Introduction to Combinatorics

Chris Godsil

February 22, 2010

Contents

Chapter 1

Permutations and Subsets

1.1 Permutations

A *permutation* of a set is an ordered sequence of the elements of the set, each element appearing once in the list. For example, there are 6 permutations of $\{1, 2, 3\}$, namely

$$123,\ 132,\ 213,\ 231,\ 312,\ 321.$$

When $n = 0$, we say that there is a single permutation, which happens to be an empty list. We begin by answering a basic counting question: how many permutations are there of $\{1, \ldots, n\}$? The answer, given below, can be compactly expressed using *factorial* notation. For each nonnegative integer n, define $n!$, by $0! = 1$, and

$$n! = \prod_{i=1}^{n} i, \qquad n \geq 1.$$

We say "n factorial" for $n!$.

1.1.1 Lemma. *If $n \geq 0$, then the number of permutations of a set with size n is $n!$.*

Proof. We prove the result by induction on n. The result is true when $n = 0$ and $n = 1$.

Suppose $k \geq 2$ and $a_1 a_2 \ldots a_k$ is a permutation of $\{1, \ldots, k\}$. We can insert $k+1$ into this sequence in $k+1$ different places, and in this way we get $k+1$ permutations of $\{1, \ldots, k+1\}$ from each permutation of $\{1, \ldots, k\}$. By

induction there are $k!$ permutations of $\{1,\dots,k\}$ and so we get $(k+1)k! = (k+1)!$ different permutations of $\{1,\dots,k+1\}$.

If we delete $k+1$ from a permutation of $\{1,\dots,k\}$, we obtain a permutation of $\{1,\dots,k\}$. Hence every permutation of $\{1,\dots,k+1\}$ can be obtained by inserting $k+1$ as described. Therefore there are $(k+1)!$ permutations of $\{1,\dots,k+1\}$. □

1.2 Subsets

A *k-subset* of $\{1,\dots,n\}$ is a subset of $\{1,\dots,n\}$ with size k. We determine the number of k-subsets of $\{1,\dots,n\}$.

We recall that the *binomial coefficient* $\binom{n}{k}$ is defined by

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

From this we see that

$$\binom{n}{0} = 1, \quad \binom{n}{1} = 1$$

and

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

Let $\mathrm{subs}(n,k)$ denote the number of k-subsets of $\{1,\dots,n\}$. Then

$$\mathrm{subs}(n,0) = 1, \quad \mathrm{subs}(n,1) = n$$

and, since the complement of a k-subset is an $(n-k)$-subset,

$$\mathrm{subs}(n,k) = \mathrm{subs}(n,n-k).$$

These observations may make the following result less surprising.

1.2.1 Lemma. *The number of k-subsets of an n-set is $\binom{n}{k}$.*

Proof. Consider the set $\mathcal{P}$ of all permutations of $\{1,\dots,n\}$. The first k elements of each such permutation determine a k-subset of $\{1,\dots,n\}$. Hence we can partition $\mathcal{P}$ into classes, one for each k-subset of $\{1,\dots,n\}$. The number of classes is $\mathrm{subs}(n,k)$.

If S is a k-subset of $\{1,\dots,n\}$, then the number of permutations in the class belonging to S is $k!(n-k)!$—this is the product of the number of permutations of S with the number of permutations of the complement of S. So the size each of our $\mathrm{subs}(n,k)$ classes is $k!(n-k)!$ and therefore

$$\mathrm{subs}(n,k)\, k!(n-k)! = n!.$$

It follows that $\mathrm{subs}(n,k) = \binom{n}{k}$. □

1.3 Separated Subsets

A subset of $\{1,\dots,n\}$ is *separated* if no two of its elements are consecutive. For example if $n=7$ and $k=3$, the separated subsets of $\{1,\dots,7\}$ are

$$\{135, 136, 137, 146, 147, 157, 246, 247, 257, 357\}.$$

1.3.1 Lemma. *The number of separated k-subsets of $\{1,\dots,n\}$ is $\binom{n-k+1}{k}$.*

Proof. We prove the result by defining a map from the set of k-subsets of $\{1,\dots,n-k+1\}$ to the set of separated k-subsets of $\{1,\dots,n\}$, and then verifying that this map is invertible.

If

$$S = \{a_1,\dots,a_k\}$$

is a k-subset of $\{1,\dots,n-k+1\}$, define $\alpha(S)$ by

$$\alpha(S) = \{a_1, a_2+1, \dots, a_k+k-1\}.$$

In other terms, add $i-1$ to the i-th element of S, for $i=1,\dots,k$. Note that $\alpha(S)$ has size k, and its largest element is at most

$$(n-k+1)+(k-1) = n,$$

so it is a k subset of $\{1,\dots,n\}$. If $\alpha(S) = \{b_1,\dots,b_k\}$, then

$$b_{i+1} - b_i = (a_{i+1}+i) - (a_i+i-1) = a_{i+1} - a_i + 1 \geq 2.$$

Therefore $\alpha(S)$ is separated.

To show that α is invertible, we construct an inverse β for it. Suppose T is a separated k-subset of $\{1,\dots,n\}$ and

$$T = \{b_1,\dots,b_k\}.$$

Define $\beta(T)$ to be the set

$$\{b_1, b_2 - 1, \ldots, b_k - k + 1\}.$$

(Thus we get $\beta(T)$ by subtracting $i - 1$ from the i-th element of T, for $i = 1, \ldots, k$.)

There is one fine point to be considered: we must verify that $\beta(T)$ is a k-subset of $\{1, \ldots, n-k+1\}$. This means we must verify that $\beta(T)$ consists of k distinct integers from the interval 1 to $n-k+1$. Suppose $T = \{b_1, \ldots, b_k\}$ and $c_i := b_i - i + 1$. Then

$$b_{i+1} \geq b_i + 2$$

and so

$$c_{i+1} = b_{i+1} - i \geq b_i - i + 2 = b_i - (i-1) + 1 = c_i + 1;$$

it follows that elements $c_1, \ldots, c_k$ of $\beta(T)$ are distinct. Since $c_1 = b_1 \geq 1$ and $c_k = b_k - k + 1 \leq n - k + 1$, we see that $\beta(T) \subseteq \{1, \ldots, n - k + 1\}$. We conclude that β maps separated k-subsets of $\{1, \ldots, n\}$ to k-subsets of $\{1, \ldots, n - k + 1\}$.

Clearly, for any k-subset S of $\{1, \ldots, n - k + 1\}$,

$$\beta(\alpha(S)) = S$$

and for any separated k-subset T of $\{1, \ldots, n\}$,

$$\alpha(\beta(T)) = T.$$

So β is an inverse for α.

Having shown that α is invertible, we conclude that it is bijective. Therefore the set of separated k-subsets of $\{1, \ldots, n\}$ has the same size as the set of k-subsets of $\{1, \ldots, n - k + 1\}$. □

1.4 Bijections

As we saw in the previous section, one way to determine the size of set A is to show that it has the same size of some set B, where $|B|$ is known.

To show that A and B have the same size, we pair off the elements of A with those of B. This means we must define a map ψ so that the element a

of A is paired with $\psi(a)$, an element of B. Clearly our 'pairing' ψ is useless if it pairs different elements of A with the same element of B, or if there is some element of B which does not have the form $\psi(a)$ for some a in A. In other words we need ψ to be injective (one-to-one) and surjective (onto). A mapping that is injective and surjective is bijective.

If A and B are sets and ψ is a bijection from A to B, then $|A| = |B|$.

In general if we have a mapping $\psi : A \to B$ and we want to prove it is a bijection, we have two choices. We can verify that it is injective and surjective, or we can show that ψ has an inverse, and then use the theorem from Calculus that tells us that a function is bijective if and only it is invertible.

In the previous section we used the second method, chiefly because the obvious way to show that α was surjective would more or less force us to construct the inverse map anyway. (It is comparatively easy to see that α is injective.)

1.5 Sums and Products

It is simple and obvious that if A and B are sets and $A \cap B = \emptyset$, then

$$|A \cup B| = |A| + |B|.$$

More generally, if we have pairwise disjoint sets $A_1, \ldots, A_k$, then

$$|A_1 \cup \cdots A_k| = |A_1| + \cdots + |A_k|.$$

As an application, let Ω denote the set of all permutations of $\{1, \ldots, k\}$. If we define Ω_i to be the set of permutations in Ω which have k in the i-th position, then Ω is the disjoint union of $\Omega_1, \ldots, \Omega_k$, and consequently

$$|\Omega| = |\Omega_1| + \cdots + |\Omega_k|$$

It is not too difficult to show that "deleting k" is a bijection from Ω_i to the permutations of $\{1, \ldots, k-1\}$, and therefore

$$|\Omega_1| = \cdots = |\Omega_k|.$$

and so $|\Omega| = k|\Omega_k|$. It follows by induction that $|\Omega| = k!$. Note that this is really a repackaging of the the proof we offered earlier.

If $A_1, \ldots, A_k$ are sets then their *Cartesian product*

$$A_1 \times \cdots \times A_k$$

is the set of all k-tuples

$$(a_1, \ldots, a_k)$$

where $a_i \in A_i$ for each i. We write A^n to denote the Cartesian product of n copies of A. We have

$$|A_1 \times \cdots \times A_k| = \prod_{i=1}^{k} |A_i|$$

whence $|A^n| = |A|^n$. As an exercise, find a bijection from the set of permutations of $\{1, \ldots, k\}$ to the product set

$$A_1 \times \cdots \times A_k$$

where $A_i = \{1, \ldots, i\}$. Note that this leads to a proof, without using induction, that the number of permutations of a set of size n is $n!$.

Chapter 2

Catalan Paths

2.1 Lattice Paths

We consider *lattice paths*, which are paths on the integer lattice in two dimensions, with steps either up (add $(1,0)$) or to the right (add $(0,1)$). We count them using a simple bijection onto subsets.

2.1.1 Lemma. *The number of lattice paths from* $(0,0)$ *to* (m,n) *is* $\binom{m+n}{n}$.

Proof. Each lattice path from $(0,0)$ to (m,n) contains exactly $m+n$ steps, with n up and m right. We can represent the steps uniquely by a sequence $s_1 \dots s_{m+n}$, in which $s_i = u$ for n choices of i, and $s_i = r$ for the remaining m choices of i. Let α denote the set of all i for which $s_i = u$. Then α is an n-subset of $\{1, \dots, n+m\}$, and this map from paths to subsets is a bijection. The result follows, since there are $\binom{m+n}{n}$ choices of α. □

For example, there are $\binom{5}{2}$ paths from $(0,0)$ to $(3,2)$, given by

$$uurrr, ururr, urrur, urrru, ruurr,$$
$$rurur, rurru, rruur, rruru, rrruu.$$

2.2 A Quadratic Recurrence

From Lemma 2.1.1 we find that there are exactly $\binom{2n}{n}$ paths from $(0,0)$ to (n,n). We want to determine how many of these paths never go below the line $y = x$; we call such a path a Catalan path. The number of Catalan paths

of length n is called the *n-th Catalan number* and is denoted by c_n. We find that $c_1 = 1$, $c_2 = 2$ and $c_3 = 5$; we list the paths when $n = 3$.

$$uuurrr, uururr, uurrur, uruurr, ururur.$$

Any Catalan path of positive length touches the line $y = x$ at least twice. A Catalan path of length n that meets $y = x$ exactly twice can be represented by a sequence of u's and r's of the form

$$u\alpha r,$$

where α is a sequence u's and r's representing a Catalan path of length $n-1$. We will use this shortly.

2.2.1 Theorem. *If c_n is the number of Catalan paths of length n, then $c_0 = 1$ and if $n \geq 1$,*

$$c_n = \sum_{i=1}^{n} c_{i-1}c_{n-i}.$$

Proof. There is exactly one Catalan path of length 0, whence $c_0 = 1$. Assume $n > 0$. Let γ denote a Catalan path of length n and let i be the least positive integer such that γ passes through (i, i). Then γ splits into two parts, the first of which is a Catalan path γ_1 of length i that meets $y = x$ only at its end points and the second, γ_2 is a Catalan path from (i, i) to (n, n).

The number of choices for γ_1 is c_{i-1} (by our remark above) and the number of choices for γ_2 is c_{n-i}. So there are exactly $c_{i-1}c_{n-i}$ Catalan paths of length n that meet $y = x$ for the second time at (i, i). Hence

$$c_n = \sum_{i=1}^{n} c_{i-1}c_{n-i}. \qquad \square$$

Using this recurrence we can compute that the first Catalan numbers are

$$1, 1, 2, 5, 14 \ldots$$

2.3 A Generating Series

We derive more information about the Catalan numbers by working with the series

$$C(x) := \sum_{n\geq 0} c_n x^n.$$

This is the *generating series* or generating function for the Catalan numbers. (But it need not be a function of x, and it is not clear what it 'generates'.)

One key fact we need is the following. If we are given series

$$A(x) = \sum_{n\geq 0} a_n x^n, \quad B(x) = \sum_{n\geq 0} b_n x^n$$

then the coefficient of x^n in $A(x)B(x)$ is

$$\sum_{k=0}^{n} a_k b_{n-k}.$$

Note that this is not a theorem, it is actually the definition of the series $A(x)B(x)$. That is,

$$A(x)B(x) := \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n.$$

2.3.1 Theorem. *If $C(x)$ is the generating series for the Catalan numbers, then*

$$C(x) = 1 + xC(x)^2.$$

Proof. We prove $C(x)$ and $1+xC(x)^2$ are equal by showing that the coefficient of x^n is the same in both cases.

The constant term of $C(x)$ is 1, the coefficient of x^0 is the same.

Assume that $n > 0$. The coefficient of x^n in $C(x)$ is c_n, by definition. The coefficient of x^n in $1 + xC(x)^2$ is the coefficient of x^n in $xC(x)^2$, and is thus equal to the coefficient of x^{n-1} in $C(x)^2$.

Now the coefficient of x^{n-1} in $C(x)^2$ is equal to

$$\sum_{k=0}^{n-1} c_k c_{n-1-k} = \sum_{i=1}^{n} c_{i-1} c_{n-i}.$$

By Theorem 2.2.1, the last sum is c_n. □

It follows that

$$1 - C(x) + xC(x)^2 = 0;$$

thus we have $C(x)$ expressed as the solution to a quadratic equation.

2.4 A Formula

We derive an explicit expression for the n-th Catalan number. In the previous section we saw that the generating series for that Catalan numbers satisfies the equation

$$1 - C(x) + xC(x)^2 = 0.$$

This is a quadratic equation over the field of rational functions in x, and we can solve it using the usual formula:

$$C(x) = \frac{1}{2x}(1 \pm \sqrt{1-4x}). \tag{2.4.1}$$

At first sight this may not seem like progress. But from Calculus we recall the binomial theorem:

$$(1+x)^a = 1 + \sum_{k\geq 1} \frac{a(a-1)\cdots(a-k+1)}{k!}x^k.$$

We define the binomial coefficient $\binom{a}{k}$ by

$$\binom{a}{0} = 1$$

and when $k > 0$,

$$\binom{a}{k} := \frac{a(a-1)\cdots(a-k+1)}{k!}$$

Then

$$(1-4x)^{1/2} = 1 + \sum_{k\geq 1} \binom{\frac{1}{2}}{k}(-4)^k x^k$$

and now some algebra yields that

$$(-4)^k \binom{\frac{1}{2}}{k} = -\frac{2}{k}\binom{2k-2}{k-1}.$$

Hence (2.4.1) becomes

$$C(x) = \frac{1}{2x} \pm \left(\frac{1}{2x} - \frac{1}{x}\sum_{k\geq 1}\frac{1}{k}\binom{2k-2}{k-1}x^k\right),$$

where we must take the minus sign to obtain non-negative coefficients. It follows that

$$C(x) = \sum_{k\geq 1} \frac{1}{k}\binom{2k-2}{k-1}x^{k-1} = \sum_{n\geq 0} \frac{1}{n+1}\binom{2n}{n}x^n.$$

2.4.1 Theorem. *The number of Catalan paths of length n is $\frac{1}{n+1}\binom{2n}{n}$.* □

2.5 The Binomial Theorem

We define the *binomial series* $(1+x)^a$ by

$$(1+x)^a := \sum_{k\geq 0} \binom{a}{k} x^k.$$

Here x and a are independent variables, thus we are viewing the binomial coefficient $\binom{a}{k}$ as a polynomial in a of degree k. If m and n are integers, the coefficient of x^k in $(1+x)^{m+n}$ is

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

while the coefficient of x^k in the product $(1+x)^m(1+x)^n$ is

$$\sum_{i\geq 0} \binom{m}{i}\binom{n}{k-i}.$$

We can prove combinatorially, or by induction, that these two expressions are equal, and consequently the difference

$$\binom{a+b}{k} - \sum_{i\geq 0} \binom{a}{i}\binom{b}{k-i}$$

is a polynomial in the two variables (a and b) which is zero whenever a and b are non-negative integers. Therefore it must be the zero polynomial and so

$$\binom{a+b}{k} = \sum_{i\geq 0} \binom{a}{i}\binom{b}{k-i}$$

for all k. From this we can now conclude that

$$(1+x)^a(1+x)^b := (1+x)^{a+b}$$

for any variables a and b.

In analysis, we would define $(1+x)^a$ by

$$(1+x)^a = \exp(a\log(1+x)).$$

Hence any question about $(1+x)^a$ reduces to a question about exp and log. So in this setting, proving that $(1+x)^a(1+x)^b = (1+x)^{a+b}$ reduces to showing that

$$\exp(a+b) = \exp(a)\exp(b)$$

for any commuting variables a and b. Note that that $\exp(x)$ is defined by

$$\exp(x) = \sum_{n\geq 0} \frac{x^n}{n!}$$

We will discuss exp and log in more detail in Chapter 3.

Chapter 3

Generating Series

This chapter introduces power series and Laurent series. It serves to justify our computations using generating series.

3.1 Laurent Series and Power Series

A polynomial in the variable x is a linear combination of powers of x:

$$a_0 + a_1 x + \cdots + a_n x^n.$$

(Note that by definition, a linear combination has only finitely many non-zero coefficients.) In this course we view polynomials as finite sequences of coefficients. We can add and multiply polynomials in the manner we have become accustomed to. However we will rarely need to evaluate them and, if we do, it will probably be at 0.

A *Laurent series* is a series

$$\sum_{n \in \mathbb{Z}} a_n x^n$$

where all but finitely many of the coefficients with negative indices are zero. A *power series* is a Laurent series of the form

$$\sum_{n \geq 0} a_n x^n.$$

In general the coefficients may a_n may lie in any ring, but here we will assume that they lie in a field.

The *order* $\mathrm{ord}(A(x))$ of a Laurent series $A(x)$ is the greatest integer k such that $x^{-k}A(x)$ is a power series. So a power series is a Laurent series with non-negative order, and its order is positive if and only if it is divisible by x.

We add and multiply Laurent series in the obvious way: if

$$A(x) = \sum_n a_n x^n, \quad B(x) = \sum_n b_n x^n$$

are two Laurent series, then

$$A(x) + B(x) := \sum_n (a_n + b_n) x^n$$

and

$$A(x)B(x) = \sum_n \Big(\sum_k a_k b_{n-k} \Big) x^n.$$

We have that

$$\begin{aligned} \mathrm{ord}(A(x) + B(x)) &\geq \min\{\mathrm{ord}(A(x)), \mathrm{ord}(B(x))\}, \\ \mathrm{ord}(A(x)B(x)) &= \mathrm{ord}(A(x)) + \mathrm{ord}(B(x)), \end{aligned}$$

from which we see that the sum and product of Laurent series is a Laurent series.

