Introduction to Combinatorics
MA3210

Jürgen Bierbrauer

November 12, 2001

Contents

Chapter 1

Subsets, paths and bitstrings

We start with the classical branch of combinatorics called **Enumerative Combinatorics.** This is the art of counting. A typical problem has the form *In how many ways can ... be done?*

For example, fix an alphabet $\mathcal{A}$ of a elements ($\mathcal{A}$ is an a-set) and a length n and ask how many n-tuples there are with entries in $\mathcal{A}$. These are also called a-ary n-tuples (clearly all we have to know about the alphabet is its cardinality a). Start from the binary case $a = 2$. for length $n = 3$ we obtain the following **bitstrings** of length 3 :

000
001
010
100
011
101
110
111

The answer to our question is 8 (in case $a = 2, n = 3$). In order to understand the pattern it may be wiser to start with small values of n. For $n = 1$ clearly the answer is 2 (the empty set and the set itself are the only subsets of a 1-set), for $n = 2$ the list is

00
01
10
11

and the answer to our problem therefore is 4. The values $2, 4, 8$ in the binary case for $n = 1, 2, 3$ make us suspect the general formula in the binary case should be 2^n.

It is easy to understand why this is true: start from $n = 3$ again. Any bitstring of length 3 has the form (x_1, x_2, x_3), where $x_i = 0$ or $x_i = 1$ for every i. There are therefore 2 possible entries in each coordinate i. Each of the 2 possibilities in coordinate 1 can be combined with each of the 2 possibilities in coordinate 2, giving $2 \cdot 2 = 4$ choices in the first two coordinates (this is the answer in case $a = 2, n = 2$). Each of these possibilities can be combined with each of the 2 possibilities in the third coordinate, and the answer to our question is $2 \cdot 2 \cdot 2 = 2^3 = 8$. In the case of general length n we obtain as answer $2 \cdot 2 \cdot \cdots \cdot 2 = 2^n$, and the answer for general a, n is a^n.

1.1 Theorem. *There are a^n a-ary n-tuples $(a, n \geq 1)$.*

This was pretty easy. We can consider Theorem 1.1 as a combinatorial interpretation of the exponentials in the sense that the number a^n counts combinatorial objects, the a-ary n-tuples.

It has to be mentioned that the set of n-tuples form a mathematical structure, which is also known as a **Cartesian product.** It is written as

$$\mathcal{A} \times \mathcal{A} \times \cdots \times \mathcal{A}$$

(the n-fold Cartesian product of $\mathcal{A}$ with itself). The Cartesian product is not restricted to using the same set in each corodinate. Let $\mathcal{A}, \mathcal{B}$ be sets. The elements of the Cartesian product $\mathcal{A} \times \mathcal{B}$ are the pairs, where the first entry belongs to $\mathcal{A}$ and the second belongs to $\mathcal{B}$. If $\mathcal{A}$ has a elements and $\mathcal{B}$ has b elements, then the number of elements of $\mathcal{A} \times \mathcal{B}$ is ab. The term **Cartesian** is in honour of the French mathematician and philosopher René Descartes. Next we will see that 2^n counts something else as well.

Fix a number n and consider a set X of n elements. Our next problem is: determine the number of **subsets** of X. Clearly this number will depend only on n. Start from case $n = 5$, using $X = \{1, 2, 3, 4, 5\}$. In order to save space let us represent the elements of subsets without braces and commas. For example 135 stands short for $\{1, 3, 5\}$. A very special subset is $\emptyset$, the empty subset. The 1-subsets are $1, 2, 3, 4, 5$, the 2-subsets are $12, 13, 14, 15, 23, 24, 25, 34, 35, 45$. The number of 3-subsets is the same as the number of 2-subsets, hence 10 (why?) and the number of 4-subsets equals the number of 1-subsets for the same reason. Finally X itself is the only

5-subset. All in all we count $1+5+10+10+5+1=32$ subsets. As $32=2^5$ and 5 is the number of elements of X this makes us suspect the general formula should be: 2^n is the number of subsets of an n-set. In case $n=1$ this is true (a set with 1 element has precisely two subsets, itself and the empty set).

1.2 Theorem. *The number of subsets of an n-set is 2^n.*

One way to prove Theorem 1.2 would be to use induction. We will come to that later. However, there is a much more satisfactory proof. We can use Theorem 1.1. All we need to do is to show that there are as many subsets of an n-set as there are binary n-tuples. That is, we have to find a one-to-one (bijective) mapping between subsets and n-tuples. A natural idea is the following, in case $n=5$: let each coordinate of our 5-tuple correspond to an element of our set X. The entry in that coordinate means

$$0 \leftrightarrow \text{ do not use } \; 1 \leftrightarrow \text{ do use the element,}$$

for example 10101 corresponds to $\{1,3,5\}$ (in coordinates $1,3,5$ the answer was $yes=1$, in the remaining coordinates was $no=0$). Here are some more examples:

00100	$=$	(no, no, yes, no, no)	$\leftrightarrow$	$\{3\}$
11101	$=$	(yes, yes, yes, no, yes)	$\leftrightarrow$	$\{1,2,3,5\}$
11111	$=$	$(yes, yes, yes, yes, yes)$	$\leftrightarrow$	$\{1,2,3,4,5\}=X$
00000	$=$	(no, no, no, no, no)	$\leftrightarrow$	$\emptyset$

In particular the empty set corresponds to the bitstring with all entries 0. The number of $1s$ in a bitstring is the number of elements in the corresponding subset. We see that we have a natural bijection between subsets and bitstrings. This completes the proof of Theorem 1.2. More importantly it shows that the combinatorics of subsets of a set is the same as the combinatorics of binary bitstrings. Bitstrings are very popular in coding theory, for example.

The next problem is closely related to subsets of sets as well, although it looks differently in the beginning. We start from a concrete instance: consider the grid in Figure 1.1.

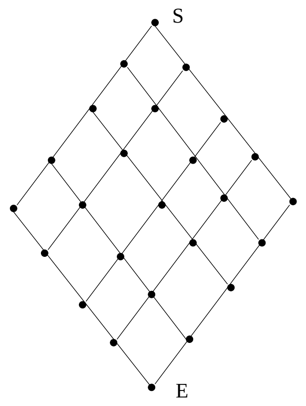

Figure 1.1: Paths on a grid

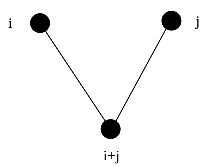

Figure 1.2: The addition rule

We want to count paths starting at S, ending at E and such that at each node we proceed either to the node in the southeast or to the node in the southwest direction. The problem is: how many such paths are there? As the nodes $\neq S$ come in 8 levels, E forming level 8, and at each step there are at most 2 possibilities, this number is certainly $< 2^8 = 256$. Can we be more precise? It is natural to consider more generally the number of paths starting at S and ending in a given node of the grid, not just in E. When we know that number we write it as an index of the node. In that way we can proceed step by step. For example, the number of paths ending in any node of the northwest or northeast boundary of the grid is 1. Here comes the decisive observation: if I know the index (the number of paths ending there) of the two points to the NW and to the NE of a node P, (let them be i and j), then the index of P is $i + j$. This is so because every path ending at P must have passed before through one of these two nodes, see Figure 1.2. We call this the **addition rule** for paths.

This makes it easy now to compute inductively the indices of all nodes in

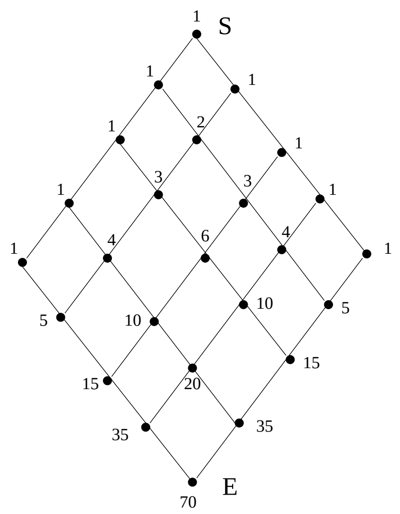

Figure 1.3: The numbers of paths

our grid. The result is Figure 1.3.

A closer look shows that there is a relationship with what we have studied before (subsets and bitstrings). In fact, as such a path goes down 8 levels and at each level there are at most 2 possibilities we can represent each path by a bitstring of length 8. We interpret entry 0 as *go left (west)* and 1 as *go right (east).* The bitstring 00001111 encodes the path, which goes left-left-left-left-right-right-right-right while goind down. This is the path following the left boundary of the grid. Analogously 11110000 follows the right boundary. The condition that the path ends in E means that the bitstring has as many 0s as it has 1s, hence four each. This gives the translation from the language of paths to the language of subsets: the number of paths we are looking for (we know they are 70) equals the number of bitstrings of length 8 with four 1s. This also equals the number of 4-subsets of an 8-set. It is clear how this generalizes. Here is a formal definition of these important numbers:

1.3 Definition. *Let $n \geq m \geq 0$ be natural numbers. Then $\binom{n}{m}$ denotes the number of m-subsets of an n-set.*

The numbers $\binom{n}{m}$ are known as **binomial numbers** or **binomial coefficients.** Some special values are obvious: $\binom{n}{0} = 1$ (every n-set has just 1

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1

Figure 1.4: Pascal's triangle

subset of 0 elements, the empty set), $\binom{n}{n} = 1$ (the only subset of n elements is the n-set itself) and $\binom{n}{1} = n$ (a set has as many 1-element subsets as it has elements). The next case $\binom{n}{2}$ poses a problem already. We do not have a short formula for these numbers yet.

Our path problem has as answer: $\binom{8}{4} = 70$. It is clear how it generalizes: our grid (Figure 1.1) went 8 levels down, 4 to the right (encoded by 1) and 4 to the left (encoded by 0). In general we can consider grids with n levels down from the starting point, where we go m times to the right and $n-m$ times to the left. The number of such paths will be the same as the number of bitstrings of length n with m entries 1. This number is $\binom{n}{m}$.

We see that it is artificial to have our grids end in a unique point in the south. All these grids are part of an infinite triangle, which is known as **Pascal's triangle.**

In Figure 1.4 we see levels from 0 down to 8 of the triangle. The numbers in the last row therefore represent the binomials $\binom{8}{m}$. The levels give the numerators n of the binomials. The denominators m are obtained by counting from left to right, starting from 0. For example, we see our familiar value $\binom{8}{4}$ on level 8, counting $0, 1, 2, 3, 4$ from the left.

Now that we know the entries of Pascal's triangle are the binomial coefficients the addition rule for paths becomes an **addition rule for binomials:**

1.4 Theorem.

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m} \textit{ for } m > 0.$$

We can also give a direct proof of Theorem 1.4 using only Definition 1.3. For that purpose fix an n-set X and one of its elements e. The m-subsets of X (we know there are $\binom{n}{m}$ of them) can be divided into two types, those containing e and the others. There are $\binom{n-1}{m-1}$ of the first type and $\binom{n-1}{m}$ of the second. This proves Theorem 1.4.

Another obvious feature of Pascal's triangle is its symmetry about the vertical middle axis. In fact, on each level we obtain the same entries if we read from left to right or from right to left. In formulas this is the rule

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

We leave it to the reader to prove this rule.

1. The number of a-ary n-tuples is a^n.

2. If set $\mathcal{A}$ has a elements and set $\mathcal{B}$ has b elements, then the elements of the **Cartesian product** $\mathcal{A} \times \mathcal{B}$ are the pairs (x, y), where x is from $\mathcal{A}$ and y is from $\mathcal{B}$. The number of these pairs is ab.

3. The subsets of an n-set are in a natural bijection with bitstrings of length n. There are 2^n such subsets.

4. The **binomial coefficient** $\binom{n}{m}$ is the number of m-subsets of an n-set.

5. The **addition rule** for binomial coefficients is
$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m} \quad (m > 0).$$

6. **Pascal's triangle** contains the binomials $\binom{n}{m}$ on level n.

7. The number $\binom{n}{m}$ is also the number of paths in Pascal's triangle from the top down to the node labelled by $\binom{n}{m}$.

8. The **rule of complements** is
$$\binom{n}{m} = \binom{n}{n-m}.$$

Problems

1. Let sets A, B, C have cardinalities (number of elements) $2, 10, 7$, respectively. What is the cardinality of the Cartesian product $A \times B \times C$?

2. Which set has more elements, the set of subsets of a 10-set or the Cartesian product $A \times A \times A$, where A is a 10-set?

3. Compute levels 9 and 10 of Pascal's triangle.

4. Find a systematic way to compute $\binom{6}{3}$ and $\binom{7}{3}$.

Chapter 2

More on binomials

Let us look for a short formula to compute $\binom{n}{2}$. In the bitstring language $\binom{n}{2}$ is the number of bitstrings of length n with two 1s in them. Let us count in how many there are. If the first entry 1 occurs in coordinate 1 there are $n-1$ choices for the second. If the first entry 1 occurs in coordinate 2 there are $n-2$ choices for the second, and so on. The total number of choices is therefore $(n-1)+(n-2)+(n-3)+\cdots+2+1$. We have seen the following:

2.1 Lemma. $\binom{n}{2}$ *equals the sum of the first* $n-1$ *natural numbers.*

For example, $\binom{4}{2}=1+2+3=6$ and $\binom{7}{2}=1+2+3+4+5+6=21$. We can check that Pascal's triangle yields the same values.

Before going on let us review some standard mathematical notation. If $\mathcal{A}$ is a set, then $|\mathcal{A}|$ denotes the number of its elements. The fact that $\mathcal{A}$ is an n-set can also be expressed as $|\mathcal{A}|=n$. The number $|\mathcal{A}|$ is also called the **cardinality** of $\mathcal{A}$. As an example, the set $\mathcal{A}=\{0,1,3,5\}$ having as elements the numbers $0,1,3,5$ therefore has cardinality $4: |\mathcal{A}|=4$. The fact that 3 is an element of $\mathcal{A}$ is written as follows in this compact notation: $3\in\mathcal{A}$. As an example for the negation we have $6\notin\mathcal{A}$ (the number 6 is not an element of $\mathcal{A}$. In order to obtain a short and clear notation for the expression in Lemma 2.1 we use the following terminology. For example, consider $\sum_{i=1}^{5} i$. The symbol $\sum$ (the Greek letter *sigma*) indicates that a sum is formed. The index i runs from 1 to 5. It therefore takes on the values $1,2,3,4,5$. For each such value of i the expression to the right is formed, and all these terms are added up. In the example the summand is i itself:

$$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15.$$

Consider $\sum_{i=1}^{5} i^2$. Here i takes on the same values as before, but the corresponding summands are i^2. This gives us

$$\sum_{i=1}^{5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 1 + 4 + 9 + 16 + 25 = 55.$$

Instead of using the phrase *sum of the first* $n-1$ *natural numbers* in Lemma 2.1 we can say now $\sum_{i=1}^{n-1} i$. The lemma is then:

2.2 Lemma. $\binom{n}{2} = \sum_{i=1}^{n-1} i$

This looks more mathematical, but still it is not a satisfactory formula for $\binom{n}{2}$. In order to compute it about n additions have to be performed. This way of computing $\binom{n}{2}$ is equivalent to using Pascal's triangle.

Here is a geometrical idea: consider a square of sidelength n, which we imagine divided into small unit squares (sidelength 1 each). The number of these unit squares is clearly n^2. How does $\binom{n}{2}$ come in? Consider the small squares *under the main diagonal:* the number of these small squares is: $0+1+2+\cdots+(n-1)$ (none in the first row, one in the second row, ..., finally $n-1$ in the last row) . By Lemma 2.2 this number is $\binom{n}{2}$. By symmetry we have the same number of small squares above the main diagonal. Finally there are n squares on the main diagonal. Counting the small squares in two ways we obtain the equation

$$n^2 = 2\binom{n}{2} + n.$$

Solving this for $\binom{n}{2}$ yields the multiplicative expression we were looking for:

2.3 Theorem. $\binom{n}{2} = n(n-1)/2$.

For example, $\binom{101}{2} = \frac{101 \cdot 100}{2} = 5050$, or in old notation: the sum of the first 100 natural numbers is 5050. Here is a different, possible easier, proof of Theorem 2.3: write

$$\binom{n}{2} = 1 + 2 + \cdots + (n-1)$$

and also, reversing the order of summation,

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

Add these two expressions and observe that the sum in each column is the same: $1 + (n-1) = 2 + (n-2) = \cdots = (n-1) + 1 = n$. As there are $n-1$ columns we obtain $2\binom{n}{2} = n(n-1)$, proving Theorem 2.3 again.

