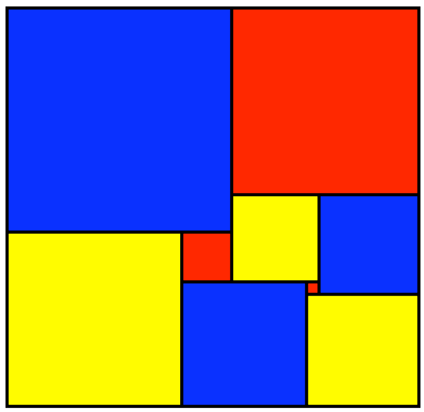
Introduction to Combinatorics

Course Notes for Math 239



Department of Combinatorics and Optimization
University of Waterloo

Contents

Chapter 1

Combinatorial Analysis

1.1 Introduction

Our goal in the first half of this course is to learn how to solve a number of interesting counting problems.

We offer some examples. A **composition** of a non-negative integer n is a sequence $(m_1, \dots, m_r)$ of positive integers such that

$$m_1 + \cdots + m_r = n.$$

The numbers $m_1, \dots, m_r$ are the **parts** of the composition. We define the **weight** of a composition to be the sum of its parts. For example, the number of different ways we can cut a piece of string of length n centimetres into pieces of length 1 and 2 cm is the number of compositions with weight n where all parts are equal to 1 or 2. (We will often use weight where the word "size" would do, because sometimes there is more than one way of defining size.)

Other questions we might ask about compositions include

(a) How many different compositions of n are there?

(b) How many compositions of n are there with exactly k parts?

(c) How many compositions of n are there where all parts of the composition are odd?

A second important class of counting problems involves **binary strings**. A binary string of length n is a sequence $a_1 \cdots a_n$ where each a_i is 0 or 1. Clearly there are 2^n binary strings of length n (so that's solved). But there are other questions:

(a) How many binary strings of length n are there that do not contain an odd string of 0's as a maximal substring? (So 1001 is OK, but 10001 is not.)

(b) How many binary strings of length n are there that do not contain 0101 as a substring?

(c) How many binary strings of length n are there that contain exactly k 1's?

1.2 Sums and Products

A natural way to determine the size of a set is to show that it has the same size as some set of known size. Usually the "known" set will be built from smaller known sets using unions and products.

We recall that if A and B are sets, then the **union** $A \cup B$ is defined by

$$A \cup B := \{x : x \in A \text{ or } x \in B\}.$$

If A and B are **disjoint**, that is, $A \cap B = \emptyset$ then

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

Here $|S|$ denotes the number of elements in the set S.

The **Cartesian product** $A \times B$ of sets A and B is the set of all ordered pairs whose first element is an element of A and second element is an element of B, that is

$$A \times B := \{(a, b) : a \in A, b \in B\}.$$

Then

$$|A \times B| = |A|\,|B|.$$

We can similarly define the **Cartesian power** A^k as ordered k-tuples of elements from A.

$$A^k := \{(a_1, a_2, \ldots, a_k) : a_1, a_2, \ldots, a_k \in A\}.$$

When A is finite, $|A^k| = |A|^k$. Thus if

$$A = \{1, 2, 3, 4, 5, 6\}$$

and $k = 3$, then the elements of A^3 correspond to the $6^3 = 216$ possible outcomes when we toss a 6-sided die three times.

For a second example, if $A = \{0, 1\}$, then the elements of A^n are the n-tuples

$$(a_1, \ldots, a_n), \qquad a_i \in \{0, 1\}.$$

1.3 Binomial Coefficients

We are interested in "enumeration problems"; these are problems that involve counting various kinds of combinatorial objects. We begin with the following easy question: *How many k–element subsets are there of an n–element set?*

Theorem 1.3.1. *For non–negative integers n and k, the number of k-element subsets of an n-element set is*

$$\frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Proof: Let $\mathscr{L}$ be the set of all ordered lists of k distinct numbers from the set $\{1,\ldots,n\}$. There are n choices for the first number in the list, and then there are $n-1$ remaining choices for the second number. In general, when choosing the i–th number in our list, we have already used $i-1$ of the n numbers and, hence, we have $n-i+1$ numbers to choose from. Thus,

$$|\mathscr{L}| = n(n-1)\cdots(n-k+1).$$

Now consider a different way of generating the elements of $\mathscr{L}$. We first choose the k elements and then order the elements in all possible ways. Let there be x ways to choose k elements from $\{1,\ldots,n\}$. There are $k! = k(k-1)\cdots 3\cdot 2\cdot 1$ ways to order, or permute, each k–element set. Thus,

$$|\mathscr{L}| = x(k!).$$

Hence

$$x = \frac{n(n-1)\cdots(n-k+1)}{k!},$$

as required. ▌

We define $\binom{n}{k}$, which we read as "n choose k", to be the number of k-element subsets of $\{1,\ldots,n\}$. So by Theorem 1.3.1,

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

Note that $\binom{n}{k} = 0$ whenever $n < k$ as it should be. It is natural to define the product of zero numbers to be one; for example, $5^2 = 5\cdot 5 = 25, 5^1 = 5$ and $5^0 = 1$, the product of zero 5's, is 1. With this interpretation, $0! = 1$ and $\binom{n}{0} = 1$.

The numerical values of the binomial coefficients form a structure known as Pascal's triangle. A few rows of the Pascal's triangle are given here.

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

The values of each row represent the values of $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ in order, where $n = 0$ in the first row, $n = 1$ in the second row, etc.

Notice that this structure is symmetric, meaning that for integers n and k where $0 \le k \le n$,

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

This can be easily explained through some arithmetic:

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}.$$

At first this seems surprising, but it follows easily from the definitions. Indeed, the number of ways of selecting k elements from an n–element set is the same as the number of ways of discarding $(n-k)$ elements from the set. We can formalize this relation using a bijection, which is described in the next section.

1.4 Bijections (One-to-One Correspondence)

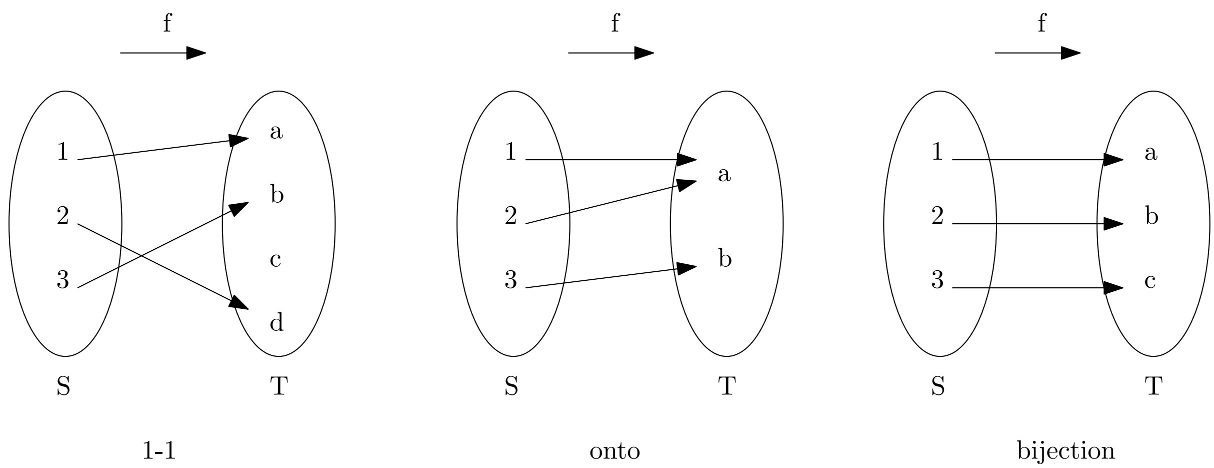
Another way of establishing that two sets have equal size is through the use of a bijection. We begin with a review of a few definitions on functions. Let S and T be sets. Let $f : S \to T$ be a function (or mapping). In particular, this means that for any $x \in S$, $f(x)$ is an element in T. Then

- f is **1-1** or **injective** if for any $x_1, x_2 \in S$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. In other words, every element in S is being mapped to a unique element in T.

- f is **onto** or **surjective** if for all $y \in T$, there exists $x \in S$ such that $f(x) = y$. In other words, every element in T is being mapped to from some element in S.

- f is a **1-1 correspondence** or **bijection** if it is both 1-1 and onto.

We can visualize these definitions using the following diagram:



The functions that you have seen in high school or calculus are typically defined for $f : \mathbb{R} \to \mathbb{R}$. For example, $f(x) = e^x$ is 1-1, but not onto; $f(x) = x^3 - x$ is onto, but not 1-1; and $f(x) = 2x + 1$ is both 1-1 and onto, hence a bijection.

In combinatorics, we use mappings to compare the cardinalities of finite sets S and T. If there exists a mapping $f : S \to T$ that is 1-1, then $|S| \leq |T|$. This is because the $|S|$ elements of S must be mapped to distinct elements in T, so there must be at least $|S|$ distinct elements in T. On the other hand, if there exists a mapping $f : S \to T$ that is onto, then $|S| \geq |T|$. This is because for the $|T|$ elements in T, each must be mapped to by a distinct element in S. Therefore, if there exists a bijection $f : S \to T$, then $|S| = |T|$, as f is both 1-1 and onto.

In addition to showing that two sets have equal size, bijections have the nice property that they "pair up" elements of S with elements of T exactly. This gives a *correspondence* between elements of S and T.

We can prove that a function is a bijection by going through the definition of 1-1 and onto. Alternatively, we could show that the mapping is "reversible", that is, there exists an inverse function. For $f : S \to T$, the **inverse** (if it exists) of f is a function $f^{-1} : T \to S$ such that for all $x \in S$, $f^{-1}(f(x)) = x$, and for all $y \in T$, $f(f^{-1}(y)) = y$.

Theorem 1.4.1. *If a function $f : S \to T$ has an inverse, then f is a bijection.*

Proof: Let $f^{-1} : T \to S$ be an inverse of f. We need to prove that f is 1-1 and onto. Suppose $f(x_1) = f(x_2)$. Then $f^{-1}(f(x_1)) = f^{-1}(f(x_2))$. By definition of inverse, $x_1 = x_2$, so f is 1-1. Let $y \in T$. Since f^{-1} is a function, $f^{-1}(y) = x$ for some $x \in S$. Then $f(f^{-1}(y)) = f(x)$, and by the definition of inverse, $y = f(x)$. Therefore, x is mapped to y, and f is onto. ∎

Usually if a bijection is clear, its inverse is also clear. So in most cases, instead of proving that a function is 1-1 and onto (which can be tedious), we can simply provide the inverse function.

Problem 1.4.2. *For some $0 \le k \le n$, let S be the set of k-subsets of $\{1, \ldots, n\}$, and let T be the set of $(n-k)$-subsets of $\{1, \ldots, n\}$. Find a bijection between S and T.*

Solution: We can define the following mapping:

$$f : S \to T, \quad f(A) = \{1, \ldots, n\} \setminus A \quad \forall\ A \in S.$$

First, we need to check that each element of S is being mapped to an element in T by f. For any $A \in S$, $|A| = k$. So $f(A) = \{1, \ldots, n\} \setminus A$ has cardinality $n-k$, meaning $f(A) \in T$.

It should be clear that in order to "reverse" the function, we simply need to apply the same operation again. So the inverse is $f^{-1} : T \to S$ where for each $B \in T$, $f^{-1}(B) = \{1, \ldots, n\} \setminus B$.

We can check that for each $A \in S$,

$$f^{-1}(f(A)) = f^{-1}(\{1, \ldots, n\} \setminus A) = \{1, \ldots, n\} \setminus (\{1, \ldots, n\} \setminus A) = A.$$

And for each $B \in T$,

$$f(f^{-1}(B)) = f(\{1, \ldots, n\} \setminus B) = \{1, \ldots, n\} \setminus (\{1, \ldots, n\} \setminus B) = B.$$

So f^{-1} is indeed the inverse of f, which proves that f is a bijection. ∎

By Theorem 1.3.1, $|S| = \binom{n}{k}$ and $|T| = \binom{n}{n-k}$. So this bijection is also a combinatorial proof of the identity $\binom{n}{k} = \binom{n}{n-k}$

We illustrate this bijection by matching the elements of S with elements of T for the case where $n = 5, k = 2$. The function f maps in the $\rightarrow$ direction, the inverse f^{-1} maps in the $\leftarrow$ direction. For example, $f(\{1,5\}) = \{2,3,4\}$ while $f^{-1}(\{1,2,5\}) = \{3,4\}$.

S		T
$\{1,2\}$	$\longleftrightarrow$	$\{3,4,5\}$
$\{1,3\}$	$\longleftrightarrow$	$\{2,4,5\}$
$\{1,4\}$	$\longleftrightarrow$	$\{1,3,5\}$
$\{1,5\}$	$\longleftrightarrow$	$\{2,3,4\}$
$\{2,3\}$	$\longleftrightarrow$	$\{1,4,5\}$
$\{2,4\}$	$\longleftrightarrow$	$\{1,3,5\}$
$\{2,5\}$	$\longleftrightarrow$	$\{1,3,4\}$
$\{3,4\}$	$\longleftrightarrow$	$\{1,2,5\}$
$\{3,5\}$	$\longleftrightarrow$	$\{1,2,4\}$
$\{4,5\}$	$\longleftrightarrow$	$\{1,2,3\}$

We can establish a bijection between two completely different looking sets of objects in order to find a correspondence between the two sets.

Problem 1.4.3. *Let S be the set of all subsets of $\{1,\dots,n\}$, and let T be the set of all binary strings of length n. Find a bijection between S and T.*

Solution: We define $f : S \to T$ in the following way: For a subset A of $\{1,\dots,n\}$, we can create a string $f(A) = a_1a_2\cdots a_n$ length n where

$$a_i = \begin{cases} 0 & i \notin A \\ 1 & i \in A \end{cases}$$

It is clear that $f(A)$ is a binary string of length n, hence in T.

This mapping is reversible: Let $t = b_1b_2\cdots b_n \in T$. Define $f^{-1} : T \to S$ where

$$f^{-1}(t) = \{i \in \{1,\dots,n\} \mid b_i = 1\}.$$

You can check that $f^{-1}(f(A)) = A$ and $f(f^{-1}(t)) = t$, so f is a bijection. ∎

This bijection tells us that the number of subsets of $\{1,\dots,n\}$ is equal to the number of binary strings of length n, which is 2^n. In addition, we can relate some subset problems to binary string problems. For example, subsets of $\{1,\dots,n\}$ of size k are mapped to binary strings of length n with exactly k 1's by f. So the number of such binary strings is equal to $\binom{n}{k}$.

We illustrate this bijection for $n = 3$.

S		T
$\emptyset$	$\longleftrightarrow$	000
$\{1\}$	$\longleftrightarrow$	100
$\{2\}$	$\longleftrightarrow$	010
$\{3\}$	$\longleftrightarrow$	001
$\{1,2\}$	$\longleftrightarrow$	110
$\{1.3\}$	$\longleftrightarrow$	101
$\{2,3\}$	$\longleftrightarrow$	011
$\{1,2,3\}$	$\longleftrightarrow$	111

1.5 Combinatorial Proofs

Any proof that involves some kind of counting argument is a *combinatorial* proof. We have seen combinatorial proofs in Theorem 1.3.1 and the previous section involving bijections. We give an example here which involves proving an algebraic identity by counting combinatorial objects.

Theorem 1.5.1. *For any non–negative integer n,*

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

This is also known as the **binomial theorem**. We first give the main idea of the proof: In the expansion of $(1+x)^n$, each term in the expansion consists of a product of n items, each one being either 1 or x. So each term is a product $a_1 a_2 \cdots a_n$ where each $a_i \in \{1, x\}$. This term is equal to x^k whenever exactly k of these a_i's are x's. The coefficient of x^k is then the number of ways that this happens, which is essentially the same as choosing subsets of $\{1, \ldots, n\}$ of size k. There are $\binom{n}{k}$ of these subsets, hence the coefficient of x^k is $\binom{n}{k}$. For example, when $n = 3$,

$$\begin{aligned}(1+x)^3 &= (1+x)(1+x)(1+x)\\ &= 1\cdot1\cdot1 + 1\cdot1\cdot x + 1\cdot x\cdot1 + 1\cdot x\cdot x + x\cdot1\cdot1 + x\cdot1\cdot x + x\cdot x\cdot1 + x\cdot x\cdot x.\\ &= 1 + 3x + 3x^2 + x^3.\end{aligned}$$

We now give a formal proof of the theorem.

Proof: We first expand $(1+x)^n$ algebraically:

$$\begin{aligned}
(1+x)^n &= (1+x)(1+x)\cdots(1+x) \\
&= \left(\sum_{a_1\in\{1,x\}} a_1\right)\left(\sum_{a_2\in\{1,x\}} a_2\right)\cdots\left(\sum_{a_n\in\{1,x\}} a_n\right) \\
&= \sum_{a_1\in\{1,x\}}\sum_{a_2\in\{1,x\}}\cdots\sum_{a_n\in\{1,x\}} a_1a_2\cdots a_n \\
&= \sum_{(a_1,a_2,\ldots,a_n)\in\{1,x\}^n} a_1a_2\cdots a_n.
\end{aligned}$$

Define S_k to be the set of elements of $\{1,x\}^n$ where exactly k of the n terms are x's. So if $(a_1,\ldots,a_n)\in S_k$, then $a_1a_2\cdots a_n = x^k$. Also,

$$\{1,x\}^n = S_0\cup S_1\cup\cdots\cup S_n.$$

This is a disjoint union of sets, so we can break up the sum at the end of the equation above to get

$$\begin{aligned}
(1+x)^n &= \sum_{k=0}^{n}\left(\sum_{(a_1,a_2,\ldots,a_n)\in S_k} a_1a_2\cdots a_n\right) \\
&= \sum_{k=0}^{n}\left(\sum_{(a_1,a_2,\ldots,a_n)\in S_k} x^k\right) \\
&= \sum_{k=0}^{n}|S_k|x^k.
\end{aligned}$$

Let T_k be the set of all subsets of $\{1,\ldots,n\}$ of size k. Then there is a bijection between S_k and T_k: define $f: S_k\to T_k$ by $f(a_1,a_2,\ldots,a_n)=\{i\mid a_i=x\}$. (This is similar to the bijection defined in Problem 1.4.3.) This gives us $|S_k|=|T_k|=\binom{n}{k}$. Therefore,

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

∎

Sometimes an algebraic identity can be established by giving a set of objects, and count the size of this set in two different ways. Since we are counting the same set of objects, the two ways of counting must result in the same number. We give two examples here.

Problem 1.5.2. *For integers* $1 \le k \le n$*, show that*

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

Solution: Let S be the set of all k-subsets of $\{1,\ldots,n\}$. By Theorem 1.3.1, $|S| = \binom{n}{k}$.

We now count $|S|$ in a different way. Partition S into two sets S_1 and S_2 where S_1 contains all k-subsets of $\{1,\ldots,n\}$ which include the element n, and S_2 contains all k-subsets of $\{1,\ldots,n\}$ which do not include the element n. Since S_1 and S_2 are disjoint, $|S| = |S_1| + |S_2|$.

Now each element of S_1 consists of n and a $(k-1)$-subset of $\{1,\ldots,n-1\}$, so $|S_1| = \binom{n-1}{k-1}$. Each element of S_2 is a k-subset of $\{1,\ldots,n-1\}$, so $|S_2| = \binom{n-1}{k}$. Hence $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. ▮

Problem 1.5.3. *For non–negative integers n and k, show that*

$$\binom{n+k}{n} = \sum_{i=0}^{k} \binom{n+i-1}{n-1}.$$

Solution: Let S denote the set of all n–element subsets of $\{1,\ldots,n+k\}$. By Theorem 1.3.1,

$$|S| = \binom{n+k}{n}.$$

Note that for any set $A \in S$, the largest element of A is at least n. Now, for each $i \in \{0,\ldots,k\}$, let S_i be the set of all sets in S whose largest element is $n+i$. Thus, $(S_0, S_1, \ldots, S_k)$ is a partition of S, so

$$|S| = |S_0| + |S_1| + \cdots + |S_k|.$$

Now, if $A \in S_i$ then $n+i \in A$ and $A \setminus \{n+i\}$ is an $(n-1)$–element subset of $\{1,\ldots,n+i-1\}$. Then, by Theorem 1.3.1,

$$|S_i| = \binom{n+i-1}{n-1}.$$

Hence,

$$\begin{aligned} |S| &= |S_0| + |S_1| + \cdots + |S_k| \\ &= \binom{n-1}{n-1} + \binom{n}{n-1} + \cdots + \binom{n+k-1}{n-1} \\ &= \sum_{i=0}^{k} \binom{n+i-1}{n-1}. \end{aligned}$$

Thus,

$$\binom{n+k}{n} = \sum_{i=0}^{k} \binom{n+i-1}{n-1},$$

as required. ∎

Problem Set 1.5

1. Consider the identity $\sum_{i\geq 0} \binom{n}{2i} = \sum_{i\geq 0} \binom{n}{2i+1}$.

   (a) Give a combinatorial proof of this identity. (Hint: Find a bijection between the even and odd subsets of $\{1, \ldots, n\}$.)

   (b) Give an algebraic proof for the identity. (Hint: Expand $(1-1)^n$.)

2. Consider the identity

   $$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i}.$$

   (Remark: We could also use $\min\{k, m\}$ as the upper limit of this sum. Because $\binom{m}{i} = 0$ whenever $i > m$, k is also a valid upper limit of this sum.)

   (a) Give a combinatorial proof of this identity. (Hint: The left side counts the number of ways of choosing k elements from a set of $(m+n)$ elements — determine a similar interpretation for the right side.)

   (b) Give an algebraic proof for the identity. (Hint: Expand both sides of the equation $(1+x)^{m+n} = (1+x)^m(1+x)^n$ using Theorem 1.5.1.)

3. Consider the identity $\sum_{i=0}^{n} \binom{n}{i} i = n2^{n-1}$.

(a) Give a combinatorial proof of this identity. (Hint: if S is a subset of $\{1,\dots,n\}$ and $\bar{S}$ is its complement then $|S|+|\bar{S}|=n$.)

(b) Give an algebraic proof for the identity. (Hint: Expand $(1+x)^n$ and take the derivatives of both versions.)

4. Show that $\sum_{i=0}^{n}\binom{n}{i}i(i-1)=n(n-1)2^{n-2}$.

5. (a) Consider the following two sets.

$$\begin{aligned} S_k &= \{(A,B) \mid A,B\subseteq\{1,\dots,n\},\ |A|=|B|=m,\ |A\cap B|=k\},\\ T_k &= \{(X,Y,Z) \mid X,Y,Z\subseteq\{1,\dots,n\},\ |X|=k,\ |Y|=|Z|=m-k,\\ &\qquad X\cap Y=X\cap Z=Y\cap Z=\emptyset\}. \end{aligned}$$

Define a bijection $f: S_k\to T_k$, explain why $f(A,B)\in T_k$ for any $(A,B)\in S_k$, and provide the inverse of your bijection.

(b) Consider the set $S=\{(A,B)\mid A,B\subseteq\{1,\dots,n\},\ |A|=|B|=m\}$. By counting S in two different ways, give a combinatorial proof of the following identity:

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

1.6 Generating Series

We begin with a very general enumeration problem.

Problem 1.6.1. *Suppose that S is a set of "configurations" and, for each configuration $\sigma\in S$, we have a non–negative integer weight $w(\sigma)$. For a given integer k, how many elements of S have weight k?*

Consider, for example, the problem from the previous section of counting subsets. Let S be the set of all subsets of $\{1,\dots,n\}$. For each subset $\sigma\in S$, we define its weight to be $w(\sigma)=|\sigma|$. Thus, the number of elements of S of weight k is $\binom{n}{k}$, the number of k element subsets of $\{1,\dots,n\}$.

Definition 1.6.2. *Let S be a set of configurations with a weight function w. The* **generating series** *for S with respect to w is defined by*

$$\Phi_S(x)=\sum_{\sigma\in S}x^{w(\sigma)}.$$

By collecting like–powers of x in $\Phi_S(x)$, we get

$$\begin{aligned}\Phi_S(x) &= \sum_{\sigma\in S} x^{w(\sigma)}\\ &= \sum_{k\geq 0}\left(\sum_{\sigma\in S, w(\sigma)=k} 1\right)x^k\\ &= \sum_{k\geq 0} a_k x^k,\end{aligned}$$

where a_k denotes the number of elements in S with weight k. That is, the coefficient of x^k in $\Phi_S(x)$ counts the number of elements of weight k in S.

Consider, again, the set S of all subsets of $\{1,2,\ldots,n\}$. Let the weight of set $\sigma\in S$ be $|\sigma|$. Then

$$\Phi_s(x) = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = \sum_{k=0}^{n}\binom{n}{k}x^k = (1+x)^n.$$

Consider the case where S is the set of all integer pairs (a,b) where $a \in \{1,3,5\}$, $b\in\{2,4,6\}$ and the weight of (a,b) is defined as $a+b$. Thus,

$$\begin{aligned}\Phi_S(x) &= x^{1+2}+x^{1+4}+x^{1+6}+x^{3+2}+x^{3+4}+x^{3+6}+x^{5+2}+x^{5+4}+x^{5+6}\\ &= x^3+2x^5+3x^7+2x^9+x^{11}.\end{aligned}$$

So, there is 1 configuration of weight 3, 2 configurations of weight 5, 3 configurations of weight 7, 2 configurations of weight 9, and 1 configuration of weight 11. Also, note that $\Phi_S(x)$ factors:

$$\begin{aligned}\Phi_S(x) &= x^{1+2}+x^{1+4}+x^{1+6}+x^{3+2}+x^{3+4}+x^{3+6}+x^{5+2}+x^{5+4}+x^{5+6}\\ &= (x^1+x^3+x^5)(x^2+x^4+x^6).\end{aligned}$$

Now, for any integer $k\geq 0$, let $N_{\geq k}$ be the set of all integers $\geq k$; thus $N_{\geq k} = \{k, k+1, k+2, \ldots\}$, and the weight of a number is its value. Then

$$\begin{aligned}\Phi_{N_{\geq k}}(x) &= x^k + x^{k+1} + x^{k+2} + \cdots\\ &= x^k(1+x+x^2+x^3+\cdots).\end{aligned}$$

In the first example above the generating series is just a polynomial, since S is finite. In the second example, $N_{\geq k}$ is infinite, so the generating series is a "formal power series"; we discuss these in greater detail in the next section.

Theorem 1.6.3. *Let $\Phi_S(x)$ be the generating series for a finite set S with respect to a weight function w. Then,*

(a) $\Phi_S(1) = |S|$,

(b) the sum of the weights of the elements in S is $\Phi'_S(1)$, and

(c) the average weight of an element in S is $\Phi'_S(1)/\Phi_S(1)$.

Proof: Note that

$$\Phi_S(1) = \sum_{\sigma \in S} 1^{w(\sigma)} = |S|,$$

which proves (a). Similarly,

$$\Phi'_S(x) = \sum_{\sigma \in S} w(\sigma) x^{w(\sigma)-1}.$$

Thus,

$$\Phi'_S(1) = \sum_{\sigma \in S} w(\sigma),$$

which proves (b). Finally, (c) follows immediately from (a) and (b). ∎

Consider again the example in which $\mathscr{S}$ is the set of all subsets of $\{1,\ldots,n\}$, and for each set $\sigma \in \mathscr{S}$, we define its weight to be $w(\sigma) = |\sigma|$. By definition, there are $\binom{n}{k}$ elements of $\mathscr{S}$ of weight k. Thus,

$$\Phi_{\mathscr{S}}(x) = \sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n.$$

Now,

$$\Phi_{\mathscr{S}}(1) = (1+1)^n = 2^n.$$

That is, there are 2^n subsets of $\{1,\ldots,n\}$. Now,

$$\Phi'_{\mathscr{S}}(x) = n(1+x)^{n-1},$$

so the sum of the sizes of the subsets of $\{1,\ldots,n\}$ is

$$\Phi'_{\mathscr{S}}(1) = n2^{n-1}.$$

Therefore, the average size of a subset of $\{1,\ldots,n\}$ is

$$\Phi'_{\mathscr{S}}(1)/\Phi_{\mathscr{S}}(1) = n2^{n-1}/2^n = n/2,$$

as expected.

Problem Set 1.6

1. Make a list of all the four-letter "words" that can be formed from the "alphabet" $\{a,b\}$. (There are 16 of them altogether). If the weight of a word is defined to be the number of occurrences of 'ab' in it, determine how many words there are of weight 0, 1 and 2. Determine the generating series.

2. Do the same for five letter words over the same alphabet, but, preferably, without listing all the words separately.

3. Two six–sided dice, one red, one blue, are thrown. Consider all 36 combinations of faces showing. Taking the weight of a throw to be the sum of the spots showing (the usual score, in other words), make a table showing the number of throws of each possible weight.

4. Construct a table, as in problem 3, for the case where the weight of a throw is defined to be the absolute value of the difference between the faces showing.

5. Find the generating series $\Phi_S(x)$ if:

   (a) $S = \{1,2,\ldots\}$ and $w(i) = i$ for all i;

   (b) $S = \{1,2,\ldots\}$ and $w(i) = i$ if i is even, $w(i) = i-1$ if i is odd.

6. If $M(x)$ is the generating series for a finite set S of objects, obtain an expression for the sum of the squares of the weights of the elements of the set S in terms of $M'(1)$ and $M''(1)$.

7. (a) Let s be a subset of $\{1,2,3,4,5\}$. The weight $w(s)$ of s is defined to be the number of pairs of consecutive integers in s. (For example, $\{1,2,4,5\}$ has 2 pairs of consecutive integers, namely $\{1,2\}$ and $\{4,5\}$, so $w(\{1,2,4,5\}) = 2$). Let S be the set of all subsets of $\{1,2,3,4,5\}$. Find the generating series $f(x)$ of S with respect to w.

   (b) Calculate $f(1)$, and justify your answer.

8. A 3 cm by 3 cm piece of cardboard is marked on one side by ruled lines into 9 equal squares. These 1 cm by 1 cm squares are coloured, independently, black or white. The weight of an object is defined to be the number of black squares it possesses. We say 2 objects are the same if one can be obtained from the other simply by rotating the first through $0°, 90°, 180°$ or $270°$. Find the generating series for the set of different objects with respect to this weight, up to and including the quadratic term.

1.7 Formal Power Series

When S is a finite set, $\Phi_S(x)$ is a polynomial. However, we are interested in cases where S is infinite, and there are some subtleties that we address in this section. For example, we implicitly assume that there are only finitely many elements of S of any given weight, so that $\Phi_S(x)$ is well defined.

Let $(a_0, a_1, a_2, \ldots)$ be a sequence of rational numbers; then $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ is called a **formal power series.** We say that a_n is the **coefficient** of x^n in $A(x)$ and write $a_n = [x^n]A(x)$. A formal power series should be regarded as a way of encoding a sequence of numbers. Thus two formal power series are equal if and only if they have the same sequence of coefficients.

In many respects, formal power series behave much like polynomials; for example, addition and multiplication are well defined. If $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ and $B(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ are formal power series then we define

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

and

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

In the case that $A(x)$ and $B(x)$ are polynomials, these definitions are consistent with their familiar usage. Indeed, this is easy to see for addition, and for multiplication

$$\begin{aligned} A(x)B(x) &= \left(\sum_{i\geq 0} a_i x^i \right) \left(\sum_{j\geq 0} b_j x^j \right) \\ &= \sum_{i\geq 0} \sum_{j\geq 0} a_i b_j x^{i+j}, \quad \text{(now, let } k = i \text{ and } n = i + j) \\ &= \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n. \end{aligned}$$

We need to be a bit careful when performing infinite sums and products, but here there is no ambiguity, since there are only finitely many terms contributing to any given coefficient. Thus, $A(x) + B(x)$ and $A(x)B(x)$ are well defined.

In many of the problems that we will encounter, we will need to solve linear equations; given two formal power series $P(x)$ and $Q(x)$ we will want to find a formal power series $A(x)$ such that $Q(x)A(x) = P(x)$. For example, suppose that

$A(x) = a_0 + a_1x + a_2x^2 + \cdots$ where a_n is the number of $\{0,1\}$-strings of length n that do not contain two consecutive ones. Using the techniques that we will develop in Chapter 2, it is straightforward to show that $A(x)$ satisfies the linear equation $(1 - x - x^2)A(x) = 1 + x$.

Problem 1.7.1. *Show that the following equation has a solution and that the solution is unique:*

$$(1 - x - x^2)A(x) = 1 + x. \tag{1.7.1}$$

Solution: We can rewrite Equation 1.7.1 as:

$$a_0 + (a_1 - a_0)x + (a_2 - a_1 - a_0)x^2 + (a_3 - a_2 - a_1)x^3 + \cdots = 1 + x. \tag{1.7.2}$$

Recall that two formal power series are equal if and only if they have the same sequence of coefficients. Therefore, by equating coefficients on either side of Equation 1.7.2, we have equality if and only if:

- $a_0 = 1$,
- $a_1 - a_0 = 1$, and
- for each $n \geq 2$, $a_n - a_{n-1} - a_{n-2} = 0$.

Therefore $a_0 = 1$, $a_1 = 2$, and, for each $n \geq 2$,

$$a_n = a_{n-1} + a_{n-2}.$$

From this *recurrence relation* and the two initial conditions, we can uniquely determine the sequence $\{a_n\}_{n\geq 0}$. Therefore, Equation 1.7.1 has a solution and the solution is unique. ▮

We can extend the method developed in Problem 1.7.1 to solve any linear equation $Q(x)A(x) = P(x)$ so long as the constant term of $Q(x)$ is non-zero.

Theorem 1.7.2. *Let $A(x) = a_0 + a_1x + a_2x^2 + \cdots$, $P(x) = p_0 + p_1x + p_2x^2 + \cdots$, and $Q(x) = 1 - q_1x - q_2x^2 - \cdots$ be formal power series. Then*

$$Q(x)A(x) = P(x)$$

if and only if for each $n \geq 0$,

$$a_n = p_n + q_1a_{n-1} + q_2a_{n-2} + \cdots + q_na_0.$$

Proof: By definition, $Q(x)A(x) = P(x)$ if and only if $[x^n]\,(Q(x)A(x)) = [x^n]P(x)$ for all $n \geq 0$. Now $[x^n]P(x) = p_n$ and

$$[x^n]\,(Q(x)A(x)) = a_n - q_1 a_{n-1} - q_2 a_{n-2} - \cdots - q_n a_0.$$

Therefore $Q(x)A(x) = P(x)$ if and only if, for each $n \geq 0$,

$$a_n - (q_1 a_{n-1} + q_2 a_{n-2} + \cdots + q_n a_0) = p_n.$$

The result follows by a simple rearrangement of this equation. ∎

Corollary 1.7.3. *Let $P(x)$ and $Q(x)$ be formal power series. If the constant term of $Q(x)$ is non-zero, then there is a formal power series $A(x)$ satisfying*

$$Q(x)A(x) = P(x).$$

Moreover, the solution, $A(x)$, is unique.

Proof: If $Q(0) \neq 0$, then, by dividing both $P(x)$ and $Q(x)$ by $Q(0)$, we may assume that $Q(0) = 1$. Then we can write $Q(x) = 1 - q_1 x - q_2 x^2 - \cdots$ and $P(x) = p_0 + p_1 x + p_2 x^2 + \cdots$. Now, by Theorem 1.7.2, $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ satisfies $Q(x)A(x) = P(x)$ if and only if for each $n \geq 0$,

$$a_n = p_n + q_1 a_{n-1} + q_2 a_{n-2} + \cdots + q_n a_0.$$

Thus $a_0 = p_0$ and, for each $n > 0$, we can determine a_n uniquely from $a_0, \ldots, a_{n-1}$. So a solution exists and it is unique. ∎

Definition 1.7.4. *We say that $B(x)$ is the* **inverse** *of $A(x)$ if*

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

we denote this by $B(x) = A(x)^{-1}$ or by $B(x) = \frac{1}{A(x)}$.

Problem 1.7.5. *Show that the inverse of $1 - x$ is*

$$1 + x + x^2 + x^3 + \cdots$$

Solution: Note that

$$(1 - x)(1 + x + x^2 + \cdots) = (1 + x + x^2 + \cdots) - (x + x^2 + x^3 + \cdots) = 1,$$

as required. ∎

The formal power series $1+x+x^2+\cdots$ arises frequently, since it is the generating series for the non-negative integers. We call this a **geometric series**. The powers of geometric series arise often in problems that we will face later.

Problem 1.7.6. *Show that*

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

Solution: We prove by induction on k. When $k=1$, $\binom{n+k-1}{k-1} = \binom{n}{0} = 1$. So $(1-x)^{-1} = \sum_{n\geq 0} x^n = \sum_{n\geq 0} \binom{n+1-1}{k-1} x^n$. So the base case holds.

Assume that for some positive integer m, $(1-x)^{-m} = \sum_{n\geq 0} \binom{n+m-1}{m-1} x^n$.

We need to prove the equation for $m+1$. We see that

$$(1-x)^{-(m+1)} = (1-x)^{-m}(1-x)^{-1}.$$

By induction hypothesis, $[x^i](1-x)^{-m} = \binom{i+m-1}{m-1}$. Also, we know that $[x^i](1-x)^{-1} = 1$. Using rules of multiplication of power series, we get

$$[x^n](1-x)^{-(m+1)} = \sum_{i=0}^{n} ([x^i](1-x)^{-m})([x^{n-i}](1-x)^{-1}) = \sum_{i=0}^{n} \binom{i+m-1}{m-1} \cdot 1 = \binom{n+m}{m}$$

where the final step uses Problem 1.5.3. Therefore,

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

The result holds by induction. ∎

This identity is sometimes known as the **negative binomial series**.

Another important set is $S = \{0, 1, \ldots, k\}$. Its generating series is

$$\Phi_S(x) = 1 + x + \cdots + x^k.$$

Note that

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

Thus,

$$\frac{1-x^{k+1}}{1-x} = 1+x+x^2+\cdots+x^k.$$

Problem 1.7.7. *Does x have an inverse?*

Solution: If $B(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ is any formal power series, then

$$xB(x) = b_0 x + b_1 x^2 + b_2 x^3 + \cdots$$

If $B(x)$ were the inverse of x then we would have

$$b_0 x + b_1 x^2 + b_2 x^3 + \cdots = 1 + 0x + 0x^2 + \cdots$$

(Here we have just expanded 1 as a formal power series $1 + 0x + 0x^2 + \cdots$.) This cannot be the case since the series on the left has constant term 0 while the series on the right has constant term 1. So x does not have an inverse. ∎

The following theorem tells us exactly which formal power series have an inverse.

Theorem 1.7.8. *A formal power series has an inverse if and only if it has a non-zero constant term. Moreover, if the constant term is non-zero, then the inverse is unique.*

Proof: Let $Q(x)$ be a formal power series. Then a formal power series $A(x)$ is the inverse of $Q(x)$ if and only if it satisfies the linear equation

$$Q(x)A(x) = 1. \tag{1.7.3}$$

If $Q(0) \neq 0$, then, by Corollary 1.7.3, Equation 1.7.3 has a unique solution. Hence $Q(x)$ has an inverse and it is unique. If $Q(0) = 0$, then the constant term on the right side of Equation 1.7.3 is 1 but the constant term on the left is $Q(0)A(0) = 0$, so there is no solution and, hence, $Q(x)$ does not have an inverse. ∎

As with polynomials, we can also consider the composition of formal power series.

Definition 1.7.9. *The* **composition** *of formal power series $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ and $B(x)$ is defined by*

$$A(B(x)) = a_0 + a_1 B(x) + a_2 (B(x))^2 + \cdots$$

However, unlike for polynomials, this composition operation is not always well defined. Consider, for example, the case that $A(x) = 1 + x + x^2 + \cdots$ and $B(x) = (1 + x)$. Then

$$A(B(x)) \quad = \quad 1 + (1+x) + (1+x)^2 + \cdots.$$

The constant term of the right-hand side has non-zero contributions from an infinite number of terms, so $A(B(x))$ is not a formal power series. The following result shows that $A(B(x))$ is well-defined so long as $B(x)$ has its constant term equal to zero (that is, $B(0) = 0$).

Theorem 1.7.10. *If $A(x)$ and $B(x)$ are formal power series with the constant term of $B(x)$ equal to zero, then $A(B(x))$ is a formal power series.*

Proof: We can write $A(x) = a_0 + a_1x + a_2x^2 + \cdots$ and $B(x) = xC(x)$. Then

$$\begin{aligned} A(B(x)) &= A(xC(x)) \\ &= a_0 + a_1 xC(x) + a_2(xC(x))^2 + \cdots \\ &= a_0 + a_1 xC(x) + a_2 x^2 (C(x))^2 + \cdots \end{aligned}$$

For each $k \geq 0$, note that $a_k x^k (C(x))^k$ is a formal power series (since it is the product of formal power series). Moreover, for each $n < k$, we have $[x^n](a_k x^k (C(x))^k) = 0$. Therefore,

$$\begin{aligned} [x^n]A(B(x)) &= [x^n](a_0 + a_1 xC(x) + a_2 x^2 (C(x))^2 + \cdots) \\ &= [x^n](a_0 + a_1 xC(x) + a_2 x^2 (C(x))^2 + \cdots + a_n x^n (C(x))^n). \end{aligned}$$

Now, $a_0 + a_1 xC(x) + a_2 x^2 (C(x))^2 + \cdots + a_n x^n (C(x))^n$ is a formal power series (since it is a finite sum of formal power series), so $[x^n]A(B(x))$ is well-defined. ∎

We can use the formula for the inverse of $1 - x$ to compute other inverses.

Problem 1.7.11. *Determine the inverse of $1 - x + 2x^2$.*

Solution: Let $P(x) = 1 - x$. Note that $1 - x + 2x^2 = 1 - (x - 2x^2) = P(x - 2x^2)$. In Problem 1.7.5 we showed that

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

Therefore

$$\begin{aligned} (1 - x + 2x^2)^{-1} &= P(x - 2x^2)^{-1} \\ &= 1 + (x - 2x^2) + (x - 2x^2)^2 + \cdots \end{aligned}$$

(We could further simplify this expression, but we only wish to demonstrate the method of computing inverses via composition.) ∎

Problem Set 1.7

1. Find the following coefficients:

   (a) $[x^8](1-x)^{-7}$

   (b) $[x^{10}]x^6(1-2x)^{-5}$

   (c) $[x^8](x^3+5x^4)(1+3x)^6$

   (d) $[x^9]\{(1-4x)^5+(1-3x)^{-2}\}$

   (e) $[x^n](1-2tx)^{-k}$

   (f) $[x^{n+1}]x^k(1-4x)^{-2k}$

   (g) $[x^n]x^k(1-x^2)^{-m}$

   (h) $[x^n]\{(1-x^2)^{-k}+(1-7x^3)^{-k}\}$

2. (a) Write out the first 5 terms and the nth term of the following power series:

   (i) $(1-x)^{-1}$

   (ii) $(1+x)^{-1}$

   (iii) $(1-x)^{-2}$

   (iv) $(1+x)^{-2}$

   (v) $(1-x)^{-3}$

   (vi) $(1+x)^{-3}$

   (b) Determine the appropriate coefficient in each case.