The Laurent series $B(x)$ is the *inverse* of the Laurent series $A(x)$ if

$$A(x)B(x) = 1.$$

If $A(x)$ has an inverse, we denote it by $A(x)^{-1}$. We will show that if $F(x)$ is a power series with positive order, then

$$(1 - F(x))^{-1} = \sum_{k \geq 0} F(x)^k.$$

However there is one problem to be faced first—we have not defined infinite sums of Laurent series! Suppose I is a set and we are given a set of Laurent series

$$A_i(x), \quad i \in I.$$

We say this set of series is *summable* if for each integer n, there are only finitely many series A_i such that the coefficient of x^n in $A_i(x)$ is not zero. If this set of series is summable, then its sum

$$\sum_{i \in I} A_i(x)$$

is the Laurent series where the coefficient of x^n is the sum of the coefficients of x^n from each of the series $A_i(x)$. This is a finite sum, and so all difficulties evaporate. By way of example, if $F(x)$ has positive order r, then $F(x)^k$ has order kr, and so the coefficient of x^n in $F(x)^k$ is zero when $kr > n$. Therefore the set of series

$$F(x)^k, \quad k \geq 0$$

is summable and so $\sum_{k \geq 0} F(x)^k$ is defined.

3.1.1 Theorem. *If $F(x)$ is a power series with positive order, then*

$$\sum_{k \geq 0} F(x)^k$$

is the inverse of $1 - F(x)$.

Proof. We have

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

If $\ell \leq n$, then the coefficient of x^ℓ in the left hand side is equal to the coefficient of x^ℓ in the constant series 1. Also the coefficient of x^ℓ in the right hand side is equal to the coefficient of x^ℓ in

$$(1 - F(x)) \sum_{k \geq 0} F(x)^n.$$

This shows that the coefficient of x^ℓ in the above series is equal to the coefficient in the constant series 1, and therefore these two series are equal. □

3.1.2 Corollary. *The set of Laurent series over a field is a field.*

Proof. We must verify that every non-zero Laurent series has an inverse. Let $A(x)$ be a Laurent series with order k and let c be the constant term of $x^{-k}A(x)$. Then $c \neq 0$ and

$$c^{-1}x^{-k}A(x) = 1 - F(x),$$

where $F(x)$ is a power series of positive order. Hence $c^{-1}x^{-k}A(x)$ is invertible and therefore $A(x)$ is invertible. □

3.1.3 Corollary. *A power series is invertible if and only if its constant term is not zero.* □

3.1.4 Corollary. *The set of rational functions over $\mathbb{C}$ is isomorphic to a subfield of the Laurent series over $\mathbb{C}$.*

Proof. Suppose $f(x)/g(x)$ is a rational function, where for convenience we assume that f and g have no common factor. Then we may express $g(x)$ in the form

$$cx^k \prod_{i=1}^{m}(1 - \lambda_i x)$$

where c is a non-zero complex number and $k \geq 0$ (and the complex numbers λ_i are the reciprocals of the non-zero zeros :-) of $g(x)$). Hence

$$\frac{f(x)}{g(x)} = c^{-1}x^{-k}f(x)\prod_{i=1}^{m}(1 - \lambda_i x)^{-1}$$

which shows that $f(x)/g(x)$ is a product of Laurent series. □

Note: what we have called Laurent series and power series are sometimes called formal Laurent series and formal power series. In this usage the adjective 'formal' has no mathematical meaning, although it may be intended as a promise that no attempt will be made to evaluate the series at some non-zero value of the variable. (These intentions often become road-paving.)

3.2 Exp, Log and Diff

We define the *exponential series* $\exp(x)$ by

$$\exp(x) := \sum_{n\geq 0} \frac{x^n}{n!}.$$

It is not hard to verify that

$$\exp(x+y)t = \exp(xt)\exp(yt).$$

We also define the *logarithmic series* by

$$\log(1+x) := \sum_{n\geq 1}(-1)^{n-1}\frac{x^n}{n}.$$

Note that if $F(x)$ is a power series, then $\exp(F(x))$ and $\log(1+F(x))$ are defined if and only if $F(0)=0$. (We cannot define these series if $F(x)$ is a Laurent series of negative order.)

To show that these series function as we would expect, we need to introduce the derivative of a series. If $C(x)$ is a Laurent series given by

$$C(x) = \sum_n c_n x^n,$$

we define its *derivative* to be the series

$$\frac{d}{dx}C(x) := \sum_{n\geq 0}(n+1)c_{n+1}x^n.$$

We will often denote the derivative of $C(x)$ by $C'(x)$. As usual differentiation is a linear mapping, on the vector space of Laurent series. We also have the product rule:

$$\frac{d}{dx}(A(x)B(x)) = A'(x)B(x) + A(x)B'(x).$$

If $F(x) = \sum_n f_n x^n$ is a Laurent series and $G(x)$ is a power series with $G(0)=0$, we define their *composition* $(F\circ G)(x)$ by

$$(F\circ G)(x) := \sum_n f_n\, G(x)^n.$$

We say that G is a *compositional inverse* for F if $(F\circ G)(x) = x$. The chain rule holds:

$$\frac{d}{dx}(F\circ G)(x) = G'(x)\,(F'\circ G)(x).$$

You may confirm that

$$\frac{d}{dx}\exp(x) = \exp(x)$$

and that

$$\frac{d}{dx}\log(1+x) = \frac{1}{1+x}.$$

We now prove that

$$\exp(\log(1+x)) = 1+x.$$

Let $F(x)$ denote $\exp(\log(1+x))$. Then $F'(x) = \frac{1}{1+x}F(x)$ and so $(1+x)F'(x) = F(x)$. If the coefficient of x^n in $F(x)$ is f_n, then

$$\begin{aligned} f_n = \langle x^n, F(x)\rangle &= \langle x^n, (1+x)F'(x)\rangle \\ &= \langle x^n, F'(x)\rangle + \langle x^{n-1}, F'(x)\rangle \\ &= (n+1)f_{n+1} + nf_n. \end{aligned}$$

Therefore

$$(n+1)f_{n+1} = (1-n)f_n, \qquad n \geq 0.$$

Since $f_0 = 1$ we deduce that $f_1 = 1$ and $f_2 = 0$; hence $f_n = 0$ if $n \geq 2$. This shows that $F(x) = 1+x$, as claimed.

We define the series $(1+x)^a$ by

$$(1+x)^a := \exp(a\log(1+x)).$$

It follows that

$$(1+x)^{a+b} = (1+x)^a(1+x)^b.$$

You should prove that

$$(1+x)^a = \sum_{n\geq 0}\binom{a}{n}x^n.$$

(Earlier we used this as the definition of the LHS; the new definition is better.)

3.3 Convergence

If $G(x)$ is a Laurent series, we define

$$\|G(x)\| := 2^{-\operatorname{ord}(G(x))},$$

and call it the norm of $G(x)$. We say that a Laurent series $F(x)$ is the *limit* of the sequence of series

$$F_0(x), F_1(x), F_2(x), \ldots$$

if $\|F_i(x) - F(x)\| \to 0$ as $i \to \infty$. We say that the above sequence is a *Cauchy sequence* if, for each positive real number ϵ, there is an integer K such that

$$\|(F_i(x) - F_j(x)\| \leq \epsilon$$

whenever $i, j \geq K$.

Prove that a Cauchy sequence always converges to a limit. If we have series

$$A_1(x),\ A_2(x), \ldots$$

prove that the sequence

$$\sum_{i=1}^{n} A_i(x)$$

is convergent if and only if such $A_i(x) \to 0$ as $i \to \infty$, that is, if and only if its terms converge to zero. (The limit of this last sequence is the *sum* of the A_i.)

3.4 Products

Later we will want work with infinite products of series:

$$\prod_{r \geq 0} A_r(x).$$

If this is to have a meaning then all but finitely many of the series must have constant term equal to 1.

The most direct direct way to prove that this product is well-defined is to write

$$\prod_{r \geq 0} A_r(x) = \exp[\sum_{r \geq 0} \log(A_r(x))]$$

and then observe that everything is OK provided that the following sum exists

$$\sum_{r \geq 0} \log(A_r(x)).$$

This holds if and only $\|log(A_r(x))\| \to 0$ as $r \to \infty$. If we set

$$B_r(x) = A_r(x) - 1$$

then $\text{ord}(\log(A_r(x))) = \text{ord}(B_r(x))$ and we conclude that our infinite product exists if $\|A_r(x) - 1\| \to 0$ as $r \to \infty$.

3.5 Generating Series over a Vector Space

The Fibonacci numbers f_n are defined by the initial conditions $f_0 = f_1 = 1$ and the linear recurrence

$$f_{n+1} = f_n + f_{n-1}, \quad n \geq 1.$$

Let F_n be the element of $\mathbb{R}^2$ defined by

$$F_n = \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix}$$

and define the series $F(t)$ by

$$F(t) := \sum_{n \geq 0} t^n F_n.$$

We can view $F(t)$ as a vector with power series for coordinates, or as a power series over $\mathbb{R}^2$.

We note that

$$F_{n+1} = \begin{pmatrix} f_{n+2} \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} f_{n+1} + f_n \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n+1} \\ f_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} F_n,$$

whence

$$F_n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n F_0$$

and

$$F(t) = \left(\sum_{n \geq 0} t^n \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \right) \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

If we set

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

then

$$\begin{aligned}\sum_{n\geq 0} t^n \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n &= (I - tA)^{-1} \\ &= \begin{pmatrix} 1-t & -t \\ -t & 1 \end{pmatrix}^{-1} \\ &= \frac{1}{1-t-t^2} \begin{pmatrix} 1 & t \\ t & 1-t \end{pmatrix}.\end{aligned}$$

Since

$$\det \begin{pmatrix} 1 & t \\ t & 1-t \end{pmatrix} = 1 - t - t^2$$

we have

$$F(t) = \frac{1}{1-t-t^2} \begin{pmatrix} 1 & t \\ t & 1-t \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{1-t-t^2} \begin{pmatrix} 1+t \\ 1 \end{pmatrix}$$

and we conclude that

$$\sum_{n\geq 0} f_n t^n = \frac{1}{1-t-t^2}.$$

Chapter 4

Languages

4.1 Strings and Languages

Let Σ denote some set of symbols (usually finite). A *word* over the alphabet Σ is a finite sequence

$$a_1 a_2 \cdots a_k,$$

where $a_i \in \Sigma$. We admit the empty word of length zero, which we denote by ϵ. If we are given words over Σ

$$\alpha = a_1 \cdots a_k, \quad \beta = b_1 \cdots b_\ell$$

then $\alpha\beta$ denotes their *concatenation*, which is the word

$$a_1 \cdots a_k b_1 \cdots b_\ell.$$

We note that

$$\epsilon\alpha = \alpha\epsilon = \alpha$$

and that concatenation is associative

$$(\alpha\beta)\gamma = \alpha(\beta\gamma)$$

but not commutative in general. A *formal language* over Σ is a subset of the set of all words over Σ. We denote the set of all words over Σ by Σ^*.

Since languages are subsets of Σ^*, the complement $\overline{L}$ of a language L is a language and, if L and M are languages, so are their union and intersection. We define the product LM by

$$LM = \{\alpha\beta : \alpha \in L, \beta \in M\}.$$

Hence we can define L^n recursively by

$$L^0 = \{\epsilon\}, \quad L^{n+1} = LL^n.$$

We commonly represent the union of L and M by $L+M$, and then we define the *Kleene closure* L^* of L by

$$L^* := L^0 + L^1 + L^2 + \cdots = \sum_{k\geq 0} L^k.$$

This is consistent with the definition of Σ^* offered above—Σ^* is the Kleene closure of the alphabet Σ.

4.2 Languages and Generating Series

A *weight function* on an alphabet Σ is a function wt from Σ to the non-negative integers. We may think of a weight function as a rule assigning a 'size' to each letter, the weight $\mathrm{wt}(\alpha)$ of a word $\alpha = a_1 \cdots a_k$ is given by

$$\mathrm{wt}(\alpha) = \sum_i \mathrm{wt}(a_i).$$

The simplest example is the weight function that assigns weight 1 to each symbol; then $\mathrm{wt}(\alpha)$ is just the length of α. The *generating series* of L relative to the weight function wt is the series

$$\sum_{n\geq 0} a_n x^n,$$

where a_n is the number of words in L of weight n.

We consider an example. Let L be the language over $\Sigma = \{a, b\}$ that consists of all words α that contain n copies of a and n of b, and have the property that if

$$\alpha = \beta\gamma$$

then the number of a's in β is at least as large as the number of b's. Thus there is a bijection between the words in L with length $2n$ and the Catalan paths from $(0, 0)$ to (n, n). If we define

$$\mathrm{wt}(a) = 1, \quad \mathrm{wt}(b) = 0$$

then the weight of the word is the length of the associated Catalan path, and the generating series for the language is $C(x)$, the generating series for the Catalan paths.

To get further we prove that the following identity holds:

$$L = \{\epsilon\} + aLbL. \tag{4.2.1}$$

First, ϵ is the unique word in L with weight 0, and so we need prove only that every word in L with positive weight is in $aLbL$. Suppose $\mathrm{wt}(\alpha) > 0$. Then we can factorize α as

$$\alpha = \beta\gamma$$

where $\beta, \gamma \in L$ and $\mathrm{wt}(\beta) > 0$, among all such factorizations there is a unique one such that $\mathrm{wt}(\beta)$ is minimal. It follows that the last element of β must be b, and so

$$\beta = a\beta_1 b$$

where $\beta_1 \in L$. This shows that each word in L of positive length lies in $aLbL$. It is clear that $aLbL \subseteq L$ and so we conclude that $L = \{\epsilon\} + aLbL$, as claimed.

Note that the above argument also establishes that each word α of positive length in L can be factorized uniquely in the form

$$a\beta b\gamma,$$

where $\beta, \gamma \in L$.

Now we define a map Ψ from languages over $\{a, b\}$ to generating series. To begin we set

$$\Psi(a) = x, \quad \Psi(b) = 1$$

and if $\alpha = a_1 \cdots a_k \in \{a, b\}^*$, then

$$\Psi(\alpha) = \prod_{i=1}^{k} \Psi(a_i).$$

Hence

$$\Psi(\alpha) = x^{\mathrm{wt}(\alpha)}.$$

Finally, if $L \subseteq \{a, b\}^*$, then

$$\Psi(L) := \sum_{\alpha \in L} \Psi(\alpha).$$

Thus $\Psi(L)$ is the generating series for L relative to the given weight function.

4.2.1 Lemma. *If M_1 and M_2 are languages over Σ and $M_1 \cap M_2 = \emptyset$, then*

$$\Psi(M_1 + M_2) = \Psi(M_1) + \Psi(M_2). \qquad \square$$

4.2.2 Lemma. *Suppose L, M_1 and M_2 are languages over Σ and $L = M_1 M_2$. If each word α in L can be expressed in exactly one way as a concatenation $\beta_1\beta_2$, where $\beta_i \in M_i$, then $\Psi(L) = \Psi(M_1)\Psi(M_2)$.* $\square$

4.2.3 Corollary. *Suppose L and M are languages over Σ and that $L = M^k$. If each word in L can be expressed in exactly one way as the concatenation of k words from M, then $\Psi(L) = \Psi(M)^k$.*

Note that if $\epsilon \in M$ then M^k will not have the 'unique factorization' property we need to be able to apply this corollary.

We now apply these results to the language corresponding to the Catalan paths. From (4.2.1), we find that

$$\Psi(L) = \Psi(\epsilon) + \Psi(a)\Psi(L)\Psi(b)\Psi(L) = 1 + x\Psi(L)^2.$$

Thus we have obtained the equation satisfied by the generating function for Catalan paths without first determining a recurrence.

4.3 Compositions

We want to find the number of ways in which we can write an integer n as a sum of k positive integers. For example, if $n = 4$ and $k = 2$, we have three ways:

$$1 + 3, 2 + 2, 3 + 1.$$

We use an alphabet Σ that contains a symbol a_i for each positive integer i and define

$$\mathrm{wt}(a_i) = i.$$

If $\alpha \in \Sigma^k$, then $\mathrm{wt}(\alpha)$ is the sum of k positive integers, and we see that the number of words in Σ^k of weight n is equal to the number of ways of writing n as a sum of k positive integers. Since

$$\Psi(\Sigma) = x + x^2 + x^3 + \cdots = \frac{x}{1 - x},$$

we have

$$\Psi(\Sigma^k) = \Psi(\Sigma)^k = \Big(\frac{x}{1-x}\Big)^k.$$

In a similar fashion we can show that the generating series for the number of ways we can write n as a sum of k odd integers is

$$\left(\frac{x}{1-x^2}\right)^k.$$

What is the generating series for the number of ways we can write n as a sum of integers, each of which is 1 or 2? Take $\Sigma = \{a_1, a_2\}$ and $\mathrm{wt}(a_i) = i$. Then the generating series for Σ^k gives the number of ways we can write n as a sum of k 1's and 2's. We have $\Psi(\Sigma) = x + x^2$ and so the number of ways we can write n as the sum of k 1's and 2's is the coefficient of x^n in

$$(x + x^2)^k.$$

Consequently the number of ways we can write n as a sum of integers, each of which is 1 or 2 is equal to the coefficient of n in

$$\sum_{k\geq 0}(x + x^2)^k = \frac{1}{1 - x - x^2}.$$

We can derive this more directly if we note that $\Psi(\Sigma^*)$ is the generating series the number of ways we can write n as a sum of integers, each of which is 1 or 2, and then use the following result.

4.3.1 Theorem. *Let* wt *be a weight function on* Σ *and let* L *be a language over* Σ *such that:*

(a) If $i \neq j$, *then* $L^i \cap L^j = \emptyset$,

(b) If $\alpha \in L^k$, *then there are unique elements* $\beta_1, \ldots, \beta_k$ *in* L *such that* $\alpha = \beta_1 \ldots \beta_k$.

Then

$$\Psi(L^*) = \frac{1}{1 - \Psi(L)}.$$

Proof. We have

$$L^* = \epsilon + L + L^2 + \cdots .$$

The sets in this sum are pairwise disjoint and each element in L^k can be expressed uniquely as a product $\beta_1 \cdots \beta_k$, where $\beta_i \in L$. So

$$\Psi(L^*) = \sum_{k \geq 0} \Psi(L)^k = \frac{1}{1 - \Psi(L)}. \qquad \square$$

Note that Σ itself satisfies the conditions of this theorem. Also, the condition in (a) will fail if $\epsilon \in L$.

By way of example, we compute the generating series for compositions of n that do not use the integer 3. For this, take Σ to be

$$\{1, 2, 4, 5, \ldots\}$$

and define $\mathrm{wt}(i) = i$ for each element i of Σ. Then our set of compositions has generating series $\Psi(\Sigma^*)$. Since

$$\Psi(\Sigma) = \frac{x}{1-x} - x^3,$$

we find that

$$\Psi(\Sigma^*) = \frac{1}{1 - \frac{x}{1-x} + x^3} = \frac{1-x}{1 - 2x + x^3 - x^4}.$$

4.4 Factoring Σ^*

If L is a language, we use L^+ to denote the set of non-empty words in L. This if $\epsilon \notin L$ then $L^+ = LL^*$, and so

$$\Psi(L^+) = \frac{\Psi(L)}{1 - \Psi(L)}.$$

We start with the identity, which we call the *b-decomposition of* $(a+b)^*$.

$$(a+b)^* = a^*\{ba^*\}^*.$$

To prove this we first make the trivial observation that the right side is contained in the left. So suppose $\alpha \in (a+b)^*$. If $\alpha = a^k$ for some k then

$\alpha \in a^*$, and therefore $\alpha \in a^*\{ba^*\}^*$. Otherwise assume that b occurs exactly m times in α. Then we can write

$$\alpha = a^k \prod_{i=1}^{m} ba^{\ell_i}$$

where k and the integers ℓ_i are non-negative. Since $ba^\ell \in ba^*$, the identity follows.

We also have the so-called *block decomposition* of $(a+b)^*$:

$$(a+b)^* = a^*\{b^+a^+\}^*b^*,$$

which may be proved in a similar fashion. In both this identity and the previous one, the implied factorization is unique.