The numbers $\binom{n}{2}$ are also known as **triangular numbers,** for obvious numbers: consider the triangle under the main diagonal, which was used in the proof of Lemma 2.2.

Here is an algebraic application of the triangular numbers: consider the expression $(x+y)^n$. How can it be written as a sum? We have a product of n factors, where all the factors are the same: $x+y$. Multiplying out will give us 2^n summands. We can represent these summands by bitstrings, where the coordinates correspond to the factors and the entries are interpreted as:

$$1 \leftrightarrow \text{ choose } y,\ 0 \leftrightarrow \text{ choose x.}$$

In case $n = 3$ the bitstring 010 would be interpreted as: choose y from the first and third factor, x from the second factor. This gives us the summand y^2x. In general all summands will be of the form $y^m x^{n-m}$ (there are n factors alltogether). Summand $y^m x^{n-m}$ occurs as often as there are bitstrings of length n with m ones in them. We know that there are $\binom{n}{m}$ such bitstrings. This proves a formula, which is known as the **binomial formula:**

2.4 Theorem (binomial formula). *For every x, y and for each natural number n we have*

$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m.$$

For $n = 2$ this says $(x+y)^2 = x^2 + 2xy + y^2$ (a familiar formula), for $n = 3$ we obtain $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$. The coefficients on the right side are the numbers on level n of Pascal's triangle (see Chapter 1).

If one has a general formula like the binomial formula it is always a good idea to check what it yields in special cases. At first let's choose $x = y = 1$. This special case of the binomial formula is

$$2^n = \sum_{m=0}^{n} \binom{n}{m}.$$

Is this new? Recall that $\binom{n}{m}$ is the number of m-subsets of an n-set (Definition 1.3). The sum of these numbers over all possible m is therefore the number of *all* subsets of an n-set. Our equation therefore says that an n-set has 2^n subsets. We knew that, see Theorem 1.2. There is another interesting special case Theorem 2.4: choose $x = 1, y = -1$. If $n > 0$ then the left side in the binomial formula is 0. The right side therefore is a nontrivial way of writing the number 0. We record this formula as a theorem:

2.5 Theorem. *If* $n > 0$, *then*

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

For example, case $n = 3$ is: $\binom{3}{0} - \binom{3}{1} + \binom{3}{2} - \binom{3}{3} = 0$, which is true $(1 - 3 + 3 - 1 = 0)$, for $n = 4$ this is a little bit less obvious:

$$\binom{4}{0} - \binom{4}{1} + \binom{4}{2} - \binom{4}{3} + \binom{4}{4} = 0,$$

but still true $(1 - 4 + 6 - 4 + 1 = 0)$. Such sums where the sign changes at every step are generally called **alternating sums.**

In case $n = 0$ the formula gives a hint how the expression 0^0 ought to be defined. We want the binomial formula to be true also in case $n = 0, x = 1, y = -1$. The right side is then $\sum_{m=0}^{0}\binom{0}{0} = 1$, the left side is 0^0. In fact, this convention is generally used: $0^0 = 1$. In the next chapter we will see a combinatorial application of Theorem 2.5.

Here is another combinatorial problem whose solution involves binomials: Imagine we want to choose alltogether 7 objects, where the objects come in 3 types. In how many ways can this be done? The three types of objects are apples, blueberries and cherries. Let a be the number of apples, b the number of blueberries and c the number of cherries. The total number of objects (fruits) is $a+b+c = 7$. This transforms the question into an algebraic form: what is the number of solutions of the equation $a + b + c = 7$ with non-negative integers a, b, c? There is an even fancier algebraic form of this problem: consider **monomials** $x^a y^b z^c$ in the three unknowns x, y, z. The **degree** of such a monomial is the total number of factors $a + b + c$. Our question therefore takes on the form: how many different monomials of degree 7 in 3 unknowns are there?

These are three ways of expressing the same problem, but how about the answer? Well, we can solve it directly: For a fixed value of a the value of b must be a number between 0 and $7-a$ ($8-a$ choices), and c is uniquely determined by a and b. The number of solutions is therefore $\sum_{a=0}^{7}(8-a)$. When a increases from 0 to 7, number $8-a$ decreases from 8 to 1. The number of sulutions is $\sum_{i=1}^{8} i = \binom{9}{2} = 36$ (see Lemma 2.2 and Theorem 2.3).

A more general method is obtained by representing these choices in an appropriate way. Consider the choice $a = 2, b = 3, c = 2$ (or: two apples, three blueberries, two cherries, or: $x^2y^3z^2$). We represent this choice by the bitstring 001000100, which we interpret as follows: the number of leading zeroes (before the first 1) is the number of apples, the number of zeroes between the two ones is the number of blueberries and the number of zeroes after the last 1 is the number of cherries. For example, 110000000 represents $a = b = 0, c = 7$ and 100000010 represents $a = 0, b = 6, c = 1$. We see that the number we are looking for is precisely the number of bitstrings of length 9 with two ones in them: $\binom{9}{2}$.

It is now clear how this generalizes, problem as well as solution:

2.6 Problem. *First form: How many ways are there to pick m objects of r different types?*
Second form: How many solutions does equation $x_1 + x_2 + \cdots + x_r = m$ have in non-negative integers x_i?
Third form: what is the number of monomials of degree m in r unknowns?

We represent each such solution as a bitstring of length $m + r - 1$ with precisely $r - 1$ ones. Here the number of leading zeroes represents x_1, the number of zeroes between the first and second 1 is x_2 and so forth. We see that the number of such bitstrings is the same as the number of solutions to the problem. The answer to Problem 2.6 is therefore $\binom{m+r-1}{r-1} = \binom{m+r-1}{m}$.

1. The numbers $\binom{n}{2}$ are called the **triangular numbers.**
2. $\binom{n}{2} = \sum_{i=1}^{n-1} i = 1 + 2 + 3 + \cdots + (n-1)$
3. A multiplicative formula is $\binom{n}{2} = n(n-1)/2$.
4. The **binomial formula** is
$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^{n-m} y^m.$$
5. A special case is the alternating sum
$$\sum_{m=0}^{n} (-1)^m \binom{n}{m} = 0 \text{ (if } n > 0).$$
6. $\binom{m+r-1}{m}$ is also the number of ways of choosing m objects of r different types, equivalently
7. the number of monomials of degree m in r unknowns, equivalently
8. the number of solutions of the equation $\sum_{i=1}^{r} x_i = m$ in non-negative integers x_i.

Problems

1. A club has 5 women and 10 men as members. In how many ways can a committee of 4 be formed, which has at least 2 women as members? Write the answer at first in terms of binomials, then compute it.

2. Expand $(2x-y)^4$ using the binomial formula.

3. What is the coefficient of x^4y^8 in the expansion of $(3x-2y)^{12}$? Express your answer in terms of binomials and powers. There is no need to compute the numerical value.

4. Use the binomial formula to compute $\sum_{i=0}^{n}\binom{n}{i}r^i$ for any r.

5. A bakery sells 6 different kinds of pastry. How many different dozens of pastry can you buy? Express your answer in terms of binomials. Do not canculate the value.

6. Same situation as in the preceding problem, but you buy at least 1 pastry of each kind.

7. How many integral solutions of

$$x_1 + x_2 + x_3 = 20$$

   satisfy $x_1 \geq 0, x_2 \geq -2, x_3 \geq 4$?

8. In how many ways can 12 undistinguishable apples and 1 orange be distributed among three children such that each child gets at least one piece of fruit?

Chapter 3

The principle of inclusion and exclusion

The idea is to make combinatorial use of the formula in Theorem 2.5. The formula states that

$$\sum_{m=0}^{n}(-1)^m\binom{n}{m}=0$$

if $n>0$, whereas in case $n=0$ the result is $=1$. We can express this in words as: for fixed $n>0$ the alternating sum over all $\binom{n}{m}$ vanishes, whereas for $n=0$ we obtain 1.

Here is the combinatorial problem to which we want to apply this formula: let S be a finite set and $A_1, A_2, \ldots, A_k$ be subsets of S. Again: we have a family of subsets of S. Each A_i is a subset of S. What we want is a formula for the number of elements of S, which do not belong to any of the A_i. This formula is much harder to state than to prove. Recall another piece of standard mathematical terminology: the **intersection** $A\cap B$ of two sets contains all elements, which are in A and also in B. The **union** $A\cup B$ is the set containing all elements of A and also all elements of B as elements. For example, let

$$\mathcal{A}=\{a,b,c,d,e\} \text{ and } \mathcal{B}=\{a,d,f,g,h\}$$

Then

$$A\cap B=\{a,d\},\ A\cup B=\{a,b,c,d,e,f,g,h\}.$$

The generalization to more than two sets is obvious.

Here is the formula:

3.1 Theorem (PIE). *Let S be a finite set and $A_1, \dots, A_k$ subsets of S. The number of elements of S which do not belong to any of the A_i is*

$$|S| - \sum_i |A_i| + \sum_{i,j} |A_i \cap A_j| - \sum_{i,j,l} |A_i \cap A_j \cap A_l| + - \dots$$

Here PIE stands for **Principle of Inclusion and Exclusion.** Do not confuse it with Prince Edward Island. The second sum is over all pairs $\{i, j\}$ where $i \neq j$. We have $\binom{k}{2}$ summands. The next term has $\binom{k}{3}$ terms and so on. As promised the proof is astonishingly easy:

Proof. Let $x \in S$. Denote by n the number of the subsets A_i to which x belongs. We want to compute how often x is counted by the expression in the statement of the theorem. This contribution is

$$1 - n + \binom{n}{2} - \binom{n}{3} + \cdots = \sum_{m=0}^{n} (-1)^m \binom{n}{m}.$$

If $n > 0$, meaning that x belongs to one or more of the A_i (x belongs to the union of the A_i), then this quantity is $= 0$ by our formula. If $n = 0$, then the result is $= 1$. $\square$

Statements like Theorem 3.1 are generally known as **sieve methods:** elements belonging to one of the A_i fall through the sieve (they contribute 0 to the sum), whereas each of the remaining elements contributes 1 to the sum.

It is at first hard to imagine that such a complicated expression can be useful. However, there are many situations when all these intersection sizes are easy to compute whereas the number of elements not in any of the A_i is not that easily determined.

Our first example involves divisibility of integers. As a preparation here is another piece of terminology:

for every real number x denote by $\lfloor x \rfloor$ the largest integer, which is $\leq x$. If x itself is an integer, then $\lfloor x \rfloor = x$. Here are some more values:

$$\lfloor 0.3 \rfloor = 0, \ \lfloor \frac{22}{7} \rfloor = 3, \ \lfloor -7.5 \rfloor = -8.$$

The following is rather clear:

3.2 Lemma. *The n, m be natural numbers. The number of multiples of m between 1 and n is $\lfloor \frac{n}{m} \rfloor$.*

Here is our first application of PIE:

3.3 Example. *Find the number of integers between 1 and 1000, inclusive, which are not divisible by $5, 6$ or 8.*

The underlying set S consists of the 1000 integers between 1 and 1000. Let A_1 consist of those integers in S, which are multiples of 5, A_2 those which are multiples of 6 and A_3 those multiples of 8. By Lemma 3.2 we know

$$|A_1| = 200,\ |A_2| = \lfloor 1000/6 \rfloor = 166,\ |A_3| = 1000/8 = 125.$$

In order to apply PIE we also need to know the sizes of the pairwise intersections of the A_i and the size of $A_1 \cap A_2 \cap A_3$. Recall that a number is a multiple of a and also a multiple of b if and only if it is a multiple of ab *provided a and b are coprime.* This shows that $A_1 \cap A_2$ consists of the multiples of 30 in S and $A_1 \cap A_3$ consists of the multiples of 40 in S, therefore

$$|A_1 \cap A_2| = \lfloor 1000/30 \rfloor = 33 \text{ and } |A_1 \cap A_3| = 1000/40 = 25.$$

However, 6 and 8 have a common divisor of 2 (they are not coprime), and $A_2 \cap A_3$ consists of the multiples of 24 in S, hence

$$|A_2 \cap A_3| = \lfloor 1000/24 \rfloor = 41.$$

Finally, $A_1 \cap A_2 \cap A_3$ consists of the integers of S, which are divisible by $5, 6$ and 8. These are the integers divisible by $5 \cdot 24 = 120$:

$$|A_1 \cap A_2 \cap A_3| = \lfloor 1000/120 \rfloor = 8.$$

We can apply PIE and obtain the following answer:

$$1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = 600.$$

Recall from Chapter 2 that we know how to count the solutions of equation

$$x_1 + x_2 + \cdots + x_r = m$$

in non-negative integers x_i. The number of solutions is $\binom{m+r-1}{r-1}$. PIE enables us to solve such problems when in addition upper bounds on the x_i are given.

3.4 Problem. *Determine the number of solutions of the equation*

$$x_1 + x_2 + x_3 = 20$$

in integers satisfying $0 \leq x_1 \leq 9,\ 0 \leq x_2 \leq 7,\ 0 \leq x_3 \leq 7$.

Let S be the set of solutions (each solution is a triple (x_1, x_2, x_3) of non-negative integers) of the corresponding problem without the upper bounds on the x_i. We know $|S| = \binom{22}{2} = 11 \cdot 21 = 231$. Let A_1 be the subset of S consisting of the solutions with $x_1 \geq 10$. Likewise A_2 is defined by $x_2 \geq 8$ and A_3 is defined by $x_3 \geq 8$. We are now in the situation of PIE. Our problem is precisely to count the elements in S which are not in $A_1 \cup A_2 \cup A_3$. Can we determine the cardinalities of the A_i and their various intersections? Consider A_1. It is defined by $x_1 \geq 9$. Define a new variable $y_1 = x_1 - 10$. Then $y_1 \geq 0$ and $y_1 + x_2 + x_3 = 20 - 10 = 10$. It is also clear that each solution of $y_1 + x_2 + x_3 = 10$ in non-negative integers y_1, x_2, x_3 yields precisely one solution in A_1. This shows $|A_1| = \begin{pmatrix} 12 \\ 2 \end{pmatrix} = 66$. For A_2, A_3 we can use the same argument (with $y_2 = x_2 - 8$ in the case of A_2 and $y_3 = x_3 - 8$ in the case of A_3). This yields

$$|A_2| = |A_3| = \begin{pmatrix} 14 \\ 2 \end{pmatrix} = 91.$$

Consider $A_1 \cap A_2$. Let $y_1 = x_1 - 10$ and $y_2 = x_2 - 8$ We have to count the solutions of $y_1 + y_2 + x_3 = 2$ in non-negative integers, hence $|A_1 \cap A_2| = \begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$. The same method yields $|A_1 \cap A_3| = 6$ and $|A_2 \cap A_3| = \begin{pmatrix} 6 \\ 2 \end{pmatrix} = 15$. Clearly $A_1 \cap A_2 \cap A_3 = \emptyset$. We can apply PIE and obtain the answer to our problem:

$$231 - (66 + 91 + 91) + (6 + 6 + 15) - 0 = 10.$$

1. The formula

$$\sum_{m=0}^{n}(-1)^m\binom{n}{m} = \begin{cases} 0 & (\text{if } n > 0) \\ 1 & \text{if } n = 0 \end{cases}$$

   follows from the binomial formula, see Chapter 2.

2. The **principle of inclusion and exclusion** is an application of this formula.

3. The PIE allows us to count the natural numbers in an interval which are not divisible by certain given numbers.

4. Another application is the determination of the number of integer solutions of $\sum_{i=1}^{r} x_i = m$ when the x_i satisfy both lower and upper bounds.

5. More applications of PIE concerning permutations follow in Chapter 4

Problems

1. Find the number of integers between 1 and $10,000$ inclusive, which are not divisible by $4, 5$ or 6.

2. Determine the ten solutions of Problem 3.4.

3. Determine the number of solutions of the equation $x_1+x_2+x_3+x_4 = 14$ in non-negative integers x_1, x_2, x_3 and x_4 not exceeding 8.