   (i) $[x^8](1-x)^{-1}$,

   (ii) $[x^5](1+x)^{-1}$,

   (iii) $[x^6](1-3x^2)^{-1}$,

   (iv) $[x^{12}](1-x)^{-2}$,

   (v) $[x^9](1+4x^3)^{-3}$,

   (vi) $[x^8](1-2x^3)^{-2}$.

   (c) Write each of the following power series in closed form.

   (i) $1-2x+3x^2-4x^3+5x^4-6x^5+\dots$

   (ii) $1+3x+6x^2+10x^3+15x^4+21x^5+\dots$

   (iii) $1-x^3+x^6-x^9+x^{12}-x^{15}+\dots$

   (iv) $1+2x^2+4x^4+8x^6+16x^8+32x^{10}+\dots$

(v) $1-4x^2+12x^4-32x^6+80x^8-192x^{10}+\dots$

(vi) $1+6x+24x^2+80x^3+240x^4+672x^5+\dots$

3. Show that

   (a) $[x^n](1-2x+x^2)^{-k} = \binom{n+2k-1}{n}$

   (b) $[x^n](1-x-x^2+x^3)^{-k} = \sum_{\substack{i\geq 0 \\ n-i\equiv 0 \pmod 2}} \binom{i+k-1}{i}\binom{\frac{n-i}{2}+k-1}{\frac{n-i}{2}}$

4. (a) Prove that $\frac{1-x^2}{1+x^3} = \frac{1}{1+\frac{x^2}{1-x}}$.

   (b) By expanding each side of the identity in (a) as a power series, and considering the coefficient of x^N, prove that

$$\left|\sum_{k\geq 0}(-1)^k\binom{N-k-1}{N-2k}\right| = \begin{cases} 0 \text{ if } N\equiv 1 \pmod 3 \\ 1 \text{ otherwise.}\end{cases}$$

5. Calculate $[x^n](1+x)^{-2}(1-2x)^{-2}$, and give the simplest expression you can find.

6. Prove that $\sum_{r+s=t}(-1)^r\binom{n+r-1}{r}\binom{m}{s} = \binom{m-n}{t}$.

7. Prove that $\sum_{m=k}^{n}\binom{m}{k} = \binom{n+1}{k+1}$. (Hint: Use the identity $(1-x)^{-1}(1-x)^{-(k+1)} = (1-x)^{-(k+2)}$.)

8. Let S be a set of configurations with weight function w. Show that for any non–negative integer n,

$$[x^n]\frac{\Phi_S(x)}{1-x}$$

   counts the number of configurations in S with weight at most n.

9. Let $A(x)$ and $B(x)$ be formal power series.

   (a) Show that if $A(x)B(x) = 0$, then $A(x) = 0$ or $B(x) = 0$. (Hint: If $A(x)\neq 0$ then we can write $A(x) = x^k\hat{A}(x)$ where $\hat{A}(x)$ has a non–zero constant term.)

   (b) Show that if $A(x)^2 = B(x)^2$, then $A(x) = \pm B(x)$.

1.8 The Sum and Product Lemmas

In this section we show that addition and multiplication of generating series correspond to natural combinatorial constructions.

Theorem 1.8.1 (The Sum Lemma)**.** *Let (A,B) be a partition of a set S. (That is, A and B are disjoint sets whose union is S.) Then,*

$$\Phi_S(x) = \Phi_A(x) + \Phi_B(x).$$

Proof:

$$\begin{aligned}
\Phi_S(x) &= \sum_{\sigma\in S} x^{w(\sigma)} \\
&= \sum_{\sigma\in A} x^{w(\sigma)} + \sum_{\sigma\in B} x^{w(\sigma)} \quad \text{(since } (A,B) \text{ partitions } S) \\
&= \Phi_A(x) + \Phi_B(x),
\end{aligned}$$

as required. ∎

More generally, if A and B are sets where $A\cap B$ need not be empty, then

$$\Phi_{A\cup B}(x) = \Phi_A(x) + \Phi_B(x) - \Phi_{A\cap B}(x).$$

Recall that, given sets A and B, the **cartesian product** of A and B is the set

$$A\times B = \{(a,b) : a\in A,\ b\in B\}.$$

Theorem 1.8.2 (The Product Lemma)**.** *Let A and B be sets of configurations with weight functions α and β respectively. If $w(\sigma) = \alpha(a)+\beta(b)$ for each $\sigma = (a,b)\in A\times B$, then*

$$\Phi_{A\times B}(x) = \Phi_A(x)\Phi_B(x).$$

Proof:

$$\begin{aligned}
\Phi_{A\times B}(x) &= \sum_{\sigma\in A\times B} x^{w(\sigma)} \\
&= \sum_{(a,b)\in A\times B} x^{\alpha(a)+\beta(b)} \quad \text{(since } w(\sigma) = \alpha(a)+\beta(b)) \\
&= \left(\sum_{a\in A} x^{\alpha(a)}\right)\left(\sum_{b\in B} x^{\beta(b)}\right) \\
&= \Phi_A(x)\Phi_B(x),
\end{aligned}$$

as required. ∎

More generally, if $A_1, \dots, A_k$ are sets then $A_1 \times \cdots \times A_k$ denotes the set of all k–tuples $(a_1, a_2, \dots, a_k)$ where $a_i \in A_i$ for all i. Now, suppose that α_i is a weight function for A_i and that w is a weight function for $A_1 \times \cdots \times A_k$. If $w(\sigma) = \alpha_1(a_1) + \cdots + \alpha_k(a_k)$ for each k-tuple $\sigma = (a_1, \dots, a_k)$, then

$$\Phi_{A_1 \times \cdots \times A_k}(x) = \Phi_{A_1}(x) \cdots \Phi_{A_k}(x).$$

We conclude this section with some applications of the Product Lemma.

Problem 1.8.3. *Let k, n be fixed non-negative integers. How many solutions are there to $t_1 + \cdots + t_n = k$, where $t_1, \dots, t_n = 0$ or 1?*

Solution: The solutions are n-tuples $(t_1, \dots, t_n)$ where $t_i \in \{0, 1\}$ for each $i = 1, \dots, n$. So we are dealing with the set $\{0, 1\}^n$. The generating series for the solutions is

$$\begin{aligned} \Phi_{\{0,1\}^n}(x) &= \left(\Phi_{\{0,1\}}(x)\right)^n \\ &= (1 + x)^n \end{aligned}$$

and the number of solutions is

$$[x^k](1 + x)^n = \binom{n}{k}.$$

∎

There is a direct combinatorial way to obtain the solution to Problem 1.8.3. A solution $(t_1, \dots, t_n)$ is a sequence of 0s and 1s of length n containing exactly k ones. The number of ways of choosing which of the k entries is 1, is $\binom{n}{k}$, as expected.

Problem 1.8.4. *Let S be the set of all k-tuples $(a_1, \dots, a_k)$ where each a_i is a non-negative integer. The weight of a k-tuple $\sigma = (a_1, \dots, a_k)$ is defined as $w(\sigma) = a_1 + \cdots + a_k$. Show that $\Phi_S(x) = (1 - x)^{-k}$.*

Solution: Let $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$. Now $S = \mathbb{N}_0 \times \cdots \times \mathbb{N}_0 = \mathbb{N}_0^k$. Then, by the Product Lemma,

$$\Phi_S(x) = \left(\Phi_{\mathbb{N}_0}(x)\right)^k.$$

Now, $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$, so

$$\Phi_{\mathbb{N}_0}(x) = 1 + x + x^2 + \cdots = \frac{1}{1 - x}.$$

Therefore,

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

∎

We have previously proved a formula involving $(1-x)^{-k}$ in Problem 1.7.6. We now give another proof by counting the number of k-tuples in S of weight n.

Theorem 1.8.5. *For any positive integer k,*

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

Proof: Let S_n be the set of all k-tuples $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$ with $a_1 + \cdots + a_k = n$. By Problem 1.8.4,

$$|S_n| = [x^n](1-x)^{-k}.$$

Let T_n denote the set of all binary strings of length $n+k-1$ with $k-1$ 1's. Then we know that

$$|T_n| = \binom{n+k-1}{k-1}.$$

We will establish a bijection between S_n and T_n, and, hence, prove that

$$[x^n](1-x)^{-k} = |S_n| = |T_n| = \binom{n+k-1}{k-1},$$

as required.

We define $f : S_n \to T_n$ as follows: For a k-tuple $A = (a_1, \ldots, a_k)$ in S_n,

$$f(A) = 0^{a_1} 1 0^{a_2} 1 \cdots 1 0^{a_k}$$

where 0^{a_i} represents a_i 0's in a row. Notice that $f(A)$ is a string with exactly $k-1$ 1's, and the length of the string is $a_1 + \cdots + a_k + (k-1) = n+k-1$ (note that $A \in S_n$, hence $a_1 + \cdots + a_k = n$). Therefore $f(A) \in T_n$.

We can easily find the inverse of f: Any binary string in T_n has the form $0^{a_1} 1 0^{a_2} 1 \cdots 1 0^{a_k}$ where $a_1 + \cdots + a_k = n$. So the inverse of f is $f^{-1} : T_n \to S_n$ where $f^{-1}(0^{a_1} 1 0^{a_2} 1 \cdots 1 0^{a_k}) = (a_1, \ldots, a_k)$. This shows that f is a bijection between S_n to T_n. ∎

Problem 1.8.6. *Let $n \in \mathbb{N}_0$. Suppose we have an unlimited supply of Canadian nickels, dimes, quarters, loonies, and toonies. How many ways can we make n cents using these coins?*

Solution: Let $C_k = \{0, k, 2k, 3k, 4k, \ldots\}$. Each collection of coins can be represented by a 5-tuple $(n, d, q, l, t) \in C_5 \times C_{10} \times C_{25} \times C_{100} \times C_{200}$. Let $S = C_5 \times C_{10} \times C_{25} \times C_{100} \times C_{200}$. We define the weight of any 5-tuple in S to be $w(n, d, q, l, t) = n + d + q + l + t$, which represents the value of this collection of coins in cents.

Using the weight function $\alpha_k(a) = a$ for the set C_k, we see that the generating series for C_k is

$$\Phi_{C_k}(x) = 1 + x^k + x^{2k} + x^{3k} + \cdots = \frac{1}{1 - x^k}.$$

Notice that for our set S, the weight function $w(n, d, q, l, t) = \alpha_5(n) + \alpha_{10}(d) + \alpha_{25}(q) + \alpha_{100}(l) + \alpha_{200}(t)$, so we can apply the Product Lemma. The generating series for S is then

$$\begin{aligned}\Phi_S(x) &= \Phi_{C_5}(x) \cdot \Phi_{C_{10}}(x) \cdot \Phi_{C_{25}}(x) \cdot \Phi_{C_{100}}(x) \cdot \Phi_{C_{200}}(x) \\ &= \frac{1}{(1 - x^5)(1 - x^{10})(1 - x^{25})(1 - x^{100})(1 - x^{200})}.\end{aligned}$$

The number of collections that are valued at n cents is then $[x^n]\Phi_S(x)$. ▌

Problem Set 1.8

1. Let A and B be sets of configurations with weight functions α and β respectively. Now define a weight function w on $A \times B$ such that $w(\sigma) = \alpha(a) + 2\beta(b)$ for each $\sigma = (a, b) \in A \times B$. Then,

$$\Phi_{A\times B}(x) = \Phi_A(x)\Phi_B(x^2).$$

2. Extend the sum lemma to any finite number of sets. That is, if $A_1, A_2, \ldots, A_k$ are disjoint sets whose union is S, prove that

$$\Phi_S(x) = \Phi_{A_1}(x) + \Phi_{A_2}(x) + \cdots + \Phi_{A_k}(x)\ .$$

3. Extend the product lemma to any finite number of sets. That is, if $S = B_1 \times B_2 \times \cdots \times B_k$ with weight functions $w_1, \ldots, w_k$ respectively, the elements of S

being k-tuples $\sigma = (b_1, b_2, \ldots, b_k)$ with $b_i \in B_i$ for each i, and if the weight of σ is

$$w(\sigma) = w_1(b_1) + w_2(b_2) + \cdots + w_k(b_k),$$

prove that

$$\Phi_S(x) = \Phi_{B_1}(x)\Phi_{B_2}(x)\cdots\Phi_{B_k}(x).$$

4. (a) Prove that there are $n!$ permutations of n distinct objects ($n! = n(n-1)\cdots 2\cdot 1$), by establishing a 1-1 correspondence between these permutations and $N_n \times N_{n-1} \times \cdots \times N_1$, where $N_i = \{1, 2, \ldots, i\}$, $i \geq 1$.

   (b) Prove that there are $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ subsets of size k in a set of n distinct objects, by establishing a 1-1 correspondence between P_n and $P_k \times P_{n-k} \times B_{n,k}$, where P_i is the set of all permutations of i distinct objects, $i \geq 1$, and $B_{n,k}$ is the set of all k-subsets of a set of n distinct objects.

5. List the set of all formal products of $(1 + x^2 + x^4)^2(1 + x + x^2)^2$ in which the exponents sum to 4.

6. Determine a generating series (as a product of polynomials or power series) for the number of 5-combinations (i.e. collections of 5 elements, where 2 or more may be alike) of the letters M, A, T, H in which M and A can appear any number of times but T and H can appear at most once. Which coefficient in this generating series do we want?

7. (a) Determine a generating series (as a product of polynomials or power series) for the number of different election outcomes in an election for class president if 27 students cast a vote among four candidates. Which coefficient do we want?

   (b) Suppose each student who is a candidate votes for herself or himself. Now what is the generating series and the required coefficient?

   (c) Repeat part (a) under the assumption that no candidate receives a majority of the votes.

8. Find a generating series (again, as a product of polynomials or power series) for the number of integers between 0 and 999,999 which have the sum of their digits equal to r.

Chapter 2

Compositions and Strings

2.1 Compositions of an Integer.

Definition 2.1.1. *For nonnegative integers n and k, a* **composition** *of n with k parts is an ordered list $(c_1, \dots, c_k)$ of positive integers $c_1, \dots, c_k$, such that $c_1 + \cdots + c_k = n$. The positive integers $c_1, \dots, c_k$ are called the* **parts** *of the composition. There is one composition of 0, the* **empty** *composition, which is a composition with 0 parts.*

The compositions of 4 are (4), with 1 part; $(3,1)$, $(2,2)$, $(1,3)$, with 2 parts; $(2,1,1)$, $(1,2,1)$, $(1,1,2)$, with 3 parts; and $(1,1,1,1)$, with 4 parts. Thus these are eight compositions of 4, one with 1 part, three with 2 parts, three with 3 parts, and one with 4 parts.

Let $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ be the set of all positive integers. Then each part of a composition is in $\mathbb{N}$.

Problem 2.1.2. *How many compositions of n are there with k parts, for $n \geq k \geq 1$?*

Solution: We let $S = \mathbb{N}^k$. Then a composition $(c_1, \dots, c_k)$ of n with k parts is an element of S with the restriction that $c_1 + \cdots + c_k = n$. Now let $w(c_1, \dots, c_k) = c_1 + \cdots + c_k$, and $w(c_i) = c_i$ for $c_i \in \mathbb{N}$, $\ i = 1, \dots, k$. Then the compositions of n with k parts are the elements of S of weight n, and we have $w(c_1, \dots, c_k) = w(c_1) + \cdots + w(c_k)$. Thus the generating series for the number of compositions of n with k parts is, from Theorem 1.6,

$$\begin{aligned}
\Phi_S(x) &= \Phi_{\mathbb{N}^k}(x) \\
&= (\Phi_{\mathbb{N}}(x))^k, \text{ from Product Lemma} \\
&= \left(\sum_{i\geq 1} x^i\right)^k \\
&= \left(x(1-x)^{-1}\right)^k, \text{ from geometric series}
\end{aligned}$$

Therefore, the number of compositions of n with k parts is

$$\begin{aligned}
[x^n]x^k(1-x)^{-k} &= [x^{n-k}](1-x)^{-k} \\
&= \binom{n-k+k-1}{k-1} \\
&= \binom{n-1}{k-1}, \text{ for } n \geq k \geq 1.
\end{aligned}$$

Thus there are $\binom{n-1}{k-1}$ compositions of n with k parts, for $n \geq k \geq 1$. ▌

The solution method for Problem 2.1.2 adapts easily to many other problems involving compositions. In general, we will be asking questions in the form of "how many compositions of n has such and such properties?" And the way we are going to answer them is to follow these steps:

1. Find the set S of all compositions that satisfy these properties (without regard for what n is);

2. Find the generating series for S (the weight of a composition is the sum of its parts, so we can apply the Sum and Product Lemmas); and

3. The answer to our question is the coefficient of x^n in $\Phi_S(x)$. Find an explicit formula for this coefficient if possible.

Problem 2.1.3. *How many k-part compositions of n are there in which each part is an odd number?*

Solution: In this case let $S = \mathbb{N}_{odd}^k$, where $\mathbb{N}_{odd} = \{1,3,5,7,\ldots\}$. Then the required compositions are the elements of S of weight n, so the required generating series is

$$\begin{aligned}
\Phi_S(x) &= \Phi_{\mathbb{N}_{odd}^k}(x) \\
&= \left(\Phi_{\mathbb{N}_{odd}}(x)\right)^k, \text{ by Product Lemma} \\
&= \left(\sum_{i\geq 0} x^{2i+1}\right)^k \\
&= (x(1-x^2)^{-1})^k, \text{ by Geometric Series}
\end{aligned}$$

It follows that the number of compositions of the required form is

$$\begin{aligned}
[x^n](x(1-x^2)^{-1})^k &= [x^n]x^k(1-x^2)^{-k} \\
&= [x^{n-k}](1-x^2)^{-k} \\
&= [x^{n-k}]\sum_{i\geq 0}\binom{i+k-1}{k-1}x^{2i}.
\end{aligned}$$

The coefficient is zero if $n-k$ is odd. If $n-k$ is even then the required coefficient occurs for $i=\frac{n-k}{2}$, and is

$$\binom{\frac{n-k}{2}+k-1}{k-1} = \binom{\frac{n+k-2}{2}}{k-1}.$$

Thus this is the number of k-part compositions of n in which each part is odd.

∎

Problem 2.1.4. *How many compositions of n are there with k parts, each part at most 5?*

Solution: In this case let $S=\{1,2,3,4,5\}^k$, and the required compositions are the elements of S of weight n. Thus the required generating series is

$$\begin{aligned}
\Phi_S(x) &= \Phi_{\{1,2,3,4,5\}^k}(x) \\
&= \left(\Phi_{\{1,2,3,4,5\}}(x)\right)^k, \text{ by Product Lemma} \\
&= (x^1+x^2+x^3+x^4+x^5)^k \\
&= \left(x(1-x^5)(1-x)^{-1}\right)^k, \text{ by finite Geometric Sum} \\
&= x^k(1-x^5)^k(1-x)^{-k}.
\end{aligned}$$

Therefore, the number of compositions is

$$\begin{aligned}
[x^n]x^k(1-x^5)^k(1-x)^{-k} &= [x^{n-k}]\sum_{i\geq 0}\binom{k}{i}(-x^5)^i\sum_{j\geq 0}\binom{j+k-1}{k-1}x^j, \\
&= [x^{n-k}]\sum_{i\geq 0}\sum_{j\geq 0}\binom{k}{i}(-1)^i\binom{j+k-1}{k-1}x^{5i+j} \\
&= \sum_{\begin{cases} i\geq 0, j\geq 0 \\ 5i+j=n-k\end{cases}}\binom{k}{i}(-1)^i\binom{j+k-1}{k-1} \\
&= \sum_{i=0}^{\lfloor\frac{n-k}{5}\rfloor}\binom{k}{i}(-1)^i\binom{n-k-5i+k-1}{k-1},
\end{aligned}$$

where $\left\lfloor\frac{n-k}{5}\right\rfloor$ is the "integer part" of $\frac{n-k}{5}$ (we use $j=n-k-5i$, so $j\geq 0$ gives $i\leq\frac{n-k}{5}$). ▌

We also have instances when the number of parts in a composition is not specified.

Problem 2.1.5. *How many compositions of n are there, n ≥ 0?*

Solution: Here we let $S=\cup_{k\geq 0}\mathbb{N}^k$, where the term $k=0$ is the empty composition (of 0). Then the compositions of n are elements of S of weight n, so the generating series is

$$\begin{aligned}
\Phi_S(x) &= \Phi_{\cup_{k\geq 0}\mathbb{N}^k}(x) \\
&= \sum_{k\geq 0}\Phi_{\mathbb{N}^k}(x), \text{ by Sum Lemma} \\
&= \sum_{k\geq 0}(\Phi_{\mathbb{N}}(x))^k, \text{ by Product Lemma} \\
&= \sum_{k\geq 0}\Big(\sum_{i\geq 1}x^i\Big)^k \\
&= \sum_{k\geq 0}\big(x(1-x)^{-1}\big)^k, \text{ by Geometric Series}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{1-x(1-x)^{-1}}, \text{ by Geometric Series}\\
&= \frac{1-x}{1-x-x}, \text{ multiplying by } 1-x \text{ on top and bottom}\\
&= \frac{1-2x+x}{1-2x}\\
&= \left(1+\frac{x}{1-2x}\right).
\end{aligned}
$$

Hence the number of compositions is

$$
\begin{aligned}
[x^n]\left(1+\frac{x}{1-2x}\right) &= [x^n]\left(1+x\sum_{i\geq 0}(2x)^i\right), \text{ by Geometric Series}\\
&= [x^n]\left(1+\sum_{i\geq 0}2^i x^{i+1}\right)\\
&= \begin{cases} 1, & n=0;\\ 2^{n-1}, & n\geq 1\end{cases}
\end{aligned}
$$

(We use $i+1=n$, so $i=n-1$, for $n\geq 1$.) Thus the number of compositions of n is 1 for $n=0$, and 2^{n-1} for $n\geq 1$. ▮

Sometimes the generating series might not give us an explicit formula for the set of compositions that we are counting. But they may give us additional information regarding the structure of these compositions.

Problem 2.1.6. *How many compositions of n are there where each part is odd? (The number of parts is not restricted.)*

Solution: Let $\mathbb{N}_{odd} = \{1,3,5,7,\ldots\}$. The set of all compositions where each part is odd is

$$S = \bigcup_{k\geq 0} \mathbb{N}_{odd}^k.$$

The generating series of $\mathbb{N}_{odd}$ is

$$\Phi_{\mathbb{N}_{odd}}(x) = x + x^3 + x^5 + \cdots = \frac{x}{1-x^2}.$$

By the product lemma, the generating series for compositions with k odd parts is then

$$\Phi_{\mathbb{N}_{odd}^k}(x) = \left(\frac{x}{1-x^2}\right)^k.$$

By the sum lemma, the generating series for our problem is

$$\begin{aligned}\Phi_S(x) &= \sum_{k\geq 0} \Phi_{\mathbb{N}_{odd}^k} \\ &= \sum_{k\geq 0} \left(\frac{x}{1-x^2}\right)^k \\ &= \frac{1}{1-\frac{x}{1-x^2}} \text{ by Geometric Series} \\ &= \frac{1-x^2}{1-x-x^2}.\end{aligned}$$

The answer to our question is $[x^n]\frac{1-x^2}{1-x-x^2}$. ∎

Here we could not use existing tools to figure out an explicit formula for the coefficient of $\frac{1-x^2}{1-x-x^2}$. But let's derive a recurrence based on the method described in Problem 1.7.1. If we let $\Phi_S(x) = \sum_{n\geq 0} a_n x^n$, then we get

$$1-x^2 = (1-x-x^2)\sum_{n\geq 0} a_n x^n = a_0 + (a_1 - a_0)x + \sum_{n\geq 2}(a_n - a_{n-1} - a_{n-2})x^n.$$

By comparing coefficients on both sides, we get

$$a_0 = 1, a_1 = 1, a_2 = 1, a_n = a_{n-1} + a_{n-2} \text{ for } n \geq 3.$$

Other than a_0, the rest are terms in the Fibonacci sequence. So for $n \geq 1$, the number of compositions of n where each part is odd is the n-th term in the Fibonacci sequence.

We will now give a combinatorial proof of the recurrence. Let S_n be the set of all compositions of n where each part is odd. The recurrence $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$ means that $|S_n| = |S_{n-1}| + |S_{n-2}|$. So we can prove the recurrence by finding a bijection between S_n and $S_{n-1} \cup S_{n-2}$. Here is one possible bijection.

Let $f : S_n \to S_{n-1} \cup S_{n-2}$ where for each composition $(a_1, \ldots, a_k) \in S_n$,

$$f(a_1, \ldots, a_k) = \begin{cases} (a_1, \ldots, a_{k-1}) & a_k = 1 \\ (a_1, \ldots, a_{k-1}, a_k - 2) & a_k \geq 3 \end{cases}$$

This means that if the last part is 1, we remove that part to get a composition of $n-1$; if the last part is 3 or more, we subtract 2 from it to get a composition of $n-2$. Either composition still consist of parts that are odd, so they are in S_{n-1} and S_{n-2} respectively.

This bijection is reversible. For the inverse $f^{-1} : S_{n-1} \cup S_{n-2} \to S_n$,

$$f^{-1}(b_1,\ldots,b_l) = \begin{cases} (b_1,\ldots,b_l,1) & b_1+\cdots+b_l = n-1 \\ (b_1,\ldots,b_{l-1},b_l+2) & b_1+\cdots+b_l = n-2 \end{cases}$$

So f is a bijection, and this proves that $|S_n| = |S_{n-1} \cup S_{n-2}| = |S_{n-1}| + |S_{n-2}|$.

One nice consequence of this bijection is that it gives a method to recursively build the set of all possible compositions of n with parts that are odd. Suppose we have built up all such compositions up to $n-1$, we can get all such compositions for n by adding a new part 1 to every composition of $n-1$, and adding 2 to the last part of every composition of $n-2$. Here are some examples:

$$\begin{aligned}
S_3 &= \{(3),(1,1,1)\} \\
S_4 &= \{(3,1),(1,3),(1,1,1,1)\} \\
S_5 &= \{(5),(1,1,3),(3,1,1),(1,3,1),(1,1,1,1,1)\} \\
S_6 &= \{(3,3),(1,5),(1,1,1,3), \\
&\quad (5,1),(1,1,3,1),(3,1,1,1),(1,3,1,1),(1,1,1,1,1,1)\}
\end{aligned}$$

Problem Set 2.1

1. How many compositions of n are there where each part is at most m? (The number of parts is not restricted.)

2. Let k be a fixed integer. How many compositions of n with k parts are there where each part is congruent to 1 modulo 5? Determine an explicit formula.

3. Let n be a non-negative integer. How many compositions of n are there where the i-th part has the same parity as i? For example, compositions of 7 that satisfy this condition are

$$(7),(5,2),(3,4),(1,6),(1,2,1,2,1).$$

4. How many k-tuples $(a_1,\ldots,a_k)$ of positive integers satisfy the inequality $a_1 + \cdots + a_k < n$?

5. Let a_n denote the number of compositions of n. From Problem 2.1.2, we see that $a_n = 2^{n-1}$ for $n \geq 1$. This tells us that for $n \geq 2$, a_n satisfies the recurrence $a_n = 2a_{n-1}$. Give a combinatorial proof of this recurrence.

6. Let n be a non-negative integer, and let S_n be the set of all compositions of n where each part is greater than 1. (The number of parts is not restricted.) Let $a_n = |S_n|$.

   (a) Prove that
   $$a_n = [x^n]\frac{1-x}{1-x-x^2}.$$

   (b) Derive a recurrence that a_n satisfies together with sufficient initial conditions

   (c) Give a combinatorial proof of the recurrence from part (b).

7. Let $n \in \mathbb{N}$. Consider the problem of finding the number of compositions of n with exactly 3 parts (a_1, a_2, a_3) such that $1 \le a_1 < a_2 < a_3$. For example, when $n = 9$, there are three such compositions: $(1,2,6), (1,3,5), (2,3,4)$. Let S be the set of all such compositions, i.e. $S = \{(a_1, a_2, a_3) \mid 1 \le a_1 < a_2 < a_3\}$. We will determine the generating series of S with the help of another set $T = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, which is the set of all compositions with exactly 3 parts.

   (a) Define a bijection $f : S \to T$, and write down its inverse f^{-1}. Illustrate your bijection by determining $f(2,3,9)$ and $f^{-1}(3,1,4)$.

   (b) Let w be the weight function on S where $w(a_1, a_2, a_3) = a_1 + a_2 + a_3$. For each $(b_1, b_2, b_3) \in T$, define a weight $w^*(b_1, b_2, b_3)$ such that $w^*(f(a_1, a_2, a_3)) = w(a_1, a_2, a_3)$ for all $(a_1, a_2, a_3) \in S$.

   (c) Determine the generating series of T with respect to w^*, and explain why this is the same as the generating series of S with respect to w.

2.2 Subsets with Restrictions.

There are many combinatorial problems that can be solved using the product lemma, but frequently one has to recast the problem first in order for it to meet the requirements of the lemma. The next problem is an example of this.

We have already noted that the number of k-subsets (i.e. subsets of size k) of $N_n = \{1, 2, \ldots, n\}$ is $\binom{n}{k}$. Now consider the related problem:

Problem 2.2.1. *How many k-subsets of N_n are there which contain no two consecutive integers?*

(For example, when $n = 6$ and $k = 3$, these subsets are {1,3,5}, {1,3,6}, {1,4,6} and {2,4,6} - considerably less than $\binom{6}{3} = 20$.)

To specify an example of such a subset we can list its elements in increasing order, as above, say as a vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ where $\alpha_1 < \alpha_2 < \cdots < \alpha_k$; but this is not enough. We must also indicate the value of n. (The subsets listed above, for example, could just as well be subsets of N_7 or N_{519}). Accordingly we define a set C_k consisting of elements (α, n) where n is a positive integer and α represents a subset of N_n in the manner just described. For example, when $k = 3$, then $(\{1,3,5\},6)$, $(\{1,4,6\},6)$ and ({1,4,6},13) are all in C_3 (though ({1,3,5},4) and ({2,5,6},10) are not).

Suppose that we let the weight of $\sigma = (\alpha, n)$ be $w(\sigma) = n$. Then Problem 2.2.1 can be rephrased as

Restatement of Problem 2.2.1: How many configurations of weight n are there in C_k?

Thus the required number is $[x^n]\Phi_{C_k}(x)$, and we show how the product lemma can be used to obtain $\Phi_{C_k}(x)$.

For an arbitrary element $\sigma = (\{\alpha_1, \ldots, \alpha_k\}, n)$ in C_k consider the vector of differences $d(\sigma) = (\alpha_1, \alpha_2 - \alpha_1, \ldots, \alpha_k - \alpha_{k-1}, n - \alpha_k)$. Thus for $\sigma = (\{1,3,6\},6)$, we have $d(\sigma) = (1, 3-1, 6-3, 6-6) = (1,2,3,0)$. Note that σ can be uniquely recovered from $d(\sigma)$. In the present example, $\sigma = (\{1, 1+2, 1+2+3\}, 1+2+3+0) = (\{1,3,6\},6)$, and in general, if $d(\sigma) = (d_1, \ldots, d_{k+1})$, then $\sigma = (\{d_1, d_1 + d_2, \ldots, d_1 + \cdots + d_k\},\ d_1 + \cdots + d_{k+1})$. Note that d_1 is any positive integer, d_{k+1} is any non-negative integer, and $d_2, \ldots, d_k$ are positive integers greater than 1. (Since we don't allow any pairs of consecutive integers). Thus there is a 1-1 correspondence, or bijection, between elements of C_k of weight n and solutions to $t_1 + \cdots + t_{k+1} = n$, with $t_1 \geq 1$, $t_{k+1} \geq 0$, $t_2, \ldots, t_k \geq 2$. Thus the required generating series is

$$\Phi_{C_k}(x) = \Phi_{\mathbb{N}}(x)\{\Phi_{N_{\geq 2}}(x)\}^{k-1}\Phi_{N_{\geq 0}}(x)$$

$$= \underbrace{(x + x^2 + \ldots)}_{\substack{\text{Power of } x \text{ gives}\\ \text{smallest element of}\\ \text{subset}}} \quad \underbrace{(x^2 + x^3 + \ldots)^{k-1}}_{\substack{\text{Power of } x \text{ gives}\\ \text{difference between}\\ \text{successive pairs in}\\ \text{subset}}} \quad \underbrace{(1 + x + x^2 + \ldots)}_{\substack{\text{Power of } x \text{ gives}\\ \text{difference between}\\ n \text{ and largest}\\ \text{element in subset}\\ \text{of } N_n}} \qquad (2.2.1)$$

$$= x(1-x)^{-1}x^{2(k-1)}(1-x)^{-(k-1)}(1-x)^{-1}, \text{ by the Geometric series.}$$

Hence the required number is

$$\begin{aligned}[x^n]x^{2k-1}(1-x)^{-(k+1)} &= [x^{n-2k+1}](1-x)^{-(k+1)} \\ &= \binom{n-2k+1+(k+1)-1}{n-2k+1} \\ &= \binom{n-k+1}{n-2k+1} \\ &= \binom{n-k+1}{k}.\end{aligned}$$

To check a special case, we found 4 subsets when $n=6$ and $k=3$ and

$$\binom{n-k+1}{k} = \binom{6-3+1}{3} = \binom{4}{3} = 4,$$

which is the number of subsets predicted by our formula.

This seems like a complicated way to obtain such a simple answer (Q: How does one obtain this formula by a "direct" argument?), but an examination of (2.2.1) allows us to solve any question involving differences of successive elements in subsets. In the following problems let $\alpha = \{\alpha_1, \ldots, \alpha_k\}$ be a subset of N_n with $\alpha_1 < \ldots < \alpha_k$.

Problem 2.2.2. *(The Terquem Problem) How many subsets α of N_n are there, which have size k, and in which $\alpha_i \equiv i \pmod 2$ for $i = 1, \ldots, k$? (i.e. the odd positions in the subset contain odd numbers, and the even positions contain even numbers.)*

Solution: The first element in such a subset must be odd, and the difference between successive pairs must also be odd. The difference between n and the largest element in the subset can be any non-negative integer. Thus we modify (2.2.1) to obtain the required number as

$$\begin{aligned}&[x^n](x+x^3+x^5+\ldots)(x+x^3+x^5+\ldots)^{k-1}(1+x+x^2+\ldots) \\ &\quad = [x^n]x^k(1+x^2+x^4+\ldots)^k(1+x+x^2+\ldots) \\ &\quad = [x^{n-k}](1-x^2)^{-k}(1-x)^{-1} \\ &\quad = [x^{n-k}](1-x^2)^{-k}(1-x^2)^{-1}(1+x) \\ &\quad = [x^{n-k}](1-x^2)^{-(k+1)}(1+x)\end{aligned}$$

$$= [x^{n-k}](1+x)\sum_{i\geq 0}\binom{k+i}{i}x^{2i}$$
$$= [x^{n-k}]\sum_{i\geq 0}\binom{k+i}{i}(x^{2i}+x^{2i+1})$$
$$= \binom{k+i}{i}, \text{ if } n-k = 2i \text{ or } 2i+1 \; .$$

The two cases can be unified by using the notation $\lfloor\frac{n-k}{2}\rfloor$, the "integer part" of $\frac{n-k}{2}$, which is defined to be the greatest integer which is not larger than $\frac{n-k}{2}$. Thus $i = \lfloor\frac{n-k}{2}\rfloor$ both when $n-k = 2i$ and $n-k = 2i+1$. The answer to problem 2.2.2 is therefore $\binom{\lfloor\frac{n-k}{2}\rfloor+k}{\lfloor\frac{n-k}{2}\rfloor}$. When $n = 7$, $k = 3$, the subsets are {1,2,3}, {1,2,5}, {1,2,7}, {1,4,5},{1,4,7}, {1,6,7}, {3,4,5},{3,4,7},{3,6,7}, {5,6,7}, which verifies the formula, since $\lfloor\frac{7-3}{2}\rfloor = 2$, and $\binom{2+3}{2} = \binom{5}{2} = 10$.

Problem 2.2.3. *How many subsets α of N_n are there, which have size k, and in which the difference between successive pairs of elements is at least c, but less than d, where $c < d$? (i.e. $c \leq \alpha_{i+1} - \alpha_i < d$ for $i = 1, \ldots, k-1$).*

Solution: The required generating series, from modifying (2.2.1) is:

$$(x+x^2+\ldots)(x^c+x^{c+1}+\cdots+x^{d-1})^{k-1}(1+x+x^2+\ldots)$$
$$= x(1-x)^{-1}\{(x^c-x^d)(1-x)^{-1}\}^{k-1}(1-x)^{-1} \; ,$$

by summing a partial geometric series. Hence the required number is

$$[x^n]x^{c(k-1)+1}(1-x)^{-(k+1)}(1-x^{d-c})^{k-1}$$
$$= [x^{n-c(k-1)-1}]\textstyle\sum_{i\geq 0}\binom{k+i}{i}x^i\sum_{j\geq 0}(-1)^j\binom{k-1}{j}x^{(d-c)j}$$
$$= \textstyle\sum_{i+(d-c)j=n-c(k-1)-1}(-1)^j\binom{k+i}{i}\binom{k-1}{j} \; .$$

This answer is not as compact as the two previous ones but is still a finite summation with single index j (since i can be determined from j by the restriction relating i and j), and is easier to calculate than actually counting the subsets.

Problem Set 2.2

1. How many subsets of N_n are there with size k? (Note: We know that the answer is $\binom{n}{k}$, so this problem is included to provide a check on our method).

2. How many subsets of N_n are there which have size k, and in which the difference between successive pairs of elements is at least c?

3. How many subsets of N_n are there which have size k, contain no consecutive integers, and in which the i^{th} smallest element is congruent to $i \pmod 5$, for $i = 1, \ldots, k$?

4. Show that the number of subsets α of N_n, of size k, with $\alpha_{i+1} - \alpha_i \geq i+1$ for $i = 1, \ldots, k-1$, is $\binom{n-\binom{k}{2}}{n-\binom{k+1}{2}}$.

5. Show that the number of subsets of N_n, which have size k, and in which the difference between successive pairs of elements is never equal to 2, is
$$\sum_{i=0}^{k-1} \binom{k-1}{i} \binom{n-k-i+1}{n-2i-k}.$$

6. Show that the number of subsets of N_{2m} of size k, in which the difference between *any* pair of elements is never equal to 2, is
$$\sum_{i=0}^{k} \binom{m-i+1}{i} \binom{m-k+i+1}{k-i}.$$
(Hint: Consider the odd elements and even elements separately.)

2.3 Binary Strings

Definition 2.3.1. *A* **binary string** *or* **{0,1}-string** *is a string of* 0*'s and* 1*'s, its* **length** *is the number of occurrences of* 0 *and* 1 *in the string.*

For example, 01101 is a binary string of length five. We will use $\ell(\alpha)$ to denote the length of a string α. There is a single string, ε, of length 0, called the **empty string**. Now there are clearly 2^n binary strings of length n, since there are 2 choices, 0 or 1, for each of the n symbols in a string of length n. In this section, we count the number of binary strings of length n subject to various restrictions. For example, we might consider strings that have no three consecutive ones. Since we will always be interested in the number of strings of a given length, the generating series for strings in this section will all use the length of a string as the weight function. Thus, for a set A of binary strings, we have

$$\Phi_A(x) = \sum_{a \in A} x^{\ell(a)}.$$

We will build up longer binary strings by piecing together short binary strings. If a_1 and a_2 are binary strings, then $a_1 a_2$ is the string formed by **concatenating** a_1 and a_2. For example, if $a_1 = 0100$ and $a_2 = 001$, then $a_1 a_2 = 0100001$. Further, if A and B are sets of binary strings, we define

$$AB = \{ab : a \in A, b \in B\}.$$

We also define

$$\begin{aligned} A^* &= \{\varepsilon\} \cup A \cup AA \cup AAA \cup \cdots \\ &= \{\varepsilon\} \cup A \cup A^2 \cup A^3 \cup \cdots . \end{aligned}$$

So A^* is the set of strings formed by concatenating any number of strings in A. For example, in this notation, the set of all binary strings is given by $\{0,1\}^*$.

For $\{0,1\}$-strings a, b, we say that b is a **substring** of a if $a = cbd$ for some $\{0,1\}$-strings c, d. Our problems will often be expressed in terms of the **blocks** of a binary string, which are maximal nonempty substrings consisting of only 0's or only 1's. For example, the string 00111001 has four blocks: $(00, 111, 00, 1)$.

Problem 2.3.2. *Let a_n be the number of $\{0,1\}$-strings of length n which contain no three consecutive 1's (or, which contain no substring "111"). Prove that*

$$a_n = [x^n]\frac{1+x+x^2}{1-x-x^2-x^3}, \text{ for } n \geq 0.$$

Solution: Let S be the set of $\{0,1\}$-strings with no three consecutive 1's. We will decompose each string by decomposing it after every occurrence of 0. For example, the string $\sigma_1 = 00011010100$ decomposes into $(0,0,0,110,10,10,0)$ and the string $\sigma_2 = 10111001$ decomposes into $(10,1110,0,1)$. This decomposition has two important properties. First, each string is decomposed uniquely. Second, the decomposition does not separate consecutive ones, so a string is in S if and only if no piece in the decomposition contains three consecutive ones. So, just by examining the pieces, we see that S contains σ_1 but not σ_2. When we decompose a string in S, each piece will be in $\{0,10,110\}$, except possibly for the last peice which can be 1 or 11. So we can write S as

$$S = \{0,10,110\}^*\{\varepsilon,1,11\}.$$

Since the length is additive under composition, we can use this expression for S together with the Sum and Product Lemmas to compute $\Phi_S(x)$. Note that

$$\begin{aligned}\Phi_{\{0,10,110\}}(x) &= x + x^2 + x^3, \text{and} \\ \Phi_{\{\varepsilon,1,11\}}(x) &= 1 + x + x^2.\end{aligned}$$

Moreover,

$$\{0,10,110\}^* = \{\varepsilon\} \cup \{0,10,110\} \cup \{0,10,110\}^2 \cup \cdots.$$

So

$$\begin{aligned}\Phi_{\{0,10,110\}^*}(x) &= 1 + \Phi_{\{0,10,110\}}(x) + \left(\Phi_{\{0,10,110\}}(x)\right)^2 + \cdots \\ &= \frac{1}{1 - \Phi_{\{0,10,110\}}(x)}.\end{aligned}$$

Therefore

$$\begin{aligned}\Phi_S(x) &= \frac{1}{1 - \Phi_{\{0,10,110\}}(x)} \Phi_{\{\varepsilon,1,11\}}(x) \\ &= \frac{1 + x + x^2}{1 - x - x^2 - x^3},\end{aligned}$$

as required. ∎

2.4 Unambiguous Expressions

The solution to Problem 2.3.2 glosses over a subtle but important point. We used the Product Lemma to expand $\Phi_{AB}(x)$, but the Product Lemma concerns the expansion of $\Phi_{A\times B}(x)$. The sets $A \times B$ and AB are closely related:

$$AB = \{ab : (a,b) \in A \times B\}.$$

So concatenation defines a map from $A \times B$ to AB. The problem lies in the fact that this map need not be a bijection; that is, there may be distinct pairs (a_1, b_1) and (a_2, b_2) in $A \times B$ with $a_1 b_1 = a_2 b_2$. Moreover, when this happens, we will not have $\Phi_{AB}(x) = \Phi_A(x)\Phi_B(x)$. For example, if $A = \{0, 01\}$ and $B = \{0, 10\}$, then $A \times B = \{(0,0), (0,10), (01,0), (01,10)\}$ and $AB = \{00, 010, 0110\}$. So $\Phi_{AB}(x) = x^2 + x^3 + x^4$ whereas $\Phi_A(x)\Phi_B(x) = \Phi_{A\times B}(x) = x^2 + 2x^3 + x^4$. The problem here is that the string 010 was created by concatenating two distinct pairs, $(0,10)$ and $(01,0)$, in $A \times B$.