If we translate the previous identity to generating series, we get

$$\frac{1}{1-2x} = \frac{1}{1-x}\frac{1}{1-\frac{x}{1-x}\frac{x}{1-x}}\frac{1}{1-x},$$

which you are invited to verify. Similarly the b-decomposition yields

$$\frac{1}{1-2x} = \frac{1}{1-x}\frac{1}{1-x\frac{1}{1-x}}.$$

We use the b-decomposition to count words over $\{0,1\}$ that do not contain 11. We have

$$(0+1)^* = 1^*(01^*)^*.$$

If L denotes the set of words that do not contain 11, then L has the factorization

$$L = (\epsilon+1)[0(\epsilon+1)]^*$$

and so the generating series for the words in L (weighted by length) is

$$(1+x)\left[\frac{1}{1-x(1+x)}\right].$$

Using the block decomposition we can determine the generating series for the words in $(0+1)^*$ that do not contain 11 as a block (that is they do not have 11 as a maximal substring). If we denote this set by L, the block decomposition yields the factorization

$$L = \{1^* \setminus 11\}\left\{0^+\{1^* \setminus 11\}\right\}^*0^*.$$

Hence the generating series for L is

$$\left(\frac{1}{1-x} - x^2\right) \frac{1}{1 - \frac{x}{1-x}\left(\frac{1}{1-x} - x^2\right)} \frac{1}{1-x}.$$

(We should express these as rational functions, that is, write top and bottom as polynomials. But you need the practice and I do not.)

4.5 Extracting Coefficients

In the previous section we saw that the generating series for compositions that do not use 3 is

$$\frac{1-x}{1-2x+x^3-x^4}.$$

To get any value from this, we need to determine the coefficients in this series.

Denote this generating series by $C(x) = \sum_{n\geq 0} c_n x^n$. Then

$$(1-2x+x^3-x^4)\sum_{n\geq 0} c_n x^n = 1-x.$$

Let $\langle x^k, A(x)\rangle$ denote the coefficient of x^k in the Laurent series $A(x)$. If $m \geq 4$, then

$$\begin{aligned}\langle x^m, 1-x\rangle &= \langle x^m, (1-2x+x^3-x^4)C(x)\rangle \\ &= \langle x^m, C(x)\rangle - \langle x^m, 2xC(x)\rangle + \langle x^m, x^3C(x)\rangle - \langle x^m, x^4C(x)\rangle \\ &= c_m - 2c_{m-1} + c_{m-3} - c_{m-4}.\end{aligned}$$

Since the coefficient of x^m in $1-x$ is zero when $m \geq 2$, we have the following recurrence:

$$c_m = 2c_{m-1} - c_{m-3} + c_{m-4}, \qquad m \geq 4.$$

We call this a *linear recurrence* for c_m with degree 4. (In general a linear recurrence for a_n with degree k expresses a_n as a linear combination of $a_{n-k}, \ldots, a_{n-1}$.) To use this recurrence we need the first four coefficients c_0, c_1, c_2 and c_3. Note that we also have

$$\begin{aligned}\langle x^3, 1-x\rangle &= \langle x^3, C(x)\rangle - \langle x^3, 2xC(x)\rangle + \langle x^3, x^3C(x)\rangle - \langle x^3, x^4C(x)\rangle \\ &= c_3 - 2c_2 + c_0,\end{aligned}$$

$$\begin{aligned}\langle x^2, 1-x\rangle &= \langle x^2, C(x)\rangle - \langle x^2, 2xC(x)\rangle + \langle x^2, x^3C(x)\rangle - \langle x^2, x^4C(x)\rangle \\ &= c_2 - 2c_1,\end{aligned}$$

and

$$\begin{aligned}\langle x, 1-x\rangle &= \langle x, C(x)\rangle - \langle x, 2xC(x)\rangle + \langle x, x^3C(x)\rangle - \langle x, x^4C(x)\rangle \\ &= c_1 - 2c_0.\end{aligned}$$

These yield the equations:

$$\begin{aligned}c_3 &= 2c_2 - c_0, \\ c_2 &= 2c_1 \\ c_1 &= 2c_0 - 1.\end{aligned}$$

Since $c_0 = 1$, these imply that $c_1 = 1$, $c_2 = 2$ and $c_3 = 3$. These values are consistent with the following calculations:

$$1 = 1, \quad 2 = 1 + 1 = 2, \quad 3 = 1 + 1 + 1 = 1 + 2 = 2 + 1.$$

(In general it will be easier to determine the initial values without appealing to the recurrence.) Given the initial values we can compute as many coefficients as we want using the recurrence.

Note: We are using $\langle x^n, A(x)\rangle$ to denote the coefficient of x^n in $A(x)$, in Math 239 they denote this by

$$[x^m]A(x).$$

4.6 Probability

Suppose we have some 'random variable' taking non-negative integer values, where p_i denotes the probability that it takes the value i. So $p_i \geq 0$ and $\sum_i p_i = 1$. The probability generating function $P(x)$ is the series

$$\sum_{n\geq 0} p_n x^n.$$

For example, if our random variable is the result of a toss of a fair coin, then

$$P(x) = \frac{1}{2} + \frac{1}{2}x$$

(where p_0 is the probability that the result is heads). If the result of our random variable is the number of times heads occurs when we toss the coin n, then

$$P(x) = \left(\frac{1}{2} + \frac{1}{2}x\right)^n = \sum_{k=0}^{n} 2^{-n}\binom{n}{k}x^k.$$

4.6.1 Theorem. *If we have independent events with probability generating functions $P(x)$ and $Q(x)$, then the probability generating function for their sum is $P(x)Q(x)$.* □

4.6.2 Lemma. *If $P(x)$ is the probability generating function of a random variable, then $P'(1)$ is the average value of the random variable.*

Proof. We have

$$P'(x) = \sum_{n\geq 0} np_n x^n$$

and so

$$P'(1) = \sum_{n\geq 0} np_n$$

which is the expectation of the random variable. Note that the series for $P'(1)$ might not converge, in which case we say that the expectation is infinite.

Thus if $P(x) = \frac{1}{2}(1+x)$, then $P'(1) = \frac{1}{2}$, as expected. If $P(x) = (\frac{1}{2}+\frac{1}{2}x)^n$, then

$$P'(x) = \frac{1}{2}n\left(\frac{1}{2} + \frac{1}{2}x\right)^{n-1}$$

and so $P'(1) = \frac{1}{2}n$.

4.7 Waiting for Words

Let Σ denote the alphabet $\{a, b\}$ and let L denote the set of words over Σ that do not contain the substring *aba*. We want to compute the number of words in L with length n, for each n.

To do this we introduce an auxiliary language. Let M denote the set of words over Σ which have the form *aba* and contain exactly one copy of *aba*—so the final copy is the only one. Then we have the following equations:

$$\begin{aligned} \epsilon + La + Lb &= L + M, \\ Laba &= M + Mba. \end{aligned}$$

Let $L(x)$ and $M(x)$ denote the generating functions $\Psi(L)$ and $\Psi(M)$. Then

$$\begin{aligned} 1 + 2xL(x) &= L(x) + M(x), \\ x^3 L(x) &= M(x) + x^2 M(x). \end{aligned}$$

Solving these yields

$$L(x) = \frac{1}{1 - 2x + \frac{x^3}{1+x^2}} = \frac{1 + x^2}{1 - 2x + x^2 - x^3}$$

and

$$M(x) = \frac{x^3}{1 - 2x + x^2 - x^3}.$$

Now suppose we play the following 'game'. We repeatedly toss a fair coin, with sides labelled a and b, stopping once we have observed the sequence aba. What is the average length of the game?

The probability that we stop on the n-th toss is 2^{-n} times the number of strings in M with length n. If

$$M(x) = \sum_i c_i x^i,$$

then this probability is $c_n/2^n$. We see that

$$\sum_n \frac{c_n}{2^n} = M(1/2) = 1,$$

as we would hope. The expected length of the game is $\frac{1}{2}M'(1/2)$. Now

$$\begin{aligned} M'(x) &= \frac{3x^2}{1 - 2x + x^2 - x^3} - \frac{x^3(-2 + 2x - 3x^2)}{(1 - 2x + x^2 - x^3)^2} \\ &= \frac{3}{x} M(x) - \frac{(-2 + 2x - 3x^2)}{x^3} M(x)^2. \end{aligned}$$

and accordingly

$$\frac{1}{2} M'(1/2) = \frac{1}{2}(6 + 14) = 10.$$

We can derive an explicit formula for the waiting time. We require some new machinery first though. A *prefix* of α is an initial subsequence of α. Thus $abaa$ has five prefixes

$$\epsilon, a, ab, aba, abaa.$$

A *suffix* of α consists of the last i letters in a, for some i. We define the *set of quotients* $\beta{:}\alpha$ of α and β to be the set of suffixes σ of β such that $\beta = \pi\sigma$ where π is a suffix of α. So there is one element of $\beta : \alpha$ for each prefix of β that is a suffix of α. Some examples will help.

If

$$\alpha = abba, \quad \beta = baba$$

then

$$\beta{:}\alpha = \{ba\}, \quad \alpha{:}\beta = \{bba\}.$$

If

$$\alpha = abba$$

then

$$\alpha{:}\alpha = \{\epsilon, bba\}.$$

We see that $\alpha{:}\beta$ and $\beta{:}\alpha$ are not equal in general and that $\epsilon \in \alpha{:}\beta$ if and only if $\alpha = \beta$. Note that $\alpha{:}\beta$ is a finite language.

If $|\alpha| = d$ and $q(x)$ is the generating series for the quotient $\alpha{:}\alpha$ and we set

$$f(x) := \frac{x^d}{q(x)}$$

then

$$M(x) = \frac{f(x)}{1 - 2x + f(x)}.$$

From this we deduce that

$$M'(x) = \frac{f'(x)}{f(x)} M(x) - \frac{f'(x) - 2}{f(x)} M(x)^2$$

and consequently $M(1/2) = 2/f(1/2)$. If the probability generating function $P(x)$ is given by $P(x) := M(x/2)$, then $P'(1) = M(1/2)2$ and so the expected waiting time for α is

$$\frac{q(1/2)}{2^d}.$$

Note that

$$1 \leq q(1/2) \leq 1 + \cdots + 2^{d-1} = 2 - 2^{-1}$$

and thus the longest waiting time is close to twice the shortest when d is large.

4.8 Choosing Words

We consider the following game. Two players toss a fair coin consecutively, recording heads as a and tails as b. Before starting they each choose distinct words α and β of length k in $\{a, b\}^*$. The player whose word appears first wins. Our problems is, given α and β, to determine the probability that the player who chooses α wins.

4.8.1 Lemma. *Let Σ be a finite alphabet and suppose α is a non-empty word over Σ. Let L denote the set of words in Σ^* that do not contain γ, and let M denote the set of words in Σ^* of the form $\alpha\gamma$ that contain exactly one copy of γ. Then $L\gamma = M\gamma{:}\gamma$.* □

Thus we can rewrite the equations relating L and M as

$$\begin{aligned} \epsilon + L\Sigma &= L + M \\ L\alpha &= M\alpha{:}\alpha. \end{aligned}$$

4.8.2 Theorem. *Let $S = \{\alpha_1, \ldots, \alpha_k\}$ be a set of words such that no word is a substring of another. Let L denote the set of words that contain no words from S. Let M_i denote the set of words that contain exactly one copy of α_i, as a suffix, and no copy of α_j if $j \neq i$. Then*

$$\begin{aligned} \epsilon + L\Sigma &= L + M_1 + \cdots + M_k \\ L\alpha_i &= M_1\alpha_i{:}\alpha_1 + \cdots + M_k\alpha_i{:}\alpha_k, \quad i = 1, \ldots, k \end{aligned}$$ □

By way of example take $\Sigma = \{a, b\}$

$$\beta = aaa, \quad \gamma = bba.$$

Let L consist of the strings that do not contain β or γ. Let B be the set of strings that contain no copy of γ and one copy of β as a suffix. Let C be the set of strings that contain no copy of β and one copy of γ as a suffix. Then

$$\begin{aligned} aaa{:}aaa &= \{\epsilon, a, a^2\}, & bba{:}aaa &= \emptyset \\ aaa{:}bba &= \{aa\}, & bba{:}bba &= \{\epsilon\}. \end{aligned}$$

Therefore

$$\begin{aligned} Laaa &= B\{\epsilon + a + a^2\} + Caa, \\ Lbba &= C, \end{aligned}$$

which yields that

$$C(x) = x^3 L(x)$$

and so

$$B(x) = \frac{1}{1+x+x^2}(x^3 L(x) - x^2 C(x)) = \frac{x^3 - x^5}{1+x+x^2} L(x).$$

Hence

$$C(1/2) = \frac{1}{8} L(1/2), \quad B(1/2) = \frac{3}{28} L(1/2)$$

and

$$L(1/2) = \frac{56}{13}.$$

Here $C(1/2)$ is the probability that γ occurs before β and $B(1/2)$ is the probability that β occurs before γ. By way of a check we find that

$$B(1/2) + C(1/2) = 1,$$

as it should. The ratio of $C(1/2)$ to $B(1/2)$ is equal to the ratio of 3/24 to 3/28.

Again we can derive a formula. If our strings have length d, we get equations

$$x^d L(x) = q_{1,1}(x) B(x) + q_{1,2}(x) C(x)$$
$$x^d L(x) = q_{2,1}(x) B(x) + q_{2,2}(x) C(x)$$

where the $q_{i,j}$ are the generating series for the appropriate quotients. From these equations we can deduce that

$$\frac{B(x)}{C(x)} = \frac{q_{2,2}(x) - q_{1,2}(x)}{q_{1,1}(x) - q_{2,1}(x)}.$$

If we set $x = \frac{1}{2}$ here, we get the odds that the player who chose β will win (on average).

Problem: If you are the first player, which three-letter string should you choose?

4.9 Plane trees

A plane tree is a tree drawn in the plane. The plane trees on at most four edges are shown in Figure 4.1. A plane tree is *planted* if its root vertex has valency one. Let $T(x)$ denote the generating series for plane trees, weighted by the number of edges. So, if the diagram is to be trusted,

$$T(x) = 1 + x + 2x^2 + 5x^3 + \cdots .$$

A plane tree with at least one edge decomposes uniquely into a leftmost planted plane tree and a plane tree. Hence we have the recurrence

$$T(x) = 1 + xT(x)^2.$$

One thing this shows is that the number of plane trees on n edges is equal to the n-th Catalan number. A second, more important thing, is that we can apply the sum and product rules for generating functions even when the objects we are counting are not encoded as strings over an alphabet. (We could encode them as strings, but the encoding is not entirely trivial, and it is not needed.)

We state the sum and product rules in a more general form. Let S be a set and let wt be a function from S to $\mathbb{N}^k$. Let $x_1, \ldots, x_k$ be independent commuting variables and if

$$\alpha = (a_1, \ldots, a_k) \in \mathbb{N}^k,$$

then define

$$x^\alpha := \prod_{i=1}^{k} x_i^{a_i}.$$

The generating series $\Psi(S)$ is defined by

$$\Psi(S) := \sum_{\sigma \in S} x^{\mathrm{wt}(\sigma)}.$$

This is a *multivariate generating series*, that is, a generating series in the variables $x_1, \ldots, x_k$. If S and T are disjoint sets and wt is defined on T too, then

$$\Psi(S \cup T) = \Psi(S) + \Psi(T).$$

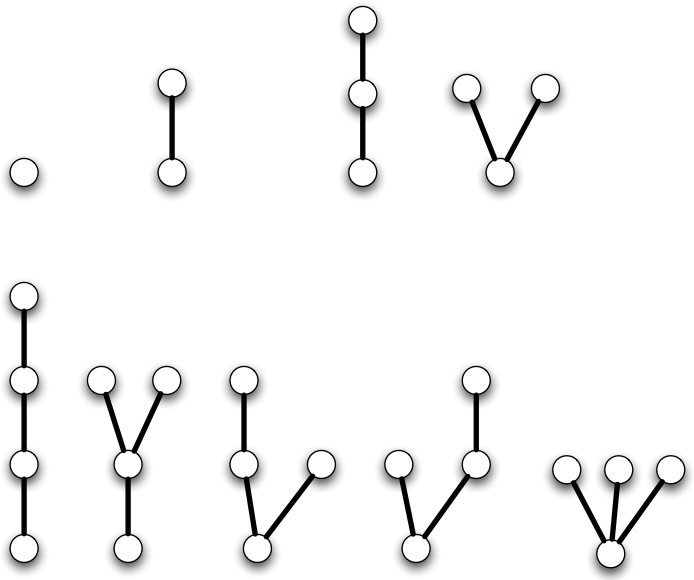

Figure 4.1: Some Plane Trees

If S and T are sets and wt is defined on the Cartesian product $S \times T$ by

$$\mathrm{wt}((\sigma, \tau)) := \mathrm{wt}(\sigma) + \mathrm{wt}(\tau),$$

then

$$\Psi(S \times T) = \Psi(S)\Psi(T).$$

Finally, if S^* denotes the set of finite sequences of elements of S, and the weight of a sequence is the sum of the weights of its terms, then

$$\Psi(S^*) = \frac{1}{1 - \Psi(S)}.$$

Chapter 5

Partitions

5.1 Partitions of an Integer

A *partition* of an integer n with k parts is an expression

$$n = a_1 + \cdots a_k$$

where $a_1, \ldots, a_k$ are positive integers and $a_i \geq a_{i+1}$ (if $i < k$). If π denotes a partition, then $|\pi|$ denotes the sum of its parts. We are generally interested in the number of partitions of n with any number of parts; this number is denoted by $p(n)$.

We have the following examples:

$$\begin{gathered} 1 = 1; \\ 2 = 2 = 1 + 1; \\ 3 = 3 = 2 + 1 = 1 + 1 + 1; \\ 4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1; \\ 5 = 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 \end{gathered}$$

whence we see that

$$p(1) = 1,\ p(2) = 2,\ p(3) = 3,\ p(4) = 5,\ p(5) = 6.$$

Let Σ be the alphabet $\{a_1, a_2, \ldots\}$, where $\mathrm{wt}(a_i) = i$. If L the language given by

$$L = \{a_1\}^*\{a_2\}^*\{a_3\}^* \cdots$$

then there is a bijection from the elements of L to partitions of integers, that maps elements of weight n to partitions of n. We deduce that the generating function for integer partitions is

$$\frac{1}{1-x}\frac{1}{1-x^2}\frac{1}{1-x^3}\cdots = \prod_{n\geq 1}\frac{1}{1-x^n}.$$

We want to relate the number of partitions with only odd parts to partitions where all parts are distinct. The tool is generating series.

The generating series for partitions with all parts odd is the generating series for the language

$$\{a_1\}^*\{a_3\}^*\{a_5\}^*\cdots;$$

thus it is

$$\prod_{n\geq 1}\frac{1}{1-x^{2n-1}}.$$

The generating function for the partitions with all parts distinct is the generating series of

$$D = (\epsilon + a_1)(\epsilon + a_2)(\epsilon + a_3)\cdots;$$

thus it is

$$\prod_{n\geq 1}(1+x^n).$$

(Note that D factorizes uniquely even though its factors contain ϵ.)

5.1.1 Lemma. *The number of partitions of n with all parts odd is equal to the number of partitions of n with all parts distinct.*

Proof. We have

$$\prod_{n\geq 1}\frac{1}{1-x^{2n-1}} = \frac{\prod_{n\geq 1}(1-x^{2n})}{\prod_{n\geq 1}(1-x^n)} = \prod_{n\geq 1}\frac{1-x^{2n}}{1-x^n} = \prod_{n\geq 1}(1+x^n). \qquad \square$$

5.2 Multivariate Series

Up till now we have been distinguishing objects by a single parameter, for example we have counted words by length. If we are considering partitions of an integer, we might consider the number of parts, or the size of the largest

part together with the sum of the parts. If we take the view that we have formed our generating series by associating a monomial x^n to each object with weight n, now we will associate the monomial

$$x^\alpha = x_1^{\alpha_1} \cdots x_k^{\alpha_k}$$

to each object with weights $(\alpha_1, \ldots, \alpha_k)$.

By way of example, we could weight partitions of n with exactly k parts by the ordered pair (n, k). The coefficient of $t^k x^n$ in

$$\prod_{i\geq 1}(1 - tx^i)^{-1}$$

is equal to the number of partitions of n with exactly k parts. This is a generating series in two variables.