4. Determine the number of integral solutions of the equation $x_1 + x_2 + x_3 + x_4 = 20$ which satisfy

$$1 \leq x_1 \leq 6,\ 0 \leq x_2 \leq 7,\ 4 \leq x_3 \leq 8,\ 2 \leq x_4 \leq 6.$$

5. In how many ways can 10 orange drinks, 1 lemon drink and 1 lime drink be distributed to 4 children so that each child gets at least one drink and the lemon and lime drinks go to different children?

6. In how many ways can 12 indistinguishable apples and 1 orange be distributed among three children such that each child gets something to eat?

Chapter 4

Permutations

We have studied both ordered and unordered structures. An n-tuple is an ordered object: there is a first coordinate, a second coordinate ,... In contrast, a set is unordered. The set $\{1, 2, 3\}$ does not have a first or second element, and $\{1, 2, 3\} = \{3, 2, 1\}$. Permutations are ordered objects. An informal description is: *a permutation of n persons is a way of arranging them on n chairs.* Here it is understood that we can distinguish not only the persons but also the chairs. There is a first chair, a second chair, ... In case $n = 4$ denote the persons (objects) as a, b, c, d. They form the underlying set $S = \{a, b, c, d\}$. Then $abcd$ is one permutation of S : a sits in chair number 1 (the first coordinate), b in chair number 2 ... In the language of tuples (Chapter 1) we can define permutations as follows:

4.1 Definition. *A* **permutation** *of an n-set S is an n-tuple with entries from S such that all entries are different.*

Once again we can express this concept in an algebraic way. Choose the underlying set to be $S = \{1, 2, \dots, n\}$. In order to describe a permutation I have to decide what to use as first element, what as second, ... Such a permutation can be described by a function (mapping): $f(1) =$ the first element, $f(2) =$ the second element ... of the permutation. For example, permutation 1423 is equivalent to the mapping $f(1) = 1, f(2) = 4, f(3) = 2, f(4) = 3$. This is a one-to-one (one also says: *bijective*) mapping $f : S \longrightarrow S$. Conversely any bijective mapping $f : S \longrightarrow S$ describes a permutation of S : simply identify f with the tuple $(f(1), f(2), \dots, f(n))$.

4.2 Lemma. *We can identify the permutations of set S with the one-to-one mappings : $S \longrightarrow S$.*

How many permutations of an n-set are there? Let $n = 2, S = \{a, b\}$. In this case there are only two permutations, ab and ba. In case $n = 3, S = \{a, b, c\}$ there are 6 permutations:

abc
acb
bac
bca
cab
cba

and in case $n = 4, S = \{a, b, c, d\}$ we count 24 permutations:

$abcd$	$bacd$	$cabd$	$dabc$
$abdc$	$badc$	$cadb$	$dacb$
$acbd$	$bcad$	$cbad$	$dbac$
$acdb$	$bcda$	$cbda$	$dbca$
$adbc$	$bdac$	$cdab$	$dcab$
$adcb$	$bdca$	$cdba$	$dcba$

In fact, using the multiplicative argument from Chapter 1, it is easy to count the permutations. Here is another piece of mathematical terminology: just as $\sum$ denotes a sum, the symbol $\prod$ denotes a product of numbers. For example, $\prod_{i=1}^{3} i$ is the product of the first 3 natural numbers $(1 \cdot 2 \cdot 3 = 6)$, and $\prod_{i=1}^{3}(i + 2) = 3 \cdot 4 \cdot 5 = 60$.

4.3 Theorem. *The number of permutations of an n-set is*

$$n! = 1 \cdot 2 \cdot \cdots \cdot n = \prod_{i=1}^{n} i$$

(the product of the first n natural numbers, pronounced n factorial).

Proof. In order to define a permutation there are n choices for the first element. Once the first element is chosen there are $n - 1$ choices for the second element (this gives $n(n - 1)$ choices for the first 2 elements). When the first two elements are chosen there are $n - 2$ possibilities for the third element, and so forth. $\square$

The proof of Theorem 4.3 shows that we can count something more general:

4.4 Theorem. *The number of m-tuples with different entries from an n-set is*

$$n(n-1)\cdot(n-m+1)=\frac{n!}{(n-m)!}.$$

For example the number of ordered 3-tuples with different entries from an n-set is $n(n-1)(n-2)=\frac{n!}{(n-3)!}$.

Unexpectedly these considerations concerning permutations give us the opportunity to derive closed formulas for the binomials $\binom{n}{m}$. Recall that we know a multiplicative formula in case $m=2$ (these are the triangular numbers $\binom{n}{2}=n(n-1)/2$) but not for any higher value of m. The number in Theorem 4.4 counts m-tuples with different entries from the alphabet. The underlying subset is therefore an m-subset and $\binom{n}{m}$ counts the m-subsets. In a way the formula $\frac{n!}{(n-m)!}$ does count all m-subsets, but it counts each such subset a large number of times. How often? As often as the elements of an m-set can be ordered in a permutation, hence $m!$ times. In order to count the m-subsets we therefore have to divide by $m!$ This shows the following:

4.5 Theorem.

$$\binom{n}{m}=\frac{n!}{m!(n-m)!}=\frac{n(n-1)\dots(n-m+1)}{m(m-1)\cdot\dots\cdot 1}$$

For example

$$\binom{8}{4}=\frac{8\cdot 7\cdot 6\cdot 5}{4\cdot 3\cdot 2\cdot 1}=7\cdot 2\cdot 5=70$$

and

$$\binom{100}{3}=\frac{100\cdot 99\cdot 98}{3\cdot 2}=100\cdot 33\cdot 49=161,700.$$

Observe that both numerator and denominator of the fraction in Theorem 4.5 has m factors.

The principle of inclusion and exclusion (Chapter 3) is often useful in problems involving permutations. Consider the following example:

How many permutations of the letters

$$M,A,T,H,I,S,F,U,N$$

are there such that none of the words $MATH, IS, FUN$ occur as consecutive letters?

We are more or less forced to use PIE. The underlying set S is the set of all $9! = 362,880$ permutations of the 9 letters. Define A_1 to consist of the permutations containing $MATH$ as a word, analogously A_2 (IS is a subword) and A_3 (FUN is a subword). The permutations in A_i are easy to count. Each element of A_1 can be seen as a permutation of the 6 objects $MATH, I, S, F, U, N$. It follows $|A_1| = 6! = 720$. For the same reason we have $|A_2| = 8! = 40,320$ and $|A_3| = 7! = 5,040$. The sizes of the various intersections are just as easily determined. The elements of $A_1 \cap A_2$ can be seen as the permutations of the 5 objects $MATH, IS, F, U, N$, hence $|A_1 \cap A_2| = 5! = 120$, analogously

$$|A_1 \cap A_3| = 4! = 24, |A_2 \cap A_3| = 6! = 720 \text{ and } |A_1 \cap A_2 \cap A_3| = 3! = 6.$$

We can apply Theorem 3.1 and obtain as answer to our little problem

$$362,880 - (720 + 40,320 + 5,040) + (24 + 120 + 720) - 6 = 317,658.$$

The same method can be applied in the following more prominent problem.

4.6 Definition. *A* **derangement** *on n objects is a permutation of the objects such that no object is in its place after applying the permutation. More precisely, a permutation f of $S = \{1, 2, \ldots, n\}$ is a derangement if $f(i) \neq i$ for all i.*

The derangements on 4 objects are

2143
2341
2413
3142
3412
3421
4123
4312
4321

A more modern name used in group theory is **fixed-point-free permutations.**

What is the number of derangements of n objects? Once again we can use PIE, with S the set of all $n!$ permutations. For each $i = 1, 2, \ldots, n$ let A_i consist of the permutations such that i is fixed. Clearly $|A_i| = (n-1)!$ We have to determine the sizes of all types of intersections of the various A_i. This, however, is immediately clear: we have

$$|A_i \cap A_j| = (n-2)!, \ |A_i \cap A_j \cap A_k| = (n-3)!, \ldots$$

As the number of such pairs is $\binom{n}{2}$, the number of triples is $\binom{n}{3}, \ldots$ we can apply Theorem 3.1 right away. The number of derangements on n objects is

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

It looks a little unnecessary to write out the term $1-1$ here, but in fact it is easier to see in this way what the general form of the alternating sum is:

4.7 Theorem. *The number of derangements on n objects is* $n! \sum_{i=0}^{n} (-1)^i \frac{1}{i!}$.

You may recognize the alternating sum from calculus. It consists of the first terms of the Taylor series for $e^{-1} = \frac{1}{e}$, where e is the famous Euler number. We conclude that for large n the number of derangements of n objects is close to $\frac{n!}{e}$.

This may be the time to introduce another basic mathematical concept, sample spaces and probability:

4.8 Definition. *Let X be a set. For each $x \in X$ let a non-negative number $p_x \geq 0$ be given such that $\sum_{x \in X} p_x = 1$. Then X is called a* **sample space** *or* **probability space.** *The number p_x is called the* **probability** *of x. The probability of a subset $Y \subseteq X$ is defined as $p(Y) = \sum_{y \in Y} p(y)$. In the special case when $|X| = n$ and $p_x = 1/n$ for all x one speaks of a* **uniform** *sample space or a uniform distribution.*

For example, a fair die defines a uniform sample space with 6 elements. The probability that the result is even is of course $\frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$.

Many problems of enumerative combinatorics have their origin (or one origin) in probability theory. The first volume of Feller's book [3] is an excellent introduction.

In the case of derangements consider the permutations of elements as a uniform sample space (with $n!$ elements). Theorem 4.7 says that when a permutation is chosen arbitrarily (according to the uniform distribution), then the probability to pick a derangement is $\sum_{i=0}^{n}(-1)^i \frac{1}{i!}$, which is close to e^{-1}.

Maybe you like the following way of expressing the concept: at a party n gentlemen check their hats. If the hats are returned by pure chance, then the probability that no gentleman gets his own hat back is about $1/e$.

Permutations are important objects in group theory. The set of all permutations on n symbols forms a group, the **symmetric group** S_n.

1. A **permutation** of n objects is an arrangement of these objects in an n-tuple, equivalently
2. a permutation on n objects is a one-to-one mapping from an n-set onto itself.
3. There are $n! = n(n-1)(n-2)\dots 2 \cdot 1$ permutations on n objects.
4. $\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$.
5. A **derangement** (the modern name is **fixed-point-free permutation**) of $\{1, 2, \dots, n\}$ is a permutation f such that $f(i) \neq i$ for all i.
6. There are about $n!/e$ derangements on n objects, in other words
7. If a permutation on n objects is picked at random, then the probability that it is a derangement is close to $1/e$.

Problems

1. Find the numbert of, derangements on 5 objects and the number of derangements on 6 objects.

2. How many orderings are there for a deck of 52 cards if all the cards of the same suit are consecutive?

3. In how many ways can 6 gentlemen and 6 ladies be seated at a round table (the seats are numbered) if the gentlemen and ladies are to sit in alternate seats?

4. In how many ways can 15 people be seated at a round table if B refuses to sit next to A?

5. Let $n = n_1 + n_2 + n_3$. In how many ways can n distinguishable objects be distributed among 3 children where the first child gets n_1 objects, the second gets n_2 and of course the third gets n_3 objects? Express the answer in terms of factorials.

Chapter 5

Binomial identities

Many formal identities are known, which involve binomials. We have encountered some already, see Theorem 1.4, the identity underlying Pascal's triangle,

$$\sum_{m=0}^{n} \binom{n}{m} = 2^n$$

expressing the fact that an n-set has 2^n subsets (see Chapter 2) and the alternating sum underlying the principle of inclusion and exclusion. The following simple identity is a direct consequence of Theorem 4.5:

5.1 Proposition.

$$\binom{n}{m} = \frac{n}{m}\binom{n-1}{m-1}.$$

As is often the case in these matters there is also a purely combinatorial proof for Proposition 5.1: fix the n-set. Now count all *pairs* (U, P), where U is an m-subset and $P \in U$ a point. There are $\binom{n}{m}$ choices for U and, for every given U, there are m choices for P. The number of our pairs is therefore $m\binom{n}{m}$. We can count that number in a different way: there are n choices for P and, for every given P, there are $\binom{n-1}{m-1}$ possibilities to complete it to an m-subset. The number of pairs is therefore $n\binom{n-1}{m-1}$. This shows that the numbers $m\binom{n}{m}$ and $n\binom{n-1}{m-1}$ are equal and proves the formula.

Here we have applied a principle which one should think is too obvious to deserve mentioning: if I count the same objects in two (correct) ways, the result must be the same. It is sometimes called the *double counting principle* and can be surprisingly effective.

Here is another elementary identity:

5.2 Proposition.

$$\sum_{m=0}^{n} m\binom{n}{m} = 1\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n2^{n-1}.$$

Proof. It is best to interpret $\binom{n}{m}$ as the number of bitstrings of length n with m ones. The sum under consideration counts the ones. Represent each of the 2^n subsets by a bitstring. The concatenation of all these bitstrings has length $n2^n$. Our sum represents the total number of ones in this long string. It is clear that 1 occurs just as often as 0. The number of ones is therefore $n2^{n-1}$ as claimed. □

5.3 Proposition.

$$\sum_{m=0}^{n} \binom{n}{m}^2 = \binom{2n}{n}$$

Proposition 5.3 computes the sum of the squares of the entries on level n of Pascal's triangle (see Chapter 1). Consider for example $n = 4$. The sum of squares on level 4 is supposed to be $\binom{8}{4} = 70$, the entry in the middle of level 8. It is in fact $1^2 + 4^2 + 6^2 + 4^2 + 1^2 = 1 + 16 + 36 + 16 + 1 = 70$.

Proof. As is often the case a combinatorial proof is easiest. Start from a set of $2n$ elements, divided in a left half and a right half. Count the n-subsets. Each such n-subset intersects the left half in some $m \leq n$ elements. For a fixed m there are $\binom{n}{m}$ choices for the left intersection. The intersection with the right half must then have $n - m$ points. For each fixed intersection with the left half there are $\binom{n}{n-m} = \binom{n}{m}$ possibilities for the intersection with the right half. The total number of n-subsets intersecting the left half in m points is therefore $\binom{n}{m}^2$. Summing up over all possible m we count all n-subsets. □

5.4 Proposition.

$$\sum_{m=1}^{n} m^2\binom{n}{m} = n(n+1)2^{n-2}.$$

Proof. The standard proof uses the binomial theorem and differentiation. However, a combinatorial reasoning is much simpler. Let S be a fixed n-set. The trick is to count the triples (U, P, Q), where U is a nonempty subset of

S and $P, Q \in U$. We count in two different ways. At first count from left to right: U is an arbitrary nonempty subset. Let m be its cardinality. When m is fixed there are $\binom{n}{m}$ choices for U, and for each such U there are m choices for P and also m choices for Q. All in all we count $\sum_{m=1}^{n}\binom{n}{m}m^2$ such triples. This is the left side of the equation.

Now count from right to left. Distinguish two cases: if $P = Q$, there are n choices for such a point, and when $P = Q$ is fixed there are 2^{n-1} choices for U. In case $P \neq Q$ there are n choices for Q, for each Q there are $n-1$ choices for P and for fixed Q, P there are 2^{n-2} choices for U. The number of triples is therefore

$$n2^{n-1} + n(n-1)2^{n-2} = n(n+1)2^{n-2}.$$

$\square$

Now let $S = \{1, 2, \dots, n+1\}$, where we use the natural ordering $1 < 2 < 3 < \dots$. Split the $\binom{n+1}{m+1}$ subsets of cardinality $m+1$ into subclasses according to their *smallest element* i. When i is fixed there are $\binom{n+1-i}{m}$ such subsets. This yields the following identity:

5.5 Proposition.

$$\binom{n+1}{m+1} = \sum_{i\geq 1}\binom{n+1-i}{m} = \binom{n}{m} + \binom{n-1}{m} + \binom{n-2}{m} + \dots$$

Problems

1. Generalize Proposition 5.3 as follows: consider a set of size $n+m$, divided in a left part of n elements and a right part of m elements. Count the n-subsets by distinguishing their intersection size with the left part. This yields an equation whose right side is $\binom{n+m}{n}$.

2. Use the variant of the counting method of Proposition 5.5, where you distinguish according to the largest number i such that $\{1, 2, \dots, i\}$ is contained in the subset. Which identity is obtained?