We say that the expression AB is **ambiguous** if there exist distinct pairs (a_1, b_1) and (a_2, b_2) in $A \times B$ with $a_1 b_1 = a_2 b_2$ —otherwise we say that AB is an **unambiguous expression**. In other words, AB is unambiguous if each string uniquely decomposes into a string in A concatenated with a string in B. Note that if A and B are finite sets, then AB is unambiguous if and only if $|AB| = |A \times B|$.

We will use similar terminology for other constructions of binary strings. For example, the expression $A \cup B$ is unambiguous when $A \cap B = \emptyset$. More generally, we will compose expressions for sets of strings using concatenation and union of smaller sets; such an expression is unambiguous when each concatenation operation and each union operation is unambiguous. Thus A^* is unambiguous if the sets $\{\varepsilon\}, A, A^2, \ldots$ are disjoint and, for each $i \in N_{\geq 0}$, A^i is unambiguous.

It is important to note that it is the description of the set of strings using sum, concatenation and the $*$-operation which might be ambiguous. A set of strings itself is never ambiguous or unambiguous.

2.5 Some Decomposition Rules

Let's return briefly to the solution of Problem 2.3.2. We expressed the set S as

$$\{0, 10, 110\}^* \{\varepsilon, 1, 11\}.$$

It is not difficult to show directly that this expression is unambiguous, however, the reason that it is unambiguous is implicit in our solution. We considered the decomposition of a binary string into a sequence of substrings, obtained by breaking the string after each occurrence of 0. The expression above is generating the pieces of that decomposition. Since the decomposition rule is unambiguous, the expression is unambiguous.

Here are some of the common decomposition rules for the set S of all binary strings.

- Decompose a string after each 0 or 1. Each piece in the decomposition will be either 0 or 1. This gives rise to the expression
$$S = \{0,1\}^*.$$
- Decompose a string after each occurrence of 0. Each piece in the decomposition will be from $\{0,10,110,\ldots\} = \{1\}^*\{0\}$ except possibly for the last piece which may consist only of 1s. This gives rise to the expression
$$S = (\{1\}^*\{0\})^*\{1\}^*.$$
- Decompose a string after each block of 0s. Each piece in the decomposition, except possibly the first and last pieces, will consist of a block of 1s followed by a block of 0s. The first piece may consist only of a block of 0s and the last piece may consist only of a block of 1s. This gives rise to the expression
$$S = \{0\}^*(\{1\}\{1\}^*\{0\}\{0\}^*)^*\{1\}^*.$$

Moreover, since each of these decomposition rules is unambiguous, the corresponding expressions are unambiguous.

2.6 Sum and Product Rules for Strings

If A and B are sets of strings and $A \cap B = \emptyset$, then
$$\Phi_{A\cup B}(x) = \Phi_A(x) + \Phi_B(x),$$
as we would hope. We also have the following.

Theorem 2.6.1. *Let A, B be sets of $\{0,1\}$-strings.*

(a) If the expression AB is unambiguous, then
$$\Phi_{AB}(x) = \Phi_A(x)\Phi_B(x).$$

(b) If the expression A^* is unambiguous, then
$$\Phi_{A^*}(x) = (1 - \Phi_A(x))^{-1}.$$

Proof:

(a)

$$\begin{aligned}\Phi_{AB}(x) &= \sum_{s\in AB} x^{\ell(s)}\\ &= \sum_{a\in A}\sum_{b\in B} x^{\ell(ab)}\end{aligned}$$

since $s = ab$ for unique $a \in A,\ b \in B$. But length (ab) = length (a)+ length (b) for all $\{0,1\}$-strings a, b, so

$$\begin{aligned}\Phi_{AB}(x) &= \sum_{a\in A}\sum_{b\in B} x^{\ell(a)+\ell(b)}\\ &= \sum_{a\in A} x^{\ell(a)} \sum_{b\in B} x^{\ell(b)}\\ &= \Phi_A(x)\Phi_B(x).\end{aligned}$$

(b)

$$\Phi_{A^*}(x) = \sum_{k\geq 0} \Phi_{A^k}(x),$$

by the Sum Lemma, since A^* is unambiguous. Note that $\varepsilon \notin A$, so the constant term of $\Phi_A(x)$ is 0. Now $\Phi_{A^k}(x) = (\Phi_A(x))^k$ from part (a), so

$$\Phi_{A^*}(x) = \sum_{k\geq 0} (\Phi_A(x))^k = (1-\Phi_A(x))^{-1}$$

by Geometric Series.

∎

2.7 Decomposition Using Blocks

The following problems involve considering strings subject to a condition on their blocks.

Problem 2.7.1. *Let b_n be the number of $\{0,1\}$-strings of length n in which no block has length exactly two. Prove that*

$$b_n = [x^n]\frac{1-x^2+x^3}{1-2x+x^2-x^3},\quad n \geq 0.$$

Solution: Let $\mathscr{B}$ be the set of all $\{0,1\}$-strings in which no block has length exactly two. Consider decomposing a string after each block of 1s. Except possibly for the first and last piece, each piece has the form

$$\{0,000,0000,\cdots\}\{1,111,1111,\cdots\}.$$

The first piece may consist only of 1s and the last piece may consist only of 0s. This gives the expression

$$\mathscr{B}=\{\varepsilon,1,111,1111,\cdots\}(\{0,000,0000,\cdots\}\{1,111,1111,\cdots\})^*\{\varepsilon,0,000,0000,\cdots\}.$$

Moreover, since the decomposition rule is unambiguous, the expression is unambiguous. So

$$\begin{aligned}
\Phi_{\mathscr{B}}(x) &= \frac{(1+x+x^3+x^4+\cdots)^2}{1-(x+x^3+x^4+\cdots)^2}\\
&= \frac{(1+x+\frac{x^3}{1-x})^2}{1-(x+\frac{x^3}{1-x})^2}, \text{ by geometric series}\\
&= \frac{1+x+\frac{x^3}{1-x}}{1-(x+\frac{x^3}{1-x})}, \text{ since } \frac{(1+A)^2}{1-A^2}=\frac{1+A}{1-A}\\
&= \frac{1-x^2+x^3}{1-2x+x^2-x^3}, \text{ multiplying top and bottom by } 1-x.
\end{aligned}$$

Now $b_n=[x^n]\Phi_{\mathscr{B}}(x)$, and the result follows. ∎

Problem 2.7.2. *Find the generating series with respect to length for* $\{0,1\}$*-strings in which an odd block of 0's is never followed by an odd block of 1's.*

Solution: Let S be the set of all $\{0,1\}$-strings in which an odd block of "0"s is never followed by an odd block of "1"s. We decompose a binary string after each block of 1s, so a string has the required property if and only if each of the pieces has. Decomposing all $\{0,1\}$-strings in this way gives rise to the unambiguous expression

$$\{0,1\}^*=\{1\}^*(\{0\}\{0\}^*\{1\}\{1\}^*)^*\{0\}^*.$$

We are excluding pieces of the form $\{0\}\{00\}^*\{1\}\{11\}^*$. So

$$S=\{1\}^*M^*\{0\}^*$$

where

$$M = \{0\}\{0\}^*\{1\}\{1\}^* \setminus \{0\}\{00\}^*\{1\}\{11\}^*.$$

Thus

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

and the required generating series is

$$\begin{aligned}\Phi_{1^*M^*0^*} &= \frac{1}{1-x}\left(1-\frac{x^3(2+x)}{(1-x^2)^2}\right)^{-1}\frac{1}{1-x}\\ &= \frac{(1+x)^2}{1-2x^2(1+x)}\,.\end{aligned}$$

∎

2.8 Recursive Decompositions of Binary Strings

Another type of decomposition that is often useful is a **recursive** decomposition, in which a set is decomposed in terms of itself. For example, let S be the set of all $\{0,1\}$-strings. We can define S in the following way.

(i) The empty string is in S.

(ii) Any other element of S consists of a symbol (either 0 or 1) followed by an element of S.

Such a definition, in which the set S is defined in terms of itself, is called a **recursive definition**. This leads immediately to the recursive decomposition

$$S = \{\varepsilon\} \cup \{0,1\}S.$$

Here the right side gives an unambiguous expression for S and so from this we obtain

$$\Phi_S(x) = 1 + \Phi_{\{0,1\}}(x)\Phi_S(x).$$

Solving for $\Phi_S(x)$ gives

$$\left(1-\Phi_{\{0,1\}}(x)\right)\Phi_S(x) = 1,$$

so

$$\Phi_S(x) = \left(1 - \Phi_{\{0,1\}}(x)\right)^{-1} = (1-2x)^{-1} = \sum_{n\geq 0} 2^n x^n,$$

as expected (since there are 2^n binary strings of length n).

Below we give a different solution to Problem 2.3.2 based on a recursive decomposition; we restate the problem here for convenience.

Problem 2.8.1. *Let a_n be the number of $\{0,1\}$-strings of length n which contain no three consecutive 1's. Prove that*

$$a_n = [x^n]\frac{1+x+x^2}{1-x-x^2-x^3}, \textit{ for } n \geq 0.$$

Solution: Let S be the set of all $\{0,1\}$-strings that do not contain three consecutive 1s. Consider decomposing a string after the first occurrence of 0. The strings $\{\varepsilon, 1, 11\}$ are indecomposable. Every other string $\sigma \in S$ can be written as $\sigma = \sigma_1\sigma_2$ where $\sigma_1 \in \{0, 10, 110\}$ and $\sigma_2 \in S$. This gives rise to the expression

$$S = \{\epsilon, 1, 11\} \cup \{0, 10, 110\}S.$$

Moreover the right hand side is an unambiguous expression, so

$$\Phi_S(x) = (1 + x + x^2) + (x + x^2 + x^3)\Phi_S(x).$$

Solving this gives

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

Hence $a_n = [x^n]\frac{1+x+x^2}{1-x-x^2-x^3}$, as required. ∎

In the previous problem we forbade the substring 111. The technique used does not adapt well to more complicated forbidden substrings, but such problems can be handled using the method outlined in the following two problems.

Problem 2.8.2. *Let L denote the set of binary strings which do not contain 11010 as a substring. Find the generating series for L.*

Solution: Let M be the set of binary strings that contain exactly one copy of 11010, at their right end or (in other words) as a suffix. We have two equations:

$$\{\varepsilon\} \cup L\{0,1\} = L \cup M,$$
$$L\{11010\} = M.$$

For the first equation, if we append a bit to ε or a string in L, the resulting string is either in L or M, which shows that $\{\varepsilon\} \cup L\{0,1\} \subseteq L \cup M$. To show the other inclusion, let $\alpha \in L \cup M$. If $\alpha \in L$, then α is either the empty string, or we can remove the last bit to obtain another string in L, so $\alpha \in L\{0,1\}$. If $\alpha \in M$, then by removing the last bit from α, it destroys the only copy of 11010 in α. The remaining string is in L, so $\alpha \in L\{0,1\}$ as well. This shows that $\{\varepsilon\} \cup L\{0,1\} \supseteq L \cup M$, hence equality holds.

For the second equation, it should be clear that if $\alpha \in M$, then $\alpha \in L\{11010\}$, which shows that $L\{11010\} \supseteq M$. On the other hand, if $\alpha \in L$, then $\alpha 11010$ certainly contains 11010 as a substring, but it takes a little effort to verify that it does not contain a second occurrence of 11010. Since α does not contain 11010, a second copy of 11010 would have to use some digits from the end of α and some digits from the start of the appended sequence 11010. We can consider cases depending upon the size of the overlap of the two copies of 11010.

- Overlap in 1 digit: $\begin{pmatrix} \cdots & * & * & * & * & 1 & 1 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 0 & * & * & * & * \end{pmatrix}$. This cannot happen, since $1 \neq 0$.
- Overlap in 2 digits: $\begin{pmatrix} \cdots & * & * & * & 1 & 1 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 0 & * & * & * \end{pmatrix}$. This cannot happen, since $11 \neq 10$.
- Overlap in 3 digits: $\begin{pmatrix} \cdots & * & * & 1 & 1 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 0 & * & * \end{pmatrix}$. This cannot happen, since $110 \neq 010$.
- Overlap in 4 digits: $\begin{pmatrix} \cdots & * & 1 & 1 & 0 & 1 & 0 \\ & 1 & 1 & 0 & 1 & 0 & * \end{pmatrix}$. This cannot happen, since $1101 \neq 1010$.

This shows that $L\{11010\} \subseteq M$, hence the second equation holds.

If we convert our two equations to generating series, we get

$$\begin{aligned} 1 + \Phi_L(x)\Phi_{\{0,1\}}(x) &= \Phi_L(x) + \Phi_M(x) \\ \Phi_L(x)\Phi_{\{11001\}}(x) &= \Phi_M(x). \end{aligned}$$

Consequently

$$\begin{aligned} 1 + 2x\Phi_L(x) &= \Phi_L(x) + \Phi_M(x) \\ x^5\Phi_L(x) &= \Phi_M(x). \end{aligned}$$

Substituting the second equation into the first equation gives

$$1 + 2x\Phi_L(x) = \Phi_L(x) + x^5\Phi_L(x).$$

Therefore

$$\Phi_L(x) = \frac{1}{1-2x+x^5}.$$

∎

Problem 2.8.3. *Let L denote the set of binary strings which do not contain 1010 as a substring. Find the generating series for L.*

Solution: Let M be the set of binary strings that contain exactly one copy of 1010, at their right end. We have two equations:

$$\begin{aligned} \{\varepsilon\} \cup L\{0,1\} &= L \cup M, \\ L\{1010\} &= M \cup M\{10\}. \end{aligned}$$

The argument to establish the first equation is similar to the case in Problem 2.8.2. For the second equation, it should be clear that $L\{1010\} \supseteq M \cup M\{10\}$. On the other hand, if $\alpha \in L$, then $\alpha 1010$ certainly contains 1010 as a substring, but it can contain two copies. For example, $0110010 \in L$ and 01100101010 contains a second copy of 1010 as shown: 01100(1010)10. More generally, if $\alpha \in L$ and $\alpha 1010$ contains two copies of 0101, then $\alpha 1010$ ends with 101010 and if we drop the last 10 we get a string in M.

If we convert our two equations to generating series, we get

$$\begin{aligned} 1 + \Phi_L(x)\Phi_{\{0,1\}}(x) &= \Phi_L(x) + \Phi_M(x) \\ \Phi_L(x)\Phi_{\{1001\}}(x) &= \Phi_M(x) + \Phi_M(x)\Phi_{\{10\}}. \end{aligned}$$

Consequently

$$\begin{aligned} 1 + 2x\Phi_L(x) &= \Phi_L(x) + \Phi_M(x) \\ x^4\Phi_L(x) &= \Phi_M(x) + x^2\Phi_M(x). \end{aligned}$$

From the second equation here

$$\Phi_M(x) = \frac{x^4}{1+x^2}\Phi_L(x)$$

and if we substitute this into the first equation, we have

$$\begin{aligned} 1 &= \Phi_L(x) - 2x\Phi_L(x) + \Phi_M(x) \\ &= \left(1 - 2x + \frac{x^4}{1+x^2}\right)\Phi_L(x) \end{aligned}$$

and therefore

$$\Phi_L(x) = \frac{1}{1 - 2x + \frac{x^4}{1+x^2}}.$$

∎

Problem Set 2.8

1. Let $A = \{10, 101\}$ and $B = \{001, 100, 1001\}$.

   (a) Is AB an unambiguous expression? Find the generating series for AB with respect to length.

   (b) Is BA an unambiguous expression? Find the generating series for BA with respect to length.

2. Let $A = \{00, 101, 11\}$ and $B = \{00, 001, 10, 110\}$. Prove that A^* is unambiguous, and that the B^* is ambiguous. Find the generating series for A^* with respect to length.

3. For each of the following sets, write an unambiguous expression generating the set of strings.

   (a) The $\{0,1\}$-strings that have no substring of 0s with length 3, and no substring of 1s of length 2.

   (b) The $\{0,1\}$-strings that have no block of 0s of size 3, and no block of 1s of size 2.

   (c) The set of $\{0,1\}$-strings in which the substring 011 does not occur.

   (d) The set of $\{0,1\}$-strings in which the substring 0110 does not occur.

   (e) The set of $\{0,1\}$-strings where the 0-blocks have even lengths and the 1-blocks have odd lengths.

(f) The set of all $\{0,1\}$-strings where each odd-length block of 0s is followed by a non-empty even block of 1s and each even-length block of 0s is followed by an odd-length block of 1s.

4. Let $S = \{0\}^* \left(\{1\}\{11\}^*\{00\}\{00\}^* \cup \{11\}\{11\}^*\{0\}\{00\}^*\right)^*$.

   (a) Describe in words the strings that belong to S.

   (b) Find the generating series for S.

   (c) Let b_n equal the number of strings in S with length n. Establish a recurrence relation with sufficient initial conditions to uniquely determine the values b_n.

5. (a) Show that the generating series by length for binary strings in which every block of 0's has length at least 2 and every block of 1's has length at least 3, is
$$\frac{(1-x+x^3)(1-x+x^2)}{1-2x+x^2-x^5}.$$

   (b) Obtain a recurrence relation for the coefficients in this generating series.

6. (a) Let a_n be the number of $\{0,1\}$-strings of length n such that each even block of 0's is followed by exactly one 1 and each odd block of 0's is followed by exactly two 1's. Show that
$$a_n = [x^n]\frac{1+x}{1-x^2-2x^3}.$$

   (b) Prove that $a_n = a_{n-2} + 2a_{n-3},\ n \geq 3$.

   (c) Find the initial values a_0, a_1, a_2.

7. (a) Let b_n be the number of $\{0,1\}$-strings of length n in which any block of 1's which immediately follows a block of 0's must have length at least as great as the length of the block of 0's. Find $\sum_{n\geq 0} b_n x^n$.

   (b) Prove that $b_n = b_{n-1} + 2b_{n-2} - b_{n-3},\ n \geq 3$.

   (c) Find the initial values b_0, b_1, b_2.

8. Let a_n be the number of $\{0,1\}$-strings of length n in which the substring "0110" does not occur.

(a) Prove that

$$a_n = [x^n]\frac{1+x^3}{1-2x+x^3-x^4},\ n \geq 0.$$

(b) Deduce from (a) a linear recurrence equation for the sequence $\{a_n\}_{n\geq 0}$, and give enough initial conditions so that $\{a_n\}_{n\geq 0}$ is uniquely specified.

9. Find the generating series, with respect to length, for {0,1}-strings in which no block has length greater than m.

10. Find the generating series, with respect to length, for {0,1}-strings in which no block of 0's has length greater than m, and no block of 1's has length greater than k.

11. Show that the generating series by length for the number of binary strings in which the substring 01110 does not occur is

$$\frac{1+x^4}{1-2x+x^4-x^5}.$$

12. (a) Let s_n be the number of $\{0,1\}$-strings of length n in which every block of 0's is followed by a block of 1's of the same parity in length (i.e. a block with an even number of 0's is followed by a block with an even number of 1's, etc.). Determine the generating series $\Phi(x) = \sum_{n\geq 0} s_n x^n$.

    (b) Show that if $n \geq 2$ then $s_n = 2\cdot 3^{\lfloor \frac{n}{2}\rfloor - 1}$.

13. Let A_i be the set of {0,1}-strings with no occurrences of substring "00" whose first symbol is an i, for $i = 0, 1$.

    (a) Show, without determining A_0 or A_1, that

$$\begin{aligned} A_0 &= \{0\}\dot\cup\{0\}A_1 \\ A_1 &= \{1\}\dot\cup\{1\}(A_1\dot\cup A_0). \end{aligned}$$

    (b) Determine $\Phi_{A_0}(x)$ and $\Phi_{A_1}(x)$ using part (a).

    (c) Deduce from (b) that the number of {0,1}-strings with no occurrences of substring "00" is

$$[x^n]\frac{1+x}{1-x-x^2}.$$

14. Let b_n be the number of $\{0,1\}$-strings of length n in which every block of 0's is followed by a block of 1's of the same length. (For example, 111010001110011 and 100000111110011 are strings of length 15 of this kind.)

    (a) Prove that
$$\sum_{n\geq 0} b_n x^n = \frac{1+x}{1-2x^2}.$$

    (b) Evaluate b_n, $n \geq 0$.

2.9 Bivariate Generating Series

In the above problems the weight function is the length of a string, or number of symbols in a string. Thus the appropriate generating series is obtained by writing down (generating) all strings in the required set and *marking* the occurrence of each symbol (0 or 1) by a single power of x. There is no reason why we can't record the number of 0's and 1's separately, say marking each 0 by x, and each 1 by y. Using the decomposition $S = \{0,1\}^*$ for the set of all binary strings, the number of strings with m occurrences of 1 and n occurrences of 0 is:

$$[x^m y^n]\frac{1}{1-(x+y)}.$$

What we have here is a "bivariate" weight function and a bivariate generating series, that is, a series of two variables. We can solve other problems by marking various particular substrings, not just a 0 or 1, and our generating series can have any number of variables. Fortunately the sum and product lemmas extend to this more general setting.

Problem 2.9.1. *Let $B(x,u)$ denote the multivariate generating series where $[x^n u^k]B(x,u)$ counts the number of binary strings with length n and k occurrences of the substring* 001. *Show that*
$$B(x,u) = \frac{1}{1-2x-(u-1)x^3}.$$

Solution: Let S be the set of all $\{0,1\}$-strings. We use the decomposition

$$S = \{1, 01, 001, \ldots\}^*\{0\}^*.$$

This gives

$$\begin{aligned} B(x,u) &= \frac{1}{1-(x+x^2+ux^3+ux^4+\cdots)}(1+x+x^2+\ldots) \\ &= \frac{1}{1-x}\frac{1}{1-\frac{x-x^3}{1-x}-u\frac{x^3}{1-x}} \\ &= \frac{1}{1-2x-(u-1)x^3}, \end{aligned}$$

as required. ∎

Problem 2.9.2. *Let $A(x,y,u)$ denote the multivariate generating series where $[x^m y^n u^k]A(x,y,u)$ counts the number of binary strings with m ones, n zeros, and k blocks. Show that*

$$A(x,y,u) = \frac{(1+(u-1)x)(1+(u-1)y)}{1-x-y-(u^2-1)xy}.$$

Solution: Let S be the set of all $\{0,1\}$-strings. We use the decomposition

$$S = \{\varepsilon,1,11,\ldots\}(\{0,00,\ldots\}\{1,11,\ldots\})^*\{\varepsilon,0,00,\ldots\}.$$

This gives

$$\begin{aligned} A(x,y,u) &= \frac{(1+ux+ux^2+\ldots)(1+uy+uy^2+\ldots)}{1-(uy+uy^2+\cdots)(ux+ux^2+\cdots)} \\ &= \frac{\left(1+\frac{ux}{1-x}\right)\left(1+\frac{uy}{1-y}\right)}{1-\left(\frac{uy}{1-y}\right)\left(\frac{ux}{1-x}\right)} \\ &= \frac{((1-x)+ux)((1-y)+uy)}{(1-x)(1-y)-u^2xy} \\ &= \frac{(1+(u-1)x)(1+(u-1)y)}{1-x-y-(u^2-1)xy}, \end{aligned}$$

as required. ∎

By making appropriate variable substituitions we can extract other interesting generating series. For example, $A(x,y,1)$ gives the generating series where x marks occurrences of 1 and y marks occurrences of 0, and $A(x,x,u)$ gives the generating series where x the length of a string and u marks each block. By Problem 2.9.2,

$$A(x,y,1) = \frac{1}{1-(x+y)}$$

and

$$\begin{aligned}
A(x,x,u) &= \frac{(1+(u-1)x)^2}{1-2x-(u^2-1)x^2} \\
&= \frac{(1+(u-1)x)^2}{(1-(u-1)x)(1+(u-1)x)} \\
&= \frac{1+(u-1)x}{1-(u-1)x}.
\end{aligned}$$

Bivariate generating series are useful for finding averages, using the following result, where “Property P" would be specified in any particular example. We will use $F_u(x,u)$ as an abbreviation for

$$\frac{\partial}{\partial u}F(x,u).$$

Theorem 2.9.3. *Let $\mathscr{R}$ be a set of $\{0,1\}$-strings, and $c_{n,k}$ be the number of strings in $\mathscr{R}$ of length n with k occurrences of property P, $n,k \geq 0$. Let μ_n be the average number of occurrences of property P among the $\{0,1\}$-strings in $\mathscr{R}$ of length n, and let*

$$F(x,u) = \sum_{n\geq 0}\sum_{k\geq 0} c_{n,k}x^n u^k.$$

Then

$$\mu_n = \frac{[x^n]F_u(x,1)}{[x^n]F(x,1)}, \quad n \geq 0.$$

Proof: The total number of strings in $\mathscr{R}$ of length n is $\sum_{k\geq 0} c_{n,k}$. The total number of occurrences of property P is strings of length n is $\sum_{k\geq 0} kc_{n,k}$. Therefore,

$$\mu_n = \frac{N}{D},$$

where $D = \sum_{k\geq 0} c_{n,k}$ and $N = \sum_{k\geq 0} kc_{n,k}$. Now

$$F(x,1) = \sum_{n\geq 0}\sum_{k\geq 0} c_{n,k}x^n,$$

so $D = [x^n]F(x,1)$. Also

$$\frac{\partial}{\partial u}F(x,u) = \sum_{n\geq 0}\sum_{k\geq 0} c_{n,k}x^n k u^{k-1},$$

so

$$F_u(x,1) = \sum_{n\geq 0}\sum_{k\geq 0} k c_{n,k}x^n.$$

Since $N = [x^n]\left(\frac{\partial}{\partial u}F(x,u)\right)|_{u=1}$, the result follows. ▮

Problem 2.9.4. *(a) Let $c_{n,k}$ be the number of $\{0,1\}$-strings of length n with k blocks. Prove that*

$$c_{n,k} = [x^n u^k]\frac{1-x+ux}{1-x-ux}, n,k \geq 0.$$

(b) Let μ_n be the average number of blocks among $\{0,1\}$-strings of length n. Determine μ_n, $n \geq 0$.

Solution: We use the block decomposition

$$\{0,1\}^* = \{0\}^*(\{1\}\{1\}^*\{0\}\{0\}^*)^*\{1\}^*$$

and mark each block by a u. Then

$$F(x,u) = \sum_{n\geq 0}\sum_{k\geq 0} c_{n,k}x^n u^k$$

is the generating series for $\{0,1\}^*$ with x marking length and u marking blocks, so

$$\begin{aligned}
F(x,u) &= \left(1+\frac{ux}{1-x}\right)\left(1-\frac{ux}{1-x}\frac{ux}{1-x}\right)^{-1}\left(1+\frac{ux}{1-x}\right)\\
&= \left(1+\frac{ux}{1-x}\right)^2\left(1-\left(\frac{ux}{1-x}\right)^2\right)^{-1}\\
&= \left(1+\frac{ux}{1-x}\right)^2\left(\left(1-\frac{ux}{1-x}\right)\left(1+\frac{ux}{1-x}\right)\right)^{-1}\\
&= \frac{1+\frac{ux}{1-x}}{1-\frac{ux}{1-x}}\\
&= \frac{1-x+ux}{1-x-ux},
\end{aligned}$$

and so (a) follows.

From Theorem 2.9.3, we have $\mathscr{R} = \{0,1\}^*$, and property P is the occurrence of a block, so
$$\mu_n = \frac{[x^n]F_u(x,1)}{[x^n]F(x,1)}, \quad n \geq 0.$$
Now in this case
$$F(x,1) = \frac{1-x+x}{1-x-x} = \frac{1}{1-2x} = \sum_{i\geq 0}(2x)^i,$$
so $[x^n]F(x,1) = 2^n$, $n \geq 0$. We also have
$$\begin{aligned} F_u(x,u) &= \frac{\partial}{\partial u}\left(\frac{1-x+ux}{1-x-ux}\right) \\ &= \frac{x(1-x-ux)-(-x)(1-x+ux)}{(1-x-ux)^2}, \end{aligned}$$
so
$$\begin{aligned} F_u(x,1) &= \frac{x(1-2x)+x}{(1-2x)^2} \\ &= \frac{x}{1-2x} + \frac{x}{(1-2x)^2} \\ &= x\sum_{i\geq 0}(2x)^i + x\sum_{j\geq 0}\binom{j+1}{j}(2x)^j \\ &= \sum_{i\geq 0}2^i x^{i+1} + \sum_{j\geq 0}(j+1)2^j x^{j+1}. \end{aligned}$$
Thus if $n = 0$ then $[x^n]F_u(x,1) = 0$ and if $n \geq 1$, then
$$[x^n]F_u(x,1) = 2^{n-1} + n2^{n-1} = (n+1)2^{n-1}$$
and so
$$\mu_n = \begin{cases} 0, & n = 0; \\ \frac{n+1}{2}, & n \geq 1. \end{cases}$$
This settles (b). ∎

Problem 2.9.5. *(a) Let $a_{n,k}$ be the number of $\{0,1\}$-strings of length n with k occurrences of* 0011 *as a substring. Prove that*
$$a_{n,k} = [x^n u^k]\{1-2x-(u-1)x^4\}^{-1}.$$

(b) *Let μ_n be the average number of occurrences of* 0011 *as a substring among* $\{0,1\}$*-strings of length n. Determine μ_n, $n \geq 0$.*

Solution: Let

$$F(x,u) = \sum_{n\geq 0}\sum_{k\geq 0} a_{n,k} x^n u^k,$$

the generating series for $\{0,1\}^*$ with x marking length and u marking occurrences of 0011 as a substring. We use the block decomposition

$$\{0,1\}^* = \{1\}^*(\{0\}\{0\}^*\{1\}\{1\}^*)^*\{0\}^*,$$

and note that 0011 occurs as a substring whenever a block of 2 or more 0's is immediately followed by a block of 2 or more 1's. Thus

$$\begin{aligned}
A(x,u) &= \frac{1}{1-x}\left\{1-\left(\frac{x}{1-x}\frac{x}{1-x}-\frac{x^2}{1-x}\frac{x^2}{1-x}+u\frac{x^2}{1-x}\frac{x^2}{1-x}\right)\right\}^{-1}\frac{1}{1-x}\\
&= \{(1-x)^2-(x^2-x^4+ux^4)\}^{-1},\\
&= \{1-2x-(u-1)x^4\}^{-1}.
\end{aligned}$$

This proves (a)

From Theorem 2.9.3 we have

$$\mu_n = \frac{[x^n]F_u(x,1)}{[x^n]F(x,1)}.$$

In this case we have

$$F(x,1) = \frac{1}{1-2x} = \sum_{i\geq 0}(2x)^i,$$

so

$$[x^n]F(x,1) = 2^n, n \geq 0.$$

We also have

$$F_u(x,u) = \frac{-(-x^4)}{(1-2x-(u-1)x^4)^2},$$

so

$$\begin{aligned}
F_u(x,1) &= \frac{x^4}{(1-2x)^2}\\
&= x^4\sum_{j\geq 0}(j+1)(2x)^j\\
&= \sum_{j\geq 0}(j+1)2^j x^{j+4}.
\end{aligned}$$

Thus

$$[x^n]F_u(x,1) = \begin{cases} 0, & n = 0,1,2,3; \\ (n-3)2^{n-4}, & n \geq 4. \end{cases}$$

so

$$\mu_n = \begin{cases} 0, & n = 0,1,2,3, \\ \frac{n-3}{16}, & n \geq 4. \end{cases}$$

∎

Note that, in general,

$$\mu_n \neq [x^n]\left(\frac{F_u(x,1)}{F(x,1)}\right),$$

so be careful to avoid this mistake!

Problem Set 2.9

1. Let $S = N^3_{\geq 0}$. Consider the two weight functions $\omega_1(t_1,t_2,t_3) = t_1 + t_2 + t_3$ and $\omega_2(t_1,t_2,t_3)$ = number of odd numbers among t_1,t_2,t_3. For example, $\omega_1(3,5,6) = 14$ and $\omega_2(3,5,6)$=2 (since 3 and 5 are odd).

   Find the generating series for S with respect to the weight functions ω_1 and ω_2 where we use the variable x to record the ω_1 weight and y to record the ω_2 weight.

2. (a) Let $a_{n,k}$ be the number of binary strings of length n containing exactly k singleton 1's, i.e. blocks consisting of a single 1. Show that

$$\sum_{\substack{n\geq 0\\ k\geq 0}} a_{n,k}x^n t^k = \frac{(1-x)^{-1} + x(t-1)}{1-x-x^2(1-x)^{-1} - x^2(t-1)}.$$

   (b) Hence find the average number of singleton 1's in strings of length n.

3. (a) Show that the number of {0,1}-strings of length n with m occurrences of 01 (for example 01011 has two occurrences of 01) is

$$\binom{n+1}{n-2m}$$

   (b) Show that the average number of occurrences of 01 is $(n-1)/4$, $n \geq 1$.

4. Find the average number of blocks of 1's in a $\{0,1\}$-string of length n.

5. Find the generating series, by numbers of 0's and 1's, for $\{0,1\}$-strings which satisfy both of the following conditions:

   (a) all blocks have odd length, and

   (b) each block of 0's has a different length from the block of 1's which follows it.

6. Find the generating series, with respect to number of 0's and number of 1's, for $\{0,1\}$-strings in which each block of 0's immediately following a block of 1's of length k has length at least k and at most $2k-1$ for all $k \geq 1$.

7. (a) Find the generating series for $\{0,1\}$-strings with respect to length and with respect to numbers of occurrences of "011" as a substring.

   (b) Find the average number of occurrences of "011" as a substring in $\{0,1\}$-strings of length n.

   (c) A gambler offers you the following proposition: First, you give him \$50. Then, you flip a fair coin 100 times. Each time you get a tail immediately followed by two heads, he gives you back \$4. On average, how much money do you win or lose in this game?

8. Let S be the set of all binary strings that do not contain the substring 000.

   (a) Determine a recursive decomposition of the set S.

   (b) Use the recursive decomposition to determine a generating series for S.

9. (a) Prove that the generating series for the number $c(n,k)$ of $\{0,1\}$-strings of length n with k occurrences of a block of 3 0's immediately followed by a block of two 1's is

$$\sum_{k,n\geq 0} c(n,k)x^n u^k = \frac{1}{1-2x+(1-u)x^5(1-x)^2} .$$

   (b) Prove that the average number of occurrences of a block of three 0's immediately followed by a block of 2 1's in $\{0,1\}$-strings of length n is $\frac{1}{128}(n-2)$ for $n > 5$.

10. Let α be a {0,1}-string; α is said to be *simple* if there are no {0,1}-strings u, v, w such that $uw = \alpha = wv$, where w is non-empty, and u, v are not both empty.

    (a) Show that 10100 is simple, but that 10101 is not.

    (b) Let S_α be the set of {0,1}-strings not containing α as a substring. If α is simple, prove that
    $$\{0,1\}^* = S_\alpha\{\alpha S_\alpha\}^*.$$

    (c) If α is simple, of length p, find the number of strings in S_α of length n.

11. The set of all {0,1,2}-strings can be decomposed as
    $$\{0,1,2\}^* = \{0\}^*((\{1,2\}^* - \varepsilon)\{0\}\{0\}^*)^*\{1,2\}^*$$

    (a) Using a similar decomposition, find the generating series by length for {0,1,2}-strings with no “22” substring. (You may assume that the generating series by length for $\{0,1\}^*$ is $(1-2x)^{-1}$.)

    (b) Let a_n be the number of strings from (a) with length n. Find a recurrence relation for a_n.

    (c) Find a formula for a_n by the method of partial fractions.

12. (a) A **Dyck** word in $\{0,1\}^*$ is a string ε or $\sigma_1 \cdots \sigma_{2n}$ such that (i) $\sigma_1 = 0$; (ii) $\sigma_1 + \cdots + \sigma_i \le i/2$ for $i = 1, \ldots, 2n-1$; (iii) $\sigma_1 + \cdots + \sigma_{2n} = n$. Let **D** be the set of all Dyck words. Prove that
    $$\mathbf{D} - \{\varepsilon\} = 0\mathbf{D}1\mathbf{D}$$
    where ε is the empty word.

    (b) Find the number of Dyck words of length $2n$.

Chapter 3

Recurrences, Binary Trees and Sorting

3.1 Coefficients of Rational Functions

Suppose that we have computed that the generating series for the sequence $\{a_n\}_{n\geq 0}$ is

$$\Phi_A(x) = \sum_{n\geq 0} a_n x^n = \frac{1}{(1-2x)(1-3x)}.$$

We show one way we can use this to produce an explicit formula for the terms of the sequence. The first step is to notice that

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

(You would not be expected to guess this, but certainly you can easily check that it is correct.) It follows that

$$\begin{aligned} a_n = [x^n]\Phi_A(x) &= [x^n]\frac{-2}{1-2x} + [x^n]\frac{3}{1-3x} \\ &= (-2)[x^n]\frac{1}{1-2x} + 3[x^n]\frac{1}{1-3x} \\ &= -2^{n+1} + 3^{n+1}. \end{aligned}$$

We will show how we can compute coefficients whenever the generating series is a rational function $\frac{f(x)}{g(x)}$. We may assume that $f(x)$ and $g(x)$ have no common factors. Also, the constant term of $g(x)$ is non-zero, for otherwise this is not a formal power series. This means that we can divide this constant term in the rational function and assume that the constant term of $g(x)$ is 1. We also make the assumption that the rational function is proper, that is, $\deg(f) < \deg(g)$. The case when it is not proper is discussed at the end of this section.

Now using the Fundamental Theorem of Algebra, we can factor $g(x)$ into linear terms

$$g(x) = (1-r_1x)^{e_1}\cdots(1-r_kx)^{e_k} \tag{3.1.1}$$

for distinct complex values $r_1,\ldots,r_k$. (More precisely, $1/r_i$ is a root of $g(x)$ with multiplicity e_i.) We now claim the following: There exist polynomials $P_1(x),\ldots,P_k(x)$ such that

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{(1-r_1x)^{e_1}} + \cdots + \frac{f_k(x)}{(1-r_kx)^{e_k}}$$

where $\deg(f_i(x)) < e_i$. This is an immediate result of the following lemma.

Lemma 3.1.1. *Suppose f and g are polynomials with $\deg(f) < \deg(g)$. If $g(x) = g_1(x)g_2(x)$ where g_1 and g_2 are coprime, then there are polynomials f_1 and f_2 such that $\deg(f_i) < \deg(g_i)$ for $i = 1,2$ and*

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)}.$$

We will give a proof of this lemma later in this section.

Now the coefficient of $\frac{f(x)}{g(x)}$ for $g(x)$ as in equation (3.1.1) can be obtained by summing up the coefficients from k terms:

$$[x^n]\frac{f(x)}{g(x)} = [x^n]\frac{f_1(x)}{(1-r_1x)^{e_1}} + \cdots + [x^n]\frac{f_k(x)}{(1-r_kx)^{e_k}}.$$

The following two lemmas tell us what each such coefficient looks like.

Lemma 3.1.2. *If $f(x)$ is a polynomial of degree less than e, then there exist constants $c_1,\ldots,c_e$ such that*

$$\frac{f(x)}{(1-rx)^e} = \frac{c_1}{1-rx} + \frac{c_2}{(1-rx)^2} + \cdots + \frac{c_e}{(1-rx)^e}.$$

We will give a proof of this lemma later in this section.

Lemma 3.1.3. *If $f(x)$ is a polynomial of degree less than e, then there is a polynomial $P(n)$ with degree less than e such that*

$$[x^n]\frac{f(x)}{(1-rx)^e} = P(n)r^n.$$

Proof: Using Lemma 3.1.2 and the negative binomial theorem, there exist constants $c_1, \ldots, c_e$ such that

$$[x^n]\frac{f(x)}{(1-rx)^e} = [x^n]\sum_{i=1}^{e}\frac{c_i}{(1-rx)^i} = \sum_{i=1}^{e} c_i \binom{n+i-1}{i-1} r^n = P(n)r^n,$$

where we define

$$P(n) = \sum_{i=1}^{e} c_i \binom{n+i-1}{i-1}.$$

Using the definition of the binomial coefficient,

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

The numerator is a product of $i-1$ terms, each containing n. So this is a polynomial in n of degree $i-1$. Therefore, $P(n)$ is a polynomial in n of degree (at most) $e-1$. ∎

Note that if $r = 1$, then the polynomial $P(x)$ will be a constant polynomial.

Combining what we have discussed, we obtain the following main theorem regarding the coefficients of rational functions.

Theorem 3.1.4. *Suppose f and g are polynomials such that* $\deg(f) < \deg(g)$. *If for $i = 1, \ldots, k$ there are complex numbers r_i and positive integers e_i such that*

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

then there are polynomials P_i such that $\deg(P_i) < e_i$ *and*

$$[x^n]\frac{f(x)}{g(x)} = \sum_{i=1}^{k} P_i(n) r_i^n.$$

We now complete the proofs of Lemmas 3.1.1 and 3.1.2, and discuss how to deal with improper rational functions.

Proof of Lemma 3.1.1: Recall that, since g_1 and g_2 are coprime, we can use the extended Euclidean algorithm (or Bezout's Lemma) to find polynomials a_1 and a_2 such that $\deg(a_1) < \deg(g_2)$, $\deg(a_2) < \deg(g_1)$ and

$$a_1(x)g_1(x) + a_2(x)g_2(x) = 1.$$

We now make two divisions: divide $f(x)a_1(x)$ by $g_2(x)$, and divide $f(x)a_2(x)$ by $g_1(x)$. By the Division Algorithm, there exist polynomials q_1, q_2, r_1, r_2 where $\deg(r_1) < \deg(g_1)$ and $\deg(r_2) < \deg(g_2)$ such that

$$f(x)a_1(x) = q_2(x)g_2(x) + r_2(x), \quad \text{and} \quad f(x)a_2(x) = q_1(x)g_1(x) + r_1(x).$$

Therefore,

$$\begin{aligned}
f(x) &= f(x)\Big(a_1(x)g_1(x) \;+\; a_2(x)g_2(x)\Big) \\
&= f(x)a_1(x)g_1(x) \;+\; f(x)a_2(x)g_2(x) \\
&= \Big(q_2(x)g_2(x) + r_2(x)\Big)g_1(x) \;+\; \Big(q_1(x)g_1(x) + r_1(x)\Big)g_2(x) \\
&= \Big(q_2(x)g_2(x)g_1(x) \;+\; r_2(x)g_1(x)\Big) \;+\; \Big(q_1(x)g_1(x)g_2(x) \;+\; r_1(x)g_2(x)\Big) \\
&= \Big(q_2(x) + q_1(x)\Big)g(x) \;+\; r_2(x)g_1(x) \;+\; r_1(x)g_2(x).
\end{aligned}$$

We see that the degree of $r_2(x)g_1(x) + r_1(x)g_2(x)$ is less than $\deg(g)$. Since $\deg(f) < \deg(g)$ by assumption, we must have $q_2(x) + q_1(x) = 0$. Dividing both sides by $g(x)$ gives

$$\frac{f(x)}{g(x)} = \frac{r_2(x)g_1(x)}{g(x)} + \frac{r_1(x)g_2(x)}{g(x)} = \frac{r_2(x)}{g_2(x)} + \frac{r_1(x)}{g_1(x)}.$$

The result follows by setting $f_1(x) = r_1(x)$ and $f_2(x) = r_2(x)$. ∎

Proof of Lemma 3.1.2: Recall from linear algebra that $\mathbb{P}_q$, the set of all polynomials of x of degree at most q, is a vector space. Since $\{1, x, \ldots, x^q\}$ is a basis for $\mathbb{P}_q$, the dimension of $\mathbb{P}_q$ is $q + 1$.