A series

$$\sum_{i,j\geq 0} c_{i,j} x^i y^j$$

can be rewritten in the form

$$\sum_{j\geq 0}\Big(\sum_{i\geq 0} c_{i,j} x^i\Big) t^j$$

which is a power series in t with coefficients from the ring of power series in x. For example, the coefficient of t^k in $\prod_{i\geq 1}(1-tx^i)^{-1}$ will be the generating series for partitions with exactly k parts, weighted by the sum of their parts.

5.3 Extracting Coefficients

The following lemma will allow us to extract the coefficient of t^k in the series $\prod_{i\geq 1}(1 - tx^i)^{-1}$.

5.3.1 Lemma. *We have*

$$\prod_{r\geq 0} \frac{1 - atx^r}{1 - tx^r} = \sum_{n\geq 0} t^n \prod_{k=1}^{n} \frac{1 - ax^{k-1}}{1 - x^k}.$$

Proof. Denote left side of this identity by $F(t)$, and suppose that

$$F(t) = \sum_{n\geq 0} c_n t^n.$$

Then $c_0 = 1$ and

$$F(xt) = \frac{1-t}{1-at} F(t).$$

Hence

$$(1-at)F(xt) = (1-t)F(t)$$

and if we equate the coefficients of x^n in each side of this, we find that

$$x^n c_n - a x^{n-1} c_{n-1} = c_n - c_{n-1}.$$

It follows easily that

$$c_n = \prod_{k=1}^{n} \frac{1-ax^{k-1}}{1-x^k}.$$ □

If we substitute 0 for a and xt for t in this lemma, we obtain

$$\prod_{r\geq 1} (1-tx^r)^{-1} = \sum_{n\geq 0} t^n x^n \prod_{k=1}^{n} (1-x^k)^{-1}.$$

Hence

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

is the generating series for partitions with exactly k parts, weighted by the sum of their parts.

5.4 Ferrer's Diagrams

There are a number of interesting facts about integer partitions which can be derived from what is called the *Ferrer's diagram* of a partition. These are best introduced by an example: Figure 5.1 shows the Ferrer's diagrams for two partitions of 10. Each row corresponds to a part of the partition, where the number of dots in a row is the size of the part, and the larger parts come first. The number of Ferrer's diagrams with n dots is equal to the number of partitions of n.

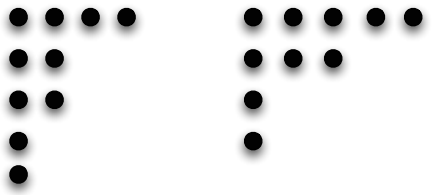

Figure 5.1: Two Ferrer's Diagrams

The second diagram in 5.1 is the transpose of the first, in which case we say that the second partition is the *conjugate* of the first. A partition may be self-conjugate. If π and π^* are conjugate partitions, the number of parts of π is equal to the largest part of π^*.

5.4.1 Lemma. *The number of partitions of n with largest part k is equal to the number of partitions of n with exactly k parts.* □

The generating series for partitions with all parts of size i, weighted by size, is

$$\frac{1}{1-x^i}$$

and therefore the generating series for partitions with largest part less than k is

$$\prod_{i=1}^{k-1} \frac{1}{1-x^i}$$

and the generating series for partitions with largest part equal to k is

$$\frac{x^k}{1-x^k} \prod_{i=1}^{k-1} \frac{1}{1-x^i} = x^k \prod_{i=1}^{k} \frac{1}{1-x^i}.$$

This is also the generating series for partitions with exactly k parts—by conjugacy or by our computation in the previous section.

5.5 Pentagonal Numbers

A *pentagonal number* is an integer of the form

$$\frac{k}{2}(3k-1),$$

where k may be positive or negative. We define a series $F(t)$

$$F(x) = \sum_{k=-\infty}^{\infty} (-1)^k t^{k(3k-1)/2};$$

this is a formal power series despite appearances. It is an amazing (and useful) fact that this series is the reciprocal of the generating series for partitions. This was first observed by Euler, and is known as *Euler's pentagonal number theorem*.

5.5.1 Theorem. *We have*

$$\prod_{j\geq 0}(1-t^j) = \sum_{k=-\infty}^{\infty} (-1)^k t^{k(3k-1)/2}.$$

Proof. We use Ferrer's diagrams. Define the *base* of a partition to be the size of the last row of its Ferrer's diagram. If

$$n = a_1 + \cdots + a_k$$

is a partition of n, the *slope* of the partition is the greatest integer j such that $a_j = a_1 + 1 - j$. The slope is clearly at most the number of parts of the partition; if equality holds we may say that the slope and base *overlap*.

If π is a partition of n with base b and slope s and the slope and base overlap, then

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

If $b = s$ or $b = s + 1$ this implies that n is pentagonal. In other words, n is pentagonal is and only if its base and slope overlap and $b \in \{s, s + 1\}$.

The left hand side of our identity is the generating series for the number of partitions of n into an even number of distinct parts, less the number of partitions of n into an odd number of distinct parts.

If $s < b$, move the slope down to form a new base. Otherwise move the base up to form a new slope. There is only a problem if $b \in \{s, s + 1\}$ and the base and slope overlap, but in this case n is pentagonal. □

Chapter 6

q-Theory

6.1 q-Counting

Let q be a variable. We define the polynomial $[n]$ by

$$[n] = \frac{q^n - 1}{q - 1};$$

if the variable q is not clear from the context, we may write $[n]_q$. We define the *q-factorial* $[n]!$ recursively for non-negative integers n by

$$[0]! := 1, \qquad [n+1]! := [n+1]\,[n]!.$$

Finally the *q-binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}$ is given by

$$\begin{bmatrix} n \\ k \end{bmatrix} := \frac{[n]!}{[k]![n-k]!}.$$

Again we may write $[n]_q!$ and $\begin{bmatrix} n \\ k \end{bmatrix}_q$ when necessary. Verify that

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}.$$

If $q = 1$, then

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}.$$

6.1.1 Lemma. *For all non-negative integers n and k,*

$$\begin{bmatrix} n \\ k \end{bmatrix}_{q^{-1}} = q^{-k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_q . \qquad \square$$

We have not one, but two, analogs of the basic binomial recurrence.

6.1.2 Lemma. *For all non-negative integers n and k,*

$$\begin{bmatrix} n \\ k \end{bmatrix} = q^k \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}. \qquad \square$$

It follows from this that $\begin{bmatrix} n \\ k \end{bmatrix}$ is a polynomial in q with non-negative integer coefficients. We will see eventually that it is a generating series for some numbers we have already met.

6.2 q-Commuting Variables

Let $\mathbb{F}$ denote the field $\mathbb{R}(q)$ of real Laurent series in the variable q. We are going to work with Laurent series with coefficients from $\mathbb{F}$; we view this set of series as a vector space over $\mathbb{F}$. (It is also a field in its own right, but this will not be important to us.)

6.2.1 Theorem. *If A and B are operators such that $BA = qAB$ and q commutes with A and B, then*

$$(A+B)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} A^k B^{n-k}.$$

Proof. Use induction and one of the recurrences above. $\square$

A natural question here is whether such operators exist. If

$$C(t) = \sum_n c_n t^n$$

then we define Q to be the linear operator that sends $C(t)$ to $C(qt)$; thus the coefficient of t^n in $C(qt)$ is $q^n c_n$. We will use M_t to denote the operation of multiplication by t; thus M_t maps $C(t)$ to $tC(t)$. Since

$$QM_t(F(t)) = qtF(qt), \quad M_tQ(F(t)) = tF(qt)$$

it follows that Q and M_t are q-commuting variables:

$$QM_t = q\, M_t Q.$$

Suppose that in Theorem 6.2.1 we take

$$A := M_t Q, \quad B = Q.$$

Then $BA = qAB$ and

$$A^k B^{n-k} 1 = A^k 1 = q^{\binom{k}{2}} t^k$$

and

$$(A+B)^n 1 = (1+t)(1+qt)\cdots(1+q^{n-1}t).$$

This yields the following result, often referred to as the q-binomial identity.

6.2.2 Corollary. *We have*

$$\prod_{i=0}^{n-1}(1+q^i t) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^{\binom{k}{2}} t^k. \qquad \square$$

This result suggests that it might be appropriate to view $\prod_{i=0}^{n-1}(1+q^i t)$ as a q-analog of the power $(1+t)^n$. We define

$$(a;q)_n := \prod_{i=1}^{n}(1-aq^{i-1})$$

with the understanding that $(a;q)_0 = 1$. Thus

$$\prod_{i=0}^{n-1}(1+q^i t) = (-t;q)_n.$$

6.3 q-Differentiation

We derive a q-analog of the identity

$$\frac{1}{(1-t)^n} = \sum_{j\geq 0} \binom{n+j-1}{j} t^j.$$

to do this we use the so-called q-derivative operator.

If $f(t)$ is a polynomial in t (over $\mathbb{F}$), then we define the *q-derivative* D_q by

$$D_q(f(t)) = \frac{f(qt) - f(t)}{qt - t}.$$

If $F(t)$ is a Laurent series, we define $D_q(F(t))$ to be the series we get by applying the q-derivative term-by-term. We note that if $n \geq 1$ then

$$D_q(t^n) = [n]t^{n-1}$$

and $D_q(1) = 0$.

For practice we note that

$$\begin{aligned} D_q((-t;q)_n) &= \frac{1}{qt-t}((-qt;q)_n - (-t;q)_n) \\ &= \frac{1}{qt-t}(1 + q^n t - 1 - t)(-qt;q)_{n-1} \\ &= [n](-qt;q)_{n-1} \end{aligned}$$

We also check that

$$\begin{aligned} D_q((t;q)_n^{-1}) &= \frac{1}{qt-t}\left(\frac{1}{(qt;q)_n} - \frac{1}{(t;q)_n}\right) \\ &= \frac{1}{qt-t}\frac{(1-t) - (1-q^n t)}{(-t;q)_{n+1}} \\ &= [n](t;q)_{n+1}^{-1}. \end{aligned}$$

6.3.1 Lemma. *We have*

$$\prod_{i=0}^{n-1} \frac{1}{1-q^i t} = \sum_{j \geq 0} \begin{bmatrix} n+j-1 \\ j \end{bmatrix} t^j.$$

Proof. The left side here is $(t;q)_n^{-1}$. It is clear that this is a power series; we write

$$(t;q)_n^{-1} = \sum_{j \geq 0} F(n,j)t^j.$$

Since $(t;q)_1^{-1} = (1-t)^{-1}$, we see that when $j \geq 0$ we have

$$F(1,j) = 1.$$

We aim to prove by induction on n that $F(n,j) = \begin{bmatrix} n+j-1 \\ j \end{bmatrix}$, and we have just seen that this is true when $n = 1$. To get further we note that

$$D_q((t;q)_n^{-1}) = [n](t;q)_{n+1}^{-1} = \sum_{j\geq 0}[n]F(n+1,j)t^j$$

while

$$D_q\Big(\sum_{j\geq 0} F(n,j)t^j\Big) = \sum_{j\geq 1} F(n,j)[j]t^{j-1}.$$

Comparing coefficients of t^j in the two power series, we see that

$$F(n+1,j) = \frac{[j+1]}{[n]}F(n,j+1).$$

By induction $F(n,k) = \begin{bmatrix} n+k-1 \\ k \end{bmatrix}$ for all k, and therefore

$$F(n+1,j) = \frac{[j+1]}{[n]}\begin{bmatrix} n+j \\ j+1 \end{bmatrix} = \begin{bmatrix} n+j \\ j \end{bmatrix}. \qquad \square$$

We should admit that this lemma can be derived from Lemma 5.3.1, thus avoiding q-derivatives. Note that we could use essentially the same proof strategy to show that the coefficient of t^j in $(1-t)^{-n}$ is $\binom{n+j-1}{j}$; this would be easier because we would be using the derivative rather than the q-derivative.

6.3.2 Theorem. *The generating series for partitions with at most k parts, the largest of which is at most ℓ, is $\begin{bmatrix} k+\ell \\ k \end{bmatrix}$.*

Proof. From the previous lemma we have that

$$\prod_{i=0}^{\ell}\frac{1}{1-q^it} = \sum_{j\geq 0}\begin{bmatrix} \ell+k \\ k \end{bmatrix}t^k$$

and basically the problem is to interpret the left-hand side. We know that

$$\prod_{i=1}^{\ell}\frac{1}{1-q^it}$$

is the generating series for the number of partitions with largest part at most ℓ, weighted by the sum of parts and the size of the largest part. Hence the

coefficient of $q^n t^k$ in this series is the number of partitions with largest part at most ℓ, such that the sum of the parts is n and size of the largest part is k. It follows that the coefficient of $q^n t^k$ in

$$\frac{1}{1-t}\prod_{i=1}^{\ell}\frac{1}{1-q^i t}$$

is the number of integer partitions of n with largest part at most ℓ and largest part at most k. So the coefficient of t^k is the generating series for integer partitions with at most k parts, the largest of which is ℓ, and weighted by the sum of their parts. □

6.4 The q-Exponential

We define the *q-exponential series* $\exp_q(t)$ by

$$\exp_q(t) := \sum_{n\geq 0}\frac{t^n}{[n]!}.$$

We see immediately that

$$D_q(\exp_q(t)) = \exp_q(t)$$

in analogy with the usual exponential.

There are many reasons to study the q-exponential, the most immediate of which is a close connection with the generating series for integer partitions. To establish this we will use the following.

6.4.1 Lemma. *If m is fixed, then*

$$\lim_{N\to\infty}\begin{bmatrix}N\\ m\end{bmatrix} = \prod_{i=1}^{m}\frac{1}{1-q^i}.$$

Proof. Recall that $\begin{bmatrix}N\\ m\end{bmatrix}$ is the generating series for partitions with largest part at most m and at most $N-m$ parts, weighted by size. Accordingly

$$\lim_{N\to\infty}\begin{bmatrix}N\\ m\end{bmatrix}$$

is just the generating series for partitions with largest part at most m, weighted by size, and therefore it is equal to the given product. □

6.4.2 Theorem. *We have*

$$\exp_q\left(\frac{t}{1-q}\right) = \prod_{n\geq 0}(1-q^n t)^{-1}.$$

Proof. We take the limit as n tends to infinity in Lemma 6.3.1. The left-hand side becomes

$$\prod_{i\geq 0}\frac{1}{1-q^i t},$$

while the right-hand side becomes

$$\sum_{j\geq 0}\frac{t^j}{(q-1)^j[j]!} = \exp_q\left(\frac{t}{1-q}\right). \qquad \square$$

One of the most important properties of the usual exponential is that

$$\exp(a+b) = \exp(a)\exp(b);$$

this is very nearly true for the q-exponential.

6.4.3 Lemma. *If $BA = qAB$, then $\exp_q(A+B) = \exp(A)\exp(B)$.* $\square$

6.5 A Reciprocal

Since

$$[n]_{q^{-1}}! = q^{-\binom{n}{2}}[n]_q!$$

it follows that

$$\exp_{q^{-1}}(t) = \sum_{n\geq 0}\frac{q^{\binom{n}{2}}}{[n]!}t^n.$$

This allows us to present the main result of this section:

6.5.1 Theorem. *We have*

$$\exp_q(t)\exp_{q^{-1}}(-t) = 1.$$

Proof. Let $A = M_t$ and $B = -M_tQ$. Then $BA = qAB$ and $\exp_q(A+B) = \exp_q(A)\exp_q(B)$. Now

$$(A+B)^n 1 = \begin{cases} 1, & n = 0; \\ 0, & n > 0, \end{cases}$$

from which we see that $\exp_q(A)\exp_q(B) = 1$. Since

$$B^n 1 = (-t)^n q^{\binom{n}{2}}$$

we have

$$\exp_q(B)1 = \sum_{n\geq 0} \frac{q^{\binom{n}{2}}}{[n]!}(-t)^n$$

and so the result follows. □

Another proof of this result follows using Corollary 6.2.2, Lemma 6.4.1 and Theorem 6.4.2.

Chapter 7

q-Practice

7.1 Squares

The *Durfee square* of a partition π is the largest square in its Ferrer's diagram that contains the top left-hand corner. Thus the Durfee square has size d if d is the largest integer such that π contains at least d parts of size at least d. Each partition π with Durfee square of side d decomposes into three pieces:

(a) The Durfee square.

(b) A partition π_1 with at most d parts.

(c) A partition π_2 with largest part at most d.

Further

$$|\pi| = d^2 + |\pi_1| + |\pi_2|.$$

Consequently the generating series for partitions with Durfee square of side d is

$$q^{d^2} \prod_{i=1}^{d} \frac{1}{(1-q^i)^2},$$

which leads to the identity

$$\sum_{d \geq 0} q^{d^2} \prod_{i=1}^{d} \frac{1}{(1-q^i)^2} = \prod_{i \geq 1} \frac{1}{1-q^i}.$$

We can refine this. Consider a partition π with at most n parts each at most n, and with Durfee square of side d. Then in the above decomposition

π_1 has at most d parts, each of size at most $n-d$ and π_2 has at most $n-d$ parts, each of size at most d. Hence the generating series for such partitions π is

$$q^{d^2}\begin{bmatrix} n \\ d \end{bmatrix}\begin{bmatrix} n \\ n-d \end{bmatrix}$$

and therefore we have

$$\sum_{d=0}^{n} q^{d^2}\begin{bmatrix} n \\ d \end{bmatrix}^2 = \begin{bmatrix} 2n \\ n \end{bmatrix},$$

since both sides equal the generating series for partitions whose Ferrer's diagrams fit in an $n \times n$ box. (This result is also an easy consequence of the q-Vandermonde identity.

7.2 Diagonals

There is a second decomposition which we need. If the Durfee square of π has side d, we can view π as the union of two partitions, each having exactly d distinct pieces, which overlap in the d diagonal elements of the Durfee square.

The generating series for partitions π with distinct parts, weighted by $|\pi|$ and the number of parts, is the coefficient of t^k in

$$A(t) := \prod_{i\geq 1}(1+q^i t).$$

The generating series for partitions π with distinct parts, weighted by $|\pi|$ less the number of parts and the number of parts, is the coefficient of t^k in

$$\prod_{i\geq 1}(1+q^{i-1}t) = A(q^{-1}t)$$

From the above decomposition we conclude that the generating series for all partitions, weighted by size, is the constant term in

$$A(t)A(q^{-1}t^{-1}).$$

In other terms

$$\prod_{i\geq 1}\frac{1}{1-q^i} = \left\langle 1, \prod_{i\geq 1}(1+tq^i)(1+t^{-1}q^{i-1})\right\rangle.$$

It is not clear what use this might be, but if it is useful then this suggests that the coefficients of t^k in $A(t)A(q^{-1}t^{-1})$ when $k \neq 0$ might also be interesting.

7.3 Jacobi's Triple Product

The following identity is known as Jacobi's triple product identity. It has a number of applications, one of which is a very efficient recurrence for the number of partitions of an integer.

7.3.1 Theorem.

$$\sum_{n=-\infty}^{\infty} q^{\binom{n+1}{2}} t^n = \prod_{n\geq 1}(1-q^n)(1+tq^n)(1+t^{-1}q^{n-1}).$$

Proof. Let $F(t)$ be defined by

$$F(t) := \prod_{n\geq 1}(1+tq^n)(1+t^{-1}q^{n-1}).$$

Then

$$\begin{aligned} F(qt) &= \prod_{n\geq 1}(1+tq^{n+1})(1+t^{-1}q^{n-2}) \\ &= \frac{1+t^{-1}q^{-1}}{1+tq}\prod_{n\geq 1}(1+tq^n)\prod_{n\geq 1}(1+t^{-1}q^{n-1}) \\ &= q^{-1}t^{-1}F(t). \end{aligned}$$

Assume

$$F(t) = \sum_{-\infty}^{\infty} f_n(q)t^n.$$

Then

$$\sum_{-\infty}^{\infty} f_n(q)q^n t^n = F(qt) = q^{-1}t^{-1}F(t) = q^{-1}t^{-1}\sum_{-\infty}^{\infty} f_n(q)t^n$$

whence $f_n(q) = q^n f_{n-1}(q)$ and $f_n(q) = q^{\binom{n+1}{2}} f_0(q)$.