Chapter 6

Unimodality and Sperner's theorem

In this chapter we will encounter our first example of a branch of structural combinatorics which is known as **extremal set theory.** This famous theorem is attributed to Sperner (1928). As a preparation we prove that the binomials $\binom{n}{m}$ grow with m ($\binom{n}{0} < \binom{n}{1} < \binom{n}{2} \dots$) until m is about $n/2$. From then on the sequence decreases. Sequences of numbers with this behaviour are called unimodal:

6.1 Definition. *A sequence of natural numbers $a_n, n = 0, 1, \dots, a_N$ is* **unimodal** *if there is some M such that*

$$a_0 \leq a_1 \leq \dots \leq a_M \geq a_{M+1} \geq a_{M=2} \geq \dots \geq a_N.$$

If we read the numbers on a fixed level of Pascal's triangle from Chapter 1, we see that these sequences display exactly this behaviour. Moreover they are **symmetric** ($\binom{n}{n-m} = \binom{n}{m}$).

6.2 Theorem. *For fixed n the sequence $\displaystyle\binom{n}{m}, m = 0, \dots, n$ is symmetric and unimodal.*

Proof. Symmetry is clear. Unimodality is easy to show using Theorem 4.5. In fact, we see $\binom{n}{m}/\binom{n}{m-1} = \frac{n-m+1}{m}$. The sequence is growing as long as this quotient is ≥ 1, equivalently $n \geq 2m - 1$. It is best to distinguish the cases n even and n odd. If $n = 2k$ is even, then the largest number in the sequence is $\binom{2k}{k} = \binom{n}{n/2}$. If $n = 2k + 1$ the factor is $geq1$ when $m \leq k + 1$. The largest binomial in this case is $\binom{2k+1}{k} = \binom{2k+1}{k}$. □

6.3 Corollary. *The largest binomial with numerator n is* $\binom{n}{\lfloor n/2 \rfloor}$.

Here we use terminology ($\lfloor x \rfloor$) that was introduced in Chapter 3.

Sperner's question concerns certain types of families of subsets of a given set.

6.4 Definition. *Let $\mathcal{F}$ be a family of subsets of the n-set S. We call $\mathcal{F}$ an* **antichain** *if no two different elements of $\mathcal{F}$ are subsets of each other. Once again: let $U \in \mathcal{F}$ and $V \in \mathcal{F}$ be different. Recall that both U and V are subsets of S. We demand that U is not a subset of V and that V is not a subset of U.*

It is then natural to ask the following question: *what is the maximum number of sets in an antichain?* Sperner's theorem gives the answer:

6.5 Theorem (Sperner). *The maximum size of an antichain in the family of subsets of an n-set is* $\binom{n}{\lfloor n/2 \rfloor}$.

Comparison with Corollary 6.3 shows that the value in Sperner's theorem is not all that surprising. In fact, it is clear that the subsets of fixed cardinality m form an antichain with $\binom{n}{m}$ members. Corollary 6.3 shows that the best choice in this construction is $m = \lfloor n/2 \rfloor$. Theorem 6.5 states that no larger antichains exist.

Our proof makes use of permutations on n objects. Write each such permutation as an n-tuple $(x_1, x_2, \ldots, x_n)$ (where $x_i \in S$, pairwise different). Let $A \subset S, |A| = k$. For the moment we say a permutation **starts with** A if $\{x_1, x_2, \ldots, x_k\} = A$ (the k first entries of the permutation form the subset A). How many permutations start with A? Clearly, this number is $k!(n-k)!$ Let now $\mathcal{F}$ be an antichain and $A, B \in \mathcal{F}, A \neq B$. Here comes the central observation: a permutation starting with A cannot start with B. This follows precisely from the antichain condition. This gives us information about which cardinalities can occur how often in our antichain: denote by a_k the number of elements of the antichain $\mathcal{F}$ which have cardinality k. Summing up the numbers of permutations starting with the various elements of our antichain we obtain $\sum_k a_k k!(n-k)!$ By the central observation we have never counted a permutation twice. This sum can therefore not exceed the number $n!$ of all permutations. We have $\sum_k a_k k!(n-k)! \leq n!$ Divide both sides by $n!$ Comparison with Theorem 4.5 shows that the binomials come in. We have proved the following:

6.6 Theorem. *If an antichain in an n-set has a_k members of cardinality k ($k = 0, 1, \ldots, n$), then the following holds:*

$$\sum_{k=0}^{n} \frac{a_k}{\binom{n}{k}} \leq 1.$$

Theorem 6.6 is known as the **LYM inequality** (named after Lubell, Yamamoto and Meschalkin). It is interesting in its own right. What is the meaning of the terms in the LYM-inequality? There are $\binom{n}{k}$ subsets of cardinality k. Our antichain uses a_k of them. The summand $a_k/\binom{n}{k}$ can therefore be interpreted as a relative size. The sum of these over all k is at most 1.

The proof of Sperner's theorem is now shockingly easy. Just observe that $\sum_k a_k$ is the size of the antichain, use the LYM inequality and Corollary 6.3:

$$|\mathcal{F}| = \sum_k a_k \leq \binom{n}{\lfloor n/2 \rfloor} \sum_k \frac{a_k}{\binom{n}{k}} \leq \binom{n}{\lfloor n/2 \rfloor}.$$

6.7 Definition. *A* **chain** *in the family of subsets of an n-set is a family of subsets U_i such that*

$$U_1 \subset U_2 \subset \cdots \subset U_r.$$

A **symmetric chain** *is a chain*

$$U_k \subset U_{k+1} \subset \cdots \subset U_{n-k},$$

where $|U_i| = i$.

The notion of a chain is probably even more natural than that of an antichain. Note that a symmetric chain is by definition gapless: for every cardinality between k and $n-k$ there is a member of our chain. The chain is called symmetric because it starts and ends in symmetric cardinalities. If the smallest cardinality is k, then the largest cardinality is $n-k$. Consider the case $n = 6$. If a symmetric chain has only one member, then its cardinality must be $6/2 = 3$. A typical example of such an extremely short symmetric chain is

$$\{1,3,4\}$$

In the other extreme, if the empty set $\emptyset$ belongs to a symmetric chain, then this chain must end in $\{1,2,3,4,5,\}$. Here is such a long symmetric chain:

$$\emptyset \subset \{1\} \subset \{1,2\} \subset \{1,2,3\} \subset \{1,2,3,4\} \subset \{1,2,3,4,5\} \subset \{1,2,3,4,5,6\}$$

Observe that each symmetric chain has a member in cardinality $\lfloor n/2 \rfloor$.

6.8 Theorem. *The family of subsets of a set can be decomposed (partitioned) in symmetric chains.*

Before proving Theorem 6.8 let us take a closer look at the statement. The number of symmetric chains in a **symmetric chain decomposition** as promised by the theorem is precisely $\binom{n}{\lfloor n/2 \rfloor}$. An antichain can have at most one subset in common with a chain. It follows that the size of an antichain is bounded by $\binom{n}{\lfloor n/2 \rfloor}$. In other words, Theorem 6.8 implies Sperner's theorem. Our first proof of Sperner's theorem was a counting proof. Theorem 6.8 gives a structural reason behind it.

The proof of Theorem 6.8 consists of a recipe to construct a symmetric chain decomposition recursively, by induction on n. For $n = 1$ there is only one chain

$$\emptyset \subset \{1\}$$

and this is also a symmetric chain decomposition. Here are symmetric chain decompositions for $n = 2$:

$$\boxed{\begin{array}{ccccc} & & \{1\} & & \\ \emptyset & \subset & \{2\} & \subset & \{1,2\} \end{array}}$$

and for $n = 3$:

$$\boxed{\begin{array}{ccccccc} & & \{1\} & \subset & \{1,3\} & & \\ & & \{2\} & \subset & \{1,2\} & & \\ \emptyset & \subset & \{3\} & \subset & \{2,3\} & \subset & \{1,2,3\} \end{array}}$$

Let a symmetric chain decomposition for the subsets of $\{1,2,\ldots,n-1\}$ be given. For each chain

$$U_k \subset U_{k+1} \subset \cdots \subset U_{n-1-k}$$

from this decomposition we construct two symmetric chains of subsets of $\{1, 2, \ldots, n\}$:

$$U_{k+1} \subset \cdots \subset U_{n-1-k}$$

and

$$U_k \subset U_k \cup \{n\} \subset \cdots \subset U_{n-1-k} \cup \{n\}.$$

This produces a symmetric chain decomposition.

The subsets of a set form what is called a **partially ordered set.** The theory of partially ordered sets or **posets** is a special branch of combinatorics.

1. A finite series of numbers is **unimodal** if it increases up to a certain point and decreases from then on.
2. For every n the sequence of the $\binom{n}{m}$ is unimodal.
3. The largest binomial number with numerator n is $\binom{n}{\lfloor n/2 \rfloor}$.
4. An **antichain** is a family of subsets such that no two of these are subsets of each other.
5. Sperner's theorem states that an antichain of subsets of an n-set cannot have more than $\binom{n}{\lfloor n/2 \rfloor}$ members.
6. The family of subsets of an n-set possesses a symmetric chain decomposition.

Problems

1. Construct symmetric chain decompositions in cases $n = 4$ and $n = 5$.
2. In a symmetric chain decomposition for $n = 10$, how many of the chains start at cardinality 2?
3. Consider symmetric chain decompositions of subsets of an n-set, $m \leq \lfloor n/2 \rfloor$. How many of the symmetric chains start in cardinality m?

Chapter 7

Generating functions

We start from the **geometric series.** Let x be any number and consider $1 + x + x^2 + \cdots + x^N = \sum_{n=0}^{N} x^n$. The basic trick is to multiply this sum by $(1 - x)$. The product is

$$(1 + x + x^2 + \cdots + x^N) - (x + x^2 + x^3 + \cdots + x^{N+1}).$$

All but two terms cancel. The result is $1 - x^{N+1}$.

7.1 Lemma.

$$\sum_{n=0}^{N} x^n = \frac{1 - x^{N+1}}{1 - x}$$

whenever $x \neq 1$.

Let $-1 < x < 1$ and consider what happens when N gets larger and larger. The term x^{N+1} will approach 0. In the limit we obtain an infinite series on the left and $1/(1 - x)$ on the right:

7.2 Proposition. *Let* $|x| < 1$. *Then*

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1 - x}.$$

The series in Proposition 7.2 is known as the **geometric series.** For example, when $x = 1/2$ we obtain

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots = \frac{1}{1 - 1/2} = 2.$$

In our combinatorial context we are really not interested, at least for the moment, in questions of convergence. Rather we interpret x as a variable and see the geometric series as a formal identity or, if you want, we see the right side $\frac{1}{1-x}$ as shorthand for the left side. The infinite sum on the left is a special case of what are known as **power series.** The general case of a power series is

$$\sum_{n=0}^{\infty} a_n x^n$$

In the special case of the geometric series we have $a_n = 1$ for all n.

7.3 Problem. *In how many ways can you make change for a dollar, using pennies, nickels, dimes and quarters?*

Clearly we can express this problem in algebraic terms: let x_1 be the number of pennies, x_2 the number of nickels, x_3 the number of dimes and x_4 the number of quarters. As we want change for 1 dollar it must be the case that $x_1 + 5x_2 + 10x_3 + 25x_4 = 100$. The x_i must be non-negative integers, and what we want to count is the number of solutions.

7.4 Problem. *Problem 7.3 is equivalent to the following: Determine the number of solutions of*

$$x_1 + 5x_2 + 10x_3 + 25x_4 = 100$$

in non-negative integers x_i.

It is clear how to generalize this in a natural way: given constants $c_i, i = 1, \dots r$ and a right side m, determine the number of solutions of the equation

$$\sum_{i=1}^{r} c_i x_i = m$$

in non-negative integers x_i. Recall that we studied the special case when $c_1 = \cdots = c_r = 1$ in Chapter 2. The answer was simply a binomial. More general cases, like Problem 7.4, require stronger methods. Power series and in particular the geometric series serve to express these problems in a different algebraic way. This is what we want to understand next.

Interpret the geometric series $G(x) = 1 + x + x^2 + x^3 + \dots$ as follows: each term x^n represents a choice of using n pennies. Call this geometric series the penny series (for the moment). The nickel series is $1 + x^5 + x^{10} + x^{15} + \cdots = \sum_{n=0}^{\infty} x^{5n} = G(x^5)$, and we interpret summand x^{5n} as our choice to use n nickels. In the same spirit the dime series is $G(x^{10}) = 1+x^{10}+x^{20}+x^{30}+\cdots = \sum_{n=0}^{\infty} x^{10n}$. It is clear now how the quarter series is defined.

Now form the product of all these series

$$G(x)G(x^5)G(x^{10})G(x^{25}).$$

Each $G(x^c)$ is a power series, in particular a long (infinite) sum. The product is obtained, via the distributive law, by multiplying out. Each summand of the product is obtained by choosing one summand from each of the factors $G(x^c)$ and multiplying.

What is the coefficient of x^{100} in this product? In order to obtain a contribution to this coefficient the exponents of the summands chosen from the factors must add up to 100. This contribution is then 1. According to our interpretation choosing x^{a_1} from $G(x)$ means *use a_1 pennies,* choosing x^{5a_2} from $G(x^5)$ represents *use a_2 nickels* and so forth. We obtain a contribution to the coefficient of x^{100} if $a_1+5a_2+10a_3+25a_4+50a_5 = 100$, equivalently when we give change for a dollar. This contribution is then $= 1$. This shows that the coefficient of x^{100} is precisely the number we are asking for in Problem 7.3 and Problem 7.4. This leads to the third equivalent form for our problem:

7.5 Problem. *The number of ways of giving change to a dollar using pennies, nickels, dimes and quarters is the coefficient of x^{100} in the product*

$$G(x)G(x^5)G(x^{10})G(x^{25}).$$

It is clear now how this generalizes.

7.6 Theorem. *Let $G(x) = \dfrac{1}{1-x}$, the geometric series. Consider the product*

$$G(x^{c_1})G(x^{c_2})\cdot\cdots\cdot G(x^{c_r}) = \sum_{n=0}^{\infty} E_n x^n.$$

Then E_n is the number of solutions of the equation $c_1x_1+c_2x_2+\cdots+c_rx_r = n$ in non-negative integers x_i.

We have reformulated and generalized the initial problem, but we do not have an answer yet. In fact, there is no short formula. We proceed recursively.

Start with $G(x)G(x^5) = \sum_{n=0}^{\infty} A_n x^n$. We know the combinatorial meaning of A_n : it is the number of ways of giving change to n cents using only pennies and nickels. It is clear that A_n is one more than the number of times 5 divides into n, in mathematical terminology $A_n = \lfloor n/5 \rfloor + 1$ (if I know how many nickels I use, possibly none, everything is uniquely determined: the remaining change is given in pennies). Next consider the product $G(x)G(x^5)G(x^{10}) = \sum_{n=0}^{\infty} B_n x^n$. Again it is clear what the coefficients B_n count (the number of ways of giving change to n cents using only pennies, nickels and dimes). Let us check out how the B_n are related to each other and to the A_n. If no dime is used at all the problem reverts to the former problem when only pennies and nickels are used. There are A_n such ways of giving change. If we do use dimes, I can imagine handing one dime already. It remains to give change to $n-10$ cents. The corresponding number is B_{n-10}. We have proved

$$B_n = A_n + B_{n-10} \text{ for } n \geq 10.$$

As we know the A_n this formula allows us to determine the B_n up to $n = 100$ in a hurry. We need these values only when n is a multiple of 5. In these cases $A_n = \frac{n}{5} + 1$.

n	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
A_n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
B_n	2	4	6	9	12	16	20	25	30	36	42	49	56	64	72	81	90	100	110	121

The entry B_n is obtained by adding the value A_n above it and the entry B_{n-10} two spaces to its left.