Consider the vector space $\mathbb{P}_{e-1}$. Let $B = \{(1-rx)^{e-1}, (1-rx)^{e-2}, \ldots, 1-rx, 1\}$. Since each polynomial in B has a different degree, B is linearly independent. Since $|B| = \dim \mathbb{P}_{e-1} = e$, B is a basis. Since $\deg(f) < e$, $f \in \mathbb{P}_{e-1}$. So $f(x)$ is a linear combination of polynomials in the basis B, i.e. there exist constants $c_1, \ldots, c_e$ such that $f(x) = c_1(1-rx)^{e-1} + \cdots + c_{e-1}(1-rx) + c_e$. The result follows by dividing both sides by $(1-rx)^e$. ∎

We now discuss the case where the rational function $\frac{f(x)}{g(x)}$ is not proper, i.e. $\deg(f) \geq \deg(g)$. By the division algorithm, there exist polynomials $q(x), r(x)$ where $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$. This means that

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}.$$

The coefficient of $\frac{f(x)}{g(x)}$ is then the sum of the coefficients of $q(x)$ and $\frac{r(x)}{g(x)}$. The coefficient of $q(x)$ is simple to compute, as it is a polynomial. Since $\frac{r(x)}{g(x)}$ is proper, its coefficient can be computed using methods described in this section.

3.2 Solutions to Recurrence Equations

In earlier sections we have met linear recurrences for sequences, when the generating series for the sequence is a rational function.

Theorem 3.2.1. *Let $C(x) = \sum_{n\geq 0} c_n x^n$ where the coefficients c_n satisfy the recurrence*

$$c_n + q_1 c_{n-1} + \cdots + q_k c_{n-k} = 0, \qquad (n \geq k). \tag{3.2.1}$$

If

$$g(x) := 1 + q_1 x + \cdots + q_k x^k,$$

there is a polynomial $f(x)$ with degree less than k such that

$$C(x) = \frac{f(x)}{g(x)}.$$

Proof: From the rule for the coefficients of a product of power series, if $n \geq k$ then

$$c_n + q_1 c_{n-1} + \cdots + q_k c_{n-k} = [x^n](1 + q_1 x + \cdots + q_k x^k)C(x).$$

So $[x^n]g(x)C(x) = 0$ if $n \geq k$ and therefore $g(x)C(x) = f(x)$ for some polynomial $f(x)$ of degree less than k. ▮

The recurrence in Equation 3.2.1 is called a **homogeneous equation** because the right-hand side of the equation is zero. (The term 'homogeneous' was used in the same way in your linear algebra courses.) The polynomial $h(x) = x^k g(x^{-1})$ in this theorem is called the **characteristic polynomial** of the recurrence. Using Theorem 3.1.4 we have at once:

Theorem 3.2.2. *Suppose $(c_n)_{n\geq 0}$ satisfies the recurrence equation (3.2.1). If the characteristic polynomial of this recurrence has root β_i with multiplicity m_i, for $i = 1, \ldots, j$, then the general solution to (3.2.1) is*

$$c_n = P_1(n)\beta_1^n + \cdots + P_j(n)\beta_j^n \tag{3.2.2}$$

where $P_i(n)$ is a polynomial in n with degree less than m_i, and these polynomials are determined by the $c_0, \ldots, c_{k-1}$.

Recall that to find roots of a polynomial, we use the Factor Theorem:: if $F(x)$ is a polynomial and $F(a) = 0$ then $x - a$ is a factor of $F(x)$.

Problem 3.2.3. *Find c_n explicitly, where*

$$c_n - 4c_{n-1} + 5c_{n-2} - 2c_{n-3} = 0, \qquad (n \geq 3)$$

with initial conditions $c_0 = 1, c_1 = 1, c_2 = 2$.

Solution: The characteristic polynomial is

$$x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2)$$

has root $\beta_1 = 1$ with multiplicity $m_1 = 2$, and root $\beta_2 = 2$ with multiplicity $m_2 = 1$. Thus

$$c_n = (A + Bn) \cdot (1)^n + C \cdot 2^n, \quad (n \geq 0)$$

where A, B and C are constants. From the initial conditions, we have

$$\begin{array}{rcrcrcr} 1 & = & A & & & + & C \\ 1 & = & A & + & B & + & 2C \\ 2 & = & A & + & 2B & + & 4C \end{array}$$

and solving this system gives (check this)

$$A = 0, \; B = -1, \; C = 1.$$

Thus, the solution to the recurrence is

$$c_n = 2^n - n, (n \geq 0).$$

∎

Problem 3.2.4. *Find c_n explicitly, where*

$$c_n + 4c_{n-1} - 3c_{n-2} - 18c_{n-3} = 0, \quad (n \geq 3)$$

with initial conditions $c_0 = 0, c_1 = 2, c_2 = 13$.

Solution: The characteristic polynomial

$$x^3+4x^2-3x-18=(x-2)(x+3)^2$$

has root $\beta_1=2$ with multiplicity $m_1=1$, and root $\beta_2=-3$ with multiplicity $m_2=2$. Thus

$$c_n=A\cdot 2^n+(B+Cn)\cdot(-3)^n,(n\geq 0),$$

where A,B,C are constants. From the initial conditions, we have

$$\begin{array}{rcrcrcr} 0 & = & A & + & B & & \\ 2 & = & 2A & - & 3B & - & 3C \\ 13 & = & 4A & + & 9B & + & 18C \end{array}$$

and solving this system gives (check this)

$$A=1,B=-1,C=1.$$

Thus the solution to the recurrence is

$$c_n=2^n+(n-1)(-3)^n,\quad (n\geq 0).$$

$\blacksquare$

Problem 3.2.5. *Let* $a_n=3^n-2^n,\ b_n=3^n+2^n,\ n\geq 0.$ *Find linear homogeneous recurrence equations with initial conditions for*

(a) $c_n=a_n^2.$

(b) $d_n=a_n^2+b_n^2.$

(c) $e_n=a_nb_n.$

(d) $f_n=b_n+5.$

Solution: (a) We have $c_n=9^n-2\cdot 6^n+4^n$, so c_n satisfies the linear recurrence equation with characteristic polynomial

$$(x-9)(x-6)(x-4)=x^3-19x^2+114x-216,$$

and thus a linear recurrence equation for c_n is

$$c_n-19c_{n-1}+114c_{n-2}-216c_{n-3}=0,\qquad n\geq 3.$$

Initial conditions are obtained from the formula for c_n above, which gives $c_0=0,\ c_1=1,\ c_2=25.$

(b) We have $d_n = 2\cdot 9^n + 2\cdot 4^n$, so d_n satisfies the linear recurrence equation with characteristic polynomial

$$(x-9)(x-4) = x^2 - 13x + 36,$$

and thus a linear recurrence equation for d_n is

$$d_n - 13d_{n-1} + 36d_{n-2} = 0, \qquad n \geq 2.$$

Initial conditions are obtained from the formula for d_n above, which gives $d_0 = 4$, $d_1 = 26$.

(c) We have $e_n = 9^n - 4^n$, so e_n satisfies the linear recurrence equation with characteristic polynomial

$$(x-9)(x-4) = x^2 - 13x + 36,$$

and thus a linear recurrence equation for e_n is

$$e_n - 13e_{n-1} + 36e_{n-2} = 0, \qquad n \geq 2.$$

Initial conditions are obtained from the formula for e_n above, which gives $e_0 = 0$, $e_1 = 5$.

(d) We have $f_n = 3^n + 2^n + 5 = 3^n + 2^n + 5\cdot 1^n$, so f_n satisfies the linear recurrence equation with characteristic polynomial

$$(x-3)(x-2)(x-1) = x^3 - 6x^2 + 11x - 6,$$

and thus a linear recurrence equation for f_n is

$$f_n - 6f_{n-1} + 11f_{n-2} - 6f_{n-3} = 0, \qquad n \geq 3.$$

Initial conditions are obtained from the formula for f_n above, which gives $f_0 = 7$, $f_1 = 10$, $f_2 = 18$. ▮

Problem Set 3.2

1. Consider the recurrence equation $c_n = 5c_{n-1} - 3c_{n-2} - 9c_{n-3} = 0$, for $n \geq 3$ with $c_0 = 1$, $c_1 = 1$, $c_2 = 29$.

   (a) Determine c_n explicitly.

(b) What is the asymptotic form for c_n?

2. Find, explicitly, b_n where $b_n - 5b_{n-1} + 8b_{n-2} - 4b_{n-3} = 0$ for $n \geq 3$ with initial conditions $b_0 = 2$, $b_1 = 2$, $b_2 = 0$.

3. Solve the recurrence relation $c_{n+4} = 5c_{n+3} - 9c_{n+2} + 7c_{n+1} - 2c_n = 0$ with initial values $c_0 = 1$, $c_1 = 0$, $c_2 = 1$, $c_3 = 0$.

4. Consider the recurrence $c_n = 5c_{n-1} - 7c_{n-2} + 3c_{n-3}$ with the initial conditions $c_0 = 3,\ c_1 = 8,\ c_2 = 21$.

   (a) Give a formula for c_n.

   (b) Determine the asymptotic behaviour of c_n.

5. Consider the recurrence equation $c_n = 4c_{n-1} - c_{n-2} - 6c_{n-3}$, for $n \geq 3$, with $c_0 = 5$, $c_1 = 0$,$c_2 = 18$.

   (a) Determine c_n explicitly.

   (b) What is the asymptotic form for c_n?

6. Consider the recurrence $c_{n+5} = 5c_{n+4} - 10c_{n+3} + 10c_{n+2} - 5c_{n+1} + c_n$, $n \geq 0$, with $c_0 = 1$, $c_1 = 5$, $c_2 = 15$, $c_3 = 35$, $c_4 = 70$. Determine c_n explicitly, $n \geq 0$.

7. A sequence $\{c_n\}$ of integers is defined by the recurrence $c_n = c_{n-1} + 2c_{n-2}$, for $n \geq 2$, together with the initial conditions $c_0 = c_1 = 1$.

   (a) Show that $c_n = [x^n]\frac{1}{1-x-2x^2}$.

   (b) Deduce that

   $$c_{2n} = [x^{2n}]\frac{1}{2}\left(\frac{1}{1-x-2x^2} + \frac{1}{1+x-2x^2}\right)$$

   and that

   $$\sum_{n\geq 0} c_{2n}x^n = \frac{1-2x}{1-5x+4x^2}$$

   and deduce, or prove otherwise, that $c_{2n} = 5c_{2n-2} - 4c_{2n-4}$ for $n \geq 2$.

   (c) Find a similar equation connecting c_{2n}, c_{2n-4} and c_{2n-8} for $n \geq 2$.

   (d) Obtain an explicit expression for c_n from (a).

3.3 Nonhomogeneous Recurrence Equations

We now wish to determine the sequence $b_0, b_1, \ldots$ satisfying the recurrence

$$b_n + q_1\, b_{n-1} + \ldots + q_k\, b_{n-k} = f(n), \qquad (n \geq k), \tag{3.3.1}$$

where $q_1, \ldots, q_k$ are constants, and $f(n)$ is a specified function of n. To uniquely determine the sequence $b_0, b_1, \ldots$, we would specify the values of $b_0, \ldots, b_{k-1}$ as initial conditions.

Theorem 3.3.1. *Suppose that $a_0, a_1, \ldots$ is a solution to (3.3.1) (*any *solution; without checking the initial conditions). Then the general solution to (3.3.1) is given by*

$$b_n = a_n + c_n, \qquad n \geq 0,$$

where c_n is given by Theorem 3.2.2, and the k constants $b_{11}, \ldots, b_{jm_j}$ in c_n can be chosen to fit the initial conditions for b_n.

Proof: We are given that

$$a_n + q_1 a_{n-1} + \cdots + q_k a_{n-k} = f(n), n \geq k,$$

and subtracting this equation from (3.3.1) above, we obtain

$$(b_n - a_n) + q_1(b_{n-1} - a_{n-1}) + \cdots + q_k(b_{n-k} - a_{n-k}) = 0,\ n \geq k.$$

But this means that $b_n - a_n$ is a solution to the homogeneous recurrence (3.2.1), and the result follows from Theorem 3.2.2. ▌

Problem 3.3.2. *Solve*

$$b_n - 4\, b_{n-1} + 5\, b_{n-2} - 2\, b_{n-3} = 24\,(-1)^n, \qquad n \geq 3, \tag{3.3.2}$$

with initial conditions $b_0 = -1,\ b_1 = -3,\ b_2 = 2$.

Solution: If we suppose that some solution to (3.3.2) has the form $b_n = \alpha(-1)^n$, for some choice of constant α, then substituting $b_n = \alpha(-1)^n$ on the left side of (3.3.2), we obtain

$$\alpha(-1)^n - 4\alpha(-1)^{n-1} + 5\alpha(-1)^{n-2} - 2\alpha(-1)^{n-3} = (1+4+5+2)\alpha(-1)^n = 12\alpha(-1)^n,$$

and from the RHS of (3.3.2), we deduce that $12\alpha = 24$, so $\alpha = 2$, and thus $b_n = 2(-1)^n$ is a solution to (3.3.2). Now, from the solution to Problem (3.2.4) and the result above, we find that the general solution to (3.3.2)is

$$b_n = 2(-1)^n + A + Bn + C \cdot 2^n, \quad n \geq 0,$$

where A, B, C are constants, whose values can be determined from the initial conditions:

$$\begin{aligned} -1 &= 2 + A + 0 \cdot B + C \\ -3 &= -2 + A + B + 2C \\ 2 &= 2 + A + 2B + 4C. \end{aligned}$$

Solving this system gives (check this) $A = -2$, $B = 3$, $C = -1$, so the solution to the recurrence is

$$b_n = 2(-1)^n - 2 + 3n - 2^n, \quad (n \geq 0).$$

▮

It is difficult to specify exactly how one might obtain some solution a_n to a nonhomogeneous recurrence. However, in general, it is useful to consider a family of solutions with unknown constants that could be solved for, like the constant α in Problem 3.3.2. In the following example, the right side is a specific polynomial in n of degree 1, and the family we consider is a general polynomial in n of degree 1. When the right side is a polynomial in n, you should always begin by trying an arbitrary polynomial, starting with one of the same degree, and if that fails, again with a polynomial of higher degree.

Problem 3.3.3. *Solve*

$$b_n + 4b_{n-1} - 3b_{n-2} - 18b_{n-3} = 2n + 1, \quad n \geq 3, \tag{3.3.3}$$

with initial conditions $b_0 = 0$, $b_1 = 27/8$, $b_2 = -67/4$.

Solution: If we suppose that some solution to (3.3.3) has the form $b_n = \alpha n + \gamma$, for some choice of constants α, γ, then substituting $b_n = \alpha n + \gamma$, on the LHS of (3.3.3), we obtain

$$\begin{aligned} &(\alpha n + \gamma) + 4(\alpha(n-1) + \gamma) - 3((\alpha(n-2) + \gamma) - 18((\alpha(n-3) + \gamma) \\ &\qquad = -16\alpha n + 56\alpha - 16\gamma, \end{aligned}$$

and from the RHS of (3.3.3), we deduce that $-16\alpha = 2$ and $56\alpha - 16\gamma = 1$, so $\alpha = -1/8$, $\gamma = -1/2$, and thus $b_n = -(n+4)/8$ is a solution to (3.3.3). Now, from the solution to Problem 3.2.4 and the result above, we have the general solution to (3.3.3) as

$$b_n = -\frac{n+4}{8} + A \cdot 2^n + (B + Cn)(-3)^n, \qquad n \geq 0,$$

where A, B, C are constants, whose values can be determined from the initial conditions:

$$\begin{aligned} 0 &= -\frac{1}{2} + A + B \\ \frac{27}{8} &= -\frac{5}{8} + 2A - 3B - 3C \\ -\frac{67}{4} &= -\frac{3}{4} + 4A + 9B + 18C, \end{aligned}$$

and solving this system gives (check this) $A = 1/2$, $B = 0$, $C = -1$, so the solution to the recurrence is

$$b_n = -\frac{n+4}{8} + 2^{n-1} - n(-3)^n, \qquad (n \geq 0).$$

∎

3.4 Aysmptotics

We say that c_n is **asymptotic** to $g(n)$ as $n \to \infty$, written $c_n \sim g(n)$, if

$$\lim_{n\to\infty} \frac{c_n}{g(n)} = 1.$$

For example, suppose that the roots $\beta_1, \ldots, \beta_j$ in (3.2.2) are all real, and that β_1 has the largest absolute value of $\beta_1, \ldots, \beta_j$. Then

$$\begin{aligned} c_n &= A_1\beta_1^n + A_2\beta_2^n + \cdots + A_j\beta_j^n \\ &= A_1\beta_1^n \left\{1 + \frac{A_2}{A_1}\left(\frac{\beta_2}{\beta_1}\right)^n + \cdots + \frac{A_j}{A_1}\left(\frac{\beta_j}{\beta_1}\right)^n\right\} \end{aligned}$$

where $A_1, A_2, \ldots A_j$ are polynomials in n. Thus

$$\frac{c_n}{A_1\beta_1^n} = 1 + \frac{A_2}{A_1}\left(\frac{\beta_2}{\beta_1}\right)^n + \cdots + \frac{A_j}{A_1}\left(\frac{\beta_j}{\beta_1}\right)^n$$

and

$$\lim_{n\to\infty}\frac{c_n}{A_1\beta_1^n} = 1+0+\cdots+0$$

since $\frac{\beta_2}{\beta_1},\ldots,\frac{\beta_j}{\beta_1}$ all have absolute value less than 1. Thus we have $c_n \sim A_1\beta_1^n$. For a more compact result, here we have

$$A_1 = b_{11} + b_{12}n + \cdots + b_{1m_1}n^{m_1-1}.$$

So, if $b_{1m_1} \neq 0$,

$$\lim_{n\to\infty}\frac{c_n}{b_{1m_1}n^{m_1-1}\beta_1^n} = 1,$$

and we also write

$$c_n \sim b_{1m_1}n^{m_1-1}\beta_1^n.$$

This answers the question, "Roughly how fast does c_n grow as n increases?"

Example 3.4.1. In Problem 3.2.3, with $c_n = 2^n - n$, we have $c_n \sim 2^n$. In Problem 3.2.4, with $c_n = 2^n + (n-1)(-3)^n$, we have $c_n \sim (n-1)(-3)^n$ and $c_n \sim n(-3)^n$.

3.5 Other Recurrence Relations

We have seen that if a generating function $C(x) = \sum_{n\geq 0} c_n x^n$ is a rational function, i.e. the ratio of two polynomials then we can easily deduce a linear homogeneous recurrence equation of fixed order, with constant coefficients, by simply multiplying on both sides of

$$C(x) = \frac{P(x)}{Q(x)}$$

by $Q(x)$. Also we can obtain an exact form for c_n for such generating functions by considering the partial fraction expansion or by repeated use of the binomial theorem. Another method of deducing a recurrence equation is by looking at the derivatives of a generating function.

By way of example, consider $F(x) = \sum_{m\geq 0} f_m x^m = (1-x)^{-k}$. Suppose we have forgotten the binomial theorem and wish to find a recurrence relation for f_n. Now

$$F'(x) = \sum_{n\geq 0} m f_m x^{m-1} = k(1-x)^{-k-1}$$

so $F'(x) = k(1-x)^{-1}F(x)$, or $(1-x)F'(x) = kF(x)$.

Thus $(1-x)\sum_{m\geq 0} m f_m x^{m-1} = k\sum_{m\geq 0} f_m x^m$ and comparing coefficients of x^{n-1} gives, when $n \geq 1$

$$\begin{aligned} n f_n - (n-1) f_{n-1} &= k f_{n-1}, \\ n f_n - (n-1+k) f_{n-1} &= 0. \end{aligned}$$

The initial condition is $f_0 = 1$, since $f_0 = F(0)$.

Conversely, there are situations where instead of being given a generating function and asked to find a recurrence equation for the coefficients, we start with a recurrence equation and are asked to find an explicit form, or generating function, for the coefficients. Such a situation arises naturally in the analysis of algorithms, which are often specified recursively, and thus naturally lead to recurrence equations. Examples are given in Sections 3.8 and 3.9.

Problem Set 3.5

1. (a) For the non-homogeneous recurrence relation

$$\begin{aligned} c_n - 4c_{n-1} + 4c_{n-2} &= 3 \\ c_0 = 4,\ c_1 &= 11, \end{aligned}$$

   determine $\sum_{n\geq 0} c_n x^n$.

   (b) Derive a homogeneous recurrence relation for c_n. Solve to obtain a formula for c_n.

   (c) What is the asymptotic behaviour of c_n?

2. Solve the nonhomogeneous linear recurrence relation

$$b_n - b_{n-1} - 16b_{n-2} - 20b_{n-3} = 36n + 15$$

   having initial conditions $b_0 = 0,\ b_1 = 1,\ b_2 = 12$.

3. Solve the nonhomogeneous linear recurrence relation

$$b_n - 3b_{n-1} + 4b_{n-3} = 3 \cdot 2^n$$

   having initial conditions $b_0 = 3,\ b_1 = 1,\ b_2 = 27$.

3.6 Binary Trees

In this section we count binary trees. A binary tree is either

(a) the empty tree, or

(b) a tree with a fixed root vertex such that each vertex has a left branch and a right branch (either of which may be empty).

Below, for example, we list all binary trees with three vertices.

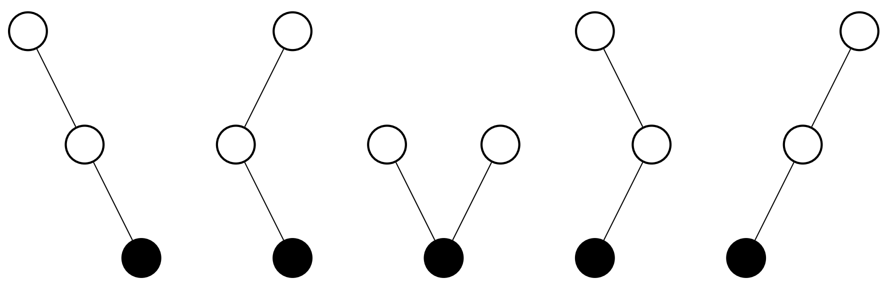


Figure 3.1: Binary trees with three vertices

We let ϵ denote the empty tree and we let $\bullet$ denote the tree with one vertex. Let $\mathscr{T}$ be the set of all binary trees. For a tree $T \in \mathscr{T}$, we let $n(T)$ be the number of vertices in T. We let $T(x)$ denote the generating function for T with respect to the weight function n. Thus $[x^n]T(x)$ is the number of binary trees with n vertices. The following problem detemines $T(x)$ implicitly.

Problem 3.6.1. *Show that*

$$(2xT(x)-1)^2 = 1-4x.$$

Solution: For any binary tree $T \neq \epsilon$, we can decompose T into $(\bullet, T_1, T_2)$, where T_1 and T_2 are, respectively, the left and right branches of the root vertex of T. This decomposition provides a bijection from $\mathscr{T} - \{\epsilon\}$ to $\{\bullet\} \times \mathscr{T} \times \mathscr{T}$. So, with a small abuse of notation, we can write

$$\mathscr{T} = \{\epsilon\} \cup \{\bullet\} \times \mathscr{T} \times \mathscr{T}.$$

Moreover, since $n(T) = 1 + n(T_1) + n(T_2)$, we can apply the Product Lemma to obtain:

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

Now

$$
\begin{aligned}
0 &= 4x\left(xT(x)^2 - T(x) + 1\right) \\
&= 4x^2T(x)^2 - 4xT(x) + 4x \\
&= (2xT(x)-1)^2 + 4x - 1.
\end{aligned}
$$

Therefore

$$(2xT(x)-1)^2 = 1-4x,$$

as required. ∎

Up to this point in the course, our generating series have been determined by linear equations, now we have a quadratic equation to solve. To determine $T(x)$ explicitly, we need to use a result, Lemma 3.7.2, from the next section giving the expansion of $(1-4x)^{\frac{1}{2}}$.

Theorem 3.6.2. *The number of binary trees with $n \geq 0$ vertices is*

$$\frac{1}{n+1}\binom{2n}{n}.$$

Proof: By Problem 3.6.1 and Lemma 3.7.2,

$$
\begin{aligned}
2xT(x) - 1 &= (1-4x)^{\frac{1}{2}} \\
&= \pm\left(2\left(\sum_{n\geq 0}\frac{1}{n+1}\binom{2n}{n}x^{n+1}\right) - 1\right).
\end{aligned}
$$

Considering the constant term reveals the sign, so

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

Hence the number of binary trees with $n \geq 0$ vertices is

$$\frac{1}{n+1}\binom{2n}{n},$$

as required. ∎

The numbers $\frac{1}{n+1}\binom{2n}{n}$ are called the **Catalan numbers**; these arise in many other counting problems.

Problem Set 3.6

1. Let t_n denote the number of binary trees with n edges. Show that, for each $n \geq 1$, we have
$$t_n = t_0 t_{n-1} + t_1 t_{n-2} + \cdots + t_{n-1} t_0.$$

2. Place $2n$ points equally spaced on a circle. A **chord** is a straight line joining two of these points. Let d_n be the number of ways we can place n chords so that no two chords have a point in common (so they do not cross, and they pair up the $2n$ points on the circle). Prove that d_{n+1} is the n-th Catalan number.

3. Show that the number of ways we can fills the entries of a $2 \times n$ matrix with the integers $1, \ldots, 2n$ such that entries increase as we move from right to left along a row, and as we move down a column, is the n-th Catalan number.

4. If C_n is the n-th Catalan number, prove that
$$\lim_{n\to\infty} \frac{C_n}{4^n} \to 0.$$

5. For which values of n is C_n odd?

6. Prove that $\sqrt{1-4x}$ is not a rational function, i.e., there are no polynomials $p(x)$ and $q(x)$ such that
$$\sqrt{1-4x} = \frac{p(x)}{q(x)}.$$
Deduce that the Catalan numbers cannot satisfy a linear recurrence of finite order.

3.7 The Binomial Series

By Theorems 1.5.1 and 1.8.5, we have expansions for $(1+x)^n$ for any integer n. What happens when n is not an integer? Indeed, what do we mean by $(1+x)^{\frac{1}{2}}$? If $B(x)$ is a formal power series such that $B(x)^2 = 1+x$ then we write $B(x) = (1+x)^{\frac{1}{2}}$. This is much the same as our interpretation of an inverse; however, unlike inverses, square–roots are not uniquely determined since $(-B(x))^2 = B(x)^2$. We can extend this interpretation to other rational powers. For example, $(1+x)^{\frac{3}{2}} =$

$\left((1+x)^{\frac{1}{2}}\right)^3$, and $(1+x)^{-\frac{3}{2}}$ is the inverse of $(1+x)^{\frac{3}{2}}$. Similarly, for any rational number a, we can interpret $(1+x)^a$ as a formal power series.

For any real number a and non–negative integer k we define

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

this is called a **binomial coefficient** . It is convenient to extend this definition to all real values of k by defining $\binom{a}{k} = 0$ when $k \not\in \{0, 1, 2, \ldots\}$.

Theorem 3.7.1 (The Binomial Theorem)**.** *For any rational number a,*

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

We will not prove the Binomial Theorem; though, the reader should recognize this, from Calculus, as the MacLaurin series expansion of $(1+x)^a$. In Calculus, we place additional conditions on x since we view power series as functions of x. Here, on the other hand, we do not evaluate formal power series; instead, we are concerned with the sequence of coefficients. Therefore, we need not address questions of convergence.

We show below that the Binomial Theorem is consistent with Theorems 1.5.1 and 1.8.5. First consider the case that $a = n$ for some non–negative integer n. Note that $\binom{n}{k} = 0$ when $n < k$. Thus, by the Binomial Theorem,

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

as expected.

Now consider the case that $a = -n$ for some positive integer n. Thus,

$$\begin{aligned}
\binom{-n}{k} &= \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!} \\
&= (-1)^k \frac{(n+k-1)(n+k-2)\cdots n}{k!} \\
&= (-1)^k \binom{n+k-1}{k} \\
&= (-1)^k \binom{n+k-1}{n-1}.
\end{aligned}$$

Then, by the Binomial Theorem,

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

as expected.

We can use the Binomial Theorem to compute $(1-4x)^{\frac{1}{2}}$, which we needed to enumerate binary trees; see Theorem 3.6.2.

Lemma 3.7.2.

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

Proof: Note that, for $k\geq 1$,

$$\begin{aligned}\binom{\frac{1}{2}}{k} &= \frac{\frac{1}{2}\frac{-1}{2}\cdots(\frac{1}{2}-k+1)}{k!}\\ &= \frac{(-1)^{k-1}(1\cdot 3\cdots(2k-3))}{2^k k!}\\ &= \frac{(-1)^{k-1}(1\cdot 2\cdots(2k-3)\cdot(2k-2))}{2^k k!(2\cdot 4\cdots(2k-2))}\\ &= \frac{(-1)^{k-1}(2k-2)!}{2^k k! 2^{k-1}(1\cdot 2\cdots(k-1))}\\ &= \frac{(-1)^{k-1}(2k-2)!}{2^{2k-1}k!(k-1)!}\\ &= \frac{(-1)^{k-1}}{2^{2k-1}k}\binom{2k-2}{k-1}.\end{aligned}$$

Hence, by the Binomial Theorem,

$$\begin{aligned}(1+x)^{\frac{1}{2}} &= \sum_{k\geq 0}\binom{\frac{1}{2}}{k}x^k\\ (1+x)^{\frac{1}{2}} &= \binom{\frac{1}{2}}{0}+\sum_{k\geq 1}\binom{\frac{1}{2}}{k}x^k\\ &= 1+\sum_{k\geq 1}\frac{(-1)^{k-1}}{2^{2k-1}k}\binom{2k-2}{k-1}x^k,\end{aligned}$$

as required. ∎

Problem Set 3.7

1. Calculate the binomial coefficients:

   (a) $\binom{7}{3}$ (b) $\binom{-2}{4}$ (c) $\binom{-\frac{1}{2}}{3}$ (d) $\binom{\frac{1}{3}}{5}$

   Answers:

   (a) 35 (b) 5 (c) $-\frac{5}{16}$ (d) $\frac{22}{729}$

2. Find the following coefficients:

   (a) $[x^8](1-x)^{-7}$ Answer: 3003

   (b) $[x^{10}]x^6(1-2x)^{-5}$ Answer: 1120

   (c) $[x^8](x^3+5x^4)(1+3x)^6$ Answer: 7533

   (d) $[x^9]\{(1-4x)^5+(1-3x)^{-2}\}$ Answer: 196830

   (e) $[x^n](1-2tx)^{-k}$ Answer: $\binom{n+k-1}{n}(2t)^n$

   (f) $[x^{n+1}]x^k(1-4x)^{-2k}$ Answer: $\binom{n+k}{n+1-k}4^{n+1-k}$

   (g) $[x^n]x^k(1-x^2)^{-m}$ Answer: $\binom{\frac{n-k}{2}+m-1}{\frac{n-k}{2}}$

   (h) $[x^n]\{(1-x^2)^{-k}+(1-7x^3)^{-k}\}$ Answer: $\binom{\frac{n}{2}+k-1}{\frac{n}{2}}+\binom{\frac{n}{3}+k-1}{\frac{n}{3}}7^{\frac{n}{3}}$

3. (a) Write out the first 5 terms and the nth term of the following power series:

   (i) $(1-x)^{-1}$
   (ii) $(1+x)^{-1}$
   (iii) $(1-x)^{-2}$
   (iv) $(1+x)^{-2}$
   (v) $(1-x)^{-3}$
   (vi) $(1+x)^{-3}$

   (b) Determine the appropriate coefficient in each case.

   (i) $[x^8](1-x)^{-1}$, Answer: 1
   (ii) $[x^5](1+x)^{-1}$, Answer: -1
   (iii) $[x^6](1-3x^2)^{-1}$, Answer: 27

(iv) $[x^{12}](1-x)^{-2}$, Answer: 13
(v) $[x^9](1+4x^3)^{-3}$, Answer: -640
(vi) $[x^8](1-2x^3)^{-2}$. Answer: 0

(c) Write each of the following power series in closed form.

(i) $1-2x+3x^2-4x^3+5x^4-6x^5+\dots$
(ii) $1+3x+6x^2+10x^3+15x^4+21x^5+\dots$
(iii) $1-x^3+x^6-x^9+x^{12}-x^{15}+\dots$
(iv) $1+2x^2+4x^4+8x^6+16x^8+32x^{10}+\dots$
(v) $1-4x^2+12x^4-32x^6+80x^8-192x^{10}+\dots$
(vi) $1+6x+24x^2+80x^3+240x^4+672x^5+\dots$

4. The coefficient notation can be extended to series of more than one variable. Thus $[x^n y^k]$ denotes the coefficient of $x^n y^k$ in the expansion of the series that follows.
Find $[x^n y^k]\frac{1}{1-\frac{xy}{1-y}}$. [Hint: Treat y as a constant, and find the coefficient of x^n; then find the coefficient of y^k in the result.]

5. Show that

(a) $[x^n](1-2x+x^2)^{-k} = \binom{n+2k-1}{n}$

(b) $[x^n](1-x-x^2+x^3)^{-k} = \sum_{\substack{i\ge 0\\ n-i\equiv 0 \pmod 2}} \binom{i+k-1}{i}\binom{\frac{n-i}{2}+k-1}{\frac{n-i}{2}}$

6. (a) Prove that $\frac{1-x^2}{1+x^3} = \frac{1}{1+\frac{x^2}{1-x}}$.

(b) By expanding each side of the identity in (a) as a power series, and considering the coefficient of x^N, prove that

$$\left|\sum_{k\ge 0}(-1)^k\binom{N-k-1}{N-2k}\right| = \begin{cases} 0 \text{ if } N\equiv 1 \pmod 3\\ 1 \text{ otherwise.}\end{cases}$$

7. Calculate $[x^n](1+x)^{-2}(1-2x)^{-2}$, and give the simplest expression you can find.

8. Prove that $\sum_{r+s=t}(-1)^r\binom{n+r-1}{r}\binom{m}{s} = \binom{m-n}{t}$.

9. Prove that $\sum_{m=k}^{n}\binom{m}{k} = \binom{n+1}{k+1}$. (Hint: Use the identity $(1-x)^{-1}(1-x)^{-(k+1)} = (1-x)^{-(k+2)}$.)

10. Using the Binomial Theorem, show that

$$(1-x)^{-\frac{3}{2}} = \sum_{k\ge 0} \frac{(k+1)}{2^{2k}}\binom{2k+1}{k}x^k.$$

11. By using the fact that $\int_0^1 x^i\,dx = \frac{1}{i+1}$ for $i \ge 0$, show that

    (a) $\sum_{i=0}^n \frac{1}{i+1}\binom{n}{i} = \frac{1}{n+1}\{2^{n+1}-1\}$.

    (b) $\sum_{i=1}^n \frac{(-1)^i}{i}\binom{n}{i} = -\sum_{k=1}^n \frac{1}{k}$

    (c) $\sum_{i=0}^n \frac{2^{i+1}}{i+1}\binom{n}{i} = \frac{1}{n+1}\{3^{n+1}-1\}$.

12. (a) Let $F(x) = \sum_{(i_1,\dots,i_k)\in S} g(i_1,\dots,i_k)x^{h(i_1,\dots,i_k)}$, where $h(i_1,\dots,i_k)$ is an integer-valued function of $i_1,\dots,i_k$ and $g(i_1,\dots,i_k)$ is independent of x. Show that

$$[x^n]F(x) = \sum_{\begin{cases} (i_1,\dots,i_k)\in S \\ h(i_1,\dots,i_k)=n \end{cases}} g(i_1,\dots,i_k).$$

    (b) Prove that

$$[x^n]e^{3x}(1-5x^2)^{-a}(1+x^3)^{2a} = \sum_{\substack{i,j,k\ge 0 \\ i+2j+3k=n}} \frac{3^i}{i!}5^j\binom{a+j-1}{j}\binom{2a}{k}$$

$$= \sum_{k=0}^{\lfloor\frac{n}{3}\rfloor}\sum_{j=0}^{\lfloor\frac{n-3k}{2}\rfloor} \frac{3^{n-2j-3k}}{(n-2j-3k)!}5^j\binom{a+j-1}{j}\binom{2a}{k}.$$

3.8 The Quicksort Algorithm

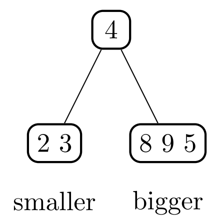
Suppose that we are given a list of n distinct numbers $x_1,\dots,x_n$, and are asked to sort them (put them in increasing order, say). Consider the following procedure:

1. Compare x_1 with each of $x_2\dots,x_n$, thus forming two lists, one consisting of those elements of $x_2,\dots,x_n$ which are bigger than x_1, and those which are smaller.

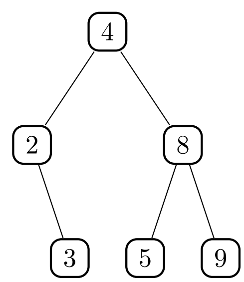
2. Repeat (1) for each of these lists unless their length is 0 or 1. This is called “Quicksort”, and is implemented as follows.

Example 3.8.1. Sort the list 4 2 8 9 3 5.

STEP 1.



STEP 2.



and we're finished. We have constructed a *binary* tree, which will be discussed later.

Problem 3.8.2. *Assuming the original list is in* random *order (i.e. all $n!$ possible orderings are equiprobable), what is the average number of comparisons needed by this algorithm to completely sort a list of n distinct numbers?*

Solution: Let this average value be a_n. Then from the algorithm,

$$a_n = n - 1 + \frac{1}{n}\sum_{i=1}^{n}(a_{i-1} + a_{n-i}). \tag{3.8.1}$$

The $n-1$ arises from comparing a_1 to $a_2, \ldots, a_n$. Further, since the list is in random order, it is equally likely (probability $= \frac{1}{n}$) that a_1 is the i^{th} ordered element in the list, for $i = 1, \ldots, n$. But if a_1 is the i^{th} ordered element, we must then sort the lists of smaller and larger elements, of lengths $i-1$ and $n-i$ respectively. For initial conditions, we have $a_0 = 0$.

Multiply both sides of (3.8.1) by n, to give

$$na_n = n(n-1) + 2\sum_{j=0}^{n-1} a_j, \quad n \geq 1.$$

Now multiply both sides by x^{n-1} and sum for $n \geq 1$. Then

$$\sum_{n\geq 1} n a_n x^{n-1} = \sum_{n\geq 1} n(n-1)x^{n-1} + 2\sum_{n\geq 1} x^{n-1}\sum_{j=0}^{n-1} a_j$$

$$\sum_{n\geq 1} n a_n x^{n-1} = x\sum_{n\geq 2} n(n-1)x^{n-2} + 2\sum_{j\geq 0} a_j \sum_{n=j+1}^{\infty} x^{n-1}\ ,$$

since

$$\sum_{n\geq 1}\sum_{j=0}^{n-1} = \sum_{n\geq j}\sum_{j\geq 0} = \sum_{j\geq 0}\sum_{n>j}.$$

Now let

$$A(x) = \sum_{n\geq 0} a_n x^n$$

so that

$$A'(x) = \sum_{n\geq 1} n a_n x^{n-1}.$$

Then the above equation becomes

$$A'(x) = x\sum_{n\geq 2} n(n-1)x^{n-2} + 2\sum_{j\geq 0} a_j \frac{x^j}{1-x}$$

which gives

$$A'(x) = 2x(1-x)^{-3} + 2(1-x)^{-1}A(x).$$

Hence we must solve the differential equation

$$A'(x) - 2(1-x)^{-1}A(x) = 2x(1-x)^{-3}. \tag{3.8.2}$$

This type of differential equation is called a **linear differential equation of the first order**. The general form is

$$\frac{dy}{dx} + P(x)y = Q(x)$$

where P and Q are functions of x alone. There is a standard method of solution for such equations.

The equation is essentially the same if we multiply both sides by any function of x, say $\mu(x)$. We get

$$\mu(x)\frac{dy}{dx} + \mu(x)P(x)y = \mu(x)Q(x) \tag{3.8.3}$$

Now the left hand side of (3.8.3) starts off like the derivative of the product of two functions $\mu(x)$ and y. We would have

$$\frac{d}{dx}[\mu(x)y] = \mu(x)\frac{dy}{dx} + \mu'(x)y.$$

In fact, if we choose $\mu(x)$ so that $\mu'(x) = \mu(x)P(x)$ then the left hand side of (3.8.3) *would* be the derivative of $\mu(x)y$. So let us take

$$\frac{\mu'(x)}{\mu(x)} = P(x)$$

or, on integrating, $\log \mu(x) = \int P(x)dx$. Then provided we can integrate $P(x)$ we have the required $\mu(x)$. The equation now becomes

$$\frac{d}{dx}[\mu(x)y] = \mu(x)Q(x)$$

and another integration gives

$$\mu(x)y = \int \mu(x)Q(x)dx + C$$

which gives us the solution, y.