Since $f_0(q)$ is the constant term in $F(t)$, it follows from the previous section that

$$F(t) = \prod_{i\geq 0}\frac{1}{1-q^i}\cdot\sum_{-\infty}^{\infty} q^{\binom{n+1}{2}}. \qquad \square$$

7.4 A Second Proof

We rederive the triple product identity. Define operators A and B on polynomials by

$$A = M_t Q,\ B = Q.$$

Then $BA = qAB$ and

$$(A+B)^{m+n} = \sum_{k=0}^{m+n} \begin{bmatrix} m+n \\ k \end{bmatrix} A^k B^{m+n-k}$$

whence

$$\begin{aligned} A^{-m}(A+B)^{m+n} &= \sum_{k=0}^{m+n} \begin{bmatrix} m+n \\ k \end{bmatrix} A^{-k-m} B^{m+n-k} \\ &= \sum_{\ell=-m}^{n} \begin{bmatrix} m+n \\ m+\ell \end{bmatrix} A^\ell B^{n-\ell} \end{aligned}$$

By applying both sides of this to 1, we get

$$\begin{aligned} (1+q^m t^{-1})(1+q^{m-1}t^{-1})\cdots(1+qt^{-1})(1+t)\cdot(1+qt)\cdots(1+q^n t) \\ = \sum_{\ell=-m}^{n} \begin{bmatrix} m+n \\ m+\ell \end{bmatrix} q^{\binom{\ell}{2}} t^\ell. \quad (7.4.1) \end{aligned}$$

Now assume $m = n$. Then

$$\lim_{n\to\infty} \begin{bmatrix} 2n \\ n+\ell \end{bmatrix} = \prod_{i\geq 1} \frac{1}{1-q^i}$$

and so

$$\lim_{n\to\infty} \sum_{\ell=-n}^{n} \begin{bmatrix} 2n \\ n+\ell \end{bmatrix} q^{\binom{\ell}{2}} t^\ell = \prod_{i\geq 1} \frac{1}{1-q^i} \cdot \sum_{-\infty}^{\infty} q^{\binom{\ell}{2}} t^\ell.$$

If we set $m = n$ in the left-hand side of (7.4.1) and let n go to infinity, the result is

$$\prod_{n\geq 1} (1+tq^n)(1+t^{-1}q^{n-1}),$$

as required.

7.5 Euler's Pentagonal Number Theorem

If $\mathcal{S}$ is a set of partitions, let $p(\mathcal{S}, n)$ denote the number of partitions of n in $\mathcal{S}$. Let $\mathcal{D}$ denote the set of all partitions with distinct parts. Let $\mathcal{E}$ denote the partitions with an even number of parts and let $\mathcal{O}$ denote the partitions with an odd number of parts.

7.5.1 Theorem.

$$p(\mathcal{D} \cap \mathcal{E}, n) - p(\mathcal{D} \cap \mathcal{O}, n) = \begin{cases} (-1)^m, & n = m(3m \pm 1)/2; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Given in lectures—move the smallest part to become the rightmost diagonal, or vice versa. □

It is useful to express result this in generating series. The generating series for partitions with distinct parts, weighted by size and number of parts, is

$$\prod_{n \geq 1} (1 + tq^n)$$

and consequently the generating series for $p(\mathcal{D} \cap \mathcal{E}, n) - p(\mathcal{D} \cap \mathcal{O}, n)$ is

$$\prod_{n \geq 1} (1 - q^n)$$

From the previous theorem we deduce that

$$\prod_{n \geq 1} (1 - q^n) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n+1)/2}. \tag{7.5.1}$$

This points us in two directions. First we will show that this is a consequence of Jacobi's triple product identity. Then we will use it to derive an efficient recurrence for the number of partitions of an integer.

In the triple product identity, substitute q^3 for q and $-q^{-1}$ for t. The right side becomes

$$\sum_{n=-\infty}^{\infty} q^{3n(n+1)/2} (-1)^n q^{-n} = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n+1)}$$

while the left side turns into

$$\prod_{n\geq 1}(1-q^{3n})(1-q^{3n-1})(1-q^{3n-2}) = \prod_{n\geq 1}(1-q^n).$$

Thus (7.5.1) follows.

Next for the recurrence. From (7.5.1) we have

$$\sum_{k=-\infty}^{\infty}(-1)^k q^{k(3k+1)} \prod_{k\geq 1}\frac{1}{1-q^k} = 1.$$

If $p(n)$ denotes the number of partitions of n and $S(n)$ denotes the set of all integers k such that $|k(3k+1)/2| \leq n$, then the coefficient of q^n in the left side of the previous equation is

$$\sum_{k\in S(n)}(-1)^k p\Big(n-\frac{1}{2}k(3k+1)\Big)$$

and so this sum is zero when $n > 0$. Suppose, for example, that $n = 10$. Then

$$S(n) = \{5, 1, 0, 2, 7\}$$

(where k runs from -2 to 2) and so

$$p(5) - p(9) + p(10) - p(8) + p(3) = 0.$$

Therefore

$$p(10) = -p(3) - p(5) + p(8) + p(9),$$

which is consistent with the following table.

7.6 Rogers and Ramanujan

We introduce two of the most important identities concerning partitions. We say a partition is *2-distinct* if any two parts differ by by at least two. First we determine the generating series for 2-distinct partitions. The key is to observe that if

$$n_1, \ldots, n_k$$

n	$p(n)$
1	1
2	2
3	3
4	5
5	7
6	11
7	15
8	22
9	30
10	42
11	56
12	77
13	101
14	135
15	176
16	231
17	297
18	385
19	490
20	627

Table 7.1: The number of integer partitions

is an increasing sequence whose terms are 2-distinct and sum to n, then the sequence

$$n_1 - 1, \ldots, n_k - (2k-1)$$

is non-decreasing and sums to $n - k^2$. This gives us a bijection between 2-distinct partitions of n with k parts and partitions of $n - k^2$ with at most k parts. The generating series for partitions with at most k parts

$$\prod_{i=1}^{k} \frac{1}{1-q^i}$$

and consequently the generating series for 2-distinct partitions with exactly k parts is

$$q^{k^2} \prod_{i=1}^{k} \frac{1}{1-q^i}.$$

We conclude that the generating series for 2-distinct partitions is

$$\sum_{k \geq 0} \frac{q^{k^2}}{(1-q)\cdots(1-q^k)}.$$

As an exercise you may prove that the generating series for 2-distinct partitions where the smallest part has size at least two is

$$\sum_{k \geq 0} \frac{q^{k^2+k}}{(1-q)\cdots(1-q^k)}.$$

7.6.1 Theorem.

$$\sum_{k \geq 0} \frac{q^{k^2}}{(1-q)\cdots(1-q^k)} = \prod_{i \geq 1} \frac{1}{(1-q^{5i-4})(1-q^{5i-1}))}$$

$$\sum_{k \geq 0} \frac{q^{k^2+k}}{(1-q)\cdots(1-q^k)} = \prod_{i \geq 1} \frac{1}{(1-q^{5i-3})(1-q^{5i-2})}.$$

7.7 Proving Rogers and Ramanujan

We prove the Rogers-Ramanujan identities. First we define five families of polynomials.

$$s_n(q) = \sum_{j=0}^{n} q^{j^2} \begin{bmatrix} n \\ j \end{bmatrix}$$

$$t_n(q) = \sum_{j=0}^{n} q^{j^2+j} \begin{bmatrix} n \\ j \end{bmatrix}$$

$$\sigma_n(q) = \sum_{j=-\infty}^{\infty} (-1)^j q^{j(5j+1)/2} \begin{bmatrix} 2n \\ n+2j \end{bmatrix}$$

$$\sigma_n^*(q) = \sum_{j=-\infty}^{\infty} (-1)^j q^{j(5j+1)/2} \begin{bmatrix} 2n+1 \\ n+2j+1 \end{bmatrix}$$

$$\tau_n(q) = \sum_{j=-\infty}^{\infty} (-1)^j q^{j(5j-3)/2} \begin{bmatrix} 2n+1 \\ n+2j \end{bmatrix}$$

The proof of our first lemma is left as an exercise.

7.7.1 Lemma. *The following recurrences hold:*

$$s_n(q) = s_{n-1}(q) + q^n t_{n-1}(q)$$
$$t_n(q) - q^n s_n(q) = (1-q^n) t_{n-1}(q).$$

7.7.2 Lemma. $\sigma_n(q) = \sigma_n^*(q)$.

Proof. Since

$$\begin{bmatrix} 2n+1 \\ n+2j+1 \end{bmatrix} = \begin{bmatrix} 2n \\ n+2j \end{bmatrix} + q^{n+2j+1} \begin{bmatrix} 2n \\ n+2j+1 \end{bmatrix}$$

we have

$$\begin{aligned} \sigma_n^*(q) - \sigma_n(q) &= \sum_{j=-\infty}^{\infty} (-1)^j q^{j(5j+1)/2} q^{n+2j+1} \begin{bmatrix} 2n \\ n+2j+1 \end{bmatrix} \\ &= q^{n+1} \sum_{j=-\infty}^{\infty} (-1)^j q^{j(5j+5)/2} \begin{bmatrix} 2n \\ n+2j+1 \end{bmatrix}. \end{aligned}$$

Now $\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}$ and so the sum in the last line is equal to

$$\begin{aligned}
&\sum_{j=0}^{\infty}(-1)^j q^{j(5j+5)/2}\begin{bmatrix} 2n \\ n+2j+1 \end{bmatrix} + \sum_{j=-\infty}^{-1}(-1)^j q^{j(5j+5)/2}\begin{bmatrix} 2n \\ n+2j+1 \end{bmatrix} \\
&\quad = \sum_{j=0}^{\infty}(-1)^j q^{j(5j+5)/2}\begin{bmatrix} 2n \\ n-2j-1 \end{bmatrix} + \sum_{j=0}^{\infty}(-1)^{-j-1} q^{(-j-1)(5-j))/2}\begin{bmatrix} 2n \\ n-2j-1 \end{bmatrix} \\
&\quad = 0.
\end{aligned}$$

The lemma follows at once. □

7.7.3 Lemma. *The following recurrences hold:*

$$\begin{aligned}
\sigma_n(q) &= \sigma_{n-1}(q) + q^n\tau_{n-1}(q) \\
\tau_n(q) - q^n\sigma_n(q) &= (1-q^n)\tau_{n-1}(q).
\end{aligned}$$

Proof. For the first, start with $\sigma_n(q) - \sigma^*_{n-1}(q)$ and use one of the recurrences for the q-binomial coefficient.

For the second, you are on your own. □

We have shown that $\sigma_n(q)$ and $\tau_n(q)$ satisfy the same recurrences as $s_n(q)$ and $t_n(q)$; since

$$s_0(q) = \sigma_0(q) = t_0(q) = \tau_0(q) = 1,$$

it follows that for all non-negative integers n,

$$s_n(q) = \sigma_n(q)$$

and

$$t_n(q) = \tau_n(q).$$

Taking the limit as n tends to infinity in each of these, we recover the Rogers-Ramanujan identities.

Chapter 8

Graphs

8.1 Graphs, Paths and Cycles

A *graph* G consists of set of vertices $V(G)$ and a set of edges $E(G)$, where each edge is an unordered pair of vertices. If $u, v \in V(G)$ and $uv \in E(G)$, we say ht at u and v are *adjacent* vertices, or that v is a *neighbour* of u. We write $u \sim v$. The set of neighbours of u is the *neighbourhood* of u in G; we may denote it by $N_G(u)$. The number of neighbours of u in G is the *degree* or *valency* of u. We denote it by $\deg(u)$ (or perhaps $\deg_G(u)$). If all vertices in G has the same degree, then we say that G is *regular*; if the common degree of a regular graph is d, we may say that G is *d-regular*.

If G is a graph, its *complement* $\overline{G}$ has the same vertex set as G but distinct vertices u and v are adjacent in $\overline{G}$ if and only if they are not adjacent in G.

The *complete graph* K_n has n vertices, and each pair of vertices is an edge. Thus it has $\binom{n}{2}$ edges. An *empty graph* is a graph no edges. The empty graph on n vertices is the complement of complete graph K_n.

We offer some more examples. The *n-cube* Q_n is defined as follows. Its vertices are the 01-vectors of length n; two vectors are adjacent if and only if they differ in exactly one coordinate. We note that Q_n has 2^n vertices and is regular with degree n. A graph is *cubic* if it is regular with degree three.

Let C be a subset of the integers modulo n such that $0 \notin C$ and, if $a \in C$ then $-a \in C$. The *circulant with connection set* C has the integers modulo n as its vertices, where $i \sim j$ if and only if $j - i \in C$. If $C = \{-1, 1\}$, then the corresponding circulant is the cycle C_n.

We say that H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H)$ is a subset

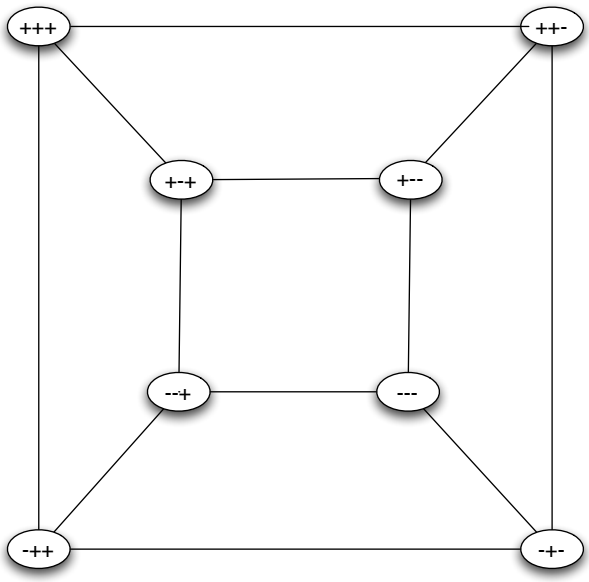

Figure 8.1: The 3-Cube

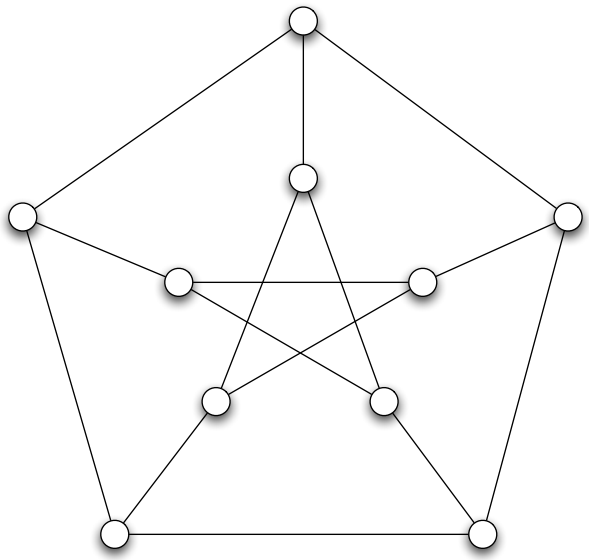

Figure 8.2: The Petersen Graph $K_{5:2}$

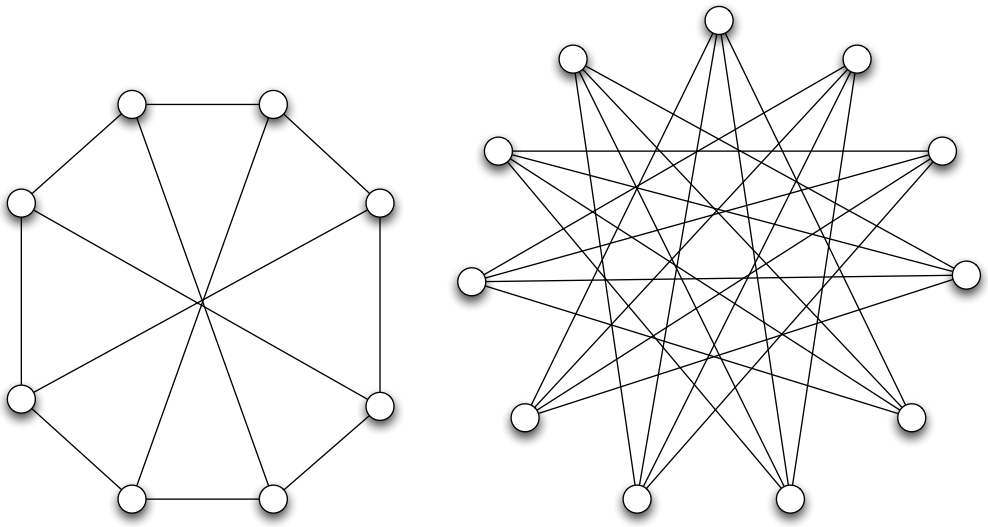

Figure 8.3: Two Circulants

of the edges in G that join two vertices in $V(H)$. There are two special cases. If $V(H) = V(G)$, then H is a *spanning subgraph* of G; if $E(H)$ consists of all edges in G that join two vertices of H, it is an *induced subgraph*. An induced subgraph is determined by its vertex set, a spanning subgraph by its edge set. (So if H is an induced spanning subgraph of G, then $H = G$. If G has n vertices and m edges, then it has 2^n induced subgraphs and 2^m spanning subgraphs.)

A *walk of length* k in a graph G is a sequence of vertices $u_0, \ldots, u_k$ such that $u_i \sim u_{i+1}$ for $i = 0, \ldots, k-1$. We say that the walk starts at u_0 and finishes at u_k. A graph G is *connected* if, for each pair of vertices in G, there is a walk in G from u to v. A subgraph P of G is a *path* on k vertices if it is the subgraph induced by a walk that does not use any vertex twice. We use P_k to denote a path with exactly k vertices. Hence a path with at least two vertices has two vertices of degree one and the rest have degree two. The vertices of valency one are the *end-vertices* of the path. A *cycle* is a connected 2-regular graph; a cycle in G is a subgraph which is a cycle. We use C_n to denote the cycle on n vertices.

The *distance* in G between vertices u and v is the length of the shortest path that contains u and v.

A *directed graph* G consists of a set of vertices, a set of arcs $\mathrm{Arc}(G)$

and two functions head and tail from $\mathrm{Arc}(G)$ to $V(G)$. If $\alpha \in \mathrm{Arc}(G)$ and $\mathrm{head}(\alpha) = \mathrm{tail}(\alpha)$, we say α is a *loop*. If α is not a loop, we may view it as directed from its tail to its head.

8.2 Components

A *component* of a graph is a subgraph which is connected, and given this is maximal under inclusion. Thus a subgraph C is a component if it is connected and any subgraph of G that contains all vertices and edges of C and is not equal to C is not connected. Equivalently, C is a component of G if it is a connected induced subgraph and there are no edges in G that join a vertex in C to a vertex not in C.

Clearly the vertex sets of the components of G partition $V(G)$. A common way to construct partitions is to use equivalence relations; we show how this can be done in this context.

Let say that vertices u and v in G are related, and write $u \approx v$, if there is a walk in G from u to v. It is easy to verify that this relation is reflexive, symmetric and transitive, that is:

(a) If $u \in V(G)$, then $u \approx u$.

(b) If $u, v \in V(G)$ and $u \approx v$, then $v \approx u$.

(c) If $u, v, w \in V(G)$ and $u \approx v$ and $v \approx w$, then $u \approx w$.

The set of vertices that $\approx$-related to u is the equivalence class of u. The equivalence classes under $\approx$ partition $V(G)$, and the subgraph induced by each equivalence class is connected. Two vertices in distinct equivalence classes cannot be adjacent.

The following result is a traditional early exercise in graph theory.

8.2.1 Lemma. *Let u and v be vertices in G. Then there is a path in G with u and v as end-vertices if and only if there is a walk in G from u to v.* □

If $e \in E(G)$, then $G \setminus e$ is the graph with vertex set $V(G)$ and edge set $E(G) \setminus e$. We say that $G \setminus e$ is obtained by *deleting* the edge e. If G is connected and e is an edge of G that lies in a cycle, then $G \setminus e$ is connected. (Why?) If G is connected then it has spanning subgraphs that are connected, G itself for example. Suppose H is a connected spanning subgraph of G with as few edges as possible. Then H cannot contain any cycles.