Now consider $G(x)G(x^5)G(x^{10})G(x^{25}) = \sum_{n=0}^{\infty} C_n x^n$. Recall that the number we are asking for in the three equivalent problems is the coefficient C_{100}. We know by now the formula, which connects the C_n and B_n. It is

$$C_n = B_n + C_{n-25} \text{ for } n \geq 25.$$

This gives us the C_n for $n = 25, 50, 75, 100$:

n	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
A_n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
B_n	2	4	6	9	12	16	20	25	30	36	42	49	56	64	72	81	90	100	110	121
C_n					13					49					121					242

We have the solution: $C_{100} = 242$. Now that the principle is clear we can easily solve such problems. For example, allow also half dollars. The half dollar series is $G(x^{50})$. The numbers we are interested in are the coefficients (call them D_n) of $G(x)G(x^5)G(x^{10})G(x^{25})G(x^{50}) = \sum_{n=0}^{\infty} D_n x^n$. The formula is

$$D_n = C_n + D_{n-50} \text{ for } n \geq 50.$$

This gives us $D_{50} = C_{50} + 1 = 50$ and $D_{100} = 242 + 50 = 292$. There are 292 ways of giving change to a dollar using pennies, nickels, quarters, dimes and half dollars.

The power series $\sum_{n=0}^{\infty} a_n x^n$ is called the **generating function** of the series of numbers a_n. For example, $\frac{1}{1-x}\frac{1}{1-x^5}$ is the generating function for the numbers A_n, where $A_n = \lfloor n/5 \rfloor$. Here is another example: let

$$S(x) = 1 + x + x^4 + x^9 + x^{16} + \cdots = \sum_{n=0}^{\infty} x^{n^2}.$$

Then $S(x)^2$ is the generating function for the numbers q_n, where q_n is the number of ways n can be written as a sum of two squares.

Equations like $B_n = A_n + B_{n-10}$ and $C_n = B_n + C_{n-25}$, expressing members of a sequence with a higher index in terms of members of the same or other sequences with a lower index are known as **recurrence relations** or **recursion formulas.**

In order to obtain more practice with generating functions consider the power series

$$(1+x)(1+x^2)(1+x^3)\cdots = \prod_{n=1}^{\infty}(1+x^n).$$

It is the generating function of which series, in other words if we write $\prod_{n=1}^{\infty}(1+x^n) = \sum_{m=0}^{\infty} a_m x^m$ what is the meaning of the coefficient a_m? Once again imagine multiplying out the long product using the distributive law. A term of degree m is obtained whenever m is written as a sum of different natural numbers. The corresponding contribution to the coefficient a_m is then $= 1$. This shows:

7.7 Proposition. *Let $\prod_{n=1}^{\infty}(1+x^n) = \sum_{m=0}^{\infty} a_m x^m$. Then a_m is the number of ways m can be written as a sum of* **different** *natural numbers.*

Is this clear? For example, consider $m = 10$. One way to write 10 as a sum of different naturals is $10 = 5 + 3 + 2$. This corresponds to choosing x^5 from the factor $(1+x^5)$, choosing x^3 from the factor $(1+x^3)$, choosing

x^2 from factor $(1+x^2)$, and choosing 1 from all other factors of the infinite product. In each factor $(1+x^n)$ we interpret the choice of 1 as *summand n not used* and the choice of x^n as **summand n used (once).**

If each natural number can be used at most twice, the factors in the infinite product would have to be $(1+x^n+x^{2n})$. This gives us the interpretation of $\prod_{n=1}^{\infty}(1+x^n+x^{2n})$ as a generating function.

1. The **geometric series** is $G(x) = \displaystyle\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$.

2. The power series $\sum_{n=0}^{\infty} a_n x^n$ in the indeterminate x is the **generating function** of the sequence of numbers a_n.

3. Let a_n be the number of solutions of the equation $c_1x_1 + c_2x_2 + \cdots + c_rx_r$ in non-negative integers x_i. Here the c_i are given natural numbers. The generating function of the a_n is the product $G(x^{c_1})G(x^{c_2})\ldots G(x^{c_r})$.

4. Let a_m be the number of ways of writing m as a sum of different natural numbers $(1, 2, 3, 4\ldots)$. Then

$$\sum_{m=0}^{\infty} a_m x^m = \prod_{n=1}^{\infty}(1+x^n).$$

Problems

1. Let a_m be the number of ways of writing m as a sum of different odd natural numbers. Write $\sum_{m=0}^{\infty} a_m x^m$ as an infinite product.

2. The square of the geometric series is the generating function of which sequence? In other words: let $G(x)^2 = \sum_{n=0}^{\infty} a_n x^n$. Find a formula for a_n.

3. Determine the number of solutions of equation $x_1+5x_2+10x_3+25x_4 = 73$ in non-negative integers x_i.

4. Let b_n be the number of solutions of $2x_1+5x_2+6x_3 = n$ in non-negative integers. Write $\sum_{n=0}^{\infty} b_n x^n$ as a product.

5. Let $\dfrac{1}{(1-x)(1-x^5)} = \sum_n A_n x^n$ and $\dfrac{1}{(1-x)(1-x^5)(1-x^6)} = \sum_n B_n x^n$. Find a recursion formula for B_n in terms of A_n and B_m for $m < n$.

6. Set up a table of values of A_n, B_n in the previous problem for $n \leq 35$.

Chapter 8

Recurrence relations

We know that the number s_n of subsets of an n-set is 2^n. This could have been proved as well by starting from the observation that

$$s_0 = 1 \text{ and } s_n = 2s_{n-1} \text{ for } n > 0.$$

This is a particularly simple example of a recurrence relation. Consider the sequence q_n defined by the recurrence relation

$$q_1 = 1, \ q_{n+1} = q_n + (2n+1) \text{ for } n > 1.$$

Clearly we can describe q_n as the sum of the n first odd natural numbers. We see

$$q_2 = 1 + 3 = 4, \ q_3 = 4 + 5 = 9, \ q_4 = 9 + 7 = 16, \ q_5 = 16 + 9 = 25, \ldots$$

This makes us conjecture the formula $q_n = n^2$ for all n.

8.1 Proposition. *Let q_n be defined by $q_1 = 1$ (the initial condition) and $q_{n+1} = q_n + (2n+1)$ for $n > 1$. Then $q_n = n^2$ for all $n \geq 1$.*

Proof. A natural proof is by induction. The claim is true for $n = 1$ because of the initial condition. It remains to prove that for arbitrary $n \geq 1$ under the assumption that the claim is true for index n it will also be true for index $n+1$. So we assume $q_n = n^2$ and we have to prove that $q_{n+1} = (n+1)^2$. As $q_{n+1} = q^n + (2n+1) = n^2 + 2n + 1$ this is true. $\square$

Next we study a famous sequence where each term depends not only on the preceding term but on the two preceding terms. These are the Fibonacci numbers.

8.2 Definition. *The Fibonacci numbers* f_n *are defined by the initial values* $f_0 = f_1 = 1$ *and the recurrence relation*

$$f_n = f_{n-1} + f_{n-2} \text{ for } n > 1.$$

It is clear that aside of the recurrence relation two initial conditions are needed to describe such a sequence. Clearly the f_n in Definition 8.2 are uniquely determined natural numbers. We would like to know how fast the sequence f_n grows. A closed formula would be welcome too. The numbers f_n can be described as the number of tuples with entries 1 and 2, which sum up to n. Clearly $f_1 = 1$ and $f_2 = 2$ (the corresponding tuples being (2) and $(1,1)$). The value $f_0 = 1$ is a convention, which can be justified by saying that the empty tuple has sum 0. These numbers f_n satisfy the recursion $f_n = f_{n-1} + f_{n-2}$. To see this distinguish the cases when the last entry of the tuple is 1 and when it is 2.

The method of generating functions from Chapter 7 is very helpful in these cases. The generating function of the Fibonacci sequence is

$$F(x) = \sum_{n=0}^{\infty} f_n x^n.$$

The aim is to use the recurrence relation to write $F(x)$ in a multiplicative form. Multiply the recurrence relation by x^n, then add:

$$\sum_{n\geq 2} f_n x^n = (\sum_{n\geq 2} f_{n-1} x^{n-1})x + (\sum_{n\geq 2} f_{n-2} x^{n-2})x^2$$

The last term is $x^2F(x)$, the other terms involve $F(x)$ with initial terms missing, more precisely:

$$F(x) - x - 1 = x(F(x) - 1) + x^2F(x).$$

Solving for $F(x)$ yields

$$F(x) = \frac{-1}{x^2 + x - 1} = \frac{1}{1 - x - x^2} = \frac{1}{(1 - \gamma_1 x)(1 - \gamma_2 x)}$$

The coefficients γ_1, γ_2 must satisfy $\gamma_1 + \gamma_2 = 1, \gamma_1\gamma_2 = -1$. They are therefore the roots of the quadratic $(x - \gamma_1)(x - \gamma_2) = x^2 - x - 1$. Solving the square we obtain

$$\gamma_1 = \frac{\sqrt{5} + 1}{2}, \gamma_2 = \frac{1 - \sqrt{5}}{2}.$$

Use the method **partial fractions.** There are constants a, b such that

$$F(x) = \frac{1}{(1-\gamma_1 x)(1-\gamma_2 x)} = \frac{a}{(1-\gamma_1 x)} + \frac{b}{(1-\gamma_2 x)}$$

The constants a, b have to satisfy the equations $a + b = 1, a\gamma_2 + b\gamma_1 = 0$. It is a good exercise to solve this. The result is

$$a = \frac{1}{\sqrt{5}}\frac{\sqrt{5}+1}{2} = \frac{1}{\sqrt{5}}\gamma_1,\ b = \frac{1}{\sqrt{5}}\frac{\sqrt{5}-1}{2} = -\frac{1}{\sqrt{5}}\gamma_2.$$

Finally, we should remember the geometric series:

$$F(x) = \frac{1}{\sqrt{5}}(\gamma_1 + \gamma_1^2 x + \gamma_1^3 x^2 \ldots) - \frac{1}{\sqrt{5}}(\gamma_2 + \gamma_2^2 x + \gamma_3^3 x^2 \ldots)$$

Finally, this gives us a formula for the Fibonacci numbers:

$$f_n = \frac{1}{\sqrt{5}}(\gamma_1^{n+1} - \gamma_2^{n+1}).$$

8.3 Theorem. *The Fibonacci numbers f_n are*

$$f_n = \frac{1}{\sqrt{5}}(\frac{\sqrt{5}+1}{2})^{n+1} - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{n+1}.$$

The explicit formula in Theorem 8.3 looks rather surprising. For example, it is not obvious from the formula that f_n is an integer. Typically the recursion formula will be more useful than the explicit formula.

Let us have a look at a different method to determine the Fibonacci numbers. At first forget the initial conditions, consider only the recursion formula. The basic idea is to find numbers α such that α^n satisfies the recursion $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$ for all n, equivalently $\alpha^2 = \alpha + 1$. The solutions are γ_1, γ_2. So we have two sequences γ_1^n and γ_2^n satisfying the recurrence. It is clear that any linear combination $a\gamma_1^n + b\gamma_2^n$ of these sequences will also satisfy the recurrence. It remains to choose the constants a, b such that the initial values are as prescribed.

This procedure recalls the solution of linear differential equations with constant coefficients, with α^n in the role of e^x. In general one speaks of a **linear recurrence relation** of depth k with constant coefficients if

$$F_n = a_1 F_{n-1} + a_2 F_{n-2} + \cdots + a_k F_{n-k}.$$

The generating function $\sum_{n=0}^{\infty} F_n x^n$ is a **rational function** (polynomial divided by polynomial), where the denominator has degree k and the numerator has degree $< k$. The numerator depends on the initial conditions. When the coefficients are not real numbers but taken from **finite fields** such sequences F_n are known as **linear shift register sequences** or **linear feedback register sequences.** They are omnipresent in cryptography and coding theory.

Observe the close relation between the Fibonacci numbers and the **golden section.** The golden section describes the division of a line segment in two parts such that the ratio of the shorter part and the longer part is the same as the ratio of the longer part and the total length of the segment. Let the segment have length 1 with longer segment of length x. The shorter segment has length $1 - x$ and our equality of ratios is

$$\frac{1-x}{x} = \frac{x}{1}, \text{ equivalently } 1 - x - x^2 = 0.$$

This quadratic $1-x-x^2$ is the denominator of power series $F(x)$. The golden section number is $\frac{\sqrt{5}-1}{2} = -\gamma_2$.

Problems

1. Consider the recursion $a_1 = 1,\ a_n = a_{n-1} + n$ for $n > 1$. Determine a_n.
2. Determine for which n the Fibonacci numbers f_n are even.
3. Prove: the sum of three consecutive Fibonacci numbers is always even.
4. Let g_n be defined by $g_0 = 2, g_1 = -1, g_n = g_{n-1} + g_{n-2}$ for $n \geq 2$ (the same recursion as the Fibonacci sequence, but different initial values). Express g_{100} in terms of Fibonacci numbers. Do not try to calculate g_{100}.
5. Define h_n by $h_0 = h_1 = 1$ and $h_n = 2h_{n-1} + h_{n-2}$ for $n \geq 2$. Determine the generating function $H(x)$ of the sequence h_n in the form of a rational function. There is no need to obtain a formula for h_n.

Chapter 9

Partition identities

Each representation of a natural number n as a sum of natural numbers

$$n = a_1 + a_2 + \cdots + a_m \text{ (where } a_i \neq 0)$$

is a **partition** of n. Here the order of the **summands** (or **parts**) a_i is irrelevant. Usually we write a partition with the a_i in non-decreasing order.

Another more combinatorial angle is obtained if we represent each partition by its **Ferrer diagram.** The Ferrer disgram of $8 = 4 + 3 + 1$ is Figure 9.1.

and the diagram describing $16 = 4 + 4 + 4 + 3 + 1$ is Figure 9.2.

Let $p(n)$ be the number of partitions of n. This defines the **partition function.** The value $p(0) = 1$ is a convention. Clearly $p(1) = 1$ and $p(2) = 2$

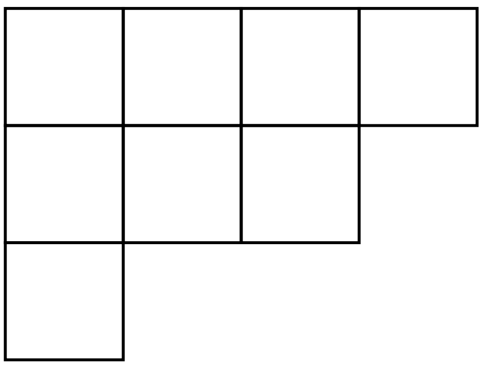

Figure 9.1: Partition $(4, 3, 1)$

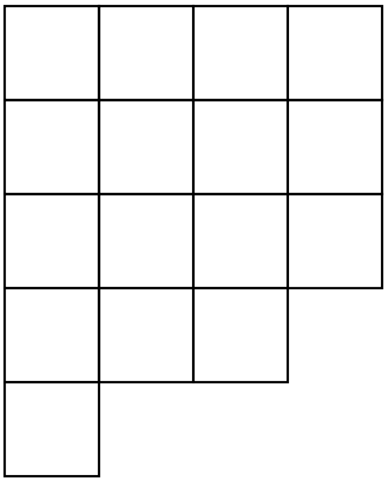

Figure 9.2: Partition $(4, 4, 4, 3, 1)$

(2 and $1+1$ are the partitions of 2), and $p(3) = 3$ $(3, 2+1, 1+1+1$ are the partitions of 3). It is equally easy to find $p(4) = 6$, $p(5) = 7$.

What is the generating function of the partition function $p(n)$? With the experience of the preceding chapters this is not hard to find:

9.1 Theorem. $1 + \sum_{n=1}^{\infty} p(n)x^n = \frac{1}{\prod_{i=1}^{\infty}(1-x^i)}$

Let us check once again why this is true: each term $\frac{1}{1-x^i}$ really stand for the infinite geometric series $1 + x^i + x^{2i} + x^{3i} + \ldots$ When multiplying out according to the distributive law, the choice of term x^{3i} say from this series means that we choose three summands i in our partition. This shows that each partition of n contributes a summand x^n to the infinite product on the right. All in all we obtain $p(n)$ as coefficient of x^n.

Once we understand this it is easy to verify the pattern.