The function $\mu(x)$ is called an **integrating factor**. In our example we have $y = A(x), P(x) = -2(1-x)^{-1}$ and $Q(x) = 2x(1-x)^{-3}$.

$$\begin{aligned} \int P(x)dx &= -2\int \tfrac{1}{1-x}dx \\ &= 2\log(1-x) \end{aligned}$$

making $\mu(x) = (1-x)^2$. Multiplying by this we get

$$(1-x)^2 A'(x) - 2(1-x)A(x) = 2x(1-x)^{-1}$$

or

$$\begin{aligned} \tfrac{d}{dx}[(1-x)^2 A(x)] &= \tfrac{2x}{1-x} \\ &= \tfrac{2}{1-x} - 2 \end{aligned}$$

Integrating, we have

$$(1-x)^2 A(x) = -2\log(1-x) - 2x + c\,.$$

Hence

$$A(x) = \{-2\log(1-x) - 2x + c\}(1-x)^{-2}.$$

We know that $A(0) = 0$, so $c = 0$. To find a_n, we expand $A(x)$ in powers of x.

$$\begin{aligned} A(x) &= \{2\log(1-x)^{-1} - 2x\}(1-x)^{-2} \\ &= 2\textstyle\sum_{k\geq 2} \frac{x^k}{k} \sum_{i\geq 0}(i+1)x^i \ . \end{aligned}$$

Hence

$$\begin{aligned} a_n &= [x^n]A(x) = 2\textstyle\sum_{\substack{k\geq 2 \\ i+k=n}} \sum_{i\geq 0} \frac{i+1}{k} \\ &= 2\textstyle\sum_{k=2}^{n} \frac{n-k+1}{k} = 2(n+1)\left\{\sum_{k=2}^{n} \frac{1}{k}\right\} - 2(n-1) \ . \end{aligned}$$

Thus

$$a_n = 2(n+1)\left\{\sum_{k=1}^{n} \frac{1}{k}\right\} - 4n \ ,$$

is the average number of comparisons needed. This might not give you much feel for how big a_n is, but a result from advanced calculus (which we won't go into) tells us that $\sum_{k=1}^{n} \frac{1}{k}$ is asymptotically $\log\ n + \gamma$ where γ is a constant, known as Euler's constant. Its value is 0.5772... . It follows from this that

$$a_n \sim 2n\log n.$$

∎

Exercise: Although the result just quoted is outside the scope of this course, it is fairly easy to show that

$$\log(n+1) < 1 + \frac{1}{2} + \cdots + \frac{1}{n} < \log n + 1$$

by considering the area under the curve $y = \frac{1}{x}$. (Use the integral test for series convergence in first year calculus).

Problem Set 3.8

1. Suppose that

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

satisfies the differential equation $F'(x) = (1+2x)F(x)$, with $F(0) = 3$. Find a recurrence equation for f_n, together with initial conditions.

2. Suppose that

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

satisfies the differential equation

$$(1-x)A'(x) = 5(1+x)A(x),$$

with $A(0) = 2$. Find the recurrence relation for $a_n, n \geq 0$ together with initial conditions.

3. If

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

satisfies the differential equation

$$F''(x) + (1-x)F'(x) - x^2 F(x) = 0,$$

with $F(0) = 1$, $F'(0) = 2$, find a recurrence for f_n, together with initial conditions.

4. Suppose

$$f(x) = \sum_{k=0}^{\infty} f_k \frac{x^k}{k!}$$

satisfies the differential equation

$$(1+2x)^2 f'(x) = 4x f(x)$$

with the boundary condition $f(0) = 1$.

   (a) Find a recurrence equation for f_n.
   (b) Solve the differential equation to find $f(x)$.
   (c) Find an expression for f_n in terms of n, for $n \geq 2$.

3.9 The Mergesort Algorithm

A list of n distinct numbers can also be sorted by the following procedure:

1. Divide the n numbers into two groups, which have sizes as close to equal as possible, (i.e., one group consists of the first $\lfloor \frac{n}{2} \rfloor$ numbers, the second group consists of the last $\lceil \frac{n}{2} \rceil$ numbers, where $\lceil x \rceil$ = smallest integer which is not less than x).

2. Sort these two groups individually by applying stage (1) to them and repeat, until each group has size 1. When these groups are sorted, merge them to create an ordered list.

This is called "Mergesort". We might implement it to sort 4 2 8 9 3 5 by first creating a binary tree with subtrees of an equal size as possible, e.g.

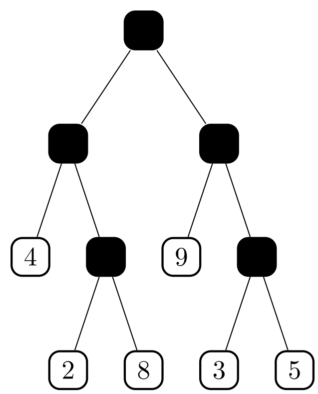
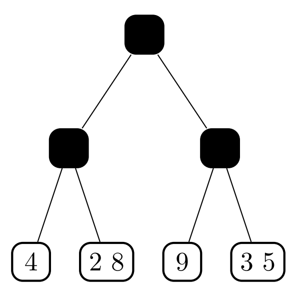
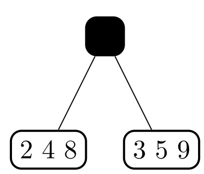


Figure 3.2: Some graphs

We now merge successive pairs of subtrees, as follows:
STEP 1.



STEP 2.



STEP 3. 2 3 4 5 8 9.

We wish to find a_n, the number of comparisons needed to sort such a list. Then, from the algorithm,

$$a_n = a_{\lfloor \frac{n}{2} \rfloor} + a_{\lceil \frac{n}{2} \rceil} + \text{ (number of comparisons needed to merge.)}$$

But the number of comparisons needed to merge lists of sizes $\lceil \frac{n}{2} \rceil$ and $\lfloor \frac{n}{2} \rfloor$ is at most $n-1$, so

$$a_n \le n - 1 + a_{\lfloor \frac{n}{2} \rfloor} + a_{\lceil \frac{n}{2} \rceil} \tag{3.9.1}$$

Thus if we solve the recurrence

$$t_n = n - 1 + t_{\lfloor \frac{n}{2} \rfloor} + t_{\lceil \frac{n}{2} \rceil}, n \ge 2,$$

with initial condition $t_1 = 0$, we will know that $a_n \le t_n$, and we have found an *upper bound* for the number of comparisons needed. The determination of the average number of comparisons is difficult, but the upper bound turns out to be quite close to the actual average. To solve our recurrence for t_n, multiply by x^n and sum for $n \ge 2$, giving

$$\sum_{n\ge 2} t_n x^n = \sum_{n \ge 2} (n-1)x^n + \sum_{n\ge 2} (t_{\lfloor \frac{n}{2} \rfloor} + t_{\lceil \frac{n}{2} \rceil})x^n,$$

and letting $T(x) = \sum_{n\ge 1} t_n x^n$, $t_1 = 0$, gives

$$\begin{aligned} T(x) &= x^2 \textstyle\sum_{i\ge 0} i x^{i-1} + \sum_{m\ge 1} 2 t_m x^{2m} + \sum_{k \ge 1} (t_k + t_{k+1}) x^{2k+1} \\ &= x^2 \textstyle\sum_{i \ge 0} i x^{i-1} + 2T(x^2) + xT(x^2) + x^{-1} T(x^2), \text{ since } t_1 = 0 \\ &= x^2 (1-x)^{-2} + (2 + x + x^{-1}) T(x^2) \end{aligned}$$

Hence

$$T(x) = x^2 (1-x)^{-2} + x^{-1}(1+x)^2 T(x^2),$$

and we must solve this functional equation. First let $S(x) = x^{-2}(1-x)^2(T(x)$, so that $S(x^2) = x^{-4}(1-x^2)^2 T(x^2)$. The equation for $T(x)$ becomes

$$S(x) = 1 + xS(x^2). \tag{3.9.2}$$

Applying this iteratively gives

$$\begin{aligned} S(x) &= 1 + x(1 + x^2 S(x^4)) \\ &= 1 + x(1 + x^2(1 + x^4(\ldots))) \\ &= 1 + x + x^3 + x^7 + \cdots \\ &= \textstyle\sum_{i\geq 0} x^{2^i - 1}, \end{aligned}$$

which easily checks to satisfy (3.9.2) above. (Exercise).

Thus we want $t_n = [x^n]T(x)$, where

$$\begin{aligned} T(x) &= x^2(1-x)^{-2} \textstyle\sum_{i\geq 0} x^{2^i-1} \\ &= x^2 \textstyle\sum_{j\geq 0}(j+1)x^j \sum_{i\geq 0} x^{2^i-1}. \end{aligned}$$

Therefore $t_n = \sum_i (j+1)$, where the summation is for $i \geq 0$, $j \geq 0$, and $2^i + 1 + j = n$. Let m be the largest possible value for i, given by $2^m \leq n-1$, or $m = \lfloor \log_2(n-1) \rfloor$. Then

$$t_n = \sum_{i=0}^{m}(n - 2^i) = (m+1)n - \frac{2^{m+1}-1}{2-1} = (m+1)n + 1 - 2^{m+1}$$

where $m = \lfloor \log_2(n-1) \rfloor$. More usefully, we have

$$t_n \sim n \log_2 n,$$

since $n \leq 2^{m+1} \leq 2(n-1)$. Finally, recall that this gives an upper bound on the average number of comparisons needed by MERGESORT.

If you take a Computer Science course on the analysis of algorithms, you will spend a lot of time developing asymptotic results of the above types (though by quite different methods).

Chapter 4

Introduction to Graph Theory

4.1 Definitions

Graph theory is the study of mathematical objects known as “graphs" — a word to which graph theorists have given a rather special meaning. So we must start by defining exactly what a graph is.

Definition 4.1.1. *A* **graph** *G is a finite nonempty set, $V(G)$, of objects, called* **vertices***, together with a set, $E(G)$, of unordered pairs of distinct vertices. The elements of $E(G)$ are called* **edges***.*

For example, we might have

$$V(G) = \{1,2,3,4,5\}$$

and

$$E(G) = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,5\},\{3,4\},\{3,5\},\{4,5\}\}.$$

For the sorts of results with which we are concerned, it is most convenient to consider the following geometric representation or diagram or **drawing** of a graph. On the page we draw a small circle to correspond to each vertex. For each edge we then draw a line between the corresponding pair of vertices. The only restriction on such a line is that it does not intersect the circle corresponding to any other vertex. For example, the above graph is represented in Figure 4.1(i), (ii) and (iii) in three ways.

If $e = \{u, v\}$ then we say that u and v are **adjacent** vertices, and that edge e is **incident** with vertices u and v. We can also say that the edge e **joins** u and v.

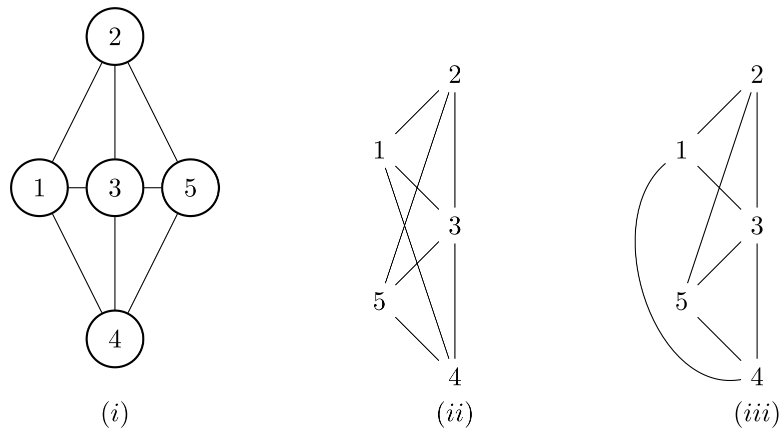


Figure 4.1: Three drawings of the same graph

Vertices adjacent to a vertex u are called **neighbours** of u. The set of neighbours of u is denoted $N(u)$. A graph is completely specified by the pairs of vertices that are adjacent, and the only function of a line in the drawing, representing an edge, is to indicate that two vertices are adjacent. In (i) of Figure 4.1, no edge crosses another; in (ii) of Figure 4.1, the edge $\{1,4\}$ crosses edges $\{2,5\}$ and $\{3,5\}$. A graph which can be represented with no edges crossing is said to be **planar**, so our graph G is planar by Figure 4.1(i).

We give a few examples to illustrate the variety of settings in which graphs arise.

Example 4.1.2. The **word graph** W_n is the graph having $V(W_n)$ equal to the set of all English words having exactly n letters. Two words are adjacent if one can be obtained from the other by replacing exactly one letter by another (in the same position). For example, *seat* is adjacent to *sent* in W_4. In Figure 4.2 we show a drawing of part of W_3.

Example 4.1.3. Given the street map of a city, one can define a **street map graph** as follows. There is a vertex for each street intersection, and an edge for each part of a street joining two intersections and traversing no other intersections. An example is given in Figure 4.3, where intersections are numbered to make the correspondence clear. Such graphs are useful in solving certain kinds of routing and scheduling problems, such as garbage pickup, or delivery of newspapers to carriers.

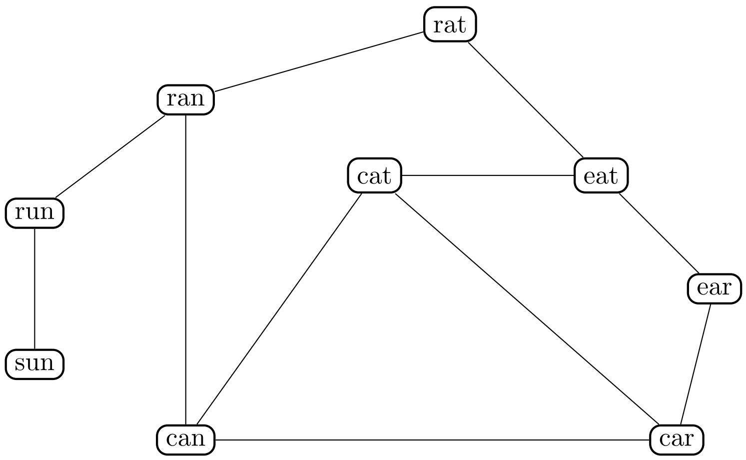


Figure 4.2: Part of W_3

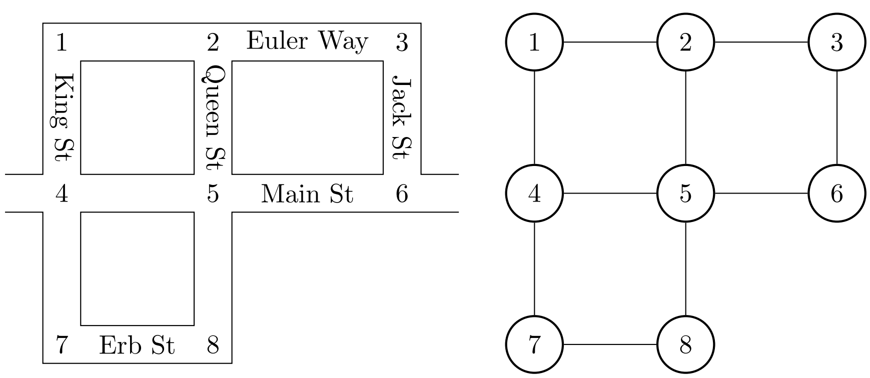


Figure 4.3: Map of Smalltown and its Graph

Example 4.1.4. Another way to obtain a graph from a map, is to begin with a political map, such as the map of the countries of a continent. There is a vertex for each country and two countries are adjacent if they share a boundary. One of the most famous problems in graph theory arose from the question of how many colours are needed to colour such maps so that adjacent countries are not assigned the same colour. Figure 4.4 shows the graph obtained from South America.

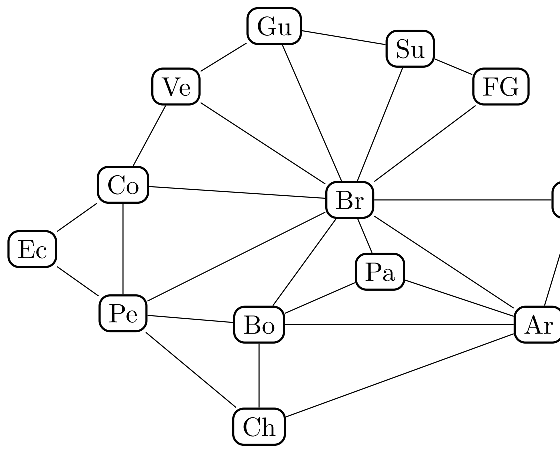


Figure 4.4: Graph of South American Countries

Example 4.1.5. Graphs are often defined from other mathematical objects. For example, we can define the graph $S_{n,k}$ to have $V(S_{n,k})$ equal to the set of k-element subsets of $\{1,2,\ldots,n\}$. Two such subsets are adjacent if they have exactly $k-1$ elements in common. Figure 4.5 shows a drawing of the graph $S_{4,2}$.

Some important points arise from our definition of a graph.

(1) Edges are **unordered** pairs of vertices. Thus the edge $\{v_1, v_2\}$ is not *from* v_1 to v_2 or vice versa; it is simply "between" v_1 and v_2. If we change Definition 4.1.1 to read "ordered pairs" we obtain the definition of a different kind of graph, a **directed graph** or **digraph**.

(2) $E(G)$, being a set, either contains a pair $\{v_1, v_2\}$ or it does not. Thus we do not allow the possibility of "multiple edges" such as exist between the vertices a and b in Figure 4.6.

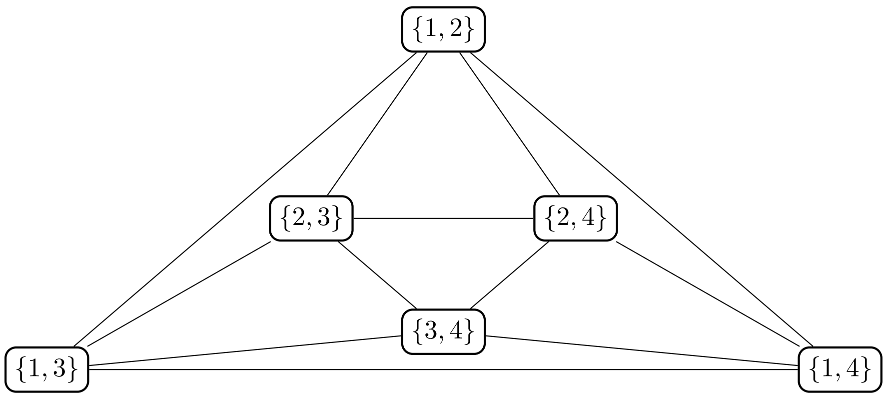


Figure 4.5: A drawing of $S_{4,2}$

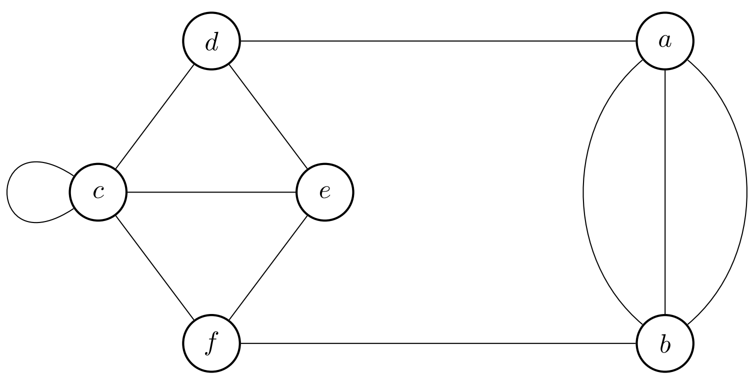


Figure 4.6: A multigraph

(3) The edges are pairs of **distinct** vertices. Hence we cannot have a loop, i.e., an edge joining a vertex to itself as shown in Figure 4.6 at vertex c. Nevertheless in some circumstances it can be convenient to consider loops and/or multiple edges. If we wish to allow loops and multiple edges we will use the term **multigraph** instead of graph. (In some texts "graph" is used to mean "multigraph", and if loops and multiple edges are not allowed the term "simple graph" is used.)

(4) Note that $V(G)$, and hence $E(G)$, is a **finite** set. If we remove this condition we find ourselves in the realm of infinite graphs—and that is a whole new ballgame!

4.2 Isomorphism

Figure 4.7(i) is the diagram of the graph G, where

$$V(G) = \{p, q, r, s\}, \qquad E(G) = \{\{p, q\}, \{p, r\}, \{q, r\}, \{q, s\}\}.$$

Figure 4.7(ii) is the diagram of the graph H, where

$$V(H) = \{a, b, c, d\}, \qquad E(H) = \{\{a, b\}, \{a, c\}, \{a, d\}, \{c, d\}\}.$$

The graphs G and H are not the same—G has vertices p, q, r, s and H has vertices a, b, c, d—but for almost all purposes they are indistinguishable. We make this idea precise.

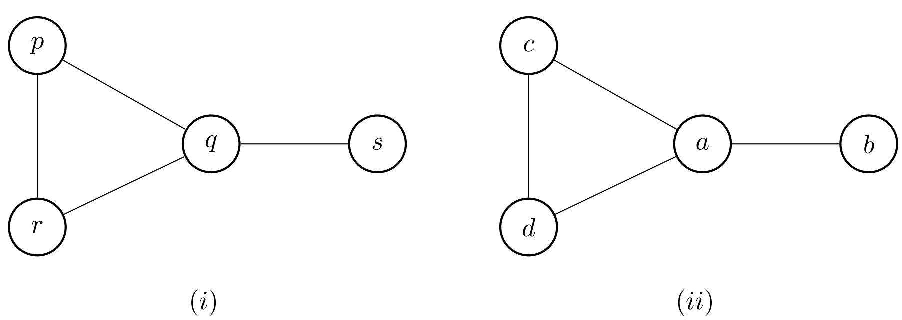


Figure 4.7: Isomorphic graphs

Definition 4.2.1. *Two graphs G_1 and G_2 are* **isomorphic** *if there exists a bijection $f : V(G_1) \to V(G_2)$ such that vertices $f(u)$ and $f(v)$ are adjacent in G_2 if and only if u and v are adjacent in G_1. (We might say that f preserves adjacency.)*

The bijection f in this definition that preserves adjacency is called an **isomorphism**. For example, an isomorphism from G to H is g, defined by

$$g(p) = c,\ g(q) = a, g(r) = d, g(s) = b.$$

Another isomorphism is h, defined by

$$h(p) = d,\ h(q) = a, h(r) = c, h(s) = b.$$

Figure 4.8 shows two other graphs, G and H, that are isomorphic. One isomorphism is the mapping $f : V(G) \to V(H)$ given by

$$\begin{array}{llll} f(1) = a, & f(2) = b, & f(3) = c, & f(4) = h, \\ f(5) = i, & f(6) = j, & f(7) = d, & f(8) = e, \\ f(9) = f, & f(10) = g. & & \end{array}$$

(This graph is called the **Petersen graph**.)

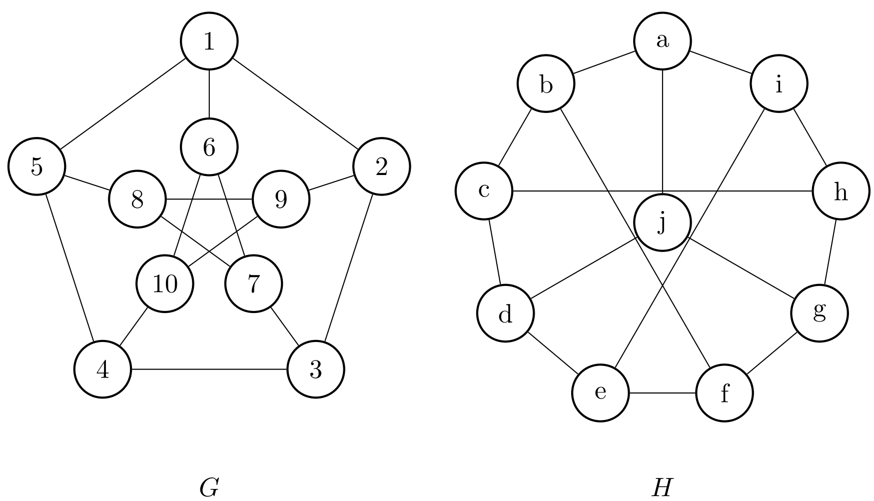


Figure 4.8: Two drawings of the Petersen graph

The collection of graphs that are isomorphic to G forms the **isomorphism class** of G. In almost all cases, a graph has some property if and only if all graphs in its isomorphism class have the property. Thus we generally regard isomorphic graphs as 'the same' even if formally they might not be equal. Even if G has only one vertex, there are infinitely many graphs in its isomorphism class. Fortunately though, the number of isomorphism classes of graphs with a given finite set of vertices is finite. For example, there are exactly 11 isomorphism classes of graphs on 4 vertices, pictured in Figure 4.9. Note that in this figure, the vertices of the graphs are not given explicitly, because however we assign vertices to the drawing, we will still get a graph in the same isomorphism class.

The identity map on $V(G)$ is an isomorphism from the graph G to itself. An isomorphism from G to itself is called an **automorphism** of G.

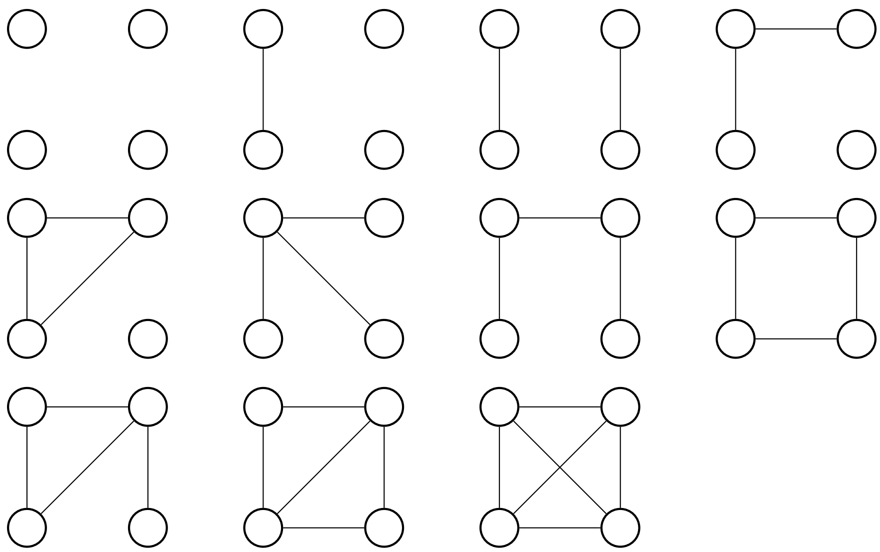


Figure 4.9: The graphs on 4 vertices, up to isomorphism

4.3 Degree

The number of edges incident with a vertex v is called the **degree** of v, and is denoted by $\deg(v)$. For example in G of Figure 4.7 we have $\deg(p) = \deg(r) = 2$, $\deg(q) = 3$, $\deg(s) = 1$; in G of Figure 4.8, all vertices have degree 3. In what follows we generally use 'p' for the number of vertices and 'q' for the number of edges.

Theorem 4.3.1. *For any graph G we have*

$$\sum_{v \in V(G)} \deg(v) = 2|E(G)|.$$

Proof: Each edge has two ends, and when we sum the degrees of the vertices, we are counting the edges twice, once for each end. ∎

This is known as the **Handshaking Lemma** or the **Degree-Sum Formula**.

Corollary 4.3.2. *The number of vertices of odd degree in a graph is even.*

Proof: The sum of all vertex degrees is $2q$, an even number. The sum of the vertices of even degrees is even. Hence the sum of the vertices of odd degrees is also an even number. This implies that there must be an even number of vertices with odd degree. ∎

Corollary 4.3.3. *The average degree of a vertex in the graph G is*

$$\frac{2|E(G)|}{|V(G)|}.$$

A graph in which every vertex has degree k, for some fixed k, is called a k-**regular** graph (or just a **regular** graph). We note one important class of regular graphs.

Definition 4.3.4. *A* **complete graph** *is one in which all pairs of distinct vertices are adjacent. (Thus each vertex is joined to every other vertex). The complete graph with p vertices is denoted by K_p, $p \geq 1$.*

In K_n each vertex is adjacent to the $n-1$ vertices distinct from it, thus K_n is regular with degree $n-1$. The number of edges in K_n is therefore $\binom{n}{2}$, following Corollary 4.3.2.

Figure 4.10 shows K_4, the complete graph on 4 vertices, and therefore 6 edges.

4.4 Bipartite Graphs

A graph in which the vertices can be partitioned into two sets A and B, so that all edges join a vertex in A to a vertex in B, is called a **bipartite** graph, with **bipartition** (A, B). The **complete** bipartite graph $K_{m,n}$ has all vertices in A adjacent to all vertices in B, with $|A| = m$, $|B| = n$. For example, Figure 4.11 is a drawing of $K_{2,3}$.

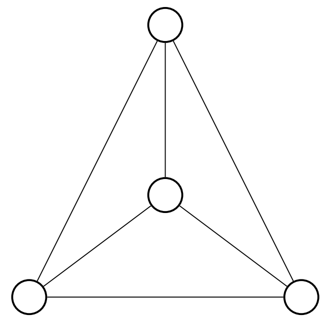


Figure 4.10: K_4

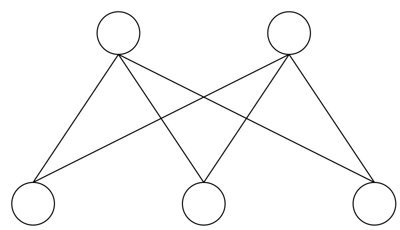


Figure 4.11: The complete bipartite graph $K_{2,3}$

Definition 4.4.1. *For $n \geq 0$, the n-***cube** *is the graph whose vertices are the $\{0,1\}$-strings of length n, and two strings are adjacent if and only if they differ in exactly one position.*

For example, Figure 4.12 shows the 3-cube.

Problem 4.4.2. *Determine the numbers of vertices and edges in the n-cube, for $n \geq 0$.*

Solution: The number of $\{0,1\}$-strings of length n is 2^n, for $n \geq 0$, so the n-cube has $p = 2^n$ vertices. Also, every vertex has degree n, since a string of length n is adjacent to the n strings that can be obtained by switching each single element in the string in turn. Thus the n-cube is an n-regular graph, and Theorem 4.3.1 gives

$$\begin{aligned}\sum_{i=1}^{2^n} n &= 2q \\ n2^n &= 2q,\end{aligned}$$

so the n-cube has $q = n2^{n-1}$ edges, for $n \geq 0$. ∎

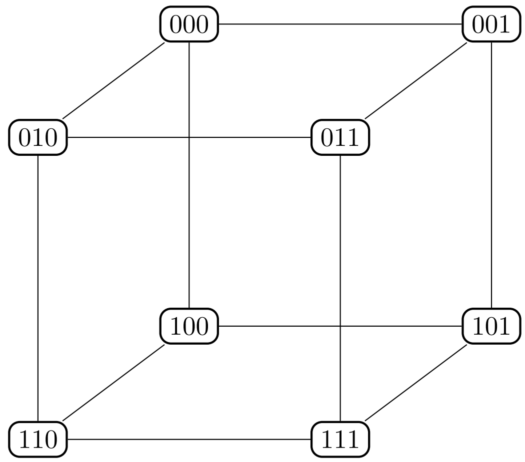


Figure 4.12: The 3-cube

Problem 4.4.3. *Show that the n–cube is bipartite, for $n \geq 0$.*

Solution: Let V be the set of all $\{0,1\}$–strings of length n; V is the vertex set of the n-cube. Partition V into the set A of strings containing an even number of ones and the set B of strings containing an odd number of ones. If vertices x and y are adjacent then the strings x and y differ in exactly one position. Thus, exactly one of x and y contain an even number of ones. Therefore (A,B) is a bipartition and hence the n-cube is bipartite. ∎

Problem Set 4.4

1. For the graphs G_1, G_2, G_3 and H in Figure 4.13, prove that no two of G_1, G_2 or G_3 are isomorphic. Prove that one of them (which?) is isomorphic to H by giving a suitable bijection.

2. A cubic graph is one in which every vertex has degree three. Find all the nonisomorphic cubic graphs with 4, 6 and 8 vertices.

3. For the subset graph $S_{n,k}$ defined in Example 4.1.5, find the number of vertices and the number of edges.

4. The **odd graph** O_n is the graph whose vertices are the n-subsets of a $(2n+1)$-set, two such subsets being adjacent if and only if they are disjoint.

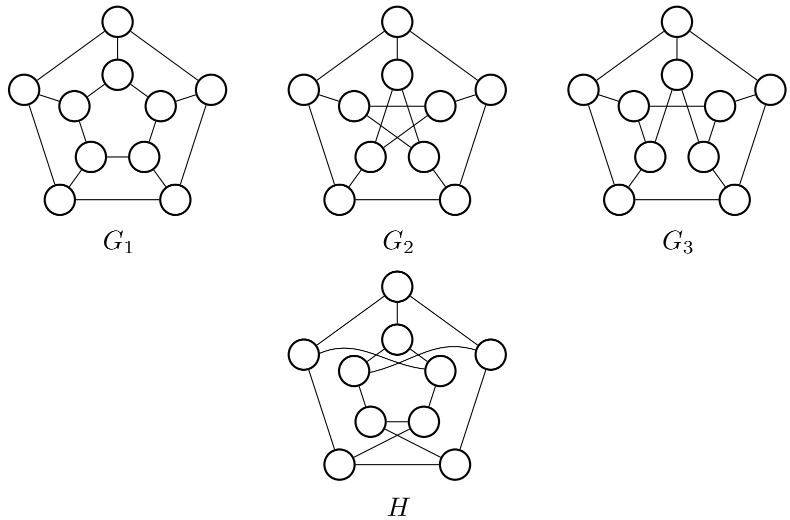


Figure 4.13: Isomorphism exercise

(a) Draw O_1 and O_2.

(b) Prove that O_2 is isomorphic to the Petersen graph (see Figure 4.8).

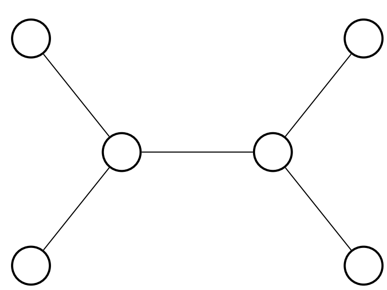
(c) How many vertices and edges does O_n have?

5. The **line-graph** $L(G)$ of a graph G is the graph whose vertex set is $E(G)$ and in which two vertices are adjacent if and only if the corresponding edges of G are incident with a common vertex.

   (a) Find a graph G such that $L(G)$ is isomorphic to G.

   (b) Find nonisomorphic graphs $G, G^{'}$ such that $L(G)$ is isomorphic to $L(G^{'})$.

   (c) If G is the graph



   find $L(G), L(L(G))$ and $L(L(L(G)))$.

6. For integer $n \geq 0$, define the graph G_n as follows: $V(G_n)$ is the set of all binary strings of length n having at most one block of 1's. Two vertices are adjacent if they differ in exactly one position.

   (a) Find $|V(G_n)|$

   (b) Make drawings of G_3 and G_4.

   (c) Find $|E(G_n)|$.

7. (a) Draw $K_{m,n}$ for all m, n such that $1 \leq m \leq n \leq 3$.

   (b) How many vertices and edges does $K_{m,n}$ have?

   (c) Let K be a complete bipartite graph on p vertices. Prove that K has at most $\lfloor p^2/4 \rfloor$ edges.

   (d) Let G be a bipartite graph on p vertices. Prove that G has at most $\lfloor p^2/4 \rfloor$ edges.

   (e) Let G be a k-regular bipartite graph with bipartition (X, Y). Prove that $|X| = |Y|$ if $k > 0$. Is this still valid when $k = 0$?

8. The **complement** of the graph G, denoted $\bar{G}$ is the graph with $V(\bar{G}) = V(G)$ and the edge $\{u, v\} \in E(\bar{G})$ if and only if $\{u, v\} \not\in E(G)$.

   (a) Let G have vertices 1, 2, 3, 4 and edges $\{1,2\}, \{2,3\}, \{3,4\}, \{1,4\}$. Draw $\bar{G}$.

   (b) Find a 5-vertex graph that is isomorphic to its complement.

   (c) Prove that no 6-vertex graph is isomorphic to its complement.

   (d) Let G_1 and G_2 be two graphs. Prove that G_1 is isomorphic to G_2 if and only if $\bar{G}_1$ is isomorphic to $\bar{G}_2$.

   (e) Find all 2-regular non-isomorphic graphs on 6 vertices (prove that these are the only ones).

   (f) Prove that there are only two 3-regular non-isomorphic graphs on 6 vertices.

9. Make drawings of the 15 nonisomorphic graphs having six vertices and six edges, such that every vertex has degree at least one.

10. Are the graphs in Figure 4.14 isomorphic? Justify your answer.

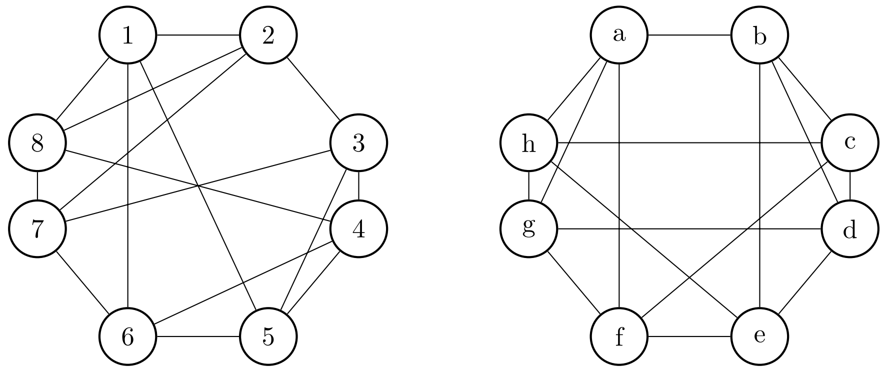


Figure 4.14: Isomorphism exercise

11. For n a positive integer, define the **prime graph** B_n to be the graph with vertex set $\{1,2,\dots,n\}$, where $\{u,v\}$ is an edge if and only if $u+v$ is a prime number. Prove that B_n is bipartite.

12. (a) Are the two graphs in Figure 4.15 isomorphic? Prove your claim.
    (b) Are the two graphs in Figure 4.16 isomorphic? Prove your claim.

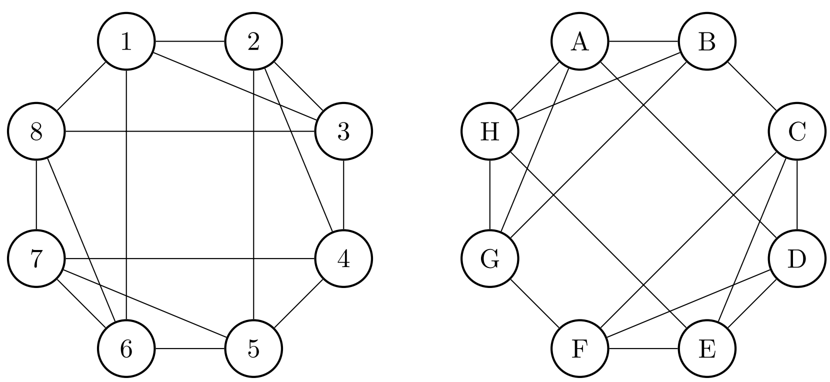


Figure 4.15: Isomorphism exercise

4.5 How to Specify a Graph

One way of specifying a particular graph is to display a drawing of it; but this is not always convenient. Another method is by means of adjacency or incidence matrices.

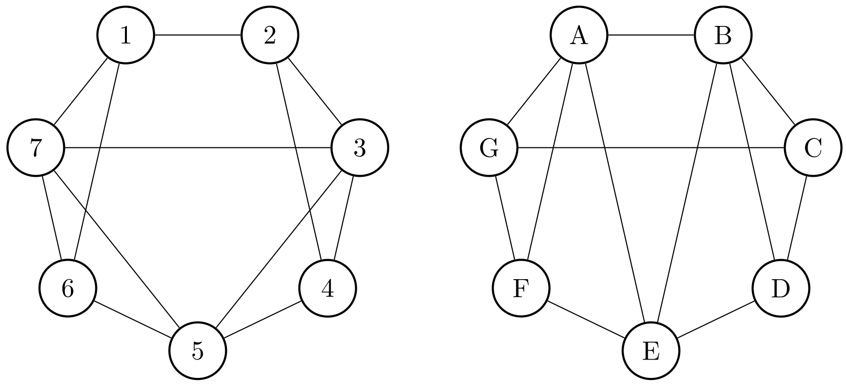


Figure 4.16: Isomorphism exercise

Definition 4.5.1. *The* **adjacency matrix** *of a graph G having vertices* $v_1, v_2, \ldots, v_p$ *is the* $p \times p$ *matrix* $A = [a_{ij}]$ *where*

$$a_{ij} = \begin{cases} 1, & \text{if } v_i \text{ and } v_j \text{ are adjacent;} \\ 0, & \text{otherwise.} \end{cases}$$

Clearly A is a symmetric matrix and, since we do not allow loops, its diagonal elements are all zero.

To define an incidence matrix we must name the edges of G; we shall call them $e_1, e_2, \ldots, e_q$.

Definition 4.5.2. *The* **incidence matrix** *of a graph G with vertices* $v_1 \ldots v_p$ *and edges* $e_1 \ldots e_q$ *is the* $p \times q$ *matrix* $B = [b_{ij}]$ *where*

$$b_{ij} = \begin{cases} 1, & \text{if } v_i \text{ is incident with } e_j; \\ 0, & \text{otherwise.} \end{cases}$$

Clearly, each column of B contains exactly two 1's.

Consider the product BB^t. Its (i, j)-element is

$$\sum_{k=1}^{q} b_{ik} b_{jk}.$$

For $i \neq j$ this sum is the number of edges incident with both v_i and v_j; for $i = j$ it is the number of edges incident with v_i, which is $\deg(v_i)$. Thus

$$BB^t = A + \operatorname{diag}(\deg(v_i), \ldots, \deg(v_p)).$$

Another way of specifying a graph is to give, for each vertex, a list of the vertices adjacent to it. For example:

vertex	adjacent vertices
1	3 4 5 7
2	3 5 7
3	1 2 4 5 6
4	1 3 5 6
5	1 2 3 4
6	3 4 7
7	1 2 6

This is called an **adjacency list**. In practice this would be stored as a dictionary or hash.

Finally we could also specify a graph by giving its vertex set together with the list of its edges. This is likely to be most useful when the graph is sparse, i.e., does not have many edges.

It is important to note that in many cases the vertices of the graph may not arrive as non-negative integers. There were examples of this in Problem Set 4.4.

Problem Set 4.5

1. (a) Find the adjacency matrix A and the incidence matrix B for the graph in Figure 4.17.

   (b) Give an interpretation of

   (i) the diagonal elements of the matrix A^2; and

   (ii) the off-diagonal elements of the matrix A^2.

2. (a) Order the vertices of the graph in Figure 4.18 so that the adjacency matrix has the form $\begin{bmatrix} 0 & \mathbf{M} \\ \mathbf{M}^t & 0 \end{bmatrix}$ for some matrix $\mathbf{M}$.

   (b) Prove that any bipartite graph has a vertex ordering which gives an adjacency matrix of the above form for some $\mathbf{M}$.