8.3 Trees

A connected graph with no cycles is called a *tree*. A graph with no cycles is a *forest*; each component of a forest is a tree. A spanning subgraph of G which is a tree is *spanning tree* of G.

The following theorem provides some of the most important properties of trees.

8.3.1 Theorem. *Let T be a tree.*

(a) If T has at least two vertices, it has at least two vertices of degree one.

(b) $|E(T)| = |V(T)| - 1$.

(c) Any two vertices in T are joined by a unique path.

(d) If we add an edge joining two vertices in T, we create a cycle.

(e) Each edge in T is a bridge.

Proof.

8.3.2 Lemma. *A tree with at least two vertices contains at least two vertices with degree one.*

Proof. Let P be a path in our tree that is as long as possible, and let u be one of the two vertices of P whose degree in P is one. Suppose w is a vertex in G adjacent to u, distinct from the vertex v in P adjacent to u. If $w \in V(P)$ then the sub-path of P that joins u to w together with the edge uw forms a cycle. However if $w \notin V(P)$, then the subgraph induced by $V(P) \cup w$ contains a path that is longer than P. So we are forced to conclude that u has degree one in G. It follows that both vertices of degree one in P has degree one in G.

Suppose $|V(T)| = v$. From (a), a tree has a vertex of degree one; if we delete this vertex then the graph left over is connected and has no cycles. So it is a tree and by induction it has $v - 2$ edges.

Next, since T is connected, any two vertices are joined by a path. Suppose P and Q are distinct paths joining u to v. As we move along P from u, let a be the first vertex in P whose neighbour in P is not on Q, and let b be the next vertex on P that is also on Q. Then the subpath of P going from a to

b, and the subpath of Q from b form a cycle. Therefore any two vertices in a tree are joined a unique cycle.

If we add an edge e joining vertices u and v, then e together with the unique uv-path forms a cycle.

Suppose $e \in E(T)$ and $e = \{u, v\}$. If $T \setminus e$ is connected, then there is a path in $T \setminus e$ from u to v, together with e this path gives a cycle in T. □

8.3.3 Lemma. *Let G be a connected graph and suppose H is a spanning subgraph that has no cycles but any spanning subgraph of G that properly contains H does contain a cycle. Then H is a spanning tree.*

Proof. Suppose H has the form described. It will suffice if we prove that H is connected.

Assume by way of contradiction that H is not connected and let A be the vertex set of a component of H, and let B be the complement of A in $V(G)$.

Thus (A, B) is a partition of $V(G)$ with two non-empty parts and, since G is connected there must be an edge e that joins some vertex a in A to some vertex b in B. Let K be the subgraph we get by adding e to the edge set of H. By hypothesis K contains a cycle, and we see that this cycle must contain e. By our choice of A and B, the two vertices that form e lie in different components of H. Since e lies in a cycle, it follows that the two vertices in e must be joined by a path in H, which contradicts the fact that they lie in separate components of H. We are forced to conclude that H must connected. □

8.3.4 Corollary. *A forest with v vertices and c components has exactly $v - c$ edges.* □

8.4 Directed Graphs

Roughly speaking a directed graph is a graph where each edge is assigned a direction, and is then called an arc. However we also allow loops and multiple arcs joining the same vertices, so setting up is more expensive. Formally a *directed graph* consists of a set of vertices V, a set of arcs E and two relations on $V \times E$. A vertex u and and arc a are incident under the first relation if u is the *head* of the arc a. They are incident with respect to the second if u is

the *tail* of a. If the *out-degree* of a vertex u is the number of arcs with tail u; the *in-degree* is the number of arcs with u as head.

If u is both the head and the tail of a, we call a a *loop*. We may denote an arc with tail u and head v by the ordered pair (u, v).

A walk in a directed graph may be defined as an alternating sequence of vertices

$$u_0, a_1, u_2, \ldots a_k, u_k$$

such that u_0 and u_k are vertices and u_i and u_{i+1} are respectively the tail and head of a_i, for all i. The length of a walk is the number of arcs that it uses. A *path* in a directed graph is the directed subgraph formed by the vertices and arcs of a walk that does not visit the same vertex twice. Thus a path in a directed graph has a direction. A *cycle* is the directed subgraph formed by the vertices and arcs of a walk which starts and finishes at the same vertex, but does not visit any other vertex twice. Hence cycles are also directed. A cycle in a directed graph may have length one or two.

If D is a directed graph that its *underlying graph* G has vertex set $V(D)$, where two vertices are adjacent in G is they are distinct and are joined by an arc in D. (It should possibly be called the underlying simple graph, but it is all that we will need.) A directed graph is *weakly connected* if its underlying graph is connected. A *weak component* is the directed subgraph induced by the vertices in a component of the underlying graph.

A directed graph is *strongly connected* if for each pair of vertices u and v, there is a walk in D from u to v. It is not hard to show that this is equivalent to requiring that there be a path in D from u to v for each pair of vertices u and v. A *strong component* of D is a directed induced subgraph that is strongly connected and, given this, has as many vertices as possible. If D is not strongly connected then there must be a partition (A, B) of $V(D)$ with two non-empty cells such that no arc of D goes from A to B. A directed path is weakly connected but not strongly connected, each vertex is a strong component. A directed cycle is strongly connected.

8.5 Isomorphisms and Automorphisms

Let G and H be graphs. A map ψ from $V(G)$ to $V(H)$ is an *isomorphism* if:

(a) it is a bijection;

(b) if $u, v \in V(G)$, then $\psi(u)$ and $\psi(v)$ are adjacent in H if and only if u and v are adjacent in G.

It follows that if ψ is an isomorphism, then ψ^{-1} exists and is an isomorphism from H to G. An *automorphism* is an isomorphism from a graph to itself. The set of all automorphisms of G is called the *automorphism group* of G, and is denoted by $\operatorname{Aut} G$. The automorphism group is never empty because it contains the identity permutation in all cases.

Suppose G and H are graphs and ψ is an isomorphism from G to H. Assume $u \in V(G)$. Then:

- The degree in H of $\psi(u)$ equals the degree of u in G.
- The subgraph of H induced by the set

$$\{f(v) : v \sim u\}$$

  is isomorphic to the subgraph induced by the neighbors of u in G.
- The number of copies of K_r in H that contain $\psi(u)$ equals the number of copies in G that contain u.
- If u and v are distance k in G, then $\psi(u)$ and $\psi(v)$ are at distance k in H.
- The number of vertices at distance k from u which have degree ℓ is equal to the number of vertices at distance k from $\psi(u)$ which have degree ℓ.

This list is not meant to be complete, but it should give some of the flavor. You should verify these assertions.

An *adjacency matrix* of a graph G with v vertices is a 01-matrix of order $v \times v$ with ij-entry equal to 1 if and only if vertices i and j are adjacent in G. The exact form of the matrix will depend on the ordering of the vertices of G. For example, you may verify that

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

are both adjacency matrices for C_4. If $e_1, \ldots, e_v$ is the standard basis for $\mathbb{R}^v$, then we have the following fundamental relation:

$$Ae_i = \sum_{j \sim i} e_i.$$

If α is an automorphism of G, then it is a permutation of $V(G)$ and we will denote the image of the vertex u under α by u^α (or even by $u\alpha$ when it is a subscript). Suppose $v = |V(G)|$. There is a unique linear mapping from $\mathbb{R}^v$ to itself that sends e_i to $e_{i\alpha}$. Let $P(\alpha)$ be the matrix that represents this linear mapping (relative to the standard basis); thus

$$P(\alpha)e_i = e_{i\alpha}, \qquad i \in V(G).$$

If $i \in V(G)$, let $N(i)$ denote the set of neighbors of i in G; we call it the *neighborhood* of i in G.

8.5.1 Theorem. *Let G be a graph with adjacency matrix A. Let α be a permutation of $V(G)$ and let $P = P(\alpha)$ be the permutation matrix that represents it. Then $\alpha \in \operatorname{Aut} G$ if and only if $PA = AP$.*

Proof. Suppose $i \in V(G)$. Then

$$PAe_i = P \sum_{j \sim i} e_j = \sum_{j \sim i} Pe_j = \sum_{j \sim i} e_{j\alpha}$$

while

$$APe_i = Ae_{i\alpha} = \sum_{j \sim i\alpha} e_j.$$

So $PAe_i = APe_i$ if and only if

$$\{j^\alpha : j \sim i\} = \{j : j \sim i^\alpha\}.$$

Thus equality holds if and only if each neighbor of i^α is the image under α of a neighbor of i, or equivalently, if $u \sim i$ if and only if $u^\alpha \sim i^\alpha$.

It follows that $APe_i = PAe_i$ for all vertices i if and only if $\alpha \in \operatorname{Aut} G$. □

If G and H are graphs with respective adjacency matrices A and B, then G is isomorphic to H if and only if there is a permutation matrix P such that $P^T AP = B$ (or $AP = PB$).

8.6 Coloring

A *coloring* of a graph G is a map from $V(G)$ to some set of size, such that adjacent vertices are mapped to distinct elements. If the codomain of the map has size k, we say that G is *k-colorable*. If G is k-colorable and there is no coloring of G using fewer than k colors, we say that the *chromatic number* of G is k. We denote the chromatic number of G by $\chi(G)$.

A subset S of $V(G)$ is *independent* if no two vertices in S are adjacent. If ψ is a coloring of G and i lies in the codomain of ψ, then the set

$$\{u \in V(G) : \psi(u) = i\}$$

is an independent set in G. Hence we have:

8.6.1 Lemma. *If G is a graph, the following are equivalent:*

(a) G is k-colorable.

(b) There is a partition of $V(G)$ with k cells, such that each cell is an independent set.

(c) There are k independent sets in G whose union is $V(G)$. □

We note the maximum size of an independent set in G by $\alpha(G)$. Note that for any graph G we have

$$\chi(G)\alpha(G) \geq |V(G)|$$

and thus $|V(G)|/\alpha(G)$ is a lower bound on $\chi(G)$.

Problems involving chromatic number are important in practice. For example, consider the exam scheduling problem in its simplest form. We have set of students and a set V of exams. Construct a graph on V by defining two exams to be adjacent if there is a student who must take both exams. A slot is a set of exams, no two of which have a student in common. An exam schedule then partitions the exams into slots, and we want schedule which use the minimum possible number of slots. Each slot is an independent set in the graph we constructed, and the minimum number of slots is its chromatic number.

A graph is 1-colorable if and only if it is empty. A graph is called *bipartite* if it is 2-colourable. All trees are bipartite (prove it) and so are all even cycles. Odd cycles have chromatic number three.

If a graph is bipartite we can certify this easily by providing the coloring. If it is not, we have the following:

8.6.2 Lemma. *A graph is bipartite if and only it does not contain an odd cycle.*

Proof. □

Thus we can certify that a graph is not 2-colorable by providing a subgraph which is an odd cycle. If $k > 2$ then there is no easy way known to prove that it is not k-colorable. There is one simple result that may be useful.

8.6.3 Lemma. *Let G be a graph. If the maximum valency of a vertex in G is k, then $\chi(G) \leq k + 1$.*

Proof. We proceed by induction on $|V(G)|$. Let v be a vertex in G. Since deleting a vertex cannot increase the maximum valency, by induction we see that $G \setminus v$ can be properly $(k + 1)$-coloured. Since v has degree k, the neighbours of v are coloured with at most k colours, and so there is colour that is not used on the neighbours of v. Use it on v. □

This bound is tight for odd cycles and complete graphs. A famous theorem of Brooks asserts that these are the only connected graphs for which the bound is tight.

8.6.4 Lemma. *Let G be a graph. If the maximum valency of a vertex in G is k, then $\alpha(G) \geq \frac{|V(G)|}{k+1}$.*

Proof. □

Chapter 9

Maps

9.1 Embeddings

In this context we will allow graphs to have loops and parallel edges. This means we should define a graph to consist of a set of vertices V, a set of edges E and a relation on $V \times E$ such that each edge is related to one or two vertices. An edge that is related to exactly one vertex is a loop. A *simple graph* is a graph with no loops and no parallel edges.

An *embedding* of a graph is a surface associates each vertex to a distinct point on the surface, and to each edge by a continuous curve that does not cross itself, such that curves representing distinct edges only meet at the point representing a common vertex (and otherwise the curves are disjoint). If real rigor were needed (and it will not be) we would assume that our continuous curves are piecewise linear. A graph is *planar* if it has an embedding in the real plane. An embedding of a graph divides a surface into connected pieces, which we will call *faces*. A face is a *2-cell* if there is a homeomorphism, a continuous invertible map, from the face to a disc. We are concerned almost entirely with embeddings where each face is a 2-cell. The graph and the faces form an incidence structure which we call a *map*.

For most of this chapter will focus on planar embeddings. It is important to note that a graph has a planar embedding if and only if has an embedding on the sphere. (Stereographic projection.) The advantage of working on the sphere is that there is no "outside" face. In particular each face is a 2-cell. All faces of a spherical embedding of G are 2-cells if and only G is connected.

If G is connected, each face of an embedding of G is bounded by a closed

walk in G, which we will call a *boundary walk*. A *cut edge* in G is an edge e such that $G \setminus e$ has more components than G does. (In some places these are unfortunately called bridges.) If e is not a cut-edge then it lies in exactly two boundary walks; if it is a cut edge then some boundary walk uses it twice. Thus an embedding is specified by G and the collection of boundary walks.

Suppose an embedding of G in a surface is given. We can define a *dual graph* G^* with the boundary walks as vertices, where if two boundary walks have μ edges in common then the corresponding vertices are joined by μ edges and each cut edge gives rise to a loop. The embedding of G determines an embedding of G^* in the same surface, and $(G^*)^*$ is equal to G. It may happen that G and G^* are isomorphic. Note that there is a natural bijection between $E(G)$ and $E(G^*)$ and in fact we will often identify the edge sets of G and its dual.

If G has an embedding on a surface and $e \in E(G)$, then $G \setminus e$ can be embedded on the same surface. Hence all subgraphs of G can be embedded on this surface. We also see that $(G \setminus e)^*$ has an embedding, and this leads us to ask for a clear description of $(G \setminus e)^*$.

If π is a partition of $V(G)$, then G/π is the graph defined as follows. The vertices of G/π are the cells of π and the edges of G/π are the edges of G. An edge of G/π is incident with a cell C of π if there is a vertex in C incident with it in G. If each cell of π is connected we say that G/π is obtained by We say that by *contracting* each cell to a vertex. If one cell of π is the edge e and all other cells are singletons, we write G/e rather than G/π and we say that G/e is obtained by *contracting* e. Note that the definition of contraction has nothing to do with embeddings, but if G has an embedding and a dual G^*, then

$$(G \setminus e)^* = G^*/e.$$

Thus, in this case, contraction is the dual of deletion.

9.2 Counting

The *degree* of a face is the length of the corresponding closed walk. In the exercises you are asked to prove that if d_i denotes the degree of the i-th vertex of G, then

$$\sum_i d_i = 2|E(G)|. \tag{9.2.1}$$

Hence we have:

9.2.1 Lemma. *Let G be a graph embedded in a surface. If d_i^* denotes the degree of the i-th face of G, then*

$$\sum_i d_i^* = 2|E(G)|. \qquad \square$$

Now a theorem of Euler.

9.2.2 Theorem. *If the connected graph G has an embedding in the plane with face set $F(G)$, then*

$$|V(G)| - |E(G)| + |F(G)| = 2.$$

Proof. We proceed by induction on the number of edges. Suppose G has exactly n vertices. Then it has at least $n-1$ edges, with equality if and only if it is a tree. An embedding of a tree has exactly one face, and so the theorem holds.

Suppose that $|E(G)| = m > n-1$, let T be a spanning tree of G and let e be an edge of G not in T. The embedding of G determines an embedding of $G \setminus e$, by induction the number of faces of this embedding is

$$2 - n + (m-1).$$

When we recover the original embedding of G by restoring the edge e, some face (of $G \setminus e$) is divided in two. Hence the number of faces increases by 1, and so the theorem follows by induction. $\square$

9.2.3 Corollary. *Let G be a connected graph and let δ^* denote the minimum degree of a face in a given planar embedding of G. Then*

$$(|E(G)| - |V(G)| + 2)\delta^* \leq 2|E(G)|;$$

If equality holds then all faces of the embedding have the same degree.

Proof. From Lemma 9.2.1 we have

$$|F(G)|\delta^* \leq 2|E(G)|$$

and equality holds if and only if all faces of the embedding have the same degree. From Theorem 9.2.2 we know that

$$|F(G)| = |E(G) - |V(G)| + 2.$$

From these, the corollary follows. $\square$

9.2.4 Lemma. *In a planar embedding of a connected graph that is not a tree, each boundary walk contains the edges of a cycle.* □

9.2.5 Lemma. *There are no planar embeddings of K_5 or $K_{3,3}$.*

Proof. Consider K_5, which is connected and not a tree. Suppose we have a planar embedding of K_5. Since each boundary walk contains a cycle, each face has degree at least three. Applying the corollary above yields the interesting inequality:

$$21 = (10 - 5 + 2)3 \leq 20.$$

We conclude that there is no planar embedding of K_5.

Now consider $K_{3,3}$ which is also connected and not a tree. Since $K_{3,3}$ is bipartite each cycle in it has even length, and hence the minimum degree of a face in a planar embedding would be four. Consequently

$$20 = (9 - 6 + 2)4 \leq 18.$$

Therefore $K_{3,3}$ does not have a planar embedding. □

9.3 Vertex and Face Degrees

A *triangulation* of a surface is an embedding where each face is a triangle. It is not hard to show that any embedding of a simple graph can be turned into a triangulation by adding edges in such a way that each faces is divided into triangles.

9.3.1 Theorem. *If G is a connected simple graph on at least three vertices with a planar embedding, then*

$$|E(G)| \leq 3|V(G)| - 6;$$

if equality holds then any planar embedding of G is a triangulation.

Proof. It is easy to check that bound holds (and is not tight) if G is a tree. If G is not a tree then the boundary walk of each face contains a cycle and therefore the minimum degree of a face is three. By Corollary 9.2.3 we than have

$$3(|E| - |V| + 2) \leq 2|E|,$$

which is equivalent to

$$|E| \leq 3|V| - 6.$$

From Corollary 9.2.3 we see that equality holds if and only

$$3|F(G)| = \sum_i d_i^*,$$

and this holds if and only if each face has degree three. □

9.3.2 Theorem. *Every simple planar graph has a vertex with degree at most five.*

Proof. If G has at most six vertices, the result is clearly true. Otherwise by the previous theorem we have

$$\sum_i d_i = 2|E| \leq 6|V| - 12.$$

It follows that the average degree of a vertex in G is

$$6 - \frac{12}{|V|}$$

and therefore the minimum degree of a vertex is at most five. □

9.4 Coloring Planar Graphs

It is now well known that every planar graph has a four-colouring, although no proof is known that does not require us to trust someone's programming skills. In this section we prove two weaker results.

9.4.1 Lemma. *Every planar graph can be 6-coloured.*

Proof. Let G be a planar graph with n vertices. We prove the result by induction on n. If $n \leq 6$ we are done. Otherwise there is a vertex v in G with degree at most five. By induction, $G \setminus v$ has a proper 6-coloring. But this coloring assigns at most five colors to the neighbours of v, and so this coloring extends to a coloring of G. □

9.4.2 Theorem. *Every planar graph can be 5-colored.*

Proof. The result holds for all planar graphs with at most five vertices. Suppose G has n vertices, where $n \geq 6$. If G contains a vertex v of degree at most four, then the argument of the previous lemma yields a proof that G can be 5-colored.

Suppose v is a vertex in G with degree 5. Since K_5 cannot be a subgraph of a planar graph, there must be two neighbors a and b of v that are not adjacent. Let H denote the subgraph we get by contracting the edges av and bv to a single vertex. Since H is obtained by contraction, it has a planar embedding and therefore by induction on n, it has a proper 5-coloring.