9.2 Theorem. *Let $p_m(n)$ be the number of partitions of n all of whose parts are $\leq m$ Then*

$$1 + \sum_{n=1}^{\infty} p_m(n)x^n = \frac{1}{\prod_{i=1}^{m}(1-x^i)}$$

In terms of Ferrer diagrams, $p_m(n)$ is the number of diagrams with n cells and not more than m columns. For example, $p_3(7) = 8$, the corresponding partitions being

$$3+3+1,\ 3+2+2,\ 3+2+1+1,\ 3+1+1+1+1,$$

$$2+2+2+1,\ 2+2+1+1+1,\ 2+1+\cdots+1,\ 1+\cdots+1.$$

Here is a geometric idea which gives a different interpretation to the number $p_m(n)$: given a Ferrer diagram, consider the **conjugate** diagram, which is obtained by reading it columnwise (reflection across the main diagonal). For example, partition $8 = 4 + 3 + 1$ from Figure 9.1 has as conjugate $8 = 3+2+2+1$ and the conjugate of the partition $16 = 4+4+4+3+1$ in Figure 9.2 is the partition $16 = 5+4+4+3$. It is clear that conjugation gives us a one-to-one mapping between Ferrer diagrams with at most m columns and Ferrer diagrams with at most m rows, and therefore between partitions all of whose parts are $\leq m$ and partitions with not more than m parts.

9.3 Theorem. *$p_m(n)$ is also the number of partitions of n with at most m parts.*

It should be obvious by now that for example

$$\frac{1}{\prod_{i=1}^{\infty}(1-x^{2i})}$$

is the generating function for the number of partitions all of whose parts are even and

$$\frac{1}{\prod_{i=0}^{\infty}\{(1-x^{5i+1})(1-x^{5i+4})\}}$$

counts the partitions of n all of whose parts are $\pm 1 \pmod 5$.

Consider the denominator

$$\prod_{i=1}^{\infty}(1-x^i)$$

of the generating function in Theorem 9.1. It should be possible to give it a combinatorial meaning as well. Let us see it as a generating function. The problem is that negative signs come in. With $+$ instead of -1 we would be back to Proposition 7.7, the generating function for the number of partitions with different parts. How much trouble does the negative sign cause? Let $n = a_1 + \cdots + a_m$ be such a partition into different parts a_i. This yields a term $+x^n$ if m is even, it yields a term $-x^n$ if m is odd. This shows that the coefficient of x^n in the product is the difference between the number of partitions of n in an even number of different parts and the number of partitions of n in an odd number of different terms.

9.4 Proposition. *Let $g(n)$ be the number of partitions of n into an even number of different parts and $u(n)$ the number of partitions of n into an odd number of different parts. Then*

$$\prod_{i=1}^{\infty}(1-x^i) = 1 + \sum_{n\geq 1}(g(n)-u(n))x^n.$$

The beginning of this infinite series is

$$\prod_{i=1}^{\infty}(1-x^i) = 1 - x - x^2 + x^5 + x^7 \ldots$$

For example, $g(6) = 2$ $(5+1 = 4+2)$, $u(6) = 2$ $(6 = 3+2+1)$. This explains why there is no term of degree 6. As $g(7) = 3, u(7) = 2$, the term of degree 7 is x^7. Term x^n will be absent on the right side if $g(n) = u(n)$. Experiments show that this is often the case, and even when it is not true the difference $g(n) - u(n)$ is never large, in fact it is always $0, 1$ or -1. It can be determined precisely when these cases arise. This is Euler's famous **pentagonal number theorem:**

9.5 Theorem.

$$\prod_{i=1}^{\infty}(1-x^i) = \sum_{m\in\mathbb{Z}}(-1)^m x^{m(3m+1)/2}.$$

Because of our combinatorial interpretation Theorem 9.5 states that $g(n) = u(n)$ whenever n is not of the special form that appears on the right side. These special numbers are called pentagonal numbers, for a geometric reason. This suggests a possible line of attack for a combinatorial proof: find a bijection between the partitions of n in an even number of different parts and the partitions of n in an odd number of different parts. This should work whenever n is not a pentagonal number and a little difficulty should arise when n is pentagonal. A combinatorial proof along these lines was found by Franklin, in 1881.

The most famous among the partition identities should at least be mentioned. These are the **Rogers-Ramanujan identities.** They can be written as equations of power series, but it is easier to describe the combinatorial content directly.

9.6 Theorem (Rogers-Ramanujan). *For every n, the number of partitions of n into parts with a pairwise difference of at least 2 equals the number of partitions of n into parts, which are ± 1 mod 5.*
The number of partitions of n into parts ≥ 2 with a pairwise difference of at least 2 equals the number of partitions of n into parts, which are ± 2 mod 5.

Ramanujan had discovered these facts empirically but was unable to find a proof. They had the status of unsolved problems until Ramanujan found them formulated **and proved** in an 1894 paper by L.J.Rogers.

Let us check the first Rogers-Ramanujan identity in case $n = 10$. The partitions of 10 into parts which are at a pairwise difference of at least 2 are

$$10, 9+1, 8+2, 7+3, 6+4, 6+3+1.$$

The partitions of 10 which use only $1, 4, 5, 9$ as parts are

$$9+1, 5+4+1, 5+1+\cdots+1, 4+4+1+1, 4+1+\cdots+1, 1+\cdots+1.$$

As predicted the number of such partitions of 10 is the same for both types.

Problems

1. Find the coefficients of x^{100} and of x^{1000} in $\dfrac{1}{(1-x)(1-x^3)}$.

2. Find the coefficient of x^{100} in $\dfrac{1}{(1-x^2)(1-x^5)}$.

3. Find the generating function for the number of partitions, where each part is used at most 3 times.

4. Let $\prod_{j=0}^{\infty}(1+x^{2(2j+1)}+x^{3(2j+1)}+x^{4(2j+1)}+\dots) = \sum_n a_n x^n$.
   Give a description of a_n in terms of partitions: a_n is the number of partitions of n such that ...

Chapter 10

The Catalan numbers

10.1 Definition. *Consider $(2n)$-tuples $x = (x_1, x_2, \ldots, x_{2n})$ with entries $x_i = \pm 1$. Such a tuple is* **balanced** *if it contains n entries $+1$ and also n entries -1, equivalently if $\sum_{i=1}^{2n} x_i = 0$.*

The n-th **Catalan number** *C_n is the number of balanced $2n$-tuples which satisfy that all the partial sums $\sum_{i=1}^{k} x_i \geq 0, k = 1, 2, \ldots, 2n$. Call these tuples* **Catalan tuples.**

We could have worked as well with binary tuples (entries 0 and 1) as we have often done before. Tuples with entries ± 1 can be seen as the multiplicative way of writing binary tuples. Using ± 1 as entries makes it easier to write the *partial sum* condition of Definition 10.1. In terms of binary tuples the partial sum condition could have been written as follows: for every k the number of ones among $x_1, \ldots, x_k$ is never smaller than the number of zeroes.

The number of balanced $2n$-tuples clearly is $\begin{pmatrix} 2n \\ n \end{pmatrix}$, the number of n-subsets of a $2n$-set and the largest of the binomial numbers $\begin{pmatrix} 2n \\ m \end{pmatrix}$.

10.2 Theorem.

$$C_n = \begin{pmatrix} 2n \\ n \end{pmatrix} - \begin{pmatrix} 2n \\ n-1 \end{pmatrix} = \frac{1}{n+1} \begin{pmatrix} 2n \\ n \end{pmatrix}.$$

Proof. For the moment, call a balanced $2n$-tuple **unacceptable** if it does not satisfy the partial sum condition. Let $U_n = \binom{2n}{n} - C_n$ be the number of unacceptable balanced $2n$-tuples. We wish to determine U_n.

Given an unacceptable balanced tuple x, there must be a smallest index k such that $\sum_{i=1}^{k} x_i < 0$. Because k is chosen minimal it must be that $\sum_{i=1}^{k} x_i = -1$ and $x_k = -1$. Consider the transformation

$$x \mapsto x' = (-x_1, \dots, -x_k, x_{k+1}, \dots, x_{2n})$$

Then x' has $n+1$ entries $+1$ and $n-1$ entries -1. The decisive point is that the mapping $x \mapsto x'$ is a one-to-one mapping (bijection) between the unacceptable balanced tuples and the tuples with $n+1$ entries $+1$. In fact, let $y = (y_1, \dots, y_{2n})$ be such a tuple with $n+1$ entries $+1$. There is a smallest k such that $\sum_{i=1}^{k} y_i > 0$. As k is minimal it must be that $\sum_{i=1}^{k} y_i = 1$ and $y_k = 1$. The same mapping as above

$$y \mapsto y' = (-y_1, \dots, -y_k, y_{k+1}, \dots, y_{2n})$$

produces a balanced unacceptable tuple y'. It is also clear that this describes a one-to-one mapping.

We have $U_n = \binom{2n}{n-1}$, consequently $C_n = \binom{2n}{n} - \binom{2n}{n-1}$. A standard calculation with factorials shows $C_n = \frac{1}{n+1}\binom{2n}{n}$. □

The first Catalan numbers are

$$C_0 = 1,\ C_1 = 1,\ C_2 = 2,\ C_3 = 5,\ C_4 = 14$$

$$C_5 = 42,\ C_6 = 132,\ C_7 = 429,\ C_8 = 1430.$$

Expressed in the language of probabilities (see Chapter 4) the formula in Theorem 10.2 says the following: if we pick a binary balanced $2n$-tuple at random, then the probability of picking a Catalan sequence is $\dfrac{1}{n+1}$.

The first expression in Theorem 10.2 shows that C_n simply is the difference between the largest and the second-largest binomial with numerator $2n$ (see Chapter 6), equivalently the difference between the number in the center and its neighbour on level $2n$ of the Pascal triangle.

We almost forgot how the binomials came up as counting paths in grids, in Chapter 1. For example, the number of paths from the top of Pascal's triangle down to the center of level $2n$ is $\binom{2n}{n}$. Recall that at each step there are two choices to continue a path. We can continue either in southeast direction or in southwest direction. That is why we can describe these paths by binary tuples. The paths ending in the center of level $2n$ are described by balanced binary $2n$-tuples.

What if we require in addition that the path should be entirely on or to the east of the vertical line joining the end points? We would cross this vertical line to the west if eventually there would be more zeroes than ones among the first k entries of the tuples. This is exactly what the partial sum condition of Definition 10.1 excludes. We have seen the following:

10.3 Proposition. *The number of paths, which start from the top of the Pascal triangle and end in the center of level $2n$ such that the entire path is on or to the east of the vertical line joining the end points is precisely C_n.*

The Catalan numbers show up in many disguises. Here is one:

10.4 Definition. *Consider $(2,n)$-rectangles where each of the $2n$ cells is occupied by one of the numbers between 1 and $2n$, each number showing up once. Such a rectangle is called a* **standard tableau** *if the entries are increasing in each row (going to the right) and in each column (going down).*

Examples of standard tableaux are

$$\begin{array}{|c|c|c|}\hline 1&3&5\\\hline 2&4&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&5&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|c|}\hline 1&2&4&6\\\hline 3&5&7&8\\\hline\end{array}$$

Consider a Catalan $(2n)$-tuple. Identify the coordinates with the numbers $1, 2, \ldots, 2n$. Now we assign a tableau to each Catalan tuple in the following way: the n numbers where the entry is $+1$ are written in the first row of the tableau, in ascending order, the remaining numbers are written in the second row, also in ascending order. By construction the entries in the tableau are increasing in each row. The non-negativity condition for Catalan tuples guarantees that the same is true for each column. Some examples for this mapping from Catalan tuples to standard tableaux are

$$(+1,-1,+1,-1,+1,-1)\mapsto\begin{array}{|c|c|c|}\hline 1&3&5\\\hline 2&4&6\\\hline\end{array}\qquad(+1,+1,-1,+1,-1,-1)\mapsto\begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&5&6\\\hline\end{array}$$

$$(+1,+1,-1,+1,-1,+1,-1,-1)\mapsto\begin{array}{|c|c|c|c|}\hline 1&2&4&6\\\hline 3&5&7&8\\\hline\end{array}$$

Fortunately this process can be reversed. Given a tableau it is clear how to construct a balanced $(2n)$-tuple from it. This tuple will be Catalan if the tableau is standard. We have constructed a one-to-one mapping between Catalan $(2n)$-tuples and standard $(2n)$-tableaux for every n. This implies the following:

10.5 Theorem. *There are precisely C_n standard $(2, n)$-tableaux.*

An important subdiscipline of group theory is **representation theory** of groups. The representation theory of the symmetric groups (these are the groups formed by all permutations on some finite set) has a combinatorial flavour, and tableaux play a prominent role.

1. The n-th **Catalan number** is $C_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$.
2. C_n is the number of balanced binary $2n$-tuples satisfying that in any initial segment the number of zeroes never ecceeds the number of ones.
3. C_n is the number of paths starting from the top and ending in the center of level $2n$ of Pascal's triangle, such that the entire path is on or to the east of the vertical line connecting the end points.
4. C_n is the number of standard $(2, n)$-tableaux.

Problems

1. $2n$ people are in line to get into a theatre in which admission is 50 cents. Of these n have a 50 cent piece and n have a dollar bill. The box office opens with an empty cash register. In how many ways can people line up such that cash is available when needed?

2. A clown stands on the edge of a swimming pool, holding a bag containing n redand n blue balls. He draws the balls out one at a time and discards them. If he draws a blue ball, he takes one step back; if a red ball, one step forward. What is the probability that the clown remains dry?

Chapter 11

The Stirling numbers

There are two types of Stirling numbers, first king and second kind.

11.1 Definition. *A* **partition** *of a set X is a subdivision into non-empty non-overlapping subsets. The Stirling number S_k^n of the second kind is the number of partitions of an n-set into precisely k nonempty subsets.*

For example, $S_1^n = 1$ as there is only way of using just one subset in a partition. On the opposite end of the spectrum we have $S_n^n = 1$: the only way of using n different subsets in a partition is when the partition consists of all the 1-subsets. The case $k = 2$ already is slightly non-trivial.

11.2 Proposition. $S_2^n = 2^{n-1} - 1$.

Proof. Each subset $Y \subseteq X$ determines a partition of X into two parts, the second part being the complement of Y. This is not really true as the elements of a partition must be non-empty. The correct statement is: every subset $Y \subset X$, which is different from $\emptyset$ and from X, determines a partition into two parts. There are $2^n - 2$ such subsets Y. Each partition is obtained twice in this way (starting either from Y or from its complement). The number of partitions into 2 parts is therefore $S_2^n = \dfrac{2^n - 2}{2} = 2^{n-1} - 1$. □

It is even easier to see what S_{n-1}^n is: each such partition must consists of $n - 2$ 1-subsets and of one 2-subset. We see that the partition is uniquely determined by the 2-subset it contains. It follows $S_{n-1}^n = \dbinom{n}{2}$.

11.3 Theorem. $S_k^n = S_{k-1}^{n-1} + kS_k^{n-1}$.

Proof. Let X be the ground set, $|X| = n$. We want to count the partitions of X into k parts. Choose $P \in X$, let $Y = X \setminus \{P\}$. Given such a partition of X, consider the partition of Y obtained by removing P. The result will be a partition π of Y into either k or $k-1$ parts. Fix now the partition π of Y and count the number of partitions of X into k parts that produce π. If π has $k-1$ parts, there is only one corresponding partition of X (it has $\{P\}$ as a part). We count S_{k-1}^{n-1} partitions of X in this case. Let now π have k parts. This time there are k corresponding partitions of X : the union of $\{P\}$ and one of the parts of π must be a subset used in the partition of X. $\square$

This recursion formula makes it easy to compute a table. Here are the second Stirling numbers S_k^n for $n \leq 8$:

$n\backslash k$	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	
8	1	127	966	1701	1050	266	28	1

The Stirling numbers of the first kind are related to permutations. In Chapter 4 permutations of a set S were defined as one-to-one mappings : $S \longrightarrow S$. For example, let $S = \{1, 2, 3, 4, 5, 6\}$ and f the permutation defined by

$$1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 6,\ 4 \mapsto 1,\ 5 \mapsto 3,\ 6 \mapsto 5$$

Another way of writing this permutation was as the tuple 246135. There is yet another way of writing permutations, which is more efficient because it reveals more about the structure. Take f as an example. We have $f : 1 \mapsto 2$. Next consider the image of $2 : f : 1 \mapsto 2 \mapsto 4$. Next consider the image of $4 :$ $f : 1 \mapsto 2 \mapsto 4 \mapsto 1$. We call $1, 2, 4$ a **cycle** of f and write it $(1, 2, 4)$. Recall the rule: f maps each element of the cycle to its right neighbour, it maps the right end of the cycle to the left end. One should really imagine a cycle as a cycle (circle), and f as mapping each element to its neighbour in clockwise direction. The permutation f has two 3-cycles, see Figure 11.1.