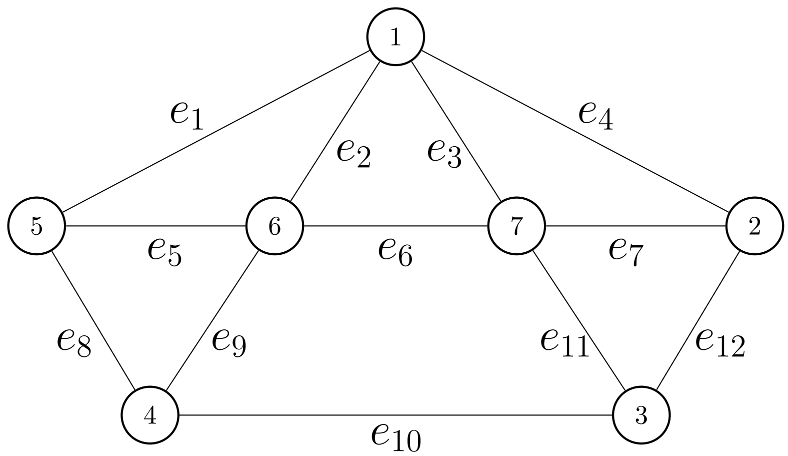


Figure 4.17: Graph for problem 1

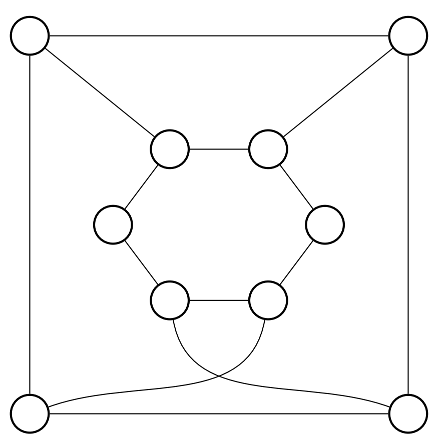


Figure 4.18: Graph for problem 2

4.6 Paths and Cycles

A subgraph of a graph G is a part of G (or possibly the whole of G). More rigorously we have

Definition 4.6.1. *A* **subgraph** *of a graph G is a graph whose vertex set is a subset U of $V(G)$ and whose edge set is a subset of those edges of G that have both vertices in U.*

Thus if H is a subgraph of G, then H has some (perhaps all) the vertices of G and some (perhaps all) the edges that, in G, join vertices of H. (Clearly we cannot have any edges in H that involve vertices not in H). If $V(H) = V(G)$, that is H has all vertices of G, we say H is a **spanning subgraph** of G.

If H is a subgraph of G and H is not equal to G, we say it is a **proper subgraph** of G. If D is a subgraph of G and C is a subgraph of D, then C is a subgraph of G.

A **walk** in a graph G from v_0 to v_n, $n \geq 0$, is an alternating sequence of vertices and edges of G

$$v_0 e_1 v_1 e_2 v_2 \ldots v_{n-1} e_n v_n$$

which begins with vertex v_0, ends with vertex v_n and, for $1 \leq i \leq n$, edge $e_i = \{v_{i-1}, v_i\}$. Such a walk can also be called a v_0, v_n**-walk**. Note that the **length** of a walk is the number of edges in it (in this case, n). Also, because we can reverse a walk to get a walk from v_n to v_0, we refer, where convenient, to a walk **between** a pair of vertices, instead of from one to the other. A walk is said to be **closed** if $v_0 = v_n$.

A **path** is a walk in which all the vertices are distinct. A path that starts at v_0 and ends at v_n is called a v_0, v_n**-path**. Observe that since all the vertices in a path are distinct, so are all the edges.

Figure 4.19 shows (by heavy lines) a path in a graph, from vertex 1 to vertex 2.

Since graphs have no multiple edges, consecutive vertices v_{i-1} and v_i determine the edge e_i of a walk. Hence, in describing a walk we often omit the edges.

Theorem 4.6.2. *If there is a walk from vertex x to vertex y in G, then there is a path from x to y in G.*

Proof: We use a form of proof by contradiction.

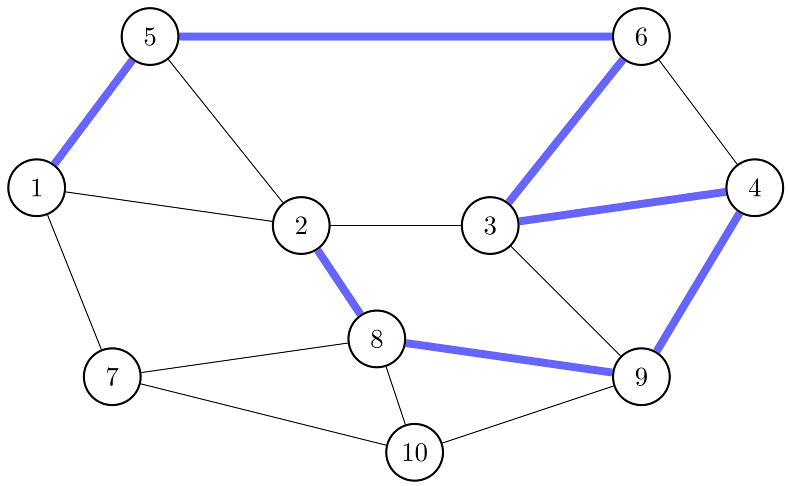


Figure 4.19: A path

Suppose that $v_0, \dots, v_n$ is a walk in G from $v_0 = x$ to $v_n = y$ with minimal length (among all walks from x to y). If the walk is not a path, then $v_i = v_j$ for some $i < j$, and then $v_0 \dots v_i v_{j+1} \dots v_n$ would be a walk from x to y whose length is less than the minimum possible. But this contradicts our initial choice, and so we conclude that the vertices in our original walk are all distinct, and therefore it is a path. ∎

Corollary 4.6.3. *Let x, y, z be vertices of G. If there is a path from x to y in G and a path from y to z in G, then there is a path from x to z in G.*

Proof: The path from x to y followed by the path from y to z is a walk from x to z in G, so by Theorem 4.6.2 there is a path from x to z in G. ∎

A **cycle** in a graph G is a subgraph with n distinct vertices $v_0, v_1 \dots v_{n-1}$, $n \geq 1$, and n distinct edges $\{v_0, v_1\}$, $\{v_1, v_2\}$, $\dots \{v_{n-2}, v_{n-1}\}$, $\{v_{n-1}, v_0\}$. Equivalently, a cycle is a connected graph that is regular of degree two. (The definition of connectedness is given in Section 4.8.)

The subgraph we get from a cycle by deleting one edge is called a **path**. This is inconsistent with the original definition of path, because we defined a path to be a type of walk, and a walk is a sequence of vertices and edges and so is not a graph. But it is very convenient to use the word path in both senses, and we will.

A cycle with n edges is called an n-cycle or a cycle of length n. A cycle of length 1 has one vertex, v_0, and one edge $\{v_0, v_0\}$ which is a loop. Therefore, since graphs have no loops, a graph has no cycle of length one. A cycle of length 2 has two vertices, v_0 and v_1, and two distinct edges, called multiple edges, joining v_0 and v_1. Therefore, a graph has no cycle of length two. Thus the shortest possible cycle in a graph is a 3-cycle, often called a triangle.

Note that for a cycle with $n \geq 3$ vertices, $v_0, \ldots, v_{n-1}$, then $v_i v_{i+1} \ldots v_{n-1} v_0 \ldots v_i$ and $v_i v_{i-1} \ldots v_0 v_{n-1} \ldots v_i$ are both closed walks for each $i = 0, \ldots, n-1$, and in this way there are $2n$ closed walks of length n associated with a given n-cycle.

Figure 4.20 shows (by heavy lines) an 8-cycle in a graph.

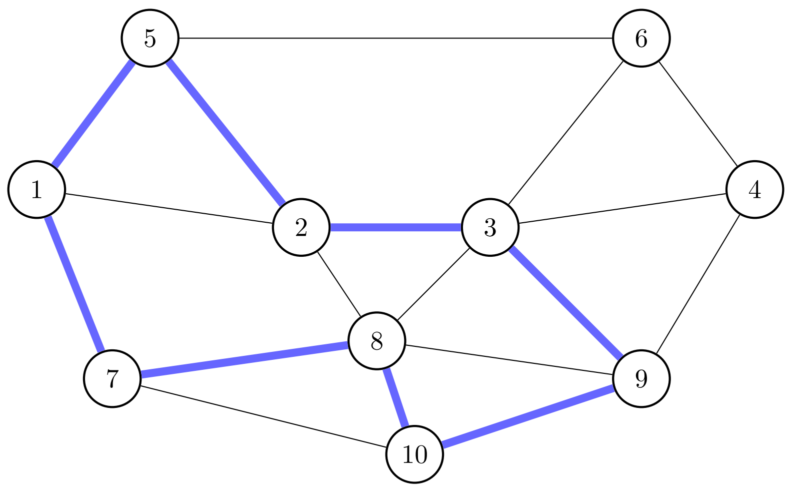


Figure 4.20: A cycle

In a cycle, every vertex has degree exactly 2. There's one condition that guarantees that a graph contains a cycle.

Theorem 4.6.4. *If every vertex in G has degree at least 2, then G contains a cycle.*

Proof: Let $v_0, v_1, \ldots, v_k$ be a longest path in G. The vertex v_0 has v_1 as one neighbour. Since v_0 has degree at least 2, v_0 has another neighbour x. If x is not on the path, then $x, v_0, v_1, \ldots, v_k$ is a path longer than our longest path, which is a contradiction. Hence x must be on the path, and $x = v_i$ for some $i \geq 2$. Then $v_0, v_1, \ldots, v_i, v_0$ is a cycle in G. ▮

The **girth** of a graph G is the length of the shortest cycle in G, and is denoted by $g(G)$. If G has no cycles, then $g(G)$ is infinite (but you may choose to ignore this fact).

A spanning cycle in a graph is known as a **Hamilton cycle** (so the cycle in Figure 4.20 is not a Hamilton cycle). Although it is easy to decide if a given cycle is a Hamilton cycle, it can be surprisingly difficult to find one in a graph or to certify that it has no Hamilton cycle.

Problem Set 4.6

1. Let G be a graph with minimum degree k, where $k \geq 2$. Prove that

   (a) G contains a path of length at least k;

   (b) G contains a cycle of length at least $k+1$.

2. Let A be the adjacency matrix of a graph G.

   (a) Show that the $(i,j)^{th}$ entry of A^k is the number of walks of length k from i to j.

   (b) Assume A satisfies the matrix equation $A^2 + A = (k-1)I + J$ where I is the identity matrix and J is the matrix of all 1's. Explain in graph theory terms the properties G possesses given by the matrix equation.

3. (a) If A is the adjacency matrix of a graph G, show that for $i \neq j$, the $(i,j)^{th}$ element of A^2 is the number of paths of length 2 in G between vertices v_i and v_j.

   (b) What are the diagonal elements of A^2?

4. Let G be the graph whose set of vertices is the set of all "lower 48" states of the United States, plus Washington, DC, with two vertices being adjacent if they share a boundary. (For example, *California* is adjacent to *Arizona*.) Let H be the subgraph of G whose vertices are those of G whose first letter is one of W, O, M, A, N, and whose edges are the edges of G whose ends have this property. (For example, *California* is not a vertex of H, but *Arizona* and *New Mexico* are, and they are adjacent in H.) Find a path in H from *Washington* to *Washington, DC*.

5. Consider the word graph W_n defined in Example 4.1.2.

   (a) Find a cycle through *math* in W_4.

   (b) Find a path from *pink* to *blue* in W_4.

6. For $n \geq 2$, prove that the n-cube contains a Hamilton cycle.

7. Prove that the complete bipartite graph $K_{m,n}$ has a Hamilton cycle if and only if $m = n$ and $m > 1$.

8. Show that if there is a closed walk of odd length in the graph G, then G contains an odd cycle (that is, G has a subgraph which is a cycle on an odd number of vertices).

9. A **diagonal** of a cycle in a graph is an edge that joins vertices that are not consecutive in the cycle.

   (a) Prove that a shortest cycle (if one exists) has no diagonal.

   (b) Prove that a shortest odd cycle (if one exists) has no diagonal.

   (c) Give an example of a graph in which a shortest even cycle has a diagonal.

10. (a) Prove that a k-regular graph of girth 4 has at least $2k$ vertices ($k \geq 2$).

    (b) For $k = 2, 3$, find a k-regular graph of girth 4 with precisely $2k$ vertices. Generalize these examples, i.e. find one for each $k \geq 2$.

    (c) Prove that a k-regular graph of girth 5 has at least $k^2 + 1$ vertices ($k \geq 2$).
    Remark: The only values of k for which such a graph with exactly $k^2 + 1$ vertices can exist are $k = 2, 3, 7, 57$. This surprising result can be proved using elementary matrix theory (i.e., what you study in MATH 235). Examples are known for $k = 2, 3, 7$, but no example has yet been found for $k = 57$. Such a graph would have $57^2 + 1 = 3250$ vertices.

    (d) Prove that a k-regular graph of girth $2t$, where $t \geq 2$, has at least $\frac{2(k-1)^t - 2}{k-2}$ vertices.

    (e) Prove that a k-regular graph of girth $2t + 1$, where $t \geq 2$, has at least $\frac{k(k-1)^t - 2}{k-2}$ vertices.

    (f) For $k = 2, 3$, give an example of a k-regular graph of girth five with exactly $k^2 + 1$ vertices.

4.7 Equivalence Relations

You have met equivalence relations in your first algebra course, but these are important in nearly all areas of mathematics, including graph theory.

Formally, if S and T are sets, then a relation $\mathscr{R}$ between S and T is a subset of $S \times T$. The idea is that if $a \in S$ and $b \in T$, then a and b are related if and only if (a, b) belongs to the subset. If a and b are related we may say that they are **incident**. Thus if G is a graph, then "is contained in" is a relation on $V(G) \times E(G)$.

We will be most concerned with the case where $S = T$. In this case we usually refer to a relation on S, and do not mention $S \times S$. By way of example, "is adjacent to" is a relation on the vertices of a graph. A relation on S is **reflexive** if each element of S is related to itself. So "is adjacent to" is not a reflexive relation on the vertex set $V(G)$ of a graph G. However this relation is **symmetric**, that is, if a is related to b then b is related to a. On the integers, the relation "divides" is reflexive but not symmetric.

There is a third important property a relation may have. Suppose that we are given a relation on a set V and, if $a, b \in V$, we write $a \approx b$ to denote that a and b are related. We say the relation is **transitive** if whenever $a \approx b$ and $b \approx c$, then $a \approx c$. The relation "divides" on the integers is transitive, as is the relation $\leq$ on $\mathbb{R}$. The relation "is a subgraph of" on the subgraphs of G is reflexive and transitive.

We say a relation is an **equivalence relation** if it is reflexive, symmetric and transitive.

As an example, the relation "is joined by a walk to" on the vertices of a graph G is an equivalence relation—each of the three properties is very easy to verify.

The canonical example is equality. Another example you have met is "congruent modulo m" on the integers. We generally use equivalence relations to partition things. Thus the equivalence relation "congruent mod 5" splits the integers into five classes. The key is that if $\approx$ is an equivalence relation on a set V and $C(a)$ is the set

$$\{v \in V : v \approx a\}$$

then any two elements of $C(a)$ are equivalent, and any element of v that is equivalent to something in $C(a)$ is itself an element of $C(a)$. Hence if $b \in V$ then either $C(a) = C(b)$ or $C(a) \cap C(b) = \emptyset$.

4.8 Connectedness

Definition 4.8.1. *A graph G is* **connected** *if, for each two vertices x and y, there is a path from x to y.*

Theorem 4.8.2. *Let G be a graph and let v be a vertex in G. If for each vertex w in G there is a path from v to w in G, then G is connected.*

Proof: For any vertices x and y in G, there is a path from v to x and a path from v to y. If we reverse the path from v to x we obtain a path from x to v, and now Corollary 4.6.3 implies that there is a path from x to y in G, so G is connected by Definition 4.8.1. ∎

If G is a graph on n vertices, then to certify that G is connected according to the definition of connected, we must provide a total of $\binom{n}{2}$ paths. The above theorem reduces the workload: only n paths are needed.

Problem 4.8.3. *Prove that the n-cube is connected for each $n \geq 0$.*

Solution: We use Theorem 4.8.2, and prove that there is a path from vertex $v_0 = 0\dots0$ (with n 0's) to x for all other vertices x in the n-cube. Now x is a $\{0,1\}$-string of length n, and suppose that x has k 1's in positions $i_1,\dots,i_k$, where $1 \leq i_1 < \dots < i_k \leq n$, with $1 \leq k \leq n$. Now let v_j be the $\{0,1\}$-string with 1's in positions $i_1,\dots,i_j$, and 0's elsewhere for $j = 1,\dots,k$. Then $v_0 v_1 \dots v_k$ is a path from $0\dots0$ to x, so the n-cube is connected, by Theorem 4.8.2. ∎

Definition 4.8.4. *A* **component** *of G is subgraph C of G such that*

(a) C is connected.

(b) No subgraph of G that properly contains C is connected.

These two conditions may sometimes be stated in the form "a component of G is a subgraph which is maximal, subject to being connected". Here when we say a subgraph C of G is maximal, subject to having some property, then this means that any subgraph that properly contains C does not have this property.

Note that we could have defined a component of G to be the equivalence class of a vertex, relative to the relation "is joined by a walk to". Since this is indeed an equivalence relation, it follows immediately that the components of G partition its vertex set.

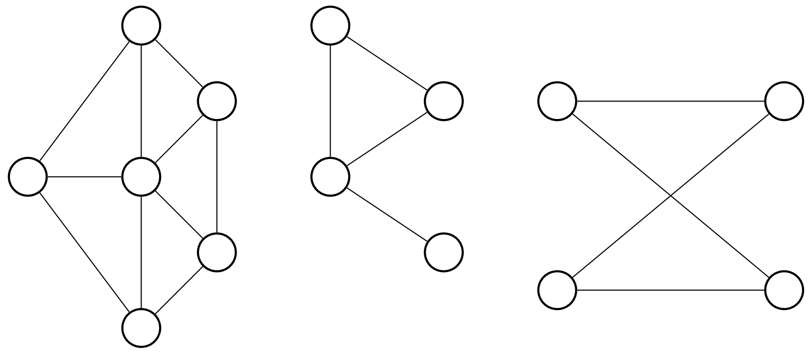


Figure 4.21: A disconnected graph

Figure 4.21 shows a graph having three components. Note that there are paths between every pair of vertices in the same component, but not between pairs of vertices in different components.

While it is easy to convince someone of the existence of a path between two vertices (show them the path), it is less clear how you might convince them that a path does not exist. We introduce a convenient way of doing this.

If we are given a partition (X,Y) of $V(G)$ such that there are no edges having an end in X and an end in Y, then there is no path from any vertex in X to any vertex in Y. So, if X and Y are both nonempty, G is not connected. Given a subset X of the vertices of G, the **cut** induced by X is the set of edges that have exactly one end in X.

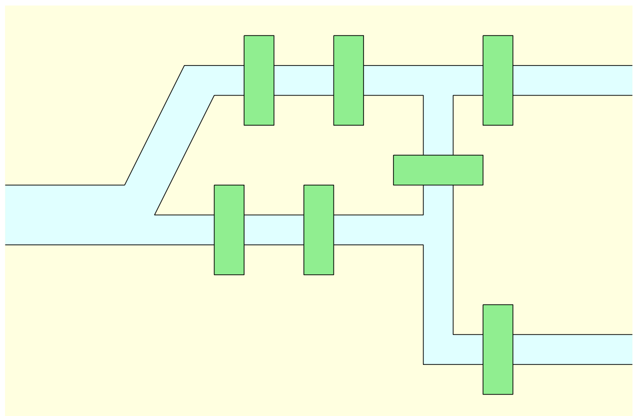
Theorem 4.8.5. *A graph G is not connected if and only if there exists a proper nonempty subset X of $V(G)$ such that the cut induced by X is empty.*

Proof: Let G be a connected graph, and let X be a proper nonempty subset of $V(G)$. Choose vertices $u \in X$ and $v \in V(G) \setminus X$. Since G is connected, there exists a path $x_0x_1 \dots x_n$ from u to v. Choose k as large as possible such that $x_k \in X$. Since $x_n = v \notin X, k < n$, the edge x_kx_{k+1} is in the cut induced by X and hence this cut is not empty.

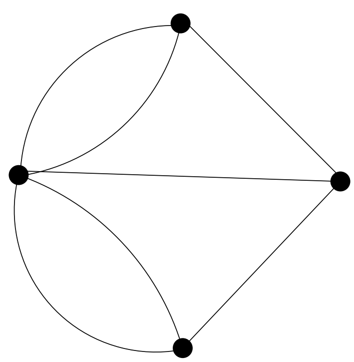
Conversely, suppose that G is not connected and let C be a component of G. Consider the partition (X,Y) of $V(G)$ where $X = V(C)$ and $Y = V(G) \setminus V(C)$. Since C is connected and G is not, X is a proper non-empty subset of $V(G)$. Since C is a component, if the vertex y is adjacent to a vertex in C, then $y \in V(C)$. Hence the cut induced by X is empty. ∎

4.9 Eulerian Circuits

One of the earliest problems in graph theory is the **Seven Bridges of Königsberg** problem. In the 18th century in the town of Königsberg (now Kaliningrad, Russia), there were 7 bridges that crossed the river Pregel, which cuts through the city and there were 2 islands in the middle of the river. The layout can be roughly represented in the following diagram:



The question is that can a resident of the city leave home, cross every bridge exactly once, and then return home? We can formulate the layout of the city as a graph: Create 4 vertices representing the land areas (two shores and two islands), and create an edge for each bridge, joining the vertices representing the two land areas on either side of the bridge. In this case, we obtain the following graph (with multiple edges):



In terms of graph theory, the question becomes "is there a closed walk that uses every edge exactly once?" We use a definition for this type of walk.

Definition 4.9.1. *An* Eulerian circuit *of a graph G is a closed walk that contains every edge of G exactly once.*

In 1736, Swiss mathematician Leonhard Euler noted that there cannot be an Eulerian circuit for the 7 bridges of Königsberg problem. The reason being that if an Eulerian circuit exists, each time we visit a vertex, we must use 2 distinct edges incident with that vertex: use one edge to go to the vertex, use one edge to leave the vertex. So every vertex must have even degree. However, in this graph, every vertex has odd degree, so such a walk is not possible.

On the other hand, suppose we have a connected graph and every vertex has even degree. Does it have an Eulerian circuit? Euler noted that this is indeed true, and we give a proof here.

Theorem 4.9.2. *Let G be a connected graph. Then G has an Eulerian circuit if and only if every vertex has even degree.*

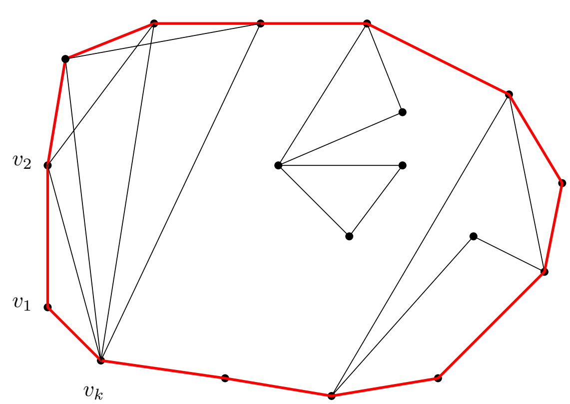
Proof: ($\Rightarrow$) A closed walk contributes 2 to the degree of a vertex for each visit. Since an Eulerian circuit uses each edge of the graph exactly once, each vertex in the graph must have even degree.

($\Leftarrow$) We will prove by strong induction on the number of edges m in G.

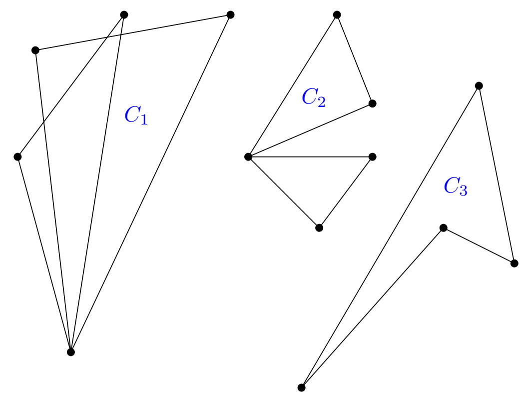
Base case: If G has 0 edges, then G consists of exactly one isolated vertex. It has a trivial closed walk as an Eulerian circuit.

Induction hypothesis: Assume that for some $m \geq 1$, any connected graph with less than m edges where every vertex has even degree has an Eulerian circuit.

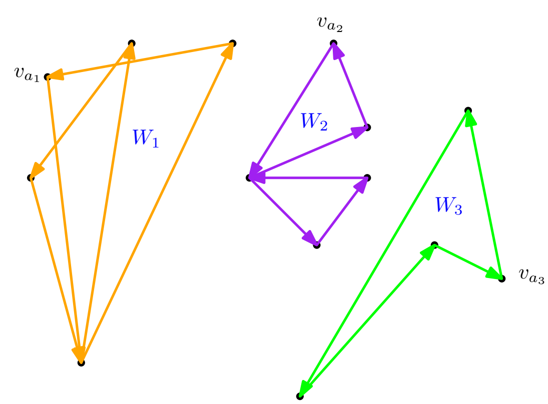
Induction step: Let G be a connected graph with m edges where every vertex has even degree. This implies that every vertex has degree at least 2. Therefore, by Theorem 4.6.4, there exists a cycle C in G, say the vertices on the cycle in order are $v_1, v_2, \ldots, v_k, v_1$.



Remove edges of C from G and remove isolated vertices to obtain G'. Since every vertex is incident with either 0 or 2 edges in C, every vertex in G' still has even degree. Now G' consists of components $C_1, \dots, C_l$, each containing less than m edges.

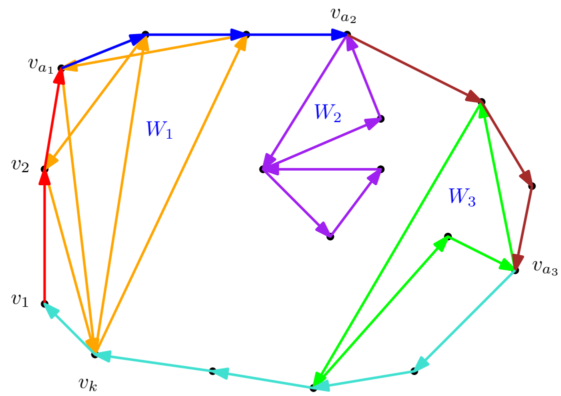


By induction hypothesis, each component C_i has an Eulerian circuit W_i. Moreover, each component must have a common vertex with C, for otherwise G is disconnected. Let v_{a_i} be one vertex of C_i. Rearrange the components so that $a_1 < a_2 < \cdots < a_l$, and let W_i start and end at v_{a_i}.



Then we can construct an Eulerian circuit for G by walking along C and making detours W_i as we hit v_{a_i}:

$$v_1, \dots, v_{a_1-1}, W_1, v_{a_1+1}, \dots, v_{a_2-1}, W_2, v_{a_2+1}, \dots\dots\dots, v_{a_l-1}, W_l, v_{a_l+1}, \dots, v_k, v_1.$$



■

4.10 Bridges

If $e \in E(G)$, we denote by $G-e$ (or by $G \backslash e$) the graph whose vertex set is $V(G)$ and whose edge set is $E(G) \backslash \{e\}$. (So $G-e$ is the graph obtained from G by deleting the edge e.)

Definition 4.10.1. *An edge e of G is a* **bridge** *if $G-e$ has more components than G.*

Thus if G is connected, a bridge is an edge such that $G-e$ is not connected. Figure 4.22 shows a connected graph with a bridge e. Some texts, and some instructors, use **cut-edge** as a synonym for bridge.

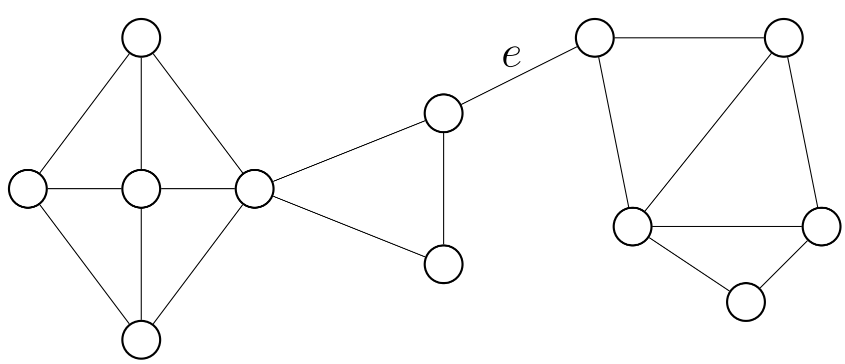


Figure 4.22: A bridge

Lemma 4.10.2. *If $e = \{x, y\}$ is a bridge of a connected graph G, then $G - e$ has precisely two components; furthermore, x and y are in different components.*

Proof: Let $e = \{x, y\}$. If e is a bridge, then $G - e$ has at least two components. Let V_x be the set of vertices in the same component of $G - e$ as x. Let z be any vertex of $G - e$ not in V_x. Because there exists a path from x to z in G but not in $G - e$, every path from x to z in G contains edge e and so must be of the form

$$xeye_2v_2e_3v_3\cdots v_{n-1}e_nz.$$

But $ye_2v_2\cdots e_nz$ is a path from y to z in $G - e$. Thus z is in the same component of $G - e$ as y, for every vertex z not in V_x. Hence, $G - e$ has 2 components, one containing vertex x and the other containing vertex y. ∎

Theorem 4.10.3. *An edge e is a bridge of a graph G if and only if it is not contained in any cycle of G.*

Proof: We begin by proving the following implication: if edge $e = \{x, y\}$ is an edge of some cycle of G, then e is not a bridge of G.

By hypothesis, there is a cycle

$$x, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, y, e, x$$

in G. Then

$$x, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, y$$

is a path from x to y in $G - e$. Hence e is not a bridge of G by Lemma 4.10.2. This establishes the implication.

To complete the proof, we must establish the converse – if edge e is not a bridge of graph G, then e is an edge of some cycle. Suppose $e = uv$ is not a bridge. Then u and v must lie in the same component of $G - e$, and so there is a path P that joins them. Together with e this path forms a cycle that contains e. ∎

Corollary 4.10.4. *If there are two distinct paths from vertex u to vertex v in G, then G contains a cycle.*

Proof: Let P_1 and P_2 be distinct paths from u to v. Suppose that P_1 is given by $x_0x_1\ldots x_n$ and P_2 is given by $y_0y_1\ldots y_m$. Thus $u = x_0 = y_0$ and $v = x_n = y_m$. Let i be the first index such that $x_{i+1} \neq y_{i+1}$. Then $e = \{x_i, x_{i+1}\}$ is an edge in P_1 but not in P_2.

Consider the walk

$$x_i, x_{i-1}, \ldots, x_0 = u = y_0, y_1, \ldots, y_m = v = x_n, x_{n-1}, \ldots, x_{i+1}.$$

It is a walk from x_i to x_{i+1} that does not use the edge e. So it is also a walk in $G-e$, hence x_i, x_{i+1} are in the same component in $G-e$. By Lemma 4.10.2, e is not a bridge. By Theorem 4.10.3, e must be part of a cycle. Hence G contains a cycle. ∎

We will often use the contrapositive form of this result: If graph G has no cycles, then each pair of vertices is joined by at most one path.

Problem Set 4.10

1. Prove that the prime graph B_n defined in Problem Set 4.4 is connected for every n. You may use without proof the following fact: For every integer $k \geq 2$ there is a prime number r such that $k < r < 2k$.

2. Prove that, if G is connected, any two longest paths have a vertex in common.

3. Which graphs, with at least one edge, have the property that every edge is a bridge?

4. If every vertex of a graph H with p vertices has degree at least $p/5$, prove that H cannot have more than 4 components.

5. If edge e is not a bridge of a connected graph G, prove that e is an edge of some cycle.

6. Prove that a 4-regular graph has no bridge.

7. Let A_n be the graph whose vertices are the $\{0,1\}$-strings of length n, and edges are between strings that differ in exactly two positions, $n \geq 2$.

   (a) How many edges does A_n have?

   (b) Is A_n bipartite for any $n \geq 2$?

   (c) How many components does A_n have?

8. Let B_n be the graph whose vertices are the $\{0,1\}$-strings of length n, and edges are between strings that differ in exactly two consecutive positions, $n \geq 2$.

(a) How many edges does B_n have?

(b) How many components does B_n have?

9. Let G be a graph in which exactly two of the vertices u, v have odd degree. Prove that G contains a path from u to v.

4.11 Certifying Properties

In graph theory we usually find that each time we meet a new property, two questions arise. First, how do we certify that a graph has the property. Second, how do we certify that a graph does not have that property.

So we can certify that a graph is connected by providing, for each pair of distinct vertices, a path in the graph the joins the two vertices. We can certify that a graph G is not connected by producing a cut—two non-empty sets of vertices A and B that partition $V(G)$, such that no edge of G joins a vertex in A to a vertex in B.

As another example, you can certify that an edge $e = uv$ in a connected graph G is a bridge by producing a cut (A,B) for $G-e$ where $u \in A$ and $v \in B$. You can certify that e is not a bridge by producing a cycle that contains e. (You could also certify this by showing that $G-e$ is connected, but this would be more work as a rule.)

Certificates are required to be easy to verify; they need not be easy to find. So you might have to work hard to find a certificate, but it must still be easy for the marker to verify. (The precise rule is that it must be possible to check the correctness of your certificate in *polynomial time*.)

It is an experimental fact that if there is a good certificate for verifying that a graph has some property, and a good certificate for verifying that it does not, then there is an efficient algorithm for testing if a graph has the property.

Chapter 5

Trees

5.1 Trees

A very special and important kind of graph is a **tree**.

Definition 5.1.1. *A* **tree** *is a connected graph with no cycles.*

Figure 5.1 shows a typical tree.

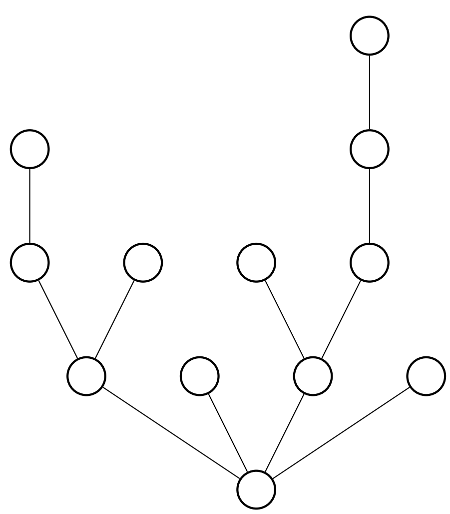


Figure 5.1: A tree

If connectedness is not required, then the graph is a **forest**.

Definition 5.1.2. *A* **forest** *is a graph with no cycles.*

We now prove some properties of trees and forests.

Lemma 5.1.3. *If u and v are vertices in a tree T, then there is a unique u,v-path in T*

Proof: For any 2 vertices u and v in T, there is at least 1 path joining them since T is connected. Since T has no cycles, there is at most one path by Corollary 4.10.4. This establishes the result. ▮

Lemma 5.1.4. *Every edge of a tree T is a bridge.*

Proof: An edge e of T is not in a cycle, so, by Theorem 4.10.3, e is a bridge. ▮

One main property of trees is that any tree with p vertices have the same number of edges: $p-1$.

Theorem 5.1.5. *If T is a tree, then $|E(T)| = |V(T)| - 1$.*

Proof: The proof is by strong induction on q, the number of edges. When $q = 0$ there is just one tree. It has one vertex and no edges, and the theorem holds for it.

Suppose that the theorem is true for trees on fewer than q edges, and let T be any tree with q edges, for $q \geq 1$. Let $e = \{u, v\}$ be any edge. By Lemma 5.1.4, e is a bridge. Therefore, $T \setminus e$ is not connected and, by Lemma 4.10.2, it has exactly two components, say T_1 and T_2. Both are connected (as they are components), and do not contain cycles (as a cycle in $T - e$ is a cycle in T). Hence both T_1 and T_2 are trees. Since both of them have fewer than q edges, by induction, $|E(T_1)| = |V(T_1)| - 1$ and $|E(T_2)| = |V(T_2)| - 1$. Then

$$|E(T)| = |E(T_1)| + |E(T_2)| + 1 = (|V(T_1)| + |V(T_2)|) - 1 = |V(T)| - 1.$$

▮

Corollary 5.1.6. *If G is a forest with k components, then $|E(G)| = |V(G)| - k$.*

Proof: Let $T_1, \ldots, T_k$ be the k components of G. Since each component is connected and G does not contain any cycle, each T_i is a tree. By Theorem 5.1.5, $|E(T_i)| = |V(T_i)| - 1$ for each i. Adding the k equations, we get

$$\sum_{i=1}^{k} |E(T_i)| = \sum_{i=1}^{k} (|V(T_i)| - 1) = \left(\sum_{i=1}^{k} |V(T_i)| \right) - k.$$

Since $|E(G)| = \sum_{i=1}^{k} |E(T_i)|$ and $|V(G)| = \sum_{i=1}^{k} |V(T_i)|$, we get $|E(G)| = |V(G)| - k$. ▮

Definition 5.1.7. *A* **leaf** *in a tree is a vertex of degree 1.*

Theorem 5.1.8. *A tree with at least two vertices has at least two leaves.*

Proof: Let P be a longest path in the tree T with end vertices u and v. Since any edge gives a path of length 1, P must have length at least 1, so $u \neq v$.

Now one vertex adjacent to v is in P. If $\deg(v) > 1$, then there must be another vertex, w, adjacent to v. Vertex w cannot be in P, since this would imply a cycle in T, whereas T has no cycles. Since w is not in P, we can extend P by adding the edge $\{v, w\}$ to it to get a longer path. This is a contradiction. Hence $\deg(v) = 1$. Similarly $\deg(u) = 1$, which proves the theorem. ∎

This proof works if, instead of choosing a longest path, we choose a path which is not a subgraph of a path in T with more edges. (We might say that our path is "maximal under inclusion".) The advantage of this choice is that it is easier to decide if a path is maximal under inclusion than to decide if it is a longest path—for to do the latter we must consider all paths in the tree.

The following alternate proof gives more detailed information about how many vertices of degree one a tree can have given the degrees of other vertices.

Alternate proof of Theorem 5.1.8: Let T be a tree and let n_r denote the number of vertices of degree r in T. Set $p = |V(T)|$ and assume $p \geq 2$. By Theorem 4.3.1 we have

$$2p - 2 = \sum_{v \in V(T)} \deg(v)$$

and therefore

$$-2 = \sum_{v} (\deg(v) - 2) = \sum_{r=0}^{p-1} n_r (r-2).$$

In the last sum, $n_0 = 0$ (because in a connected graph with at least two vertices, every vertex has degree at least 1) and so we find that

$$-2 = -n_1 + \sum_{r \geq 3} (r-2) n_r.$$

Therefore

$$n_1 = 2 + \sum_{r \geq 3} (r-2) n_r.$$

Since $(r-2) n_r \geq 0$ when $r \geq 3$, it follows that $n_1 \geq 2$. ∎

The above proof implies that if T contains a vertex of degree r, where $r \geq 3$, then $n_1 \geq 2 + (r-2) = r$. As an exercise, use a version of the first proof to show that a tree that contains a vertex of degree r has at least r vertices of degree one.

Problem Set 5.1

1. (a) Draw one tree from each isomorphism class of trees on six or fewer vertices.

   (b) For each tree in (a), exhibit a bipartition (X, Y) by coloring the vertices in X with one colour and the vertices in Y with another.

2. Prove that every tree is bipartite.

3. What is the smallest number of vertices of degree 1 in a tree with 3 vertices of degree 4 and 2 vertices of degree 5? Justify your answer by proving that this is the smallest possible number, and by giving a tree which has this many vertices of degree 1.

4. Find the smallest number r of vertices in a tree having two vertices of degree 3, one vertex of degree 4, and two vertices of degree 6. Justify your answer by proving that any such tree has at least r vertices, and by giving an example of such a tree with exactly r vertices.

5. A **cubic** tree is a tree whose vertices have degree either 3 or 1. Prove that a cubic tree with exactly k vertices of degree 1 has $2(k-1)$ vertices.

6. Prove that a forest with p vertices and q edges has $p-q$ components.

7. Let $p \geq 2$. Show that a sequence $(d_1, d_2, \ldots, d_p)$ of positive integers is the degree sequence of a tree on p vertices if and only if $\sum_{i=1}^{p} d_i = 2p-2$. (Hint: use induction on p.)

5.2 Spanning Trees

A spanning subgraph which is also a tree is called a **spanning tree**. The reason that spanning trees are important is that, of all the spanning subgraphs, they have the fewest edges while remaining connected. Figure 5.2 shows a graph with a spanning tree indicated by heavy lines.

Theorem 5.2.1. *A graph G is connected if and only if it has a spanning tree.*

Proof: ("if" part.) We are given that G has a spanning tree T. Then Lemma 5.1.3 implies that there is a path in T between every pair of vertices of T. But each

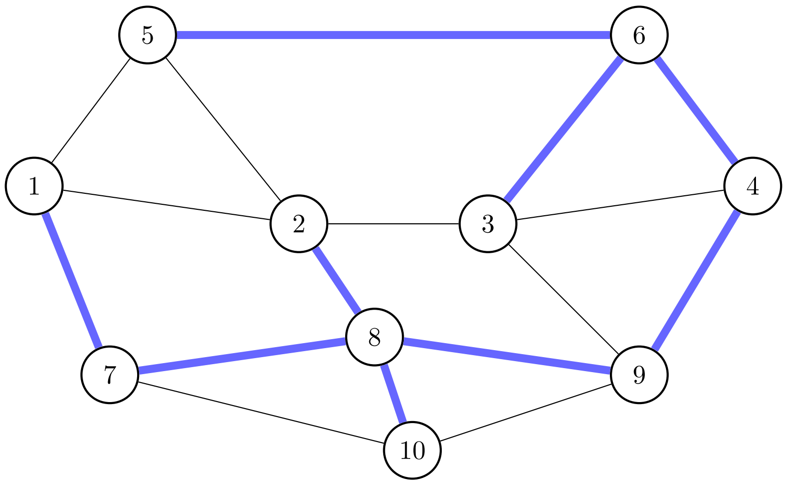


Figure 5.2: A spanning tree

of these paths is also contained in G, and G has the same vertices as T, so from Definition 4.8.1 we conclude that G is connected.

("only if" part.) We are given that G is connected. If G has no cycles, then G itself is a spanning tree of G. Otherwise G has a cycle. Remove any edge e of some cycle. Then $G - e$ is connected, by Theorem 4.10.3, and has fewer cycles than G.

Repeat this process, removing an edge on a cycle at each stage, until we have a connected, spanning subgraph with no cycles. This subgraph is a spanning tree of G. ▮

To show that a graph is connected, using the definition, you need to give a path between any pair of vertices. However, Theorem 5.2.1 provides a much more succinct method: give a spanning tree.

Corollary 5.2.2. *If G is connected, with p vertices and $q = p - 1$ edges, then G is a tree.*

Proof: Let G be a connected graph with p vertices and $q = p - 1$ edges. By Theorem 5.2.1, G has a spanning tree T. Now T is a tree with p vertices, so, by Theorem 5.1.5, T has $p - 1$ edges. However, as G has only $p - 1$ edges, it must be the case that $G = T$. Therefore, G is a tree. ▮

There are a couple of ways to get different spanning trees by exchanging two edges.