This 5-coloring provides us with a 5-coloring of $G \setminus \{a, b, v\}$, we extend this to a 5-coloring of G. Color a and b with the color assigned to vertex in H that represents $\{a, b, v\}$. (As a and b are not adjacent, this is proper.) This gives us a proper 5-coloring of $G \setminus v$ where at most four colors are used on the neighbors of v; hence there is a fifth color available to use on v. □

9.5 Abstract Maps

A *matching* is a graph such that each component is an edge, and a *k-matching* is a matching with exactly k components—so it has k edges and $2k$ vertices. Our matchings will usually arise as subgraphs of some larger (and more interesting) graph. A *perfect matching* in G is a spanning subgraph which is a matching. If G has a perfect matching, then $|V(G)|$ is even. A matching is a regular graph with valency one.

A *flag* of an embedding is an ordered triple (v, e, f) where v is a vertex, e is an edge on v and f is a face on e. The number of flags associated with an embedding of G is $4|E(G)|$. We construct the *flag graph* of the embedding, which is a cubic graph with its edges partitioned into three perfect matchings. It is constructed as follows. Its vertices are the flags of G; two flags are adjacent in the flag graph if they have exactly two elements in common. We say two flags are 0-related if the adjacent and contain different vertices; they are 1-related if they are adjacent and contain different edges; if they are adjacent and contain different vertices they are 2-related. This assigns an index from $\{0, 1, 2\}$ to each edge, and the edges with a given index form a perfect matching of the flag graph.

Each of our perfect matchings may be viewed as a permutation on the flags, we denote these permutations by π_0, π_1 and π_2.

9.5.1 Lemma. *We have* $\pi_i^2 = 1$ *and* $\pi_0\pi_2 = \pi_2\pi_0$.

Suppose now that we found three permutations of a set $\{1, \ldots, f\}$ such that

(a) Each cycle of π_i has length two.

(b) If $i \neq j$ then $\pi_i\pi_j$ has no fixed points.

(c) $\pi_0\pi_2 = \pi_2\pi_0$.

We can construct an embedding from this data as follows. View the three permutations as matchings on the vertex set $\{1, \ldots, f\}$. If $i \neq j$, then the union of π_i and π_j is a 2-regular graph and so each component is a cycle. Construct a graph with the cycles of $\pi_1\pi_2$ as its vertices and the cycles of $\pi_0\pi_2$ as its edges. Note that each cycle of $\pi_0\pi_2$ has length four.

We *orient* a face by orienting the edges in it in such a way that the result directed graph is a directed cycle. If the edge e is common to two faces, we say that two face-orientations are consistent on e if they orient e in opposite directions. A map on a surface is *orientable* if there is an orientation of its faces such that each pair of adjacent faces are consistent on their common edge(s).

For example, if we have a map on the sphere, we can orient each face clockwise and this is clearly an orientation of the map. In general a map is orientable if and only if its flag graph is bipartite.

9.6 Euler Characteristic

The *Euler characteristic* of a map with v vertices e edges and f faces is $v - e + f$.

We can define a surface as a set of triangles with vertices labelled by distinct integers such that:

(a) If ij is an edge of a triangle, it occurs in exactly two triangles.

(b) If we take the triangles that contain the vertex i, the edges that do not use i form a cycle.

(c) The graph formed by the vertices and edges of the triangles is connected.

Such a set of triangles determines a map. Two maps lie in the same surface if and only if

(a) They have the same Euler characteristic.

(b) They are both orientable, or else they are both non-orientable.

The *genus* of an orientable surface with Euler characteristic k is $\frac{1}{2}(2-k)$; the genus of a non-orientable surface with Euler characteristic k is $2-k$. The plane is the unique surface with Euler characteristic 2.

9.6.1 Lemma. *The Euler characteristic of a surface is at most two.*

Proof. Suppose we have a 2-cell embedding of a graph G in a surface with Euler characteristic k. Then the barycentric subdivision of this map is a triangulation with the same Euler characteristic as the original embedding. Thus $|V|-|E|+|F| = k$. Choose a spanning tree of G and contract each edge in it. This produces a map with one vertex (whose dual is the embedding of a tree) and with the same Euler characteristic. If there is an edge of the map in two faces, delete it. By continuing to delete such edges, if they exist, we produce a map with one vertex and one face and the same Euler characteristic. But the Euler characteristic of a map with 1 vertex, m edges and 1 face is $2 - m$. □

If a simple graph G embeds on a surface with Euler characteristic k, then

$$|V| - |E| + |F| = k.$$

If G is not a tree, then any face contains at least three edges, $3|F| \leq 2|E|$ and so

$$3k = 3|V| - 3|E| + 3|F| \leq 3|V| - 3|E| + 2|E| = 3|V| - |E|$$

whence

$$|E| \leq 3|V| - 3k.$$

Consequently the average degree of a vertex in G is at most

$$6 - \frac{6k}{|V|}.$$

9.7 Heawood

We know that a graph with a planar embedding has chromatic number at most four. It is natural to ask what is the maximum chromatic number of a graph that can be embedded on a give surface. In 1890, Heawood derived the following upper bound.

9.7.1 Theorem. *If G can be embedded on a surface with Euler characteristic k and $k \leq 0$, then*

$$\chi(G) \leq \frac{1}{2}(7 + \sqrt{49 - 24k})$$

Proof. Choose a graph G that embeds in a surface with Euler characteristic k. Suppose that $c = \chi(G)$ and that any proper subgraph of G has chromatic number less than c. (Otherwise delete some edges of G.) Then the minimum degree of G is at least $c - 1$ and so $|V(G)| \geq c$.

Using our bound on the average degree $\hat{d}$, we deduce that

$$c - 1 \leq \hat{d} \leq 6 - \frac{6k}{|V|} \leq 6 - \frac{6k}{c}.$$

This implies that

$$c^2 - 7c + 6k \leq 0$$

The roots of the quadratic on the left are

$$\frac{1}{2}(7 \pm \sqrt{49 - 24k}),$$

from which the bound follows. □

Note that if we put $k = 2$ in the bound we have $\chi(G) \leq 4$! Unfortunately this is not a proof of the 4-color theorem.

A graph G is *minimally n-chromatic* if $\chi(G) = n$ and for each proper subgraph H of G we have $\chi(H) < n$. The complete graph K_n is minimally n-chromatic, otherwise a critically n-chromatic graphs has at least $n + 2$ vertices (as you are invited to prove). In the previous proof we observed that a minimally n-chromatic graph has minimum degree at least $n - 1$.

Brook's theorem asserts that a graph with chromatic number equal to the maximum degree of a vertex if either an odd cycle or a complete graph.

9.7.2 Theorem. *Supppose $k \leq 0$ and $n = \lfloor(7 + \sqrt{49 - 24k})/2\rfloor$. If $k \notin \{-1, -2, -7\}$ and G is embedded on a surface of Euler characteristic k and G is minimally n-chromatic, then $G = K_n$.*

Proof. Suppose G has an embedding on a surface of Euler characteristic k and is minimally n-chromatic. Note that we must have $|E(G)| \leq 3(|V(G)| - k)$.

If $|V(G)| = n + 2$ then it can be shown that G is the complement of C_5 and a bunch of isolated vertices. Then

$$|E(G)| = \binom{n+2}{2} - 5 > 3(n + 2 - k).$$

So G has at least $n + 3$ vertices. Since it is minimally n-chromatic, its minimum degree is at least $n - 1$ and by Brooks theorem, it is not regular. Consequently

$$|E(G)| > |V(G)|(n - 1)/2$$

and therefore

$$|V|(n - 1) + 1 \leq 6(|V| - k).$$

Since $n \geq 1$, this inequality must hold when $|V| = n + 3$, which yields that

$$n^2 + 2n - 2 \leq 6n + 18 - 6k$$

and

$$n^2 - 4n + 6k - 20 \leq 0.$$

Hence

$$n \leq \frac{1}{2}(4 + \sqrt{96 - 24k}) = 2 + \sqrt{24 - 6k}.$$

This inequality fails if $k \leq -20$ or $-19 \leq k \leq 0$ and k is not on the list above??

Chapter 10

Eigenvalues and Eigenvectors

All graphs are simple, again.

10.1 Walks

10.1.1 Theorem. *If A is the adjacency matrix of the graph G and u, v are vertices of G, then $(A^r)_{u,v}$ is equal to the number of walks of length r in G from u to v.*

Proof. The lemma is trivially true when $i = 0$ (because $A^0 = I$) and true by definition when $r = 1$. We proceed by induction on r. Assume $r > 1$. Then

$$(A^{r+1}_{u,v}) = (AA^r)_{u,v} = \sum_i A_{u,i}(A^r)_{i,v}.$$

Since A is a 01-matrix,

$$\sum_i A_{u,i}(A^r)_{i,v} = \sum_{i\sim u}(A^r)_{i,v}.$$

Now the walks in$G$ from u to v can be partitioned according to their second vertex, which is a neighbour of u. By induction, the number of walks of length r from i to v is $(A^r)_{i,v}$ and consequently the number of walks of length $r + 1$ from u to v is $\sum_{i\sim u}(A^r)_{i,v}$. □

A *closed walk* is a walk that starts and finishes at the same vertex. The number of closed walks of length r in G that start and finish at v is $(A^r)_{v,v}$, and the number of closed walks of length r in G is therefore equal to $\mathrm{tr}(A^r)$.

Recall that the trace of matrix is equal to the sum of its eigenvalues, and if the eigenvalues of the $n \times n$ matrix A are $\theta_1, \ldots, \theta_n$, then the eigenvalues of A^r are

$$\theta_1^r, \ldots, \theta_n^r.$$

So if A is the adjacency matrix of G, the number of closed walks of length in G is equal to the sum of the r-th powers of the eigenvalues of A.

10.1.2 Lemma. *Let G be a graph on n vertices and let $\theta_1, \ldots, \theta_n$ be the eigenvalues of the adjacency matrix of G. Then*

(a) $\sum_{i=1}^n \theta_i = 0$.

(b) $\sum_{i=1}^n \theta_i^2 = 2|E(G)|$.

Proof. □

If all eigenvalues of the symmetric matrix A are zero, then $A = 0$. So it follows that if G is a non-empty graph, then it has both positive and negative eigenvalues. Since $2|E(G)|/n$ is the average degree of a vertex in G, we see that the average value of θ_i^2 is equal to the average degree of a vertex. Therefore if $\hat{d}$ is the average degree of a vertex in G, then G has an eigenvalue θ such that

$$\theta \geq \sqrt{\hat{d}}.$$

10.2 Moore Graphs

Let G be a graph with maximum degree k and diameter d. How many vertices can G have? Suppose $u \in V(G)$. The number of vertices at distance one from u is at most k. The number of vertices at distance two is at most $k(k-1)$ and if $i \geq 1$ then the number at distance i is at most $k(k-1)^{i-1}$. Therefore if $d \geq 2$,

$$|V(G)| \leq 1 + k + k(k-1) + \cdots + k(k-1)^{d-1}. \tag{10.2.1}$$

If G is connected and the bound is tight we call G a *Moore graph*. If $k > 2$ then the sum is equal to

$$1 + k\frac{(k-1)^d - 1}{k-2}.$$

We will call the bound in (10.2.1) the Moore bound.

10.2.1 Lemma. *If G is a Moore graph with diameter d then G is regular and its girth is $2d+1$.*

Proof. Let k be the maximum degree of a vertex in G. If the bound in (10.2.1) is tight, then u has valency k and if $1 \leq i < d$, then each vertex at distance i from u has one neighbor at distance $i-1$ from u and $k-1$ at distance $i+1$. So each vertex distance i from u has degree k, and therefore G is regular.

If the Moore bound is tight, it is tight no matter which vertex in G we choose as u. So if w is at positive distance from v then w has at most one neighbour which is closer to v and has a neighbor at the same distance from v if and only if it is at distance d. Hence the shortest cycle in G has length $2d+1$. □

W consider some examples. An odd cycle is a Moore graph. A complete graph is a Moore graph of diameter 1. The Petersen graph is a Moore graph with diameter two. (The easiest way for you to verify this is to show that Moore bound is tight.) A Moore graph with dimaeter two and degree k has exactly k^2+1 vertices.

10.3 Moore Graphs with Diameter Two

The cycle C_5 and Petersen graph are two Moore graphs with diameter two. We show that there are at most two more Moore graphs.

We use J to denote a matrix with all entries equal to 1. If $\overline{G}$ is the complement of G and $A = A(G)$ is its adjacency matrix, then

$$A(\overline{G}) = J - I - A.$$

10.3.1 Lemma. *Suppose G is a Moore graph with diameter two and valency k and let A be its adjacency matrix. Then $AJ = JA = kJ$ and*

$$A^2 + A - (k-1)I = J.$$

Proof. Since G is k-regular, each row and column of A sums to k and therefore $AJ = JA = kJ$.

If $u, v \in V(G)$, then $(A^2)_{u,v}$ is the number of walks length two from u to v. If $u = v$, there are k walks of length two that start and end on u—corresponding to the k edges on u. If $u \sim v$, then the number of walks of

length two from u to v is equal to the number of triangles on the edge uv, which is zero. If v is not equal or adjacent to u then it is is at distance two from v and there is a unique walk of length two from u to v. Thus

$$(A^2)_{u,v} = \begin{cases} k, & u = v; \\ 0, & u \sim v \\ 1, & \text{otherwise.} \end{cases}$$

Accordingly

$$A^2 = kI + A(\overline{G}) = kI + J - I - A,$$

which yields the result. □

We can use Lemma 10.3.1 to determine the eigenvalues of A. Since $AJ = kJ$, each column of J is an eigenvector for A with eigenvalue k. Suppose z is an eigenvector for A and z is orthogonal to $\mathbf{1}$. If $Az = \theta z$, then

$$0 = Jz = (A^2 + A - (k-1)I)z = \theta^2 z + \theta z - (k-1)z = (\theta^2 + \theta - (k-1))z$$

and therefore θ is a zero of

$$t^2 + t - (k-1).$$

Since A is symmetric there is an orthogonal basis for $\mathbb{R}^n$ that consists of eigenvectors for A, and we may one vector in this basis to be $\mathbf{1}$. Hence we have proved:

10.3.2 Lemma. *If G is a Moore graph with diameter two and valency k and θ is an eigenvalue of G, then either $\theta = k$ or it is a zero of the quadratic*

$$t^2 + t - (k-1).$$ □

10.4 Multiplicities

We determine the multiplicities of the eigenvalues of a Moore graph with diameter two. The zeros of $t^2 + t - k + 1$ are

$$\frac{1}{2}(-1 \pm \sqrt{4k-3}).$$

We denote the positive zero by θ and the negative zero by τ. It is easy to verify that neither θ nor τ is equal to k.

Suppose that $z_1, \ldots, z_n$ is an orthogonal basis of eigenvectors of A and $z_1 = \mathbf{1}$. If $i \neq 1$ then z_i is orthogonal to $\mathbf{1}$ and so from the previous section we see that the eigenvalue belonging to z_i is θ or τ. Thus k is an eigenvalue for A with multiplicity 1.

Denote the multiplicities of θ and τ by m_θ and m_τ respectively. Then

$$1 + m_\theta + m_\tau = n$$

and since $\mathrm{tr}(A) = 0$,

$$k + \theta m_\theta + \tau m_\tau = 0.$$

So we have two linear equations with m_θ and m_τ as unknowns. Solving them, we find that

$$m_\tau = \frac{(n-1)\theta + k}{\theta - \tau}, \qquad m_\theta = \frac{(n-1)\tau + k}{\tau - \theta}.$$

10.4.1 Lemma. *Suppose G is a Moore graph with diameter two and valency k. If $4k-3$ is not a perfect square, then $k = 0$ (and $G = K_1$) or $k = 2$ (and $G = C_5$).*

Proof. Note that

$$\theta - \tau = \sqrt{4k-3}.$$

From the formulas above,

$$m_\tau - m_\theta = \frac{(n-1)(\theta+\tau) + 2k}{\theta - \tau}$$

and since $\theta + \tau = -1$, we have

$$(m_\theta - m_\tau)(\theta - \tau) = n - 1 - 2k = k^2 - 2k.$$

If $4k-3$ is not a perfect square, then $\theta - \tau$ is irrational and this equation implies that $m_\theta = m_\tau$ and $k^2 - 2k = 0$. □

If $k = 3$ then $4k - 3 = 9$, which is a perfect square.

10.4.2 Lemma. *Suppose G is a Moore graph with diameter two and valency k. If $4k-3$ is a perfect square, then θ and τ are integers.*

Proof. We note that $4k-3$ is odd, and so $4k-3$ is the square of an odd integer, $2s+1$ say. So the eigenvalues θ and τ are

$$\frac{1}{2}(-1 \pm (2s+1))$$

that is, they are s and $-s-1$. □

10.5 The Main Result

10.5.1 Theorem. *If G is a Moore graph of diameter two and degree k, then $k \in \{2, 3, 7, 57\}$.*

Proof. If $4k - 3$ is not a square then $k = 2$, as we have seen. We assume $4k - 3$ is a square, and hence we have

$$4k - 3 = (2s + 1)^2$$

for some s and so $k = s^2 + s + 1$. As we saw at the end of the last section, $\theta = s$ and $\tau = -s - 1$. Hence we have the following expression for m_τ:

$$m_\tau = \frac{(n-1)s + k}{2s+1} = \frac{k^2 s + k}{2s+1} = \frac{(s^2+s+1)(s^2+1)(s+1)}{2s+1}$$

The remainder when we divide $(s^2 + s + 1)(s^2 + 1)(s + 1)$ by $2s + 1$ is $\frac{15}{32}$. So if we set $r = 2s$ we find that

$$32m_\tau = \frac{(4s^2+4s+4)(4s^2+4)(2s+2)}{2s+1} = \frac{(r^2+2r+4)(r^2+4)(r+2)}{r+1}$$

The remainder of $(r^2 + 2r + 4)(r^2 + 4)(r + 2)$ on division by $r + 1$ is 15, hence $r + 1 = 2s + 1$ must divide 15. Since the divisors of 15 are

$$\{1, 3, 5, 15\}$$

we conclude that

$$k \in \{1, 3, 7, 57\}.$$

Hence the theorem is proved. □

10.6 The Hoffman-Singleton Graph

The Moore graph of diameter two and valency seven is called the *Hoffman-Singleton graph* after its discoverers. We give a description of it. We first construct a bipartite graph on 50 vertices with degree 5.

The vertices of our bipartite graph will consist of the points and some of the lines in the vector space of dimension two over $\mathbb{Z}_5$. We represent the points by ordered pairs (x, y). A *line* consists of the five points (x, y) such

that $y = ax + b$ for given a and b; we denote this line by $[a, b]$. Thus we have 25 points and 25 lines. (We do not use the five lines parallel to the y-axis.) We declare (x, y) and $[a, b]$ to be adjacent if (x, y) is on $[a, b]$. Thus we have a 5-regular bipartite graph on 50 vertices. We will transform it into a 7-regular graph by adding 10 copies of C_5.

We claim that this graph has girth at least six and diameter four.

We can divide the 25 points into five classes, according to their x-coordinate. We divide the lines into five classes according to their slope a.

We claim that two distinct vertices u and v are in the same class if and only if $\text{dist}(u, v) = 4$.

Now we add 5-cycles: join (x, i) to $(x, i \pm 1)$, join $[a, j]$ to $[a, j \pm 2]$.

If A is a point class and B is a line class, the subgraph induced by $A \cup B$ is isomorphic to the Petersen graph.

10.7 Strongly Regular Graphs

A graph G is *strongly regular* if it is regular but not complete or empty, and there are constants a and c such that

(a) If x and y are adjacent in G, they have exactly a common neighbors.

(b) If x and y are distinct and not adjacent, they have exactly c common neighbors.

If G has v vertices and is k-regular, we say that it is a $(v, k; a, c)$ strongly regular graph. If G is strongly regular, the number of walks of length two between vertices u and v is determined by whether u and v are equal, adjacent, or distinct and not adjacent.

If $m, n > 1$, then mK_n is strongly regular. A Moore graph of diameter two is strongly regular with parameters $(k^2 + 1, k; 0, 1)$. The complement of a strongly regular graph is strongly regular.

