poincaré polynomials of character varieties, Macdonald polynomials and affine Springer fibers*, Ann. of Math. (2) **192** (2020), 165-228. MR4125451, arxiv:1710.04513.
- [OY14] A. Oblomkov and Z. Yun, *Geometric representations of graded and rational Cherednik algebras*, Adv. Math. **292** (2016) 601–706, MR3464031, arxiv:1407.5685.
- [Ra91] A. Ram, *A Frobenius formula for the characters of the Hecke algebras*, Invent. Math. **106** (1991), 461-488, MR1134480.
- [VV07] M. Varagnolo and E. Vasserot, *Finite dimensional representations of DAHA and affine Springer fibers: The spherical case*, Duke Math. J. **147** (2009) 439-540, MR2510742, arxiv:0705.2691.
- [WW12] J. Wan and W. Wang, *Frobenius map for the centers of Hecke algebras*, Trans. Amer. Math. Soc. **367** (2015) 5507–5520, MR3347181, arxiv:1208.4446.