Theorem 5.2.3. *If T is a spanning tree of G and e is an edge not in T, then $T+e$ contains exactly one cycle C. Moreover, if e' is any edge on C, then $T+e-e'$ is also a spanning tree of G.*

Proof: Let $e = \{u, v\}$. Any cycle in $T+e$ must use e, since T has no cycles. Such a cycle consists of e along with a u, v-path in T. By Lemma 5.1.3, there is a unique u, v-path in T, hence there is exactly one cycle C in $T+e$.

If e' is any edge in C, then e' is not a bridge (Theorem 4.10.3). So $T+e-e'$ is still connected. Since it has $n-1$ edges, by Corollary 5.2.2, it is a tree. ▮

Theorem 5.2.4. *If T is a spanning tree of G and e is an edge in T, then $T-e$ has 2 components. If e' is in the cut induced by one of the components, then $T-e+e'$ is also a spanning tree of G.*

Proof: The first statement is a direct consequence of Lemma 4.10.2. Let C_1 and C_2 be the two components of $T-e$. Suppose $e' = \{u, v\}$ where $u \in V(C_1)$ and $v \in V(C_2)$.

We wish to show that $T-e+e'$ is connected using Theorem 4.8.2. Let $x \in V(C_1)$. For any $y \in V(C_1)$, there exists an x, y-path since C_1 is connected. Suppose $y \in V(C_2)$. Since C_1 and C_2 are connected, there exist an x, u-path P_1 and a v, y-path P_2. Then P_1, e, P_2 form an x, y-path. Since there exists an x, y-path for any vertex y, $T-e+e'$ is connected.

Since $T-e+e'$ has $n-1$ edges, by Corollary 5.2.2, it is a tree. ▮

5.3 Characterizing Bipartite Graphs

Using Theorem 5.2.1 we will prove an important characterization of bipartite graphs. Note that, we can convince someone that a graph is bipartite by giving them a bipartition. However, it is not so clear how you would convince them that a graph does not have a bipartition. (Checking every partition of $V(G)$ would be tedious.)

One idea is to note that any subgraph of a bipartite graph is bipartite, and so we could try to find a subgraph that is "obviously" not bipartite. An **odd cycle** is a cycle on an odd number of vertices.

Lemma 5.3.1. *An odd cycle is not bipartite.*

Proof: Suppose that C is a cycle with vertex set

$$\{-k, -k+1, \ldots, k\}$$

where $i \sim i+1$ if $-k \le i < k$ and $k \sim -k$. Suppose C is bipartite with bipartition (A, B). Without loss of generality, $0 \in A$. Then $1, -1 \in B$ and it follows easily that for $j = 1, \ldots, k$, the vertices j and $-j$ must be in the same partition. But k and $-k$ are adjacent and they are in the same partition. This is a contradiction, hence C is not bipartite. ∎

So you could certify a graph is not bipartite by producing a subgraph that is an odd cycle. It is quite surprising, but this is all you need to do.

The converse is also true, as we see in the following result.

Theorem 5.3.2. *A graph is bipartite if and only if it has no odd cycles.*

Proof: Given Lemma 5.3, it suffices to prove that if G is not bipartite, then it contains an odd cycle.

Since G is not bipartite, at least one component H of G is not bipartite. (If all components are bipartite, then we could find a bipartition of G by combining the bipartitions of the individual components.) Since H is connected, by Theorem 5.2.1, there exists a spanning tree T in H.

Trees are bipartite (see Problem Set 5.1, Problem 2), so let (A, B) be a bipartition of T. Since H is not bipartite, (A, B) is not a bipartition of H and therefore there exists an edge $\{u, v\}$ of H such that both u and v are in A, or both are in B. By swapping A and B if needed, we may assume that $u, v \in A$.

Since T is connected, there exists a u, v-path P in T, with vertices $x_0 x_1 \ldots x_n$ where $u = x_0$ and $v = x_n$. Since $x_0 = u \in A$ and T is bipartite, the vertices along P must alternate between A and B. So $x_0, x_2, x_4, \ldots \in A$ and $x_1, x_3, x_5, \ldots \in B$. Since $x_n \in A$, n must be even, hence P has even length. However, $x_0 x_n = uv \in E(H)$, so $P + \{u, v\}$ is an odd cycle in H, which is in G. Hence G contains an odd cycle, as claimed. ∎

Problem Set 5.3

1. Let r be a fixed vertex of a tree T. For each vertex v of T, let $d(v)$ be the length of the path from v to r in T. Prove that

   (a) for each edge uv of T, $d(u) \neq d(v)$, and

(b) for each vertex x of T other than r, there exists a unique vertex y such that y is adjacent to x and $d(y) < d(x)$.

2. Let r be a fixed vertex in a graph G. Suppose that, for each vertex v of G we have an integer $d(v)$ such that

   (i) for each edge uv of G, $d(u) \neq d(v)$, and

   (ii) for each vertex x of G other than r, there exists a unique vertex y such that y is adjacent to x and $d(y) < d(x)$.

   Prove that G is a tree.

5.4 Breadth-First Search

We now consider an algorithm for finding a spanning tree in a graph G, if one exists. Note that, by Theorem 5.2.1, this is also a very good way of deciding whether a graph is connected. To describe the algorithm properly we must decide how our graph will be presented to us, and also in what form we will present its output. We assume that the graph is given as a list of edges.

We could present the spanning tree (if it exists) as a list of edges but, given a list of edges it is not obvious if it is a tree, and so we take a more sophisticated approach. We will represent a tree by a function.

Suppose T is a tree and u is a vertex in T. For each vertex x in T distinct from u there is a unique path of length at least one from x to u. Define $\mathrm{pr}(x)$ to be the neighbour of x in this path. We define $\mathrm{pr}(u)$ to be $\emptyset$. The pr is a function from $V(T)$ to $V(T)$. We might call $\mathrm{pr}(x)$ the **parent** or **predecessor** of x.

Clearly if we are given a tree it is easy to write down its predecessor function and, conversely, given the predecessor function we can recover the tree.

So suppose we are given a graph G and we want to find a spanning tree in G. Choose a vertex u in G and set $D = \{u\}$. Define $\mathrm{pr}(u) = \emptyset$.

Now suppose we are given a subset D and a partially completed predecessor function. If $D \neq V(G)$, look for an edge that joins a vertex in D to a vertex not in D. If there is none, then D determines an empty cut and we deduce that G is not connected. If there is an edge vw where $v \in D$ and $w \notin D$, then add w to D and define $\mathrm{pr}(w) = v$. If $D = V(G)$, then our predecessor function describes a spanning tree in G.

Algorithm 5.4.1. *To find a spanning tree of a graph G: Select any vertex r of G as the initial subgraph D, with* $\mathrm{pr}(r) = \emptyset$. *At each stage, find an edge in G that joins a vertex u of D to a vertex v not in D. Add vertex v and edge $\{u, v\}$ to D, with* $\mathrm{pr}(v) = u$. *Stop when there is no such edge.*

Claim:

If $|V(D)| = |V(G)|$ when the algorithm terminates, then D is a spanning tree of G. If $|(D)| < |V(G)|$ when the algorithm terminates, then G is not connected and so, from Theorem 5.2.1, G has no spanning tree.

Proof:

We begin by using mathematical induction on the number of iterations to show that the subgraphs D produced by the algorithm are subtrees of graph G.

Basis Case: Initially, D is a tree with 1 vertex.

Induction Hypothesis: For $k \geq 0$, assume that the subgraph D produced in the k-th iteration is a tree with $k+1$ vertices and k edges.

Inductive Step: If the algorithm terminates in the $(k+1)$st iteration, then there is nothing to prove. Otherwise, the $(k+1)$st iteration produces a subgraph E by adding vertex v and edge $\{u, v\}$ to D. Therefore E has $k+2$ vertices and $k+1$ edges. Since D is tree, there is a path from u to every vertex in D. Since u, v is a path from u to v, there is a path from u to every vertex in E. Therefore, E is connected by Theorem 4.8.2. By Corollary 5.2.2, E is a tree. The iteration ends by redefining D to be the subtree E. By Mathematical Induction, D is a subtree of G in every iteration.

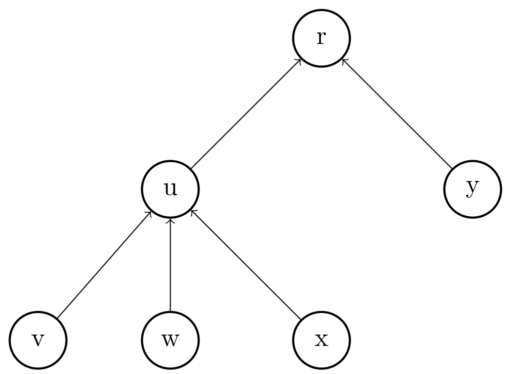
If D has p vertices when the algorithm terminates, then D is a spanning tree because it includes all the vertices of G, as required.

If D has fewer that p vertices when the algorithm terminates, then $V(D)$ is a nonempty, proper subset of $V(G)$. Since the algorithm has terminated, no edge joins a vertex u in D to a vertex v not in D. Therefore, the cut induced by $V(D)$ is empty. This implies that G is not connected by Theorem 4.8.5, as required. ▮

Spanning trees have the important property of being connected. If u and v are vertices of a connected graph, then in any spanning tree there is a unique path joining u and v. Hence spanning trees provide a nice “small" structure by which one can search all the vertices in a graph using only edges of the tree. This is the reason for the parent function $\mathrm{pr}(v) = u$, in which vertex v is referred to as a **child** of u. In a diagram we display this information by placing an arrow on the edge between u and v, pointing from the child v to the parent u, as in Figure 5.3. The initial vertex r is called the root vertex, and has no parent. One can now easily recover paths in the tree. For vertex $v \neq r$, there is a unique positive integer k such that $\mathrm{pr}^k(v) = r$, and the path from v to r is

$$v, \mathrm{pr}(v), \mathrm{pr}^2(v), \ldots, \mathrm{pr}^k(v) = r$$

A path between two vertices u, v can be recovered from Corollary 4.6.3, using the paths from u and v to the root r. Alternatively, we examine parents from u and v until we find a common “ancestor". A spanning tree with this extra structure, provided by the parent functions (the pointers, or the arrows on the diagram) is often called a **search tree**. If $\mathrm{pr}^k(v) = r$ we say that the **level** of v is k, and write level $(v) = k$. We define level (r) to be 0.



$$pr(r) = \phi$$
$$pr(u) = r$$
$$pr(y) = r$$
$$pr(v) = u$$
$$pr(w) = u$$
$$pr(x) = u$$

Figure 5.3: A search tree

In Figure 5.3, r is at level 0, u and y are at level 1, while v, w and x are at level two.

In Algorithm 5.4.1, we looked for edges incident with a vertex in the tree and a vertex not in the tree. Thus it is convenient at each stage to say that a vertex in the tree is **exhausted** if it is not adjacent to a vertex outside the tree. Of course, if a vertex is exhausted at any stage, then it will remain exhausted at all later stages. In Algorithm 5.4.1, we can ignore edges incident with exhausted vertices, since the only possible edges that will allow the tree to increase in size must be incident with an unexhausted vertex in the tree. Now we consider a refinement of Algorithm 5.4.1 called **breadth-first search**, in which the unexhausted vertex u at each stage is chosen in a special way.

Algorithm 5.4.2. *Breadth-first search. Follow Algorithm 5.4.1 with the following refinement: At each stage consider the unexhausted vertex u that joined the tree earliest among all unexhausted vertices (called the* **active** *vertex), and choose an edge incident with this vertex and a vertex v not in the tree.*

A **breadth-first search tree** is any spanning tree that is created by applying breadth-first search to a connected graph.

One way to implement breadth-first search is to use a “queue", that is, a first-in, first-out list for vertices in the tree, where vertices are placed at the end of the queue when they are first added to the tree. At each stage the vertex at the head of the queue is examined. If it is exhausted, it is removed from the queue. Otherwise, it is the active vertex.

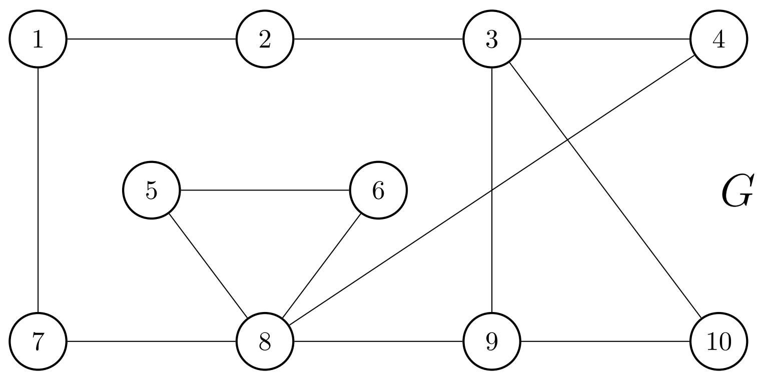


Figure 5.4: Graph G

In Figure 5.5, we illustrate an example of breadth-first search, applied to the connected graph G. We begin the breadth-first search tree B by (arbitrarily) selecting vertex 9 as the root, with pr(9) = $\emptyset$, and thus the queue then consists of vertex 9 alone. Vertex 9 becomes active, and we add vertices 3, 8, 10 to B, at level 1, in that (arbitrary) order, with pr(3) = pr(8) = pr(10) = 9, and the queue becomes 9, 3, 8, 10 (ordered with the head of the queue on the left, and each new vertex joining the queue on the right). Now vertex 9 is exhausted, so it is removed from the queue, and vertex 3 becomes active. Next, vertices 4 and 2 are added to B, with pr(4) = pr(2) = 3, and so vertices 4 and 2 are at level 2, and the queue becomes 3, 8, 10, 4, 2. Vertex 3 is now exhausted, so it is removed from the queue, vertex 8 becomes active, and we add vertices 7, 5, 6 to B in that order, so the queue becomes 8, 10, 4, 2, 7, 5, 6. Now vertices 8, 10, 4 are all exhausted, so the queue becomes 2, 7, 5, 6, and vertex 1 is added to B, at level 3. Finally, all vertices of G are now in B, so all vertices in the queue are exhausted, and we stop. In Figure 5.5, we have placed the vertices at each level from left to right, in the order that they joined the breadth-first search tree B. As a summary, note that the order in which the vertices of G joined B is 9, 3, 8, 10, 4, 2, 7, 5, 6, 1.

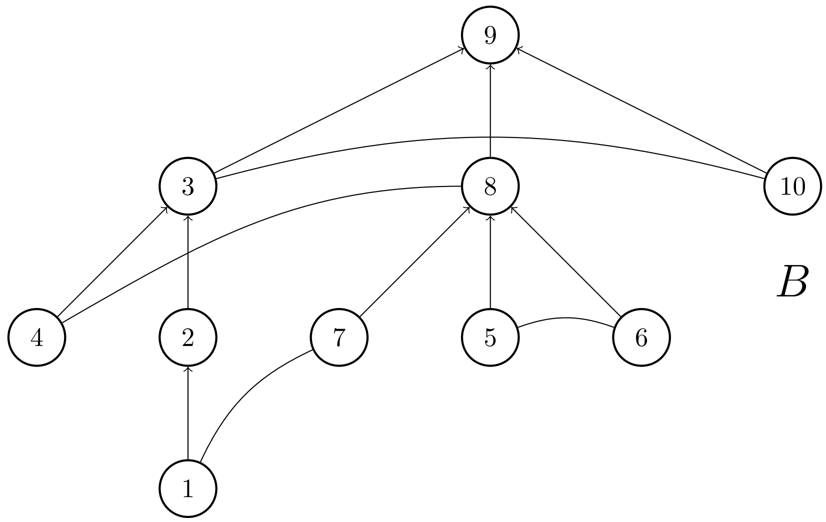


Figure 5.5: A re-drawing of G, with the edges of a breadth-first search tree B indicated with arrows

In Figure 5.5, the edges of B have an arrow to specify the parent. The edges of G that are not contained in the breadth-first search tree B (called **non-tree** edges) have been added to the drawing of B, without arrows. This gives a re-drawing of G that will illustrate the primary property of breadth-first search, given below. First we need a preliminary lemma.

Lemma 5.4.3. *The vertices enter a breadth-first search tree in non-decreasing order of level.*

Proof: We prove this by induction on the number of vertices in the tree at each stage of the algorithm. The first vertex in the tree is the root vertex, with level 0, and the result is true for this first stage.

Now we make the induction hypothesis, that the result is true for the first m vertices in the tree, $m \geq 1$, and consider the next vertex v, that joins the tree at stage $m+1$. Now $\mathrm{pr}(v) = u$, where u is active when v joins the tree, and $\mathrm{level}(v) = \mathrm{level}(u) + 1$. Consider any other non-root vertex x in the tree at stage $m+1$. Then $\mathrm{pr}(x) = y$, and $\mathrm{level}(x) = \mathrm{level}(y) + 1$. But either $y = u$ or y is active before u. In the latter case, y joined the tree before u, so by the induction hypothesis, in either case we have $\mathrm{level}(y) \leq \mathrm{level}(u)$. Thus we have

$$\mathrm{level}(v) = \mathrm{level}(u) + 1 \geq \mathrm{level}(y) + 1 = \mathrm{level}(x),$$

so level(v) ≥ level(x) for all other vertices x in the tree at stage $m+1$, so the result is true at stage $m+1$.

Hence, the result is true by mathematical induction. ▌

For example, it is easy to check that Lemma 5.4.3 holds for the breadth-first search tree B given in Figure 5.5.

This result allows us to establish the following important fact about breadth-first search.

Theorem 5.4.4. *(The primary property of breadth-first search.)*
In a connected graph with a breadth-first search tree, each non-tree edge in the graph joins vertices that are at most one level apart in the search tree (of course each tree edge joins vertices that are exactly one level apart).

Proof: Suppose that vertices u and v are joined by an edge, and without loss of generality, that u joins the tree before v. Thus u is active before v, and there are two cases:

Case 1. v is in the tree when u first is active. Then u and v are joined by a non-tree edge, and $\mathrm{pr}(v) = w$, where w joined the tree before u. Thus level(w) ≤ level(u), by Lemma 5.4.3, so we have

$$\mathrm{level}(v) = \mathrm{level}(w) + 1 \leq \mathrm{level}(u) + 1.$$

But also level(v) ≥ level(u), by Lemma 5.4.3, so we conclude in this case that u and v are joined by a non-tree edge with

$$\mathrm{level}(u) \leq \mathrm{level}(v) \leq \mathrm{level}(u) + 1,$$

and the result is true in this case.

Case 2. v is not in the tree when u first is active. Then v will be added to the tree, with $\mathrm{pr}(v) = u$ and level (v) = level (u) + 1, and the edge between u and v is a tree edge. ▌

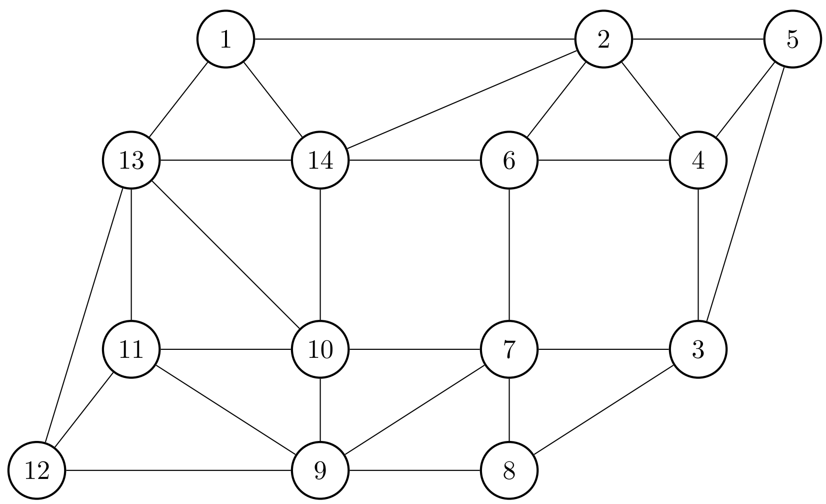
For example, it is easy to check that Theorem 5.4.4 holds for graph G and breadth-first search tree B in Figure 5.5. Here, non-tree edges $\{3,10\}$, $\{5,6\}$ join vertices at the same level, and $\{4,8\}, \{1,7\}$ join vertices one level apart.

Problem Set 5.4

1. Prove that if Algorithm 5.4.1 terminates with subgraph D containing fewer than p vertices, then D is a spanning tree for the component of G containing the initially chosen vertex.

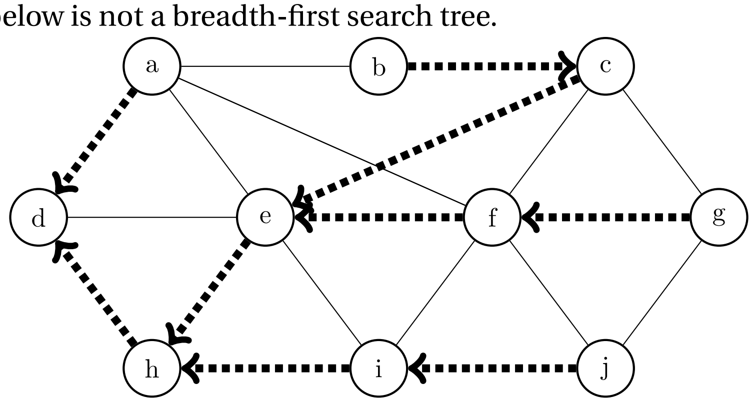
2. Consider a graph G with $V(G) = \{3, 4, 5, \ldots, 25\}$ and with $\{p, q\} \in E(G)$ if and only if either $p|q$ or $q|p$. (Definition: $p|q$ if and only if $q = pr$ for some integer r.) Give a spanning forest of G with the largest number of edges and hence determine the number of components of G.

3. Construct a breadth-first search tree for the graph below, taking vertex labelled 1 as root. When considering the vertices adjacent to the vertex being examined, take them in increasing order of their labels.



4. What graphs have the property that, for a suitable choice of root, the breadth-first search algorithm yields a tree in which all vertices (except the root) are at level 1?

5. Explain why the search tree, rooted at d and indicated by dotted lines in the graph below is not a breadth-first search tree.



6. Prove that if a non-tree edge joins vertices u and v in adjacent levels, say level (v) = level $(u)+1$, then the parent of v is at the same level as u, and was active *before* u.

5.5 Applications of Breadth-First Search

Theorem 5.3.2 provides a nice characterization of bipartite graphs. Moreover, the ideas in Section 5.3 do provide an algorithm to find a bipartition or to find an odd cycle. However, breadth-first search provides a compact and efficient algorithm, as given in the proof of the following result. We refer to this proof as **constructive** because it allows us to construct directly either an odd cycle or a bipartition. Of course, for a graph that is not connected, we would carry this out by applying the construction for each component (and an odd cycle in any component would demonstrate that the graph is not bipartite).

Theorem 5.5.1. *A connected graph G with breadth-first search tree T has an odd cycle if and only if it has a non-tree edge joining vertices at the same level in T.*

Proof: (i) Suppose G has a non-tree edge joining distinct vertices u, v at the same level in T. Then the paths from u and v to the root vertex first meet at a vertex (possibly the root vertex) which is m levels less than u and v, for some $m \geq 1$. Then the path in T between u and v has length $2m$, and together with the non-tree edge $\{u, v\}$ this gives a cycle of length $2m+1$ in G, so G has an odd cycle. (ii) If G has no non-tree edge joining vertices at the same level, then G is bipartite, with bipartition into sets of vertices $A = \{v \in V(G) : \text{level}(v) \text{ is odd }\}$, $B = \{v \in V(G) : \text{ level}(v) \text{ is even}\}$. All edges in G are incident with vertices whose levels differ by one; hence one level must be even and one must be odd, so every edge of G is incident with one vertex in A and one vertex in B. But, from Lemma 5.3, this means that G has no odd cycles. ▮

To find an odd cycle in a connected graph G, we need not construct the entire breadth-first search tree and then look for an edge between vertices at the same level. Instead, we can look for these edges when the tree is being built. At each stage, when we examine the vertex at the head of the queue to see if it is exhausted, we check if there is an edge joining it to a vertex already in the tree, at the same level.

Theorem 5.5.1 illustrates an important application of breadth-first search dealing with parity of cycle lengths. We now consider an application of breadth-first search dealing with shortest paths.

Theorem 5.5.2. *The length of a shortest path from u to v in a connected graph G is equal to the level of v in any breadth-first search tree of G with u as the root.*

Proof: From the primary property of breadth-first search trees we know that no edge of G joins vertices that are more than one level apart. If vertex v is at level k in a breadth-first search tree rooted at u, then there is a path (in the tree) of length k from u to v. There can be no shorter path from u to v in G, since such a path would have to contain an edge joining vertices more than one level apart. ∎

The length of the shortest path between two vertices is often called the **distance** between the vertices. Theorem 5.5.2 implies that we can determine the distance between vertex u and any other vertex in a connected graph G by finding a breadth-first search tree of G rooted at u.

Problem Set 5.5

1. Describe a general procedure to determine a maximal bipartite subgraph of any connected graph G. (A proof that your procedure works is not necessary.)

2. The **diameter** of a graph is the largest of the distances between the pairs of vertices in the graph. Let G be a connected graph of diameter three with exactly 20 vertices at distance three from a given vertex v. Prove that G has some spanning tree T with exactly 20 vertices of degree one at level three.

3. (a) Describe an algorithm to determine the diameter of a graph.

   (b) Prove that this algorithm works.

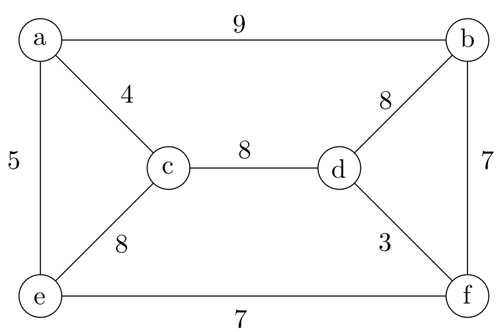
4. Let m, n be integers with $m, n \geq 1$. Let G be a graph (connected) with m vertices at distance n from a given vertex v. Prove that G has a spanning tree with at least m vertices of degree 1.

5. Suppose that a connected graph G has a breadth-first search tree T for which every non-tree edge joins vertices at equal levels. Prove that every cycle of G contains an even number of tree edges.

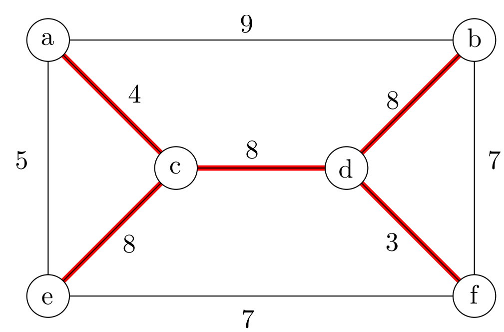
5.6 Minimum Spanning Tree

In the minimum spanning tree (MST) problem, we are given a connected graph G and a weight function on the edges $w : E(G) \to \mathbb{R}$. The goal is to find a spanning tree in G whose total edge weight is minimized.

For example, in the graph to the left, we have a connected graph with the edges being labelled with their weights. In the graph to the right, we have a spanning tree of total weight 31. But is there another spanning tree of smaller weight?



Edge-weighted connected graph G



A spanning tree of weight 31.

This problem is useful in the design of various networks, such as computer networks, road networks, and power grids. The edge weights would represent the costs of building between the two locations. A minimum spanning tree would represent the least amount of cost required to completely connect every location.

There are several efficient algorithms that can solve the MST problem. We present Prim's algorithm here. The idea of Prim's algorithm is that we start with a vertex, and iteratively grow the tree one edge at a time. Each time we grow the tree, we increase the total weight as small as possible.

Prim's algorithm:

1. Let v be an arbitrary vertex in G, let T be the tree consists of just v.

2. While T is not a spanning tree of G...

   (a) Look at all the edges in the cut induced by $V(T)$.

(b) Let $e = uv$ be an edge with the smallest weight in the cut (where $u \in V(T), v \notin V(T)$).

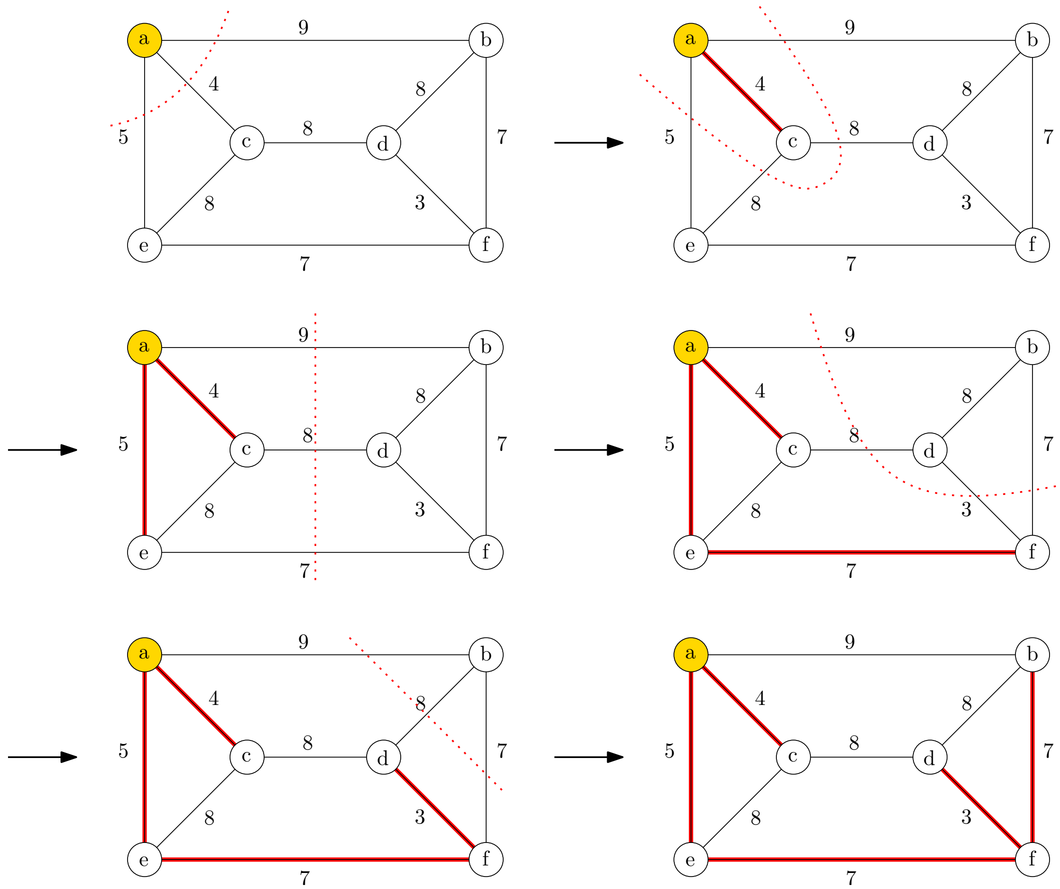
(c) Add v to $V(T)$ and add e to $E(T)$.

Note that in step 2, since T is not a spanning tree of G, $V(T)$ is a non-empty proper subset of $V(G)$. Therefore, by Theorem 4.8.5, the cut induced by $V(T)$ is non-empty, so it is possible to pick an edge from the cut in step 2(b).

Here is an illustration of the algorithm using the example above. We start with the vertex a. In the first iteration, we look at the edges in the cut induced by $\{a\}$, which are $\{ab, ac, ae\}$. Since ac has the smallest weight, we add it to the tree along with vertex c.

In the second iteration, we look at the edges in the cut induced by $\{a, c\}$, which are $\{ab, cd, ce, ae\}$. Since ae has the smallest weight, we add it to the tree along with the vertex e.

We repeat this process until we have a spanning tree. We claim that the tree we produce is a minimum spanning tree.



Prim's algorithm is a greedy algorithm, meaning at each step in the process, we pick the edge that is "best" for our problem. But how do we know that it will always produce a tree of minimum weight? This requires the following proof. For any graph H, we will use the notation $w(H) = \sum_{e \in E(H)} w(e)$.

Theorem 5.6.1. *Prim's algorithm produces a minimum spanning tree for G.*

Proof: Let $T_1, T_2, \ldots, T_n$ be the trees produced by the algorithm at each step, where the order of selection of the edges is $e_1, e_2, \ldots, e_{n-1}$ (i.e. you get T_{i+1} by adding e_i to T_i). We will prove by induction on k that there exists a MST containing T_k as a subgraph.

Base case: For $k = 1$, it is just a vertex, so every MST contains T_1 as a subgraph.

Induction hypothesis: Assume that there exists a MST containing T_k as a subgraph.

Induction step: We need to prove that there is a MST containing T_{k+1} as a subgraph.

Let T^* be a MST that contains T_k as a subgraph, which is assumed by the induction hypothesis. If T^* also contains e_k, then T^* contains T_{k+1} as a subgraph, and we are done. If not, then $e_k \not\subseteq E(T^*)$. This means that $T^* + e_k$ contains a unique cycle C. Now $C - e_k$ is a path between the two endpoints of e_k, one of which is in $V(T_k)$ and the other is not. Therefore, there is at least one edge e' in $C - e_k$ in the cut induced by $V(T_k)$. By Theorem 5.2.3, $T' = T^* + e_k - e'$ is also a spanning tree.

In Prim's algorithm, when we picked e_k, it is an edge in the cut induced by $V(T_k)$ of minimum weight. So $w(e') \geq w(e_k)$. If $w(e') > w(e_k)$, then $w(T') = w(T^*) + w(e_k) - w(e') < w(T^*)$, which is not possible since T^* is a minimum spanning tree. Therefore, $w(e') = w(e_k)$, which means that $w(T') = w(T^*)$. So T' is also a minimum spanning tree, which contains all edges in T_{k+1}. Therefore, T' is the tree we are looking for.

This induction tells us that there is a MST that contains T_n, meaning T_n must equal to the MST. Hence the algorithm produces a MST. ▮

Chapter 6

Codes

6.1 Vector Spaces and Fundamental Cycles

Let $S(G)$ be the set of all spanning subgraphs of the graph G. Let the element of $S(G)$ with no edges be denoted by Z.

The field $GF(2)$ of integers modulo 2 contains two elements, 0 and 1, whose elements are added and multiplied modulo 2 (e.g. $0 \oplus 0 = 1 \oplus 1 = 0$, $1 \oplus 0 = 0 \oplus 1 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$). For any $H \in S(G)$, we define multiplication of H by an element of $GF(2)$ as follows:

$$0 \cdot H = Z, \quad 1 \cdot H = H.$$

Addition of elements of $S(G)$ is also defined.

Definition 6.1.1. *For $H_1, H_2 \in S(G)$ the* **modulo 2 sum** *of H_1 and H_2, denoted by $H_1 \oplus H_2$, is the element of $S(G)$ whose edge set consists of all the edges of G that are in H_1 or H_2* but not in both *(the "symmetric difference" of $E(H_1)$ and $E(H_2)$).*

The set of all spanning subgraphs of G forms a vector space under the operation of mod 2 sum.

Theorem 6.1.2. *The set $S(G)$ is a vector space over $GF(2)$.*

Proof: Look up the definition of a vector space in your linear algebra text. You will find that the scalar multiplication and vector addition defined above must satisfy a list of axioms. These are all easy to verify.

For example, for any $H \in S(G)$,

$$Z \oplus H = H \oplus Z = H,$$

so Z is the “zero" element in $S(G)$. Also

$$H \oplus H = Z,$$

so each element of $S(G)$ has an additive inverse, namely itself. We have defined

$$0 \cdot H = Z,$$

and have, for instance,

$$1 \cdot H \oplus 1 \cdot H = H \oplus H = Z = 0 \cdot H = (1 \oplus 1) \cdot H.$$

Proving that all the axioms of a vector space are satisfied by $S(G)$ is left as an exercise. ∎

Suppose that the edges of G are $e_1, e_2, \ldots, e_q$, and let A_i be the element of $S(G)$ that contains edge e_i, and no other edges, for $i = 1, 2, \ldots, q$.

Theorem 6.1.3. $\{A_1, A_2, \ldots A_q\}$ *forms a basis for* $S(G)$.

Proof: The graphs $A_1, A_2, \ldots A_q$ are all contained in $S(G)$. To prove that they form a basis for $S(G)$, it is sufficient to prove that they (i) span $S(G)$ and (ii) form a linearly independent set.

(i) The elements of $S(G)$ are uniquely specified by their edges. For $H \in S(G)$, if H contains edges $e_{i_1}, e_{i_2}, \ldots, e_{i_k}$, then H can be written as the linear combination

$$H = \alpha_1 A_1 \oplus \cdots \oplus \alpha_q A_q$$

where $\alpha_{i_1} = \alpha_{i_2} = \cdots = \alpha_{i_k} = 1$, and all other α's are equal to 0. Thus $\{A_1, A_2, \ldots, A_q\}$ spans $S(G)$.

(ii) Suppose $\beta_1, \ldots, \beta_q$ are such that

$$\beta_1 A_1 \oplus \cdots \oplus \beta_q A_q = Z.$$

If $\beta_j = 1$ for some j, then the graph on the LHS contains edge e_j. But the graph on the RHS contains no edges, so for equality to hold, we must have $\beta_j = 0$ for all $j = 1, \ldots, q$. Thus $\{A_1, A_2, \ldots, A_q\}$ is a linearly independent set.

∎

This means that $S(G)$ is a vector space of dimension q and contains 2^q elements. Now we look at a subspace of $S(G)$.

Definition 6.1.4. *A graph in which all degrees are even non-negative integers is called an* **even** *graph.*

Let $C(G)$ be the set of even spanning subgraphs of a graph G, so $C(G)$ is a subset of $S(G)$.

Theorem 6.1.5. *The set $C(G)$ forms a vector space over $GF(2)$. (This is a subspace of $S(G)$.)*

Proof: Clearly $Z \in C(G)$, so $C(G)$ is not empty. Thus, to prove that $C(G)$ is a subspace of $S(G)$, it is sufficient to prove that (i) $C(G)$ is closed under scalar multiplication and (ii) $C(G)$ is closed under addition.

(i) Suppose $H \in C(G)$. Then $1 \cdot H = H \in C(G)$, and $0 \cdot H = Z \in C(G)$, since Z has all vertex degrees equal to zero, which is an even non-negative integer.

(ii) Suppose $H_1, H_2 \in C(G)$, and let $d_1(v)$ and $d_2(v)$ denote the degree of v in H_1 and H_2, respectively, for all $v \in V(G)$. Let $m(v)$ be the number of edges incident with v that are contained in both H_1 and H_2. Then the degree of v in $H_1 \oplus H_2$ is

$$(d_1(v) - m(v)) + (d_2(v) - m(v)) = d_1(v) + d_2(v) - 2m(v),$$

which is even, since both $d_1(v)$ and $d_2(v)$ are even, and non-negative, since $d_1(v) \geq m(v)$ and $d_2(v) \geq m(v)$. Thus $H_1 \oplus H_2 \in C(G)$.

∎

We have proved that $C(G)$ is a subspace of $S(G)$, so $C(G)$ is a vector space itself.

In order to find a basis for $C(G)$, we consider a result about trees.

Theorem 6.1.6. *Let T be a spanning tree of a connected graph G. If e is an edge of G that is not in T, then $T + e$ contains a unique cycle. (This cycle contains edge e.)*

Proof: Suppose $e = \{u, v\}$. Since T contains no cycles, any cycle in $T + e$ must contain edge e, so it must consist of e together with a path from u to v in T. But from the Lemma 5.1.3 there is a unique such path, and so $T + e$ contains a unique cycle, which passes through e. ∎

Edges e as described in the above result are called **non-tree** edges. If G has q edges and p vertices, then T has $p-1$ edges, so G has $q-(p-1) = q-p+1$ non-tree edges. Suppose that the non-tree edges are $e_1, e_2, \ldots, e_{q-p+1}$. Let C_i be the spanning subgraph of G whose edges are the edges of the unique cycle in $T+e_i$, for $i = 1, \ldots, q-p+1$. Then C_i is called a **fundamental cycle**, and $\{C_1, C_2, \ldots, C_{q-p+1}\}$ is the set of fundamental cycles of G determined by T.

Lemma 6.1.7. *For a fixed spanning tree T of a connected graph G, no two elements of $C(G)$ contain exactly the same set of non-tree edges.*

Proof: Consider $H \in C(G)$ with no non-tree edges. Then H is a spanning subgraph of T, and is thus a spanning forest of G. If any component of H has more than one vertex, then there are at least two vertices of degree 1 in that component, by Theorem 5.1.8. But H is an even graph, so it can have no vertices of degree 1. Thus all components of H are isolated vertices, so H must be equal to Z. Hence Z is the unique elment in $C(G)$ with no non-tree edges.

Suppose that $H_1, H_2 \in C(G)$, where H_1 and H_2 contain exactly the same set of non-tree edges. Then $H_1 \oplus H_2$ has no non-tree edges. But $H_1 \oplus H_2 \in C(G)$, so $H_1 \oplus H_2 = Z$, since Z is the unique element of $C(G)$ with no non-tree edges. This gives $H_1 = H_2$ and the result follows. ∎

Theorem 6.1.8. $\{C_1, C_2, \ldots, C_{q-p+1}\}$ *forms a basis for $C(G)$, where G is connected.*

Proof: We have $C_i \in C(G)$, for $i = 1, \ldots q-p+1$, since the vertex degrees in C_i are either 2 (for vertices on the cycle in $T+e_i$) or 0 (for the remaining vertices). Thus, to prove that $\{C_1, \ldots, C_{q-p+1}\}$ forms a basis for $C(G)$, it is sufficient to prove that (i) it spans $C(G)$ and (ii) it is a linearly independent set.

(i) From Lemma 6.1.7, the elements of $C(G)$ are uniquely specified by their non-tree edges. For $H \in C(G)$, where H contains non-tree edges $e_{i_1}, e_{i_2}, \ldots, e_{i_m}$, then H can be written as the linear combination

$$H = \alpha_1 C_1 \oplus \cdots \oplus \alpha_{q-p+1} C_{q-p+1}$$

where $\alpha_{i_1} = \alpha_{i_2} = \cdots = a_{i_m} = 1$ and all other α's are equal to 0. Thus $\{C_1, \ldots, C_{q-p+1}\}$ spans $C(G)$.

(ii) Suppose $\beta_1, \ldots, \beta_{q-p+1}$ such that

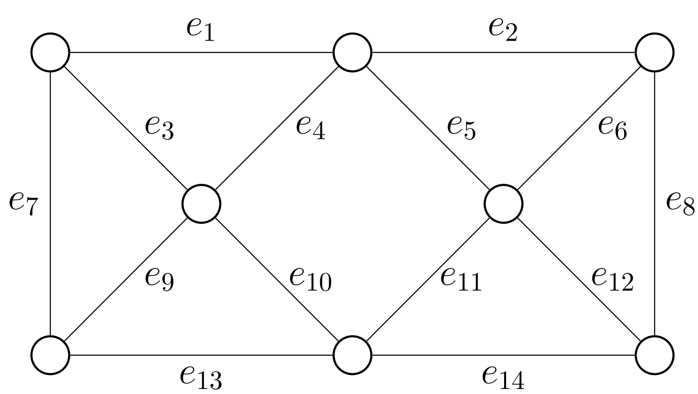
$$\beta_1 C_1 \oplus \cdots \oplus \beta_{q-p+1} C_{q-p+1} = Z.$$

If $\beta_j = 1$ for some j, then the graph on the LHS contains non-tree edge e_j, since C_j is the only fundamental cycle containing non-tree edge e_j. But the graph on the RHS contains no edges, so for equality to hold, we must have $\beta_j = 0$ for all $j = 1, \ldots, q-p+1$. Thus $\{C_1, \ldots, C_{q-p+1}\}$ is a linearly independent set.