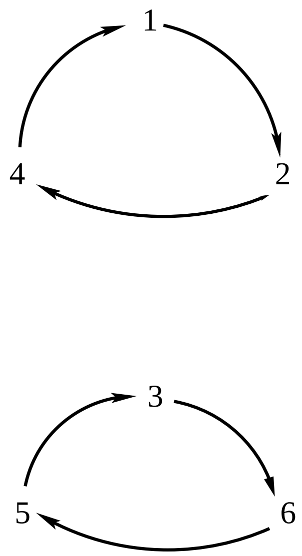

Figure 11.1: The cycles of permutation f

We write $f = (1, 2, 4)(3, 6, 5)$. Permutation f does not have fixed points (f is a derangement in the terminology of Chapter 4). In general a fixed point is a cycle of length 1. It is a convention to omit fixed points in the algebraic representation of a permutation. For example, one writes $g = (1, 2)(3, 6, 5)$ short for $g = (1, 2)(3, 6, 5)(4)$. Observe that in this **cycle representation** of a permutation the cycles are pairwise disjoint, the order in which the cycles are written is irrelevant and also the representation of each cycle can start at any of its points. For example $(1, 3, 4, 2) = (3, 4, 2, 1) = (4, 2, 1, 3) = (2, 1, 3, 4)$.

11.4 Definition. *The* **cycle representation** *of a permutation is obtained by writing the permutation as a union of disjoint cycles. If a permutation is the union of cycles of lengths $a_1, a_2, \ldots, a_k$, where $a_1 \geq a_2 \geq a_k$, then $(a_1, a_2, \ldots, a_k)$ is the* **cycle type** *of the permutation*

For example $f = (1, 2, 4)(3, 6, 5)$ has cycle type $(3, 3)$ and $g = (1, 2)(3, 6, 5)$ (on six objects) has cycle type $(3, 2, 1)$.

11.5 Definition. *The Stirling number σ_k^n of the first kind is the number of permutations on n objects, which have precisely k cycles.*

Our permutation f has 2 cycles, and g has 3 cycles. It is clear that $\sigma_n^n = 1$: the only permutation on n objects, which has n 1-cycles (fixed points) is the identity permutation. On the other extreme of the spectrum it should be easy to determine σ_1^n. This is the number of n-cycles.

11.6 Proposition. $\sigma_1^n = (n-1)!$

Proof. Start from symbol 1. In order to obtain an n-cycle its image must be different from 1. There are $n-1$ choices for this image. If the cycle starts $(1, 2, \dots)$ the image of 2 must be different from 1 and 2. There are $n-2$ choices. Continuing in this fashion we count $(n-1)(n-2)\dots 2\cdot 1 = (n-1)!$ cycles of length n. $\square$

11.7 Proposition. $\sigma_{n-1}^n = \binom{n}{2}$

Proof. There is only one way to have $n-1$ cycles: one cycle must have length 2, the rest are fixed points. There are as many 2-as there are unordered pairs of elements. This number is $\binom{n}{2}$. $\square$

Just as in the case of the Stirling numbers of the second kind there is a recursion formula, which simplifies counting. Also, it looks very similar to the recursion formula for the Stirling numbers of the second kind.

11.8 Theorem. $\sigma_k^n = \sigma_{k-1}^{n-1} + (n-1)\sigma_k^{n-1}$.

Proof. Fix a symbol, say 1. Let f be a permutation on n symbols with k cycles. Define a mapping $\alpha : S_n \mapsto S_{n-1}$ as follows: $\alpha(f)$ is obtained from f by omitting symbol 1 from the cycle of f containing 1. All other cycles of f are left untouched. If for example $(1, 2, 3, 7, 8)$ is the cycle of f containing 1, the corresponding cycle of $\alpha(f)$ is $(2, 3, 7, 8)$. Let f have k cycles. Then $\alpha(f)$ has either k or $k-1$ cycles. In fact, it has $k-1$ cycles only if 1 is a fixed point of f. Each permutation g of $n-1$ symbols with $k-1$ cycles has precisely one preimage f with k cycles. This gives us already σ_{k-1}^n permutations on n symbols with k cycles. Let now g have k cycles. How many permutations f with k cycles satisfy $g = \alpha(f)$? We have to fit in 1 in some cycle of g, between two consecutive symbols. If for example $(2, 3, 7, 8)$ is a cycle of g we can use $(1, 2, 3, 7, 8), (2, 1, 3, 7, 8), (2, 3, 1, 7, 8)$ or $(2, 3, 7, 1, 8)$ as a cycle of f. Clearly the number of preimages f is $n-1$. This leads to our formula. $\square$

Problems

1. Determine the number of mappings from an 8-set **onto** a 2-set.

2. Find a general formula for the number of mappings from an n-set **onto** a k-set, where $n \geq k$.

3. We have k different colours of paint and we wish to paint n houses (each house is painted with a single colour). In how many ways can we do this?

4. This problem is like the previous problem, but we add the condition that each of the k colours must be used at least once. In how many ways can this be done?

5. Determine $\displaystyle\sum_{k=1}^{n} \sigma_k^n$.

6. Determine $\displaystyle\sum_{k=0}^{n} S_k^n$.

Chapter 12

Graphs

Graphs are a vast class of combinatorial structures. Each graph consists of two very different kinds of objects. There is an underlying finite set, the set of **vertices.** Some pairs of vertices are in a special relation. These form the **edges** of the graph. So each edge is a pair of vertices, each pair of vertices may or may not form an edge of the graph. This leads to the following formal definition:

12.1 Definition. *A* **graph** *is a pair* $G = (V, E)$*, where* V *is a finite set (the set of* **vertices***) and* E *is a family of* 2*-subsets (unordered pairs) of vertices.*

Sometimes the graphs of Definition 12.1 are called **simple graphs.** All sorts of generalizations are being considered. When one allows ordered pairs as edges one speaks of directed graphs, short digraphs. Sometimes edges consisting of only one vertex (loops) are allowed. One also considers weighted edges, weighted vertices, multiples edges and edges with more than two vertices (hyperedges). We will generally stick to Definition 12.1. Figure 12.1 is the picture of a graph with 8 vertices and 12 edges.

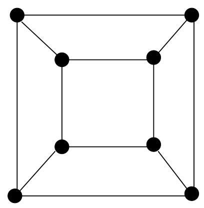

Figure 12.1: A graph with 8 vertices

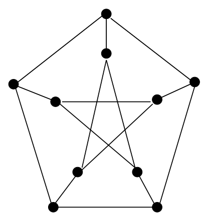

Figure 12.2: The Petersen graph

We may call it a prism. The graph in Figure 12.2 is the famous Petersen graph. It has 10 vertices and 15 edges.

It is important to remember that the representation of the points in the plane, the lengths of the edges and so forth are irrelevant. A graph is simply given by a finite set of points and a family of pairs of points. The pictures serve only as an illustration.

It is natural to count the edges passing through each point. This number is the degree of the point.

12.2 Definition. *The* **degree** $deg(P)$ *of a vertex* P *in a graph is the number of edges passing through* P. *A graph is called* **regular** *if all its vertices have the same degree.*

Sometimes the degree is called the **valency.** This suggests to interpret the vertices as atoms in a molecule. We come to our first theorem.

12.3 Theorem. *The number of vertices of odd degree in any graph is even.*

Proof. This follows from the familiar technique of double counting. Count the number of pairs (P, e), where P is a vertex, e is an edge and $P \in e$. As every edge e has 2 vertices this number is $2|E|$, double the number of edges. On the other hand this number also equals $\sum_P deg(P)$, the sum of all degrees of vertices. In order for this number to be even the number of odd degree vertices must be even. $\square$

Theorem 12.3 is also known as the handshaking lemma.

12.4 Definition. *A graph is* **connected** *if for any two vertices* P, Q *vertex* Q *can be reached starting from* P *and moving along edges. The smallest number of edges leading from* P *to* Q *is the* **distance** $d(P, Q)$. *In particular the only vertex at distance* 0 *from* P *is* P *itself, and the points* Q *of distance* $d(P, Q) = 1$ *(the* **neighbours** *of* P*) are the vertices such that* $\{P, Q\}$ *is an edge.*

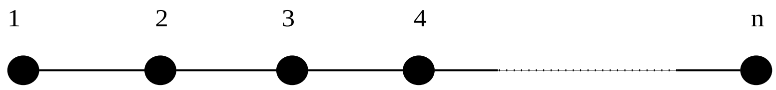

Figure 12.3: The path P_n

This may be the most important feature of connected graphs: they define a notion of distance between vertices. In mathematics one speaks of **metric spaces** when a distance is defined in a natural way. It is easy to convince ourselves that the distance in graphs satisfies $d(P,Q) = d(Q,P$ (symmetry) and $d(P,Q) \leq d(P,R) + d(R,Q)$ (the triangle inequality). In the Petersen graph all pairs of vertices are at distance $0, 1, 2$ or 3 from one another, and the same is true in our prism.

Paths and cycles are particularly simple graphs. The **path** P_n on n vertices looks as in Figure 12.3.

It should be clear how a **cycle** C_n on n vertices looks like. In the Petersen graph the 5 outside vertices form a cycle C_5, and in fact the 5 vertices on the inside form a C_5 as well.

Let n vertices be given. What is the minimum number of edges needed in order to obtain a connected graph on these n vertices? In order to answer this let us consider connected components. The empty graph on n vertices (the graph without edges) has n connected components. The graph will be connected when the number of connected components is reduced to 1. Each edge can reduce the number of connected components by at most 1. This shows that a connected graph has at least $n-1$ edges. On the other hand it is clear that connected graphs with $n-1$ edges can be costructed. Whenever a graph with $c > 1$ connected components are given I can add an edge which turns two such components into one (call it a bridge).

12.5 Definition. *A* **tree** *on n vertices is a connected graph with $n-1$ edges.*

We see that paths are trees, but cycles $C_n, n \geq 3$ are not trees (C_n has n edges). The argument above yields a different characterization of trees:

12.6 Proposition. *A graph on n vertices is a tree if and only if each of its edges is a bridge, meaning that the removal of the edge produces a graph, which is not connected.*

The best known characterization of trees is in terms of cycles. It is clear that a tree cannot contain a cycle, as the removal of one edge from a cycle

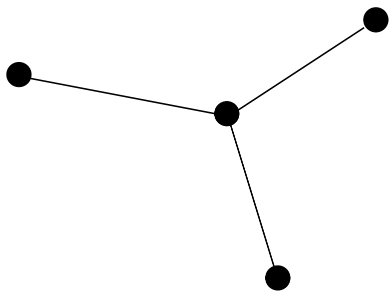

Figure 12.4: A star

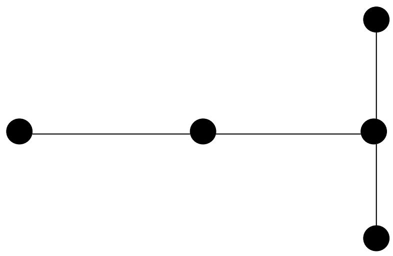

Figure 12.5: A tree on 5 vertices

does not destroy connectedness. On the other hand, consider a connected graph that does not contain any cycle of length ≥ 3. There must then be only one shortest path between any two vertices. Removal of one edge must therefore produce a disconnected graph. This shows the following:

12.7 Theorem. *A connected graph is a tree if and only if it does not contain cycles.*

The essentially different trees on 4 vertices are the path P_4 and the star (on 4 vertices), see Figure 12.4.

The trees on 5 vertices are the path P_5 (all degrees ≤ 2), the star (a vertex has degree 4) and the tree from Figure 12.5.

Problems

1. Decide if there is a simple graph on 8 vertices with degrees $6, 4, 4, 4, 3, 3, 3, 3$. If not give a reason, if yes draw a picture of the graph.

2. Same as above, but with degree sequence $5, 4, 4, 4, 3, 3, 3, 3$.

3. Prove: every tree has a leaf, meaning a vertex of degree 1.

4. Define a graph as follows: start from the set $S = \{1, 2, 3, 4, 5\}$. The vertices of our graph are the unordered pairs from S. Two vertices form an edge if the pairs have empty intersection.

   Draw this graph and identify it with one of the graphs that occurred in this chapter.

Chapter 13

Eulerian trails

The **Königsberg bridge problem** asks if it is possible to walk through the center of Königsberg such that the walk ends where it started and each bridge is crossed exactly once. The old city of Königsberg was situated on both banks of the river Pregel and on two islands, see Figure 13.1.

Euler formulated this as a graph problem, replacing the map by the graph in Figure 13.2.

The parts of the city have become vertices, the bridges are now edges. This not really a (simple) graph in the sense of Definition 12.1 as it has repeated edges. The problem takes on the following form: is there a closed trail that uses each edge precisely once? This leads to the following definition, where we generalize the problem by admitting also trails, which are not closed:

13.1 Definition. *Let $G = (V, E)$ be a graph, possibly with repeated edges. An* **Euler trail** *is a path along edges of G which uses each edge precisely once.*

Euler observed that the Königsberg bridge graph does not possess an Euler trail.

Instead of proceeding by trial and error let us observe basic facts concerning Euler trails. Clearly the graph must be connected in order to possess an Euler trail. Now assume our arbitrary connected graph G does possess an Euler trail. Fix attention on a vertex P, which is not the starting point or the end point of the trail. Whenever the trail passes through P it uses ano edge coming into P and a second edge leaving P. That means the trail uses these edges in pairs. It follows that $deg(P)$ must be even. As a trail cannot

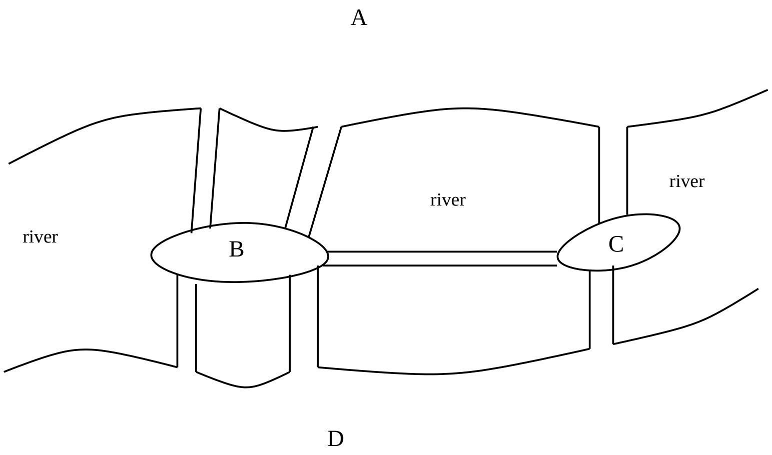

Figure 13.1: Königsberg bridge problem

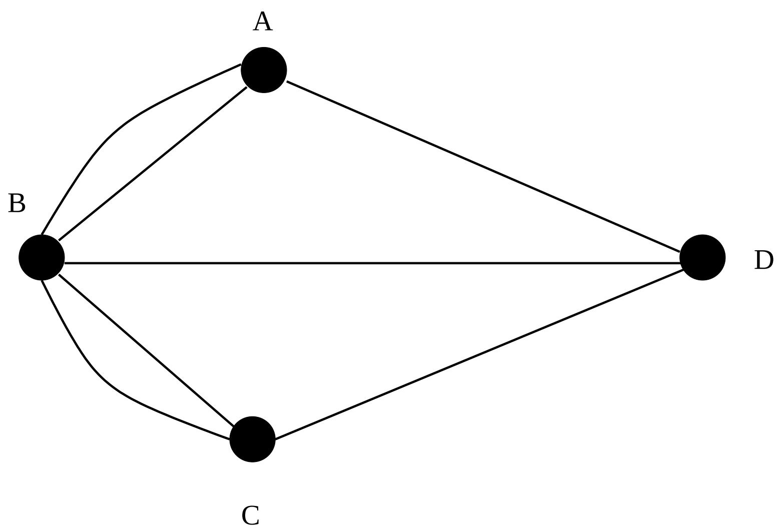

Figure 13.2: Königsberg bridge graph

have more than one starting point and one end point, it follows that all but two of the vertices must have even degree.