10.7.1 Theorem. *Let G be a graph with adjacency matrix A. Then G is strongly regular if and only if there are integers k, a and c such that*

$$A^2 - (a - c)A - (k - c)I = cJ.$$

Proof. Let $\overline{A}$ denote the adjacency matrix of $\overline{G}$. Then $\overline{A} = J - I - A$ and G is strongly regular if and only if there are integers k, a and c such that

$$A^2 = kI + aA + c\overline{A}.$$

This is equivalent to the equation in the statement of the theorem. □

If G has v vertices and $A^2 = kI + aA + c\overline{A}$, then since the diagonal entries of A^2 are the row sums of A, we see that G is k-regular. Hence

$$cv\mathbf{1} = cJ\mathbf{1} = (A^2 - (a-c)A - (k-c)I)\mathbf{1} = (k^2 - (a-c)k - (k-c))\mathbf{1}.$$

It follows that v is determined by k, a and c.

We can use the matrix equation in the above theorem to determine the eigenvalues of a strongly regular graph and their multiplicities, just as we did for Moore graphs.

Examples: Clebsch, $L(K_n)$.

10.8 Paley Graphs

Let $\mathbb{F}$ be a finite field of odd order and let $\mathbb{F}^*$ denote the non-zero elements of $\mathbb{F}$. Let S denote the set of non-zero squares in $\mathbb{F}$ and let N be the set of non-squares. Thus S and N partition $\mathbb{F}^*$. The set S is the image of the map $\sigma : \mathbb{F} \to \mathbb{F}$ given by $\sigma(x) = x^2$. Since $\mathbb{F}$ has odd order, if $c \in \mathbb{F}^*$ then $-c \neq c$ so σ maps two elements of $\mathbb{F}^*$ to each element of S. Consequently

$$|N| = |S| = \frac{q-1}{2}.$$

If $b \in \mathbb{F}^*$ and $bx^2 = y^2$, then b is the square of y/x. Therefore if $b \in N$,

$$bS \cap S = \emptyset$$

and so $bS = N$. Hence

$$S = b^2 S = bN.$$

Thus the product of a two non-squares is a square and the product of a square and a non-square is a non-square.

Suppose now that $-1 \in S$. (We will see that this implies that $q \equiv 1$ modulo 4.) The *Paley graph* has $\mathbb{F}$ as its vertex set, and elements a and b of $\mathbb{F}$ are adjacent if $a - b \in S$. Note that since $-1 \in S$, if $a - b \in S$ then $b - a \in S$.

If $-1 \notin S$ then

$$(a-b)(b-a) = -(a-b)^2$$

is not a square and so either $a - b \in S$ or $b - a \in S$, but not both. The *Paley tournament* is the directed graph with vertex set $\mathbb{F}$, where (a, b) is an arc if $b - a \in S$.

10.8.1 Lemma. *If $\mathbb{F}$ is a field of odd order q, then -1 is a square if and only if $q \equiv 1$ modulo 4.*

Proof. Suppose -1 is not a square and let G be the Paley tournament with vertex set $\mathbb{F}$. If $a \in S$, let τ_a be the map from $\mathbb{F}$ to itself given by $\tau_a(x) := ax$. If a is a square then τ_a is an automorphism of G that fixes 0 and maps S to S and N to N. Moreover if x and y are squares and $a = y/x$, then τ_a fixes S and maps x to y.

Hence the tournament induced by the vertices of S is vertex transitive and so its vertices all have the same in-degree and the same out-degree. Since both the in-degrees and the out-degrees sum to the number of arcs, it follows that the in-degree and out-degree of each vertex are the same. Since exactly one of the pairs (x, y) and (y, x) is an arc, it follows that $|S|$ is odd and therefore

$$q = 2|S| + 1 \equiv 3 \mod 4.$$

Now assume -1 is a square and let G be the Paley graph with vertex set $\mathbb{F}$. Suppose that x in S has exactly r neighbors in N. Using the maps τ_a, we can show that each vertex in S has exactly r neighbors in N.

Assume $b \in N$. If $x \in S$ and $y \in N$ and $y - x \in S$, then $by - bx \in N$. Now $by \in S$ and $bx \in N$ and x is adjacent to y if and only if by is not adjacent to bx. So bx is not adjacent to r vertices in N and therefore it is adjacent to $|N| - r$ vertices. Accordingly

$$r = |N| - r,$$

which implies that N is even and that $q \equiv 1$ modulo 4. □

If we use the result that $\mathbb{F}^*$ is a cyclic group, it is easy to provide another proof of this result. When q is prime, you may use Fermat's little theorem to the same end.

The proof of the previous lemma also yields that if $q \equiv 1$ modulo 4, then each vertex in S has exactly $r = (q-1)/4$ neighbors in N. Hence the Paley graph on q vertices is strongly regular, with parameters

$$\left(q, \frac{q-1}{2}; \frac{q-5}{4}, \frac{q-1}{4}\right).$$

If A is the adjacency matrix, then

$$A^2 + A = \frac{q-1}{4}(J + I).$$

If A is the adjacency matrix of the Paley tournament on q vertices (so $A_{x,y} = 1$ if and only if $y - x$ is a square), then you may show that

$$A^2 + A = \frac{q+1}{4}(J - I)$$

and, for later use, that

$$(2A - J)(2A^T - J) = (q+1)I - J. \tag{10.8.1}$$

10.9 Independent Sets

Recall that a subset S is $V(G)$ is independent if it induces a subgraph with no edges. The maximum size of an independent set is G is denoted by $\alpha(G)$.

Suppose $S \subseteq V(G)$. We call the vector x the characteristic vector of S if x is a 01-vector and $x_i = 1$ if and only if $i \in S$.

10.9.1 Lemma. *If x is the characteristic vector of a subset S of the graph G and A is the adjacency matrix of G, then S is independent if and only if $x^T Ax = 0$.*

Proof. We have

$$x^T Ax = \sum x_i A_{i,j} x_j = \sum_{ij \in E(G)} x_i x_j. \qquad \square$$

10.9.2 Lemma. *Suppose A is the adjacency matrix of the k-regular graph G on v vertices. If τ is the least eigenvalue of A, then the matrix*

$$A - \tau I - \frac{k-\tau}{v} J$$

is positive semidefinite.

Proof. A matrix is positive semidefinite if and only if its eigenvalues are non-negative. We check that

$$(A - \tau I - \frac{k-\tau}{v} J)\mathbf{1} = (k-\tau)\mathbf{1} - \frac{k-\tau}{v} v\mathbf{1} = 0.$$

Thus 0 is an eigenvalue of $A - \tau I - \frac{k-\tau}{v} J$ with $\mathbf{1}$ as an eigenvector. Suppose now that z is an eigenvector for A that is orthogonal to $\mathbf{1}$ and has eigenvalue θ. Then

$$(A - \tau I - \frac{k-\tau}{v} J)z = (A - \tau I)z = (\theta - \tau)z.$$

Since τ is the least eigenvalue of A, we see that $\theta - \tau \geq 0$. Therefore $A - \tau I - \frac{k-\tau}{v} J$ is positive semidefinite. $\square$

10.9.3 Theorem. *Let G be a k-regular graph with least eigenvalue τ. Then*

$$\alpha(G) \leq \frac{v}{1 - \frac{k}{\tau}}.$$

Proof. 'Recall' that a matrix M is positive semidefinite if and only if it is symmetric and $x^T M x \geq 0$ for all x. So

$$0 \leq x^T \left(A - \tau I - \frac{k-\tau}{v} J \right) x = x^T A x - \tau x^T x - \frac{k-\tau}{v} x^T J x.$$

If x is the characteristic vector of the independent set S, then

$$x^T A x = 0, \quad x^T x = |S|, \quad x^T J x = |S|^2$$

and therefore

$$0 \leq -\tau |S| - \frac{k-\tau}{v} |S|^2,$$

from which the theorem follows. □

10.9.4 Corollary. *If the bound in theorem is tight and x is the characteristic vector of an independent set S with maximum size, then $x - \frac{|S|}{v}\mathbf{1}$ is an eigenvector for A with eigenvalue τ.*

Proof. If the bound is tight, then

$$0 = x^T \Big(A - \tau I - \frac{k-\tau}{v} J \Big) x$$

and from this it follows that

$$\Big(A - \tau I - \frac{k-\tau}{v} J \Big) x = 0.$$

(This holds because the matrix is positive semidefinite.) From this point it is a routine exercise to verify the claim. □

Consider a Moore graph G of diameter two and valency $k = s^2 + s + 1$. Then

$$\begin{aligned} v &= (s^2 + s + 1)^2 + 1 \\ &= s^4 + 2s^3 + 2s^2 + s^2 + 2s + 2 \\ &= (s^2 + 1)(s^2 + 2s + 2) \end{aligned}$$

and

$$1 + \frac{k}{\tau} = 1 + \frac{s^2 + s + 1}{s + 1} = \frac{s^2 + 2s + 2}{s + 1}.$$

Therefore

$$\alpha(G) \leq (s^2 + 1)(s + 1).$$

For $k = 2$, 3 and 57, the respective bounds on $\alpha(G)$ are 4, 15 and 400. The first two bounds are tight.

10.10 Eigenvectors

Let A be the adjacency matrix of the graph G. Assume $n = |V(G)|$ and let $e_1, \ldots, e_n$ denote the standard basis for $\mathbb{R}^n$. Then since A is a 01-matrix, if $f \in \mathbb{R}^n$, then

$$(Af)_i = \sum_{j=1}^{n} A_{i,j} f_j = \sum_{j \sim i} f_j.$$

This can be expressed another way. Suppose f is a function on the vertices of G. There is a linear transformation S (on the space of functions on $V(G)$) defined by

$$(Sf)(i) := \sum_{i \sim j} f(j);$$

the adjacency matrix is the matrix that represents S relative to the standard basis.

A function f is an eigenvector for S (or A) if it is not zero and there is a scalar θ such that $Tf = \theta F$, or equivalently if

$$\theta f(i) = \sum_{j \sim i} f(j).$$

For example, if G is k-regular then any non-zero constant function is an eigenvector, with eigenvalue k. If G is k-regular and bipartite then the function taking value 1 on white vertices and -1 on black vertices is an eigenvector with eigenvalue $-k$. Since A is symmetric this eigenvector is orthogonal to any non-zero constant function and so we conclude that in a regular bipartite graph, there are an equal number of vertices of each color. (There are other proofs of this.)

We determine eigenvectors and eigenvalues for the complete graphs. Since K_n is regular, a non-zero constant function is an eigenvector with eigenvalue

$n-1$. Suppose f is a non-zero function on $V(K_n)$ whose values sum to zero. Then

$$(Af)_i = \sum_{j \neq i} f_j = -f_i + \sum_{j=1}^{n} f_j = -f_i.$$

Note that the values of f sum to zero if and only if f is orthogonal to the constant functions. The constant functions span a space with dimension 1, and so its orthogonal complement has dimension $n-1$. It follows that -1 is an eigenvalue of A with dimension $n-1$. Hence the eigenvalues of K_n are $n-1$ (with multiplicity 1) and -1 (with multiplicity $n-1$).

Chapter 11

Matchings

All graphs are simple, still.

11.1 Matchings

A *matching* in a graph is a set of edges, no two with a vertex in common. (So a matching is not a graph.) The size of a matching is the number of edges in it, and a *k-matching* is a matching of size k. Our basic problem is the following: we are given a graph and we want to find a matching in it with as many edges as possible. The maximum number of edges in a matching from G is often denoted by $\nu(G)$. We often say that a vertex of G in a matching M is *covered* by M. A k-matching covers $2k$ vertices and so $2\nu(G) \leq |V(G)|$. A matching is *perfect* if it covers every vertex. Clearly a graph with a perfect matching must have an even number of vertices.

11.1.1 Lemma. *If M is matching in G that is not contained in a matching with more edges, then the vertices not covered by M form an independent set.*

Proof. Suppose M is as stated and let S be the set of vertices of G not covered by M. If e is an edge of G that joins two vertices of S, then $M \cup e$ is a matching that contains G and is larger. We conclude that S is an independent set. □

The matching M in this lemma is **maximal under inclusion**. Generally we are only interested in finding matchings that have as many edges as possible.

We can establish a lower bound on $\nu(G)$ by finding a matching with as many edges as possible. Somewhat surprisingly, there is a good way to get an upper bound. A subset C of $V(G)$ is a *vertex cover* if every edge of G contains at least one vertex of C. As a somwhat trivial example, if G is bipartite, then the vertices in a color class form a vertex cover.

11.1.2 Lemma. *If C is a vertex cover in G and M is a matching, then $|M| \leq |C|$.*

Proof. Suppose M is a matching and C is a vertex cover in G. Then each edge in M must contain a vertex in C; since the edges of M disjoint it follows that there is at least one vertex in C for each edge of M, and consequently $|M| \leq |C|$. □

For an odd cycle C_{2k+1}, we have $\nu(G) = k$ while any vertex cover must have at least $k+1$ vertices in it. We will see that if G is bipartite, there is always a vertex cover C such that $|C| = \nu(G)$.

11.2 Augmenting Paths

Let M be a matching in G. A path P in G is an *alternating path* relative to M if $E(P) \setminus M$ is a matching; thus P is alternating if every other edge is in M. Similarly a cycle C is alternating if $E(C) \setminus M$ is a matching. (Hence an alternating cycle has even length.)

If M and N are sets, then $M \oplus N$ denotes their symmetric difference.

11.2.1 Lemma. *If M and N are matchings in G, then the components (of the subgraph formed by) $M \oplus N$ are even cycles and paths; each component is alternating relative to either matching.*

Proof. The graph formed by the edges in $M \oplus N$ has maximum degree two, and therefore its components are cycles and paths. If H is one of the components of this graph, then $E(H) \setminus M$ is a matching, and so H is an alternating cycle or path. □

An *augmenting path* relative to a matching M is an alternating path whose first and last vertices are not covered by M. So if P is an augmenting path, then

$$|E(P) \setminus M| > |E(P) \cap M|.$$

11.2.2 Lemma. *If M is a matching in G and P is an augmenting path relative to M, then $M \oplus E(P)$ is a matching with one more edge than M.* □

11.2.3 Theorem. *A matching M in G has maximum size if and only if there is no augmenting path relative to M.*

Proof. Clearly if M has an augmenting path, it is not maximal. Assume conversely that M no augmenting path.

Let N be a second matching in G and consider the subgraph formed by the edges in $M \oplus N$. If H is a component of this graph and H contains more edges from N than M, then H cannot be an even cycle and so it is an alternating path with neither end covered by M—thus it is an augmenting path relative to M. Therefore each component of $M \oplus N$ contains as many edges from M as from N, and consequently $|M| \geq |N|$. This implies that M has maximal size. □

11.3 A Royal Theorem

If S is a subset of the vertices of G, then $N(X)$ denotes the set of vertices of G which are adjacent to a vertex in S. The following result is due to König.

11.3.1 Theorem. *If G is a bipartite graph and M is a matching with maximum size, there is a vertex cover C such that $|M| = |C|$.*

Proof. Let A and B be the two colour classes of G and let M be a matching in G. We construct a vertex cover.

Let X_0 denote the vertices in A not covered by M. Let X denote the set of vertices in A that are joined to a vertex in X_0 by an alternating path. Let Y denote the vertices in B joined to a vertex in X_0 by an alternating path. Let Y_0 be the set of vertices in Y not covered by M.

We claim that

$$C := (A \setminus X) \cup Y$$

is a vertex cover. Clearly $(A \setminus X) \cup X$ is a vertex cover, so to prove the claim we show that each edge that contains a vertex in X must contain a vertex in Y. Equivalently, we must show that if $u \in X$, then $N(u) \subseteq Y$. Let P be an alternating path joining a vertex in X_0 to u in X. Note that the edge of P on u lies in M. If b is a neighbour of u, then $b \in B$. If $ub \in M$, then ub is the last edge of P and therefore b is joined by an alternating path to a vertex in X, and therefore $b \in Y$. If $ub \notin M$, then P extended by ub is an alternating path from a vertex in X_0 to b, and therefore $b \in Y$. Thus $N(u) \subseteq Y$ and therefore $(A \setminus X) \cup Y$ is a vertex cover.

Now we claim that

$$|M| = |A \setminus X| + |Y \setminus Y_0|.$$

Let D denote the set $(A \setminus X) \cup (Y \setminus Y_0)$. Since C is a vertex cover, each edge of M contains a vertex in $A \setminus X$ or a vertex in Y. Any vertex of Y that lies on an edge of M must be in $Y \setminus Y_0$, and therefore the vertices in D cover the edges in M. So our claim will follow if no edge in M joins two vertices in D. But no edge joins two vertices in $A \setminus X$ or two in $Y \setminus Y_0$, and since an alternating path from a vertex in X_0 to a vertex in B ends with an edge not in M, any vertex paired by M with a vertex in Y lies in X. So each matching edge contains exactly one vertex from D, and thus our claim holds.

Consequently we have

$$|M| = |A \setminus X| + |Y \setminus Y_0| = |C| - |Y_0|.$$

If $Y_0 \neq \emptyset$ and $y \in Y_0$, then there is an alternating path from a vertex in X_0 to y. Neither end of this path is covered by M and so it is an augmenting path. This implies that M does not have maximum size. Therefore if M does have maximum size, then $Y_0 = \emptyset$ and $|C| = |M|$. □

If M does not have maximum size, the above proof provides an augmenting path for M; if M does have maximum size it provides a vertex cover C of the same size as M. In fact it yields an algorithm for finding a maximum matching in a bipartite graph.

11.4 Hall's Theorem

Suppose G is a bipartite graph with bipartition (A, B). If $D \subseteq A$ and $|N(D)| < |D|$, there is no matching of G that covers A. Surprisingly the converse is true; this is Hall's theorem:

11.4.1 Theorem. *Suppose G is a bipartite graph with bipartition (A, B). There is a matching of G that covers A if and only if for each subset X of A we have $|N(X)| \geq |X|$.*

Proof. We derive this from König's theorem. Let M be a matching of maximum size and let C be a vertex cover such that $|C| = |M|$.

We assume M does not cover A, and prove that $|N(A \setminus C)| < |A \setminus C|$. Since C is a cover, no edge joins a vertex in $A \setminus C$ to a vertex in $B \setminus C$, and therefore $N(A \setminus C) \subseteq B \cap C$. As $B \cap C = C \setminus A$ and $|C| < |A|$,

$$|N(A \setminus C)| \leq |B \cap C| = |C \setminus A| = |C| - |A \cap C| < |A| - |A \cap C| = |A \setminus C|.$$

Conversely, if M covers A and $C' \subseteq A$ then $N(C')$ contains the vertices that are paired with vertices in C' by M; hence $N(C') \geq |C'|$. □

If M is a matching of maximum size and X and Y are sets used in our proof of König's theorem, then $N(X) \subseteq Y$. Since M is maximum, it covers each vertex in Y and, as we saw in the proof, the vertices paired with vertices in Y by M all belong to X. Since X contains the vertices in A not covered by M, it follows that $|X| > |Y|$. This provides another proof of Hall's theorem.

We offer a third proof of Hall's theorem. Assume G is bipartite with bipartition (A, B). Assume that if $C' \subseteq A$, then $|N(C')| \geq |D|$. If $|N(D)| > |D|$ for each proper subset D of A and $e \in E(G)$, then Hall's condition holds in $G \setminus e$ and so $G \setminus e$ has a matching that covers A. So we assume there is a proper subset D_0 of A such that $|N(D_0)| = |D_0|$.

If $D \subseteq A$ and $D_0 \subseteq D$, then $N(D)$ contains $N(D_0)$ and so each vertex in $N(D) \setminus N(D_0)$ is a neighbor of a vertex in $D \setminus D_0$. Since

$$|N(D)| \geq |D|, \quad |N(D_0)| = |D_0|$$

it follows that $|N(D \setminus D_0)| \geq |D \setminus D_0|$. It follows that by induction that there is a matching in G that covers D_0 and a matching that covers $A \setminus D_0$ but not any vertices in D_0. The union of these two matchings is a matching that covers A. □

Index