13.2 Lemma. *A graph with more than two vertices of odd degree cannot possess an Euler trail.*

Lemma 13.2 suffices already to answer the original Königsberg bridge problem in the negative: there is no Eulerian trail for the Königsberg bridge graph. It is clear that Theorem 12.3 is true also for graphs with repeated edges. The number of vertices of odd degree in a graph possessing an Eulerian trail is therefore 0 or 2.

13.3 Theorem. *Let G be a connected graph, possibly with repeated edges, where all vertices have even degree. Then G possesses a closed Eulerian trail.*

Proof. The proof describes an algorithm, which will produce an Eulerian trail.

Pick an arbitrary starting vertex A and walk along arbitrary edges, never using an edge twice. This trail must end somewhere. Let B be the vertex where the trail $\mathcal{T}$ ends. This means all edges passing through B have been used by our trail, and we are stuck at B. We claim $B = A$. Assume $B \neq A$. Each time (if any) the trail passed through B two edges were used. Coming into B for the last time uses only one of its edges. All in all the trail used therefore an odd number of edges through B. However, $deg(B)$ is even, so we cannot get stuck. This shows $B = A$. Observe that each vertex is on an even number of edges from $\mathcal{T}$.

Two possibilities arise. One is that our (closed) trail $\mathcal{T}$ is an Eulerian trail already. Assume this is not the case. This means some edges have not been used yet. As G is connected there must be a vertex P touched by $\mathcal{T}$ which is on some unused edge. Consider the connected graph containing vertex P, which is induced by the unused edges. All vertices have an even degree in this graph. Start a trail $\mathcal{S}$ at P. We are in the same situation as when we constructed $\mathcal{T}$. The new trail $\mathcal{S}$ will necessarily end at P.

Now we construct a trail for G, which is longer than $\mathcal{T}$: start at A, follow $\mathcal{T}$ until P is reached for the first time. Then follow $\mathcal{S}$ to its end, from where we continue with $\mathcal{T}$.

We have seen that when $\mathcal{T}$ is not an Eulerian trail it can be embedded in a longer trail. Repeat this process. It can end only when an Eulerian trail has been constructed. $\square$

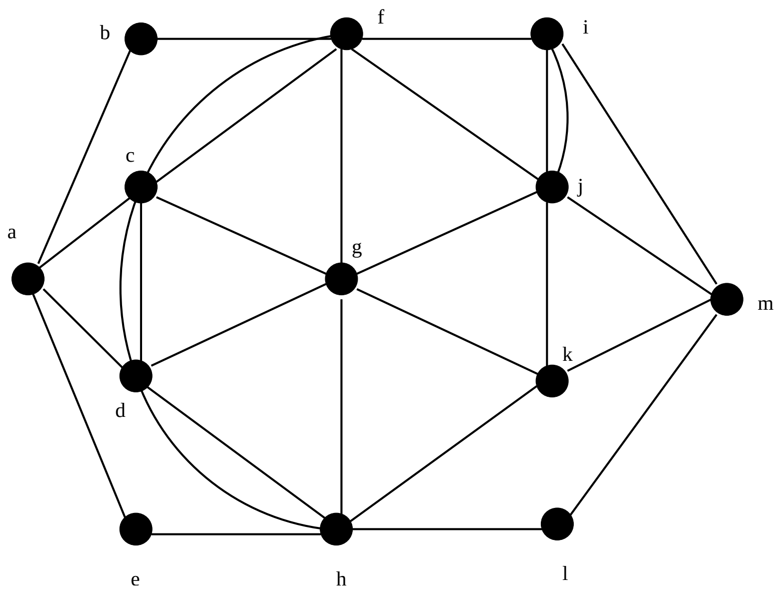

Figure 13.3: Finding an Eulerian trail

The case when precisely two vertices have odd degree is similar. An Eulerian trail must start at one these odd degree vertices and end at the other.

13.4 Theorem. *A graph G, possibly with repeated edges, has an Eulerian trail if and only if it has at most two vertices of odd degree.*

Let us try out the algorithm of Theorem 13.3 to find an Eulerian trail. Start at a, walk along edges. We write the trail as a sequence of vertices. In case of multiple edges it does not matter which of these are used first:

$$\mathcal{T} = (a, b, f, g, h, e, a, c, f, c, g, d, a).$$

At this point we cannot continue. The unused edges form the graph in Figure 13.4, where we have also removed the isolated vertices (vertices of degree 0).

We can start at vertex c.

$$\mathcal{S} = (c, d, h, l, m, i, f, j, i, j, g, k, m, j, k, h, d, c).$$

As this uses all unused edges the composition of $\mathcal{T}$ and $\mathcal{S}$ is an Eulerian trail. It is

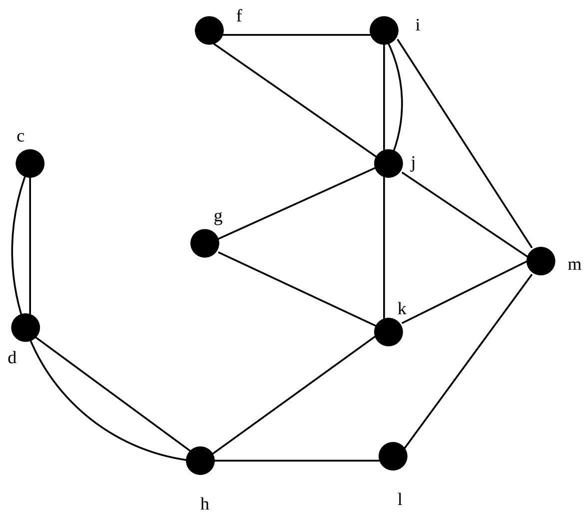

Figure 13.4: The unused edges

$$(a, b, f, g, h, e, a, c, d, h, l, m, i, f, j, i, j, g, k, m, j, k, h, d, c, f, c, g, d, a)$$

Problems

1. Let G be a connected graph, possibly with repeatd edges, which has precisely two vertices A, B of odd degree. Show that an Eulerian trail must start at A or B and end in the other.

Chapter 14

De Bruijn sequences

The problem we want to solve is sometimes called the *rotating drum problem.* Figure 14.1 shows an example of length 16.

The problem is to find a distribution of 2^n zeroes and ones on a circle (the drum) such that the n-tuples obtained by starting in some position and reading clockwise are pairwise different, equivalently each binary n-tuple is represented this way. Check that this is true for Figure 14.1 (case $n = 4$). On top we see a string of four zeroes. This gives us the tuple 0000. Moving clockwise we obtain 0001, then $0011, 0111$ and so forth. Such a circular arrangement is called a **De Bruijn sequence.** So the question is if these sequences exist for every n.

Consider Figure 14.1 again. Moving from one quadruple to the next, for example from 1110 to 1100 on the east side of the drum, we see that the final triple of 1110 equals the initial triple of 1100. This suggests we could see the triples as basic objects. When leaving a triple we have to make a

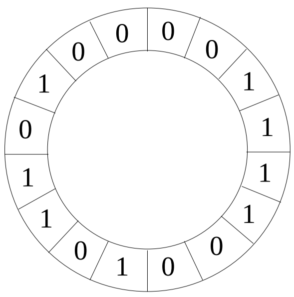

Figure 14.1: A rotating drum

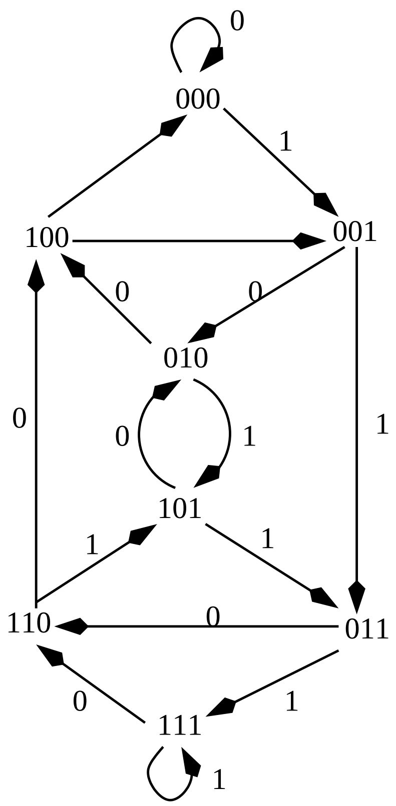

Figure 14.2: A directed graph

choice what the next symbol will be (0 or 1). For example, movement on the east side of our drum can be described as moving out of 111, generating symbol 0, to triple 110, then generating 0 on the move to 100 and so on. All possible movements are described by paths in a graph, which has the triples as vertices, with directed edges, see Figure 14.2.

It has 8 vertices. Its edges are directed. Also, there are loops (directed edges with starting point and end point identical). Comparing with the notion of a simple graph from Definition 12.1 we see that we have been led to consider more general types of graphs. Clearly this digraph is connected (given two vertices P, Q it is always possible to start a trail in P, walk along directed edges in the direction of the arrow and reach Q). The most important property of this directed graph (short **digraph**) is that precisely 2 edges lead into each vertex and precisely 2 edges lead out of each vertex. Let us define this graph for general n.

14.1 Definition. *Let B_n be the digraph whose vertices are the binary $(n-1)$, where the edges originating in $(x_1, x_2, \ldots, x_{n-1})$ end in $(x_2, \ldots, x_{n-1}, 0)$ (labelled 0) and in $(x_2, \ldots, x_{n-1}, 1)$ (labelled 1).*

Moves on a rotating drum of length 2^n can be described by paths in B_n. Using the edge labelled i out of $(x_1, x_2, \ldots, x_{n-1})$ means that we generate the n-tuple $(x_1, x_2, \ldots, x_{n-1}, i)$ on the drum. This shows how to express the defining property of a De Bruijn sequence in terms of our digraph:

14.2 Lemma. *De Bruijn sequences of length 2^n are equivalent with closed Eulerian trails on the digraph B_n.*

We have found a link to Chapter 13. In fact, although the situation is slightly different (a digraph instead of an undirected graph), the situation is the same as in Theorem 13.3. This algorithm will produce an Euler trail, and the trail will automatically be closed.

14.3 Theorem. *De Bruijn sequences of length 2^n exist for all n.*

It is not all too hard to count all de Bruijn sequences. A subclass is particularly important. These are the **linear shift register sequences.** They can be constructed via recurrence relations with binary coefficients and are closely related to finite fields, see the remark at the end of Chapter 8.

Problems

1.

Chapter 15

Latin squares

The following problem was posed in the eighteenth century by L.Euler:

Given 36 officers of 6 ranks and from 6 regiments, can they be arranged in a 6-by-6 formation so that in each row and in each column there is one officer of each rank and one officer from each regiment?

This famous **problem of the** 36 **officers** remained unsolved until 1901, when Tarry proved nonexistence by way of an exhaustive search. In order to understand this type of problem let us concentrate on the officers' ranks first, and forget about the regiments. The officers are supposed to form a 6-by-6 formation (a square) such that in each row and in each column each rank appears precisely once. This leads to the following definition:

15.1 Definition. *A* **latin square** *of order n is an (n, n)-square (also called* **matrix** *or* **array***) whose n^2 cells are filled with the elements of an n-set such that each row and each column contains each symbol exactly once.*

In the new terminology the ranks of the 36 officers are supposed to form a latin square. The same is true of the regiments.

Can we construct latin squares? Here are examples of latin squares of orders $2, 3$ and 4 :

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

Let us calculate in the integers **mod** n. Recall what that means: Loosing speaking, we calculate just as in the integers, but we identify n with 0.

15.2 Example. *Let us calculate mod* 3. *We have only* 3 *different numbers mod* 3. *These are* $0, 1, 2$. *This is so because* $3 = 0, 4 = 3 + 1 = 1$ *and so forth. As* $1 + 2 = 3 = 0$ *we have that* 1 *and* 2 *are additive inverses. This can also be written as* $2 = -1$ *and* $1 = -2$. *Also* $2^2 = 4 = 1$.

15.3 Example. *Now calculate mod* 4. *There are* 4 *different numbers mod 4. These are* $0, 1, 2, 3$. *We have for example* $2 + 3 = 5 = 1$ *and* $2 + 2 = 4 = 0$, *hence* $2 = -2$. *What the multiplication is concerned:* $2 \cdot 3 = 6 = 2, 3^2 = 9 = 1$ *and* $2 \cdot 2 = 4 = 0$.

This gives us a construction of latin squares of order n, for every n :

15.4 Definition. *Construct an* (n, n)*-array as follows: rows and columns are indexed by the numbers* $0, 1, \dots, n - 1$ *(mod* n*). The entry in row* i *and column* j *is* $i + j$ *(mod* n*).*

15.5 Theorem. *The square from Definition 15.4 is a latin square of order* n.

Proof. The entries in row i are $i, i + 1, \dots, i + n - 1$. These numbers are all different mod n. The same is true for each column. $\square$

The latin squares of Definition 15.4 are called **cyclic.** They can be described as follows: write a 0 in the top left (northwest) cell. Every time you go right or down increase the entry by 1, always observing that we calculate mod n $(n = 0)$. Here is the cyclic latin square of order 6 :

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

Let L be a latin square of order n. If I write the rows and columns of L in a permuted order the result will still be a latin square. Concentrate on the rows. Each row of L can be seen as a permutation of the underlying set (an element of S_n, see Chapter 4). That means we can see L as set of n permutations on n symbols (recall that the order in which the rows of L are written does not really matter). Which property of this family of permutations will turn it into a latin square? For each i and j there must be a unique permutation in our family, which maps $i \mapsto j$.

15.6 Theorem. *A family of n permutations of n objects forms the rows of a latin square if and only if for any pair i, j of symbols there is precisely one permutation in the family, which maps $i \mapsto j$.*

Consider the cyclic latin square of order 6. The first row is the identity permutation (leaving all symbols fixed), the second row is $(0,1,2,3,4,5)$, the third $(0,2,4)(1,3,5) = (0,1,2,3,4,5)^2$ (check that) and so forth (recall the cycle notation for permutations from Chapter 11). In fact the rows are the powers of $(0,1,2,3,4,5)$. They form the elements of a **cyclic group.** This is a special case of the following, which makes sense only if you are familiar with the concept of a **group:**

15.7 Theorem. *The group table of a group of order n is a latin square.*

Here is an example of a latin square of order 4 which is based on a group, but not a cyclic group (of 4 elements, of course):

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

The elements of this group are the identity permutation (first row), $(0,1)(2,3)$ (second row), $(0,2)(1,3)$ (third row) and $(0,3)(1,2)$ (fourth row). These four permutations form a group because the product of any two of them is one of those four permutations again (check that). In fact, the product of any those permutations with itself is the identity, and the product of any two different nonidentity permutations is the third nonidentity permutation.

So why is there no solution to the problem of the 36 officers? We have seen that such a solution could be described by two latin squares of order 6 (the regiment square and the rank square), and there is no problem with the existence of latin squares. The problem is that these two latin squares have to be in a certain relation with one another. Each of the 36 (regiment,rank)-pairs has to occur precisely once in the 6-by-6 formation. This leads to the following notion:

15.8 Definition. *Let L_1, L_2 be latin squares of order n, where we choose notation such that the set of entries is the same for both. We call L_1 and L_2* **orthogonal** *if, when superimposing the squares each of the pairs of entries occurs in precisely one cell.*

Here is a pair of orthogonal latin squares of order 3 :

$$L_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \quad L_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

In fact, superinpose them and check the pairs of entries:

$$\begin{pmatrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{pmatrix}$$

Euler's conjecture concerning the nonexistence of a solution of the problem of the 36 officers can be expressed in modern language as: there is no pair of orthogonal latin squares of order 6.

Bibliography

[1] Richard A. Brualdi: Introductory Combinatorics, Prentice Hall 1992.

[2] Peter J.Cameron: *Combinatorics - topics, techniques, algorithms,* Cambridge University Press 1994.

[3] W.Feller: An Introduction to Probability Theory and Its Applications I, Wiley 1950.

[4] The CRC Handbook of Combinatorial Designs,
C.J. Colbourn and J.H.Dinitz (eds.), CRC Press 1996.

[5] Hedayat, N.J.A.Sloane and J.Stufken:
Orthogonal Arrays: Theory and Applications, Springer 1999.

[6] G.Polya, R.E. Tarjan, D.R. Woods: Notes on Introductory Combinatorics, Birkhäuser 1983.