∎

This means that $C(G)$ has dimension $q-p+1$ and contains 2^{q-p+1} elements. The cycles of G (together with some isolated vertices) are elements of $C(G)$ and thus can be uniquely expressed as a mod 2 sum of fundamental cycles. We call $C(G)$ the **cycle space** of G. The number $q-p+1$ is known as the **cyclomatic** number of G.

Problem Set 6.1



1. (a) Find the fundamental cycles corresponding to the spanning tree T with edges

$$e_1, e_2, e_5, e_7, e_{10}, e_{11}, e_{14}$$

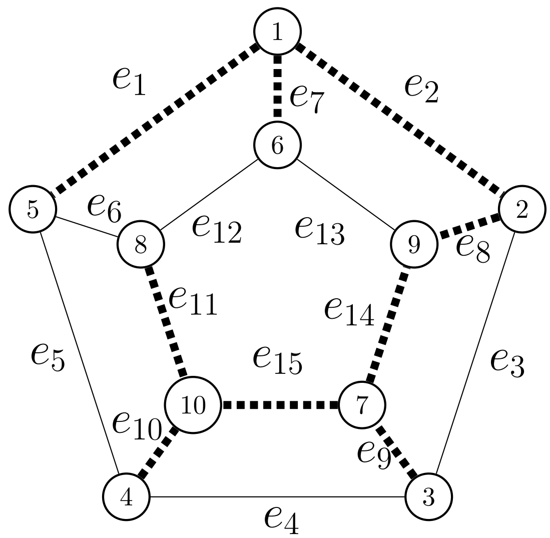
in the above graph. (List their edges.)

(b) Express the spanning even subgraphs with the following edge sets as modulo 2 sums of fundamental cycles from (a):

(i) $E(H_1) = \{e_1, e_2, e_4, e_5, e_7, e_8, e_{10}, e_{11}, e_{13}, e_{14}\}$

(ii) $E(H_2) = \{e_3, e_7, e_9, e_{11}, e_{12}, e_{14}\}$

2. (a) Let T be the spanning tree given by dotted lines in the graph below. Write down the edges in each of the fundamental cycles determined by T.



(b) Express the cycle whose edges are $e_1, e_7, e_{13}, e_{14}, e_{15}, e_{10}$ and e_5, as a modulo 2 sum of fundamental cycles from (a).

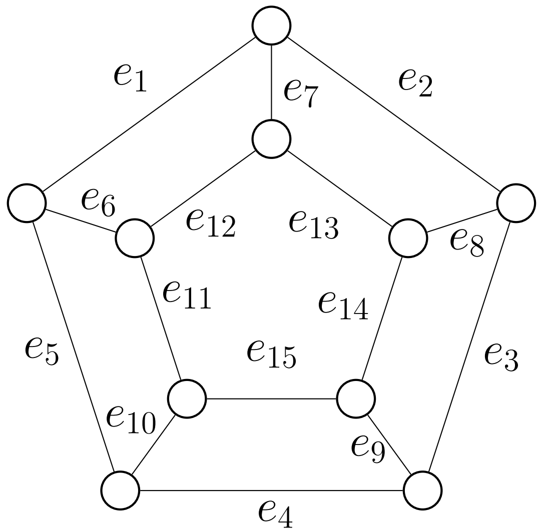
3. In the graph shown below, let T be the spanning tree with edges

$$e_1, e_5, e_6, e_8, e_9, e_{10}, e_{13}, e_{14}, e_{15}.$$

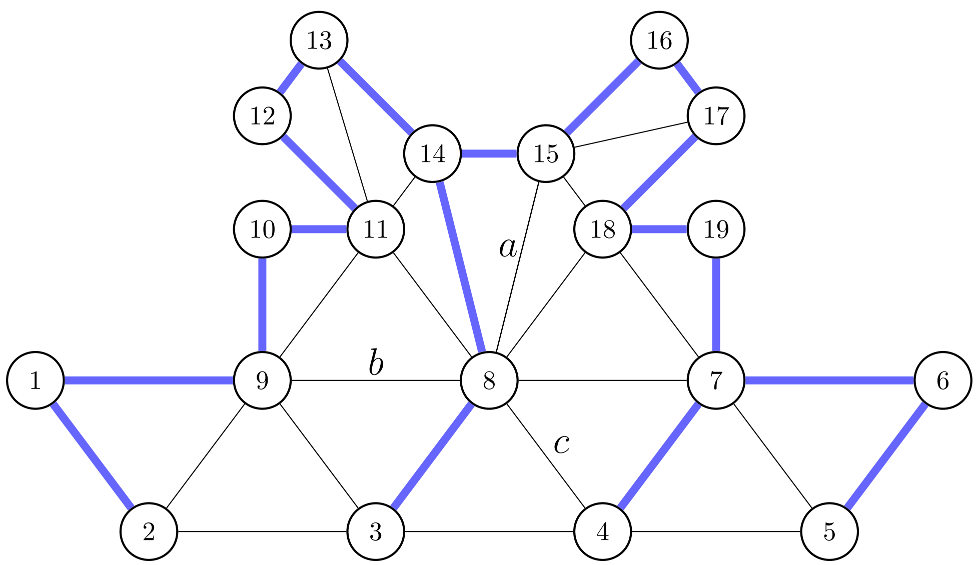
Write down the fundamental cycles determined by T. Also, express the cycle C, whose edges are

$$e_2, e_7, e_{12}, e_{11}, e_{15}, e_{14}, e_8$$

as a linear combination of fundamental cycles.



4. (a) In the graph below, a spanning tree has been constructed. Find the fundamental cycles C_a, C_b and C_c that are determined by the edges a, b and c.



(b) Find also the subgraph $C_a \oplus C_b \oplus C_c$.

5. G is a connected graph with a spanning tree T. For each statement below, either give a proof or find a counterexample.

(a) If G is bipartite, then every fundamental cycle of T must have even length.

(b) If every fundamental cycle of T has even length, then every cycle of G must have even length.

(c) If every fundamental cycle of T has length divisible by 3, then every cycle of G must have length divisible by 3.

6. Prove that a graph which is connected, with 13 vertices and 18 edges, must have at least 6 distinct cycles. Can you find such a graph with 6 edge-disjoint cycles (edge-disjoint means that no edge may belong to more than one of the cycles)?

7. Prove that an edge belongs to $H_1 \oplus H_2 \oplus \cdots \oplus H_k$ if, and only if, it belongs to an odd number of the H_i's where $H_1, H_2, \ldots, H_k \in S(G)$.

8. What is the dimension of $C(G)$ if G has m components, for arbitrary $m \geq 1$?

9. Let $\mathbf{F}(G)$ be the set of spanning subgraphs with an even number of edges of a graph G. (The spanning subgraph containing no edges belongs to $\mathbf{F}(G)$. **Note:** $\mathbf{F}(G)$ is **<u>not</u>** the set of even spanning subgraphs of G.)

   (a) If $F_1, F_2 \in \mathbf{F}(G)$, prove that $F_1 \oplus F_2 \in \mathbf{F}(G)$, where $F_1 \oplus F_2$ is the modulo 2 sum of F_1 and F_2.

   (b) Part (a) implies that $\mathbf{F}(G)$ is a vector space over $GF(2)$. Find a basis for $\mathbf{F}(G)$, and prove that it is a basis. What is the dimension of $\mathbf{F}(G)$, in terms of p and q, the number of vertices and edges in G?

6.2 Graphical Codes

We now explore a nice application of the cycle space of a graph.

Let $G = (V, E)$, $E = \{e_1, \ldots, e_q\}$ be a fixed connected graph. The **characteristic vector** $(x_1, \ldots, x_q)$ of subgraph (V, F) has $x_i = 1$ if $e_i \in F$ and $x_i = 0$ otherwise for $1 \leq i \leq q$. Suppose that $\underline{x}$ and $\underline{y}$ are characteristic vectors of two even subgraphs of G. How many nonzero elements does $\underline{x} \oplus \underline{y}$ contain? It may contain none, if $\underline{x} = \underline{y}$. But if $\underline{x} \neq \underline{y}$, then $\underline{x} \oplus \underline{y}$ is an even subgraph which necessarily contains a cycle; then $\underline{x} \oplus \underline{y}$ must have at least three nonzero entries.

Definition 6.2.1. *The* **Hamming distance** *between two binary vectors $\underline{x}$ and $\underline{y}$ of the same length is the number of 1's in $\underline{x} \oplus \underline{y}$.*

We can equally well speak about the Hamming distance between subgraphs, using their characteristic vectors.

We have essentially proved the following:

Lemma 6.2.2. *In the cycle space of a graph G, any two distinct vectors have Hamming distance at least three.*

Now let us see how to use this observation. Suppose that two people want to communicate over a "channel" (such as a telephone line), capable of sending $0,1$-sequences, but this channel on rare occasions introduces an error by transmitting a 0 when a 1 was intended, or vice versa.

The two people, say Alice and Bob, can agree on a graph $G = (V, E)$ and a labelling $E = \{e_1, \ldots, e_q\}$ of its edges, and further agree only to transmit as messages the characteristic vectors of even subgraphs of G. Suppose that Alice sends a message m to Bob and that Bob receives a message m'; both m and m' are binary vectors of length q. Bob can check whether m' is an even subgraph easily, but can he be sure that the message m' is in fact the message m? If m' is not an even subgraph, Bob is absolutely sure that $m' \neq m$ (naturally, assuming that Alice is playing by the rules and transmitting an even subgraph). But if m' *is* an even subgraph, Bob can only be sure that *either*

- m' is indeed m; or

- the channel introduced at least *three* errors (since m' and m must be at Hamming distance at least three by Lemma 6.2.2).

If errors on the channel are indeed rare, then Bob can reasonably suppose that, if m' is even, it is indeed the message sent by Alice.

Bob can actually do better than this. If only one error was introduced (i.e. $m \oplus m'$ has only one '1' in it), then there is a *unique* even subgraph closest to m. For suppose that $m_1 \oplus m'$ and $m_2 \oplus m'$ both have only one 1; then $(m_1 \oplus m') \oplus (m_2 \oplus m') = m_1 \oplus m_2$ has at most two 1's, and by Lemma 6.2.2, we must have $m_1 = m_2$. So, in particular, m is the **unique** closest vector to m' if only one error was made. Of course, this does not tell us how to *correct* the single error, just that a single error has a unique correction; more on this later.

Let us formalize this. Let C be a set of binary vectors of length q forming a vector space of dimension d; then C has 2^d vectors in it. The **distance** t of C is the minimum Hamming distance between any two distinct vectors of C. Such a set C is called a **binary** (q, d, t)**-error correcting code**, or just a (q, d, t)**-code**. Vectors in C are called **codewords**. The distance of a code is of fundamental importance in its use:

Lemma 6.2.3. *If fewer than t errors are made in the transmission of a codeword, then the received message is either the original codeword, or it is not a codeword at all.*

Lemma 6.2.4. *If at most $\lfloor \frac{t-1}{2} \rfloor$ errors are made in the transmission of a codeword m, the Hamming distance between the received message m' and a codeword is minimum for the unique codeword m.*

Prove these two lemmas for yourself.

Lemma 6.2.5. *The cycle space of a connected graph G on p vertices and q edges is a*
$(q, q-p+1, t)$-code for some $t \geq 3$.

This code is called the **even graphical code** of G. What is the distance of such a code?

If G has a cycle of length ℓ, this cycle has Hamming distance ℓ from the void graph Z. So evidently the girth g of G is an upper bound on the distance. Can two even subgraphs S_1 and S_2 have Hamming distance less than g? Consider $S_1 \oplus S_2$. If $S_1 \neq S_2$, then $S_1 \oplus S_2$ is an even subgraph, and hence it contains a cycle. But all cycles have at least g edges, and so

Lemma 6.2.6. *The distance of the even graphical code of G equals the girth of G.*

As an aside, let's observe that we can extend our definition of cycle space to multigraphs in which repeated edges are permitted. If we choose the two vertex multigraph with q edges between the vertices, the cycle space is just the set of all binary vectors of length q with an even number of 1's. This is the standard **even parity** code.

We are left with a significant question: correcting errors. Suppose that an even subgraph M is transmitted, but that a subgraph S is received which is *not* even. Now $S = M \oplus E$, where E marks the positions in which a transmission error was made; equivalently, $M = S \oplus E$. Both E and M are unknown to us; however, we do know *all* of the valid codewords, and when G has girth g, we assume that at most $\lfloor \frac{g-1}{2} \rfloor$ errors were introduced. Under this assumption, E cannot contain a cycle (why?). To find E, let's observe that a vertex v has odd degree in S if and only if it has odd degree in E (for it surely has even degree in M). So E is a subgraph of G with a specified set of odd degree vertices and as few edges as possible. There is only one candidate for E, since if $S \oplus E_1$ and

$S \oplus E_2$ are codewords and $E_1 \neq E_2$, $E_1 \oplus E_2$ is a nonzero codeword — so we have a contradiction unless more than $\lfloor \frac{g-1}{2} \rfloor$ errors were made. When the number of errors is "small", E can easily be found by brute-force techniques; when larger, algorithms for weighted matching in graphs can be used (this material is covered in C&O 450).

(Aside: Essentially what we do in the general case is to identify the set W of odd degree vertices of S. There must be an even number $2s$ of them by the handshake theorem. We choose a labelling of the vertices in W as $x_1, \ldots, x_s,\ y_1, \ldots, y_s$ so that the sum of the distances between x_i and y_i for $i = 1, \ldots, s$ is *minimum* over all labellings of the vertices. Then find paths $P_1, \ldots, P_s$ where P_i is a shortest path between x_i and y_i. Determine $E = P_1 \oplus P_2 \oplus \cdots \oplus P_s$. Finally compute $M = S \oplus E$ to correct the errors, if any.)

One topic of interest is to determine which graphs give "good" codes (large distance, large dimension and small length). These amount to requiring "large" girth, "large" cyclomatic number, and "small" number of edges. The Petersen graph gives a $(15,6,5)$-code, for example. Finding the best codes (and even the best graphical codes) is a challenging problem, discussed in much more detail in CO 331.

Problem Set 6.2

1. Produce all codewords in the even graphical code of K_4. Determine the length, distance and dimension.

2. Produce all codewords in the even graphical code of $K_{3,3}$. Determine the length, distance and dimension.

3. Prove that every connected graph on an even number of vertices has a spanning subgraph in which all vertices have odd degree. (Hint: consider modulo 2 sums of paths.)

4. If G is a connected graph on an even number of vertices, Problem 3 ensures that G has an odd subgraph S. Consider the vector space $C(G)$ of even subgraphs and let $C^+(G) = C(G) \cup \{H \oplus S : \ H \in C(G)\}$. Is $C^+(G)$ a vector space under modulo 2 sum? Compute the length, distance and dimension of the corresponding code.

5. Using Problem 4, extend the $(15,6,5)$-code from the Petersen graph to a $(15,7,5)$-code. Describe all codewords.

Chapter 7

Planar Graphs

7.1 Planarity

Definition 7.1.1. *A graph G is* **planar** *if it has a drawing in the plane so that its edges intersect only at their ends, and so that no two vertices coincide. The actual drawing is called a* **planar embedding** *of G, or a* **planar map**.

For example, the 3-cube, which we previously considered in Figure 4.12, is a planar graph, with a planar embedding given in Figure 7.1. A planar graph may have a number of essentially different embeddings.

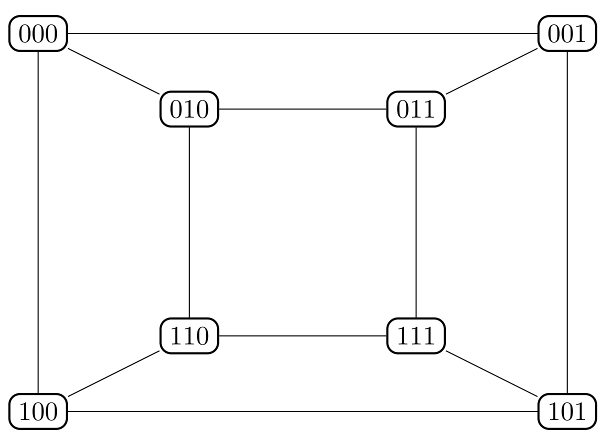


Figure 7.1: A planar embedding of the 3-cube

It is clear that a graph is planar if and only if each of its components is planar. So it is often sufficient to consider only connected planar graphs and connected planar embeddings.

A planar embedding partitions the plane into connected regions called **faces**; one of these regions, called the outer face, is unbounded. For example, the planar embedding given in Figure 7.2 has 4 faces, identified as f_1, f_2, f_3, f_4 in the diagram. In this case, the outer face is f_4.

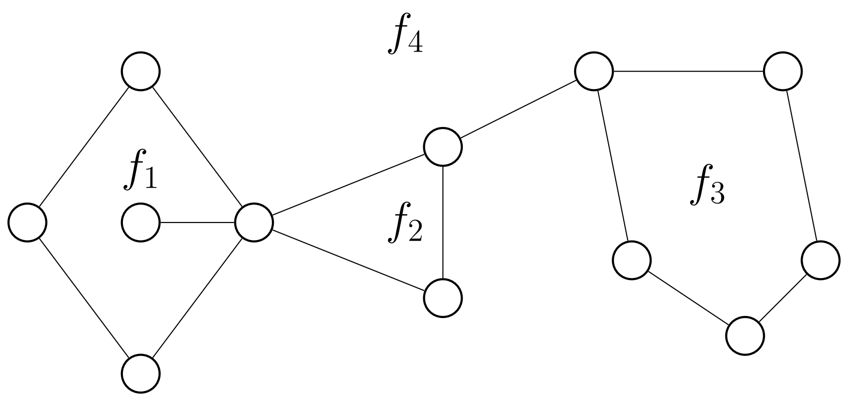


Figure 7.2: A planar embedding with 4 faces

Consider a planar embedding of a connected graph G. The subgraph formed by the vertices and edges in a face is called the **boundary** of the face. We say that two faces are **adjacent** if they are incident with a common edge. Assume, for the moment, that G is connected. As one moves around the entire perimeter of a face f, one encounters the vertices and edges in a fixed order, say

$$W_f = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_n)$$

where $v_n = v_0$. This sequence is a closed walk of the graph G, and we call it the **boundary walk** of face f. (The boundary walk can start at any vertex, and can proceed around the perimeter in either a clockwise or counterclockwise direction.) The number of edges in the boundary walk W_f is called the **degree** of the face f. For example, in Figure 7.2,

$$\deg(f_1) = 6,\ \deg(f_2) = 3,\ \deg(f_3) = 5,\ \deg(f_4) = 14.$$

In Figure 7.1, all faces have degree 4. Note that a bridge of a planar embedding is incident with just one face, and is contained in the boundary walk of that face twice, once for each side. Thus a bridge contributes 2 to the degree of the face with which it is incident. On the other hand, if e is an edge of a cycle of an embedding, e is incident with exactly two faces, and is contained in the boundary walk of each face precisely once.

Every edge in a tree is a bridge, so a planar embedding of a tree T has a single face of degree $2|E(T)| = 2|V(T)| - 2$.

In what follows we may use 's' for the number of faces in a planar embedding.

Theorem 7.1.2. *If we have a planar embedding of a connected graph G with faces $f_1, \ldots, f_s$, then*

$$\sum_{i=1}^{s} \deg(f_i) = 2|E(G)|.$$

Proof: Each edge has two sides, and when we sum the degrees of the faces we are counting the edges twice, once for each side. ▌

Note the similarity between Theorem 7.1.2 and Theorem 4.3.1. This theorem is colloquially known as the **Faceshaking Lemma** or the **Handshaking Lemma for Faces**. We shall make a direct link between these results later when we consider the dual of a planar embedding.

Corollary 7.1.3. *If the connected graph G has a panar embedding with f faces, the average degree of a face in the embedding is $\frac{2|E(G)|}{f}$.*

So far our discussion deals with planar embeddings that are *connected.* For a planar embedding of a disconnected graph, there could be faces whose boundaries lie on several components, and a closed walk around the boundary is not possible. For such faces, we alternatively define their degrees to be the sum of the lengths of the boundaries around each component. For example, in the embedding in Figure 7.3, the face f is incident with 3 components of the graph. The boundary walks around these 3 components have lengths 5, 4, and 2, so the degree of face f is 11.

Note that each edge is still counted twice among all boundaries walks, so Theorem 7.1.2 also holds for disconnected graphs.

7.2 Euler's Formula

There are often a number of completely different planar embeddings of a planar graph. However, every planar embedding of a given connected planar graph has the same number of faces, a fact that we can deduce from the following result, called **Euler's Formula**.

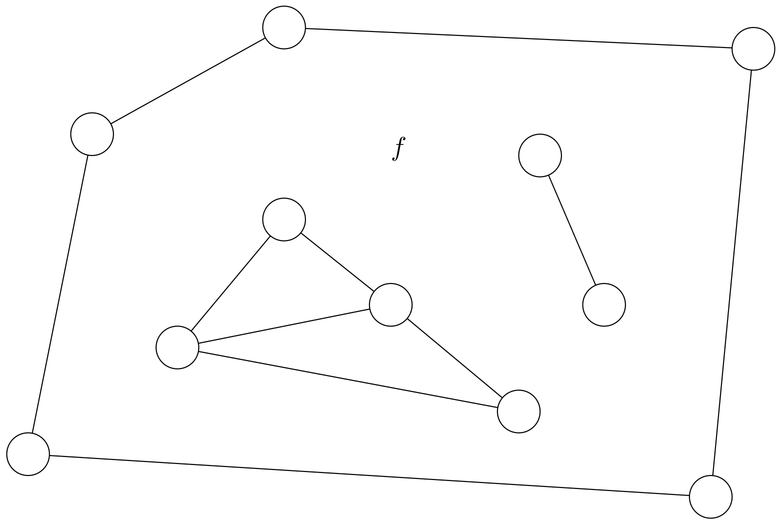


Figure 7.3: A planar embedding of a disconnected graph

Theorem 7.2.1. *(Euler's Formula) Let G be a connected graph with p vertices and q edges. If G has a planar embedding with f faces, then*

$$p - q + f = 2.$$

Proof: For each positive integer p, we prove this result by induction on q. Since G is a connected, it has a spanning tree and so $q \geq p - 1$.

As a tree has no cycles, any planar embedding of a tree has just one face, and the theorem holds.

So assume $q > p - 1$, and assume inductively that Euler's formula is true for any connected graph on p vertices with fewer than q edges. Suppose that we have a planar embedding of G with f faces. Since $q \geq p$ we see that G is not a tree and therefore it has an edge $e = \{u, v\}$ that is not a bridge. Then we also have a planar embedding of $G \setminus e$ (the graph we get from G by deleting the edge e). Since $G \setminus e$ has p vertices and $q - 1$ edges and is connected, it follows by induction that if it has f_1 faces, then

$$p - (q - 1) + f_1 = 2$$

and therefore $f_1 = q + 1 - p$. If we put e back into our drawing, it divides a face into two. So the embedding of G has one more face than that of $G \setminus e$. Hence the number of faces in the embedding of G is $q + 2 - p$ and then

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

As an example of Euler's Formula, consider the connected planar embedding in Figure 7.2. In this case there are 12 vertices, 14 edges and 4 faces and $12 - 14 + 4 = 2$, as expected.

7.3 Stereographic Projection

There is a lack of symmetry among the faces of a planar map—one of the faces is unbounded. Symmetry can be achieved, making all the faces bounded, by considering embeddings on the surface of a sphere rather than on the plane. The main result in this section is the following:

Theorem 7.3.1. *A graph is planar if and only if it can be drawn on the surface of a sphere.*

Any drawing on the plane can be converted to a drawing on the sphere via **stereographic projection**. Let the sphere be tangent to the plane at point A, and let B be antipodal to A on the sphere. In stereographic projection, the image of each point x on the plane is the unique point x' on the surface of the sphere that lies on the line between x and B. This is illustrated in Figure 7.4.

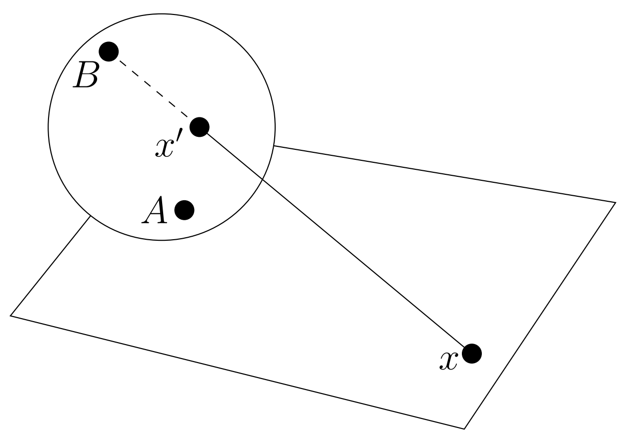


Figure 7.4: Stereographic projection

If we apply stereographic projection to a planar embedding, we obtain a drawing of the graph on the surface of the sphere (with no edges crossing), in which all faces are bounded, and B is in the interior of a face.

On the other hand, given any face f of an embedding G on the sphere, stereographic projection provides a way to obtain a planar embedding H in which the outer (unbounded) face corresponds to f—turn the sphere so that point B lies in face f, and then project the embedding G to the plane to get H. If we redraw an embedding so that a different face becomes the outside face, we consider this to be the same as the original embedding. Roughly speaking, we have the same graph, and the same faces, and the same faces are incident with the the same edges, so they are essentially the same embedding. In particular the number of faces of degree i in two embeddings related in this way will be equal.

A graph may have a number of essentially different planar embeddings. Figure 7.5 exhibits two embeddings of a planar graph. In the first embedding there are two faces of degree three and two of degree five; in the second, there are two faces of degree three, one of degree four and one of degree six. It is reassuring to note that in both embeddings there are four faces (so Euler is happy) and the sum of the faces degrees is 16 in both embeddings, as it should be by Theorem 7.1.2.

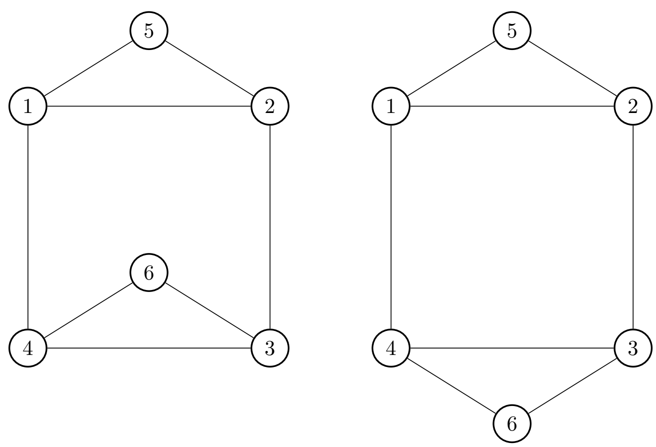


Figure 7.5: Embeddings of a Planar Graph

Problem Set 7.3

1. Prove that every planar embedding has either a vertex of degree at most 3 or a face of degree 3.

2. Prove that each of the graphs shown in Figure 7.6 is planar, by exhibiting a planar embedding.

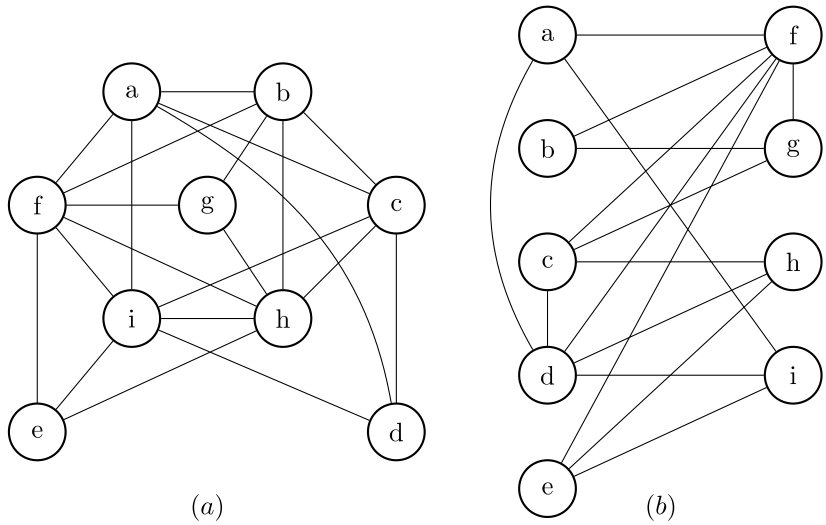


Figure 7.6: Planarity exercises

3. Let $n \geq 3$ be an integer. Suppose that a convex n-gon is drawn in the plane, and then each pair of nonadjacent corner points is joined by a straight line through the interior. Suppose that no 3 of these lines through the interior meet at a common point in the interior. (Figure 7.7 shows such a drawing with $n = 6$.)

   Let f_n be the number of regions into which the interior of the n-gon is divided by this process. (So $f_3 = 1,\ f_4 = 4,\ f_5 = 11$.) Use Euler's Formula to find f_n. (Hint: any set of 4 corner points of the n–gon uniquely determines a pair of intersecting lines in the interior.)

7.4 Platonic Solids

Consider the two geometric solids in Figure 7.8; the cube and the tetrahedron. These polyhedra exhibit a great deal of symmetry. In particular, the faces have the same degree and the vertices have the same degree. We call all such polyhedra **platonic solids**. Surprisingly, there are just five platonic solids: the tetrahedron, the cube, the octahedron, the dodecahedron, and the icosahedron. In this section we will outline a proof of this remarkable fact.

From each platonic solid, we can obtain a planar embedding in which all vertices have the same degree $d \geq 3$ and all faces have the same degree $d^* \geq 3$;

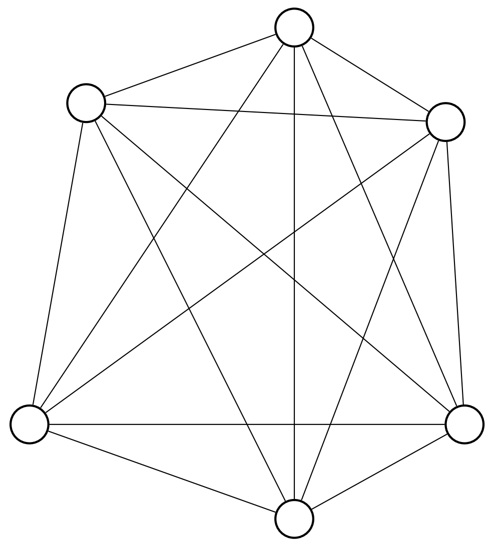


Figure 7.7: A convex 6-gon with diagonals

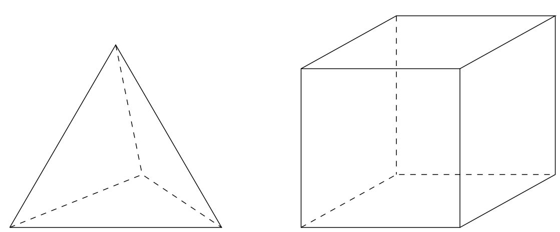


Figure 7.8: The tetrahedron and the cube

see Figure 7.9. We call a graph **platonic** if it admits a planar embedding in which each vertex has the same degree $d \geq 3$ and each face has the same degree $d^* \geq 3$. We will show that the only platonic graphs are those given in Figure 7.9, from which it is easy to deduce that there are just five platonic solids.

Theorem 7.4.1. *There are exactly five platonic graphs.*

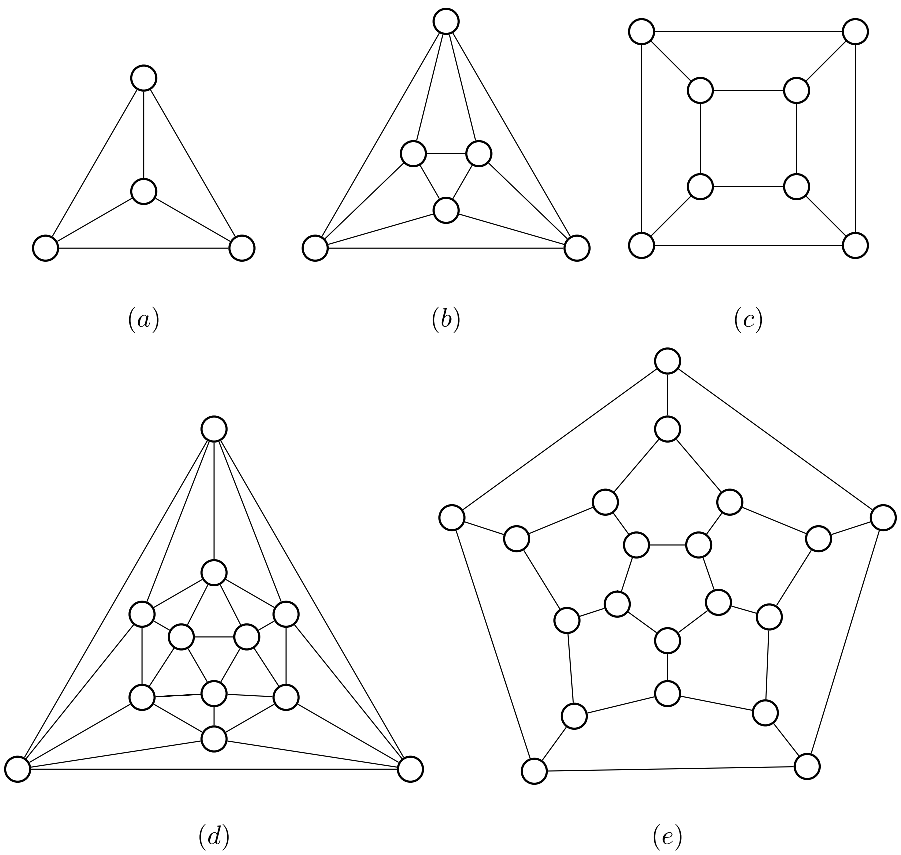


Figure 7.9: (a) the tetrahedron; (b) the octahedron; (c) the cube;(d) the icosahedron; (e) the dodecahedron

We require the following lemma.

Lemma 7.4.2. *Let G be a planar embedding with p vertices, q edges and s faces, in which each vertex has degree $d \geq 3$ and each face has degree $d^* \geq 3$. Then (d, d^*) is one of the five pairs*

$$\{(3,3),\ (3,4),\ (4,3),\ (3,5)\ (5,3)\}.$$

Proof: Assume $p = |V(G)|$, $q = |E(G)|$ and that there are exactly f faces in the embedding. From Euler,

$$p - q + f = 2.$$

Since G is regular with degree d, we have $2q = dp$ by Theorem 4.3.1. Since each face of the embedding has degree d^*, we have $2q = d^* f$ by Theorem 7.1.2. Hence $p = 2q/d$ and $f = 2q/d^*$. So we can write Euler's equation as

$$2 = \frac{2q}{d} - q + \frac{2q}{d^*} = q\left(\frac{2}{d} - 1 + \frac{2}{d^*}\right).$$

We rewrite this in turn as

$$\frac{2}{d} + \frac{2}{d^*} = 1 + \frac{2}{q}. \tag{7.4.1}$$

The basic idea now is to note that the right side of this equality is greater than 1, while the left is struggling to reach 1.

If $d = 3$ and $d^* \geq 6$, then

$$\frac{2}{d} + \frac{2}{d^*} \leq \frac{2}{3} + \frac{2}{6} = 1.$$

If $d = 4$ and $d^* \geq 4$, then

$$\frac{2}{d} + \frac{2}{d^*} \leq \frac{2}{4} + \frac{2}{4} = 1.$$

If $d = 5$ and $d^* \geq 4$, then

$$\frac{2}{d} + \frac{2}{d^*} \leq \frac{2}{5} + \frac{2}{4} = \frac{18}{20} < 1.$$

Finally, if $d \geq 6$ and $d^* \geq 3$, then

$$\frac{2}{d} + \frac{2}{d^*} \leq \frac{2}{6} + \frac{2}{3} = 1.$$

It follows that (d, d^*) must be one of the five pairs in the statement of lemma. ∎

Lemma 7.4.3. *If G is a platonic graph with p vertices, q edges and f faces, where each vertex has degree d and each face degree d^*, then*

$$q = \frac{2dd^*}{2d + 2d^* - dd^*}$$

and $p = 2q/d$ and $f = 2q/d^*$.

Proof: In proving the previous lemma we saw that

$$2 = q\left(\frac{2}{d} - 1 + \frac{2}{d^*}\right).$$

and the formula for q follows at once from this. We also saw that $2q = pd = fd^*$, which yields the other two claims. ∎

To prove Theorem 7.4.1, we look at the five possible values for (d, d^*) given in the previous lemma, and show that in each case there is a unique planar embedding with the required parameters. We will consider the first two cases; the remaining three cases are left as exercises.

Case 1: $d = 3$, $d^* = 3$.

Thus $q = \frac{2\cdot3\cdot3}{2\cdot3+2\cdot3-3\cdot3} = 6$, $p = \frac{2\cdot6}{3} = 4$, and $s = \frac{2\cdot6}{3} = 4$. Note that K_4 is the only graph having 4 vertices and 6 edges.

Case 2: $d = 3$, $d^* = 4$.

Thus $q = \frac{2\cdot3\cdot4}{2\cdot3+2\cdot4-3\cdot4} = 12$, $p = \frac{2\cdot12}{3} = 8$, and $s = \frac{2\cdot12}{4} = 6$. Consider a planar embedding G with these parameters. Since each face has degree 4, no vertex can be repeated in a boundary walk, so each face boundary is a 4–cycle. Let $C = (v_1, v_2, v_3, v_4, v_1)$ be the boundary of one of the faces of G. If v_1 is adjacent to v_3 then (v_2, v_3, v_1, v_2) is part of some boundary walk. This contradicts that each face is bounded by a 4–cycle. Therefore, v_1 is not adjacent to v_3, and, similarly, v_2 is not adjacent to v_4. Since each vertex has degree 3, v_i has a unique neighbour u_i not in C, for $i = 1, 2, 3, 4$. Note that u_1, v_1, v_2, u_2 is part of the boundary walk of some face, so $u_1 \neq u_2$ and u_1u_2 is an edge. Similarly u_2u_3, u_3u_4, and u_4u_1 are also edges. If $u_1 = u_3$ then u_4 is only incident with two faces, namely $(u_4, v_4, v_1, u_1, u_4)$ and $(u_4, v_4, v_3, u_1, u_4)$. This contradicts that u_4 has degree 3, and, hence, $u_1 \neq u_3$. By symmetry, $u_2 \neq u_4$. Therefore G is the 3–cube.

Problem Set 7.4

1. Show that there is a unique planar embedding in which each vertex has degree 4 and each face has degree 3.

2. Show that there is a unique planar embedding in which each vertex has degree 3 and each face has degree 5.

3. Show that there is a unique planar embedding in which each vertex has degree 5 and each face has degree 3.

7.5 Nonplanar Graphs

In order to prove that a graph is planar, we can find a planar embedding. How would we prove that a graph is nonplanar? In this section we will see that in some case we can use Euler's formula to do this.

We need one technical result before we can start.

Lemma 7.5.1. *If G does not contain a cycle, then in a planar embedding of G, the boundary of each face contains a cycle.*

Proof: Since G has a cycle, it has more than one face.

Therefore, every face f is adjacent to at least one other face, say g.

Let $e_1 = \{v_0, v_1\}$ be an edge that is incident with both f and g. Let H be the component in the boundary of face f containing the edge e_1. Let

$$W_f = (v_0, e_1, v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_0)$$

be the boundary walk of H. Since the edge e_1 is incident with both f and g, it is contained in W_f precisely once.

The edge e_1 is not a bridge of H because

$$(v_1, e_2, v_2, \ldots, v_{n-1}, e_n, v_0)$$

is a walk from v_1 to v_0 in $H - e_1$. Therefore, by Theorem 4.10.3, H contains a cycle. This establishes the result. ∎

Lemma 7.5.2. *Let G be a planar embedding with p vertices and q edges. If each face of G has degree at least d^*, then $(d^* - 2)q \leq d^*(p-2)$.*

Proof: We first deal with the case when G is connected. Let $f_1, f_2, \ldots, f_s$ be the faces of G. Thus, applying Theorem 7.1.2, we have

$$2q = \sum_{i=1}^{s} \deg(f_i) \geq \sum_{i=1}^{s} d^* = d^* s.$$

Now, by Euler's Formula, $s = q + 2 - p$. So,

$$2q \geq d^* s = d^*(q + 2 - p) = d^* q + 2d^* - d^* p.$$

Therefore, $(d^* - 2)q \leq d^*(p-2)$.

If G is not connected, then we obtain G' as follows: For each face f in the embedding incident with at least 2 components, pick two of these components, and pick one vertex from each component that is incident with f. Add an edge joining these two vertices. Since we may draw the edge in f, the resulting embedding is still planar. Also, the number of components is reduced by 1. Repeat this process until we have a connected planar embedding G'. Since the degree of a face does not decrease in this process, every face of G' still has degree at least d^*. Therefore, the inequality holds for G'. But G has fewer edges than G', so the inequality also holds for G. ▌

Lemma 7.5.2 relies on a given planar embedding, since it involves the face degrees. We would like similar inequalities for *planar graphs*. The following lemma allows us to relate face degrees to the lengths of cycles, which are independent of the embedding.

Note that a graph with p vertices can have as many as $p(p-1)/2$ edges, a quadratic function of p. However, this is not the case for planar graphs. The following theorem shows that the number of edges in a planar graph is bounded by a linear function in the number of vertices p. (Note that if we allow multiple edges or loops, fixing p does not bound the number of edges; for example, the graph in Figure 7.10 has $p = 2$ vertices and q edges for any positive integer q.)

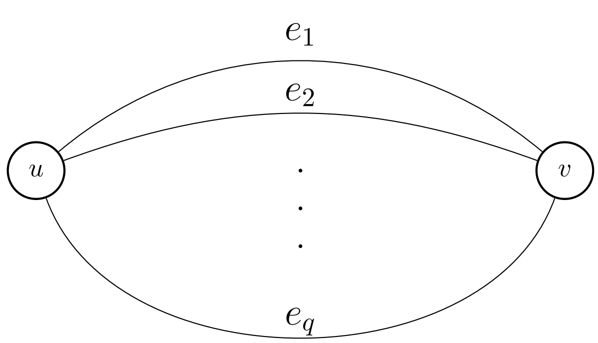


Figure 7.10: Multiple edges in a planar multigraph

Theorem 7.5.3. *In a planar graph G with $p \geq 3$ vertices and q edges, we have*

$$q \leq 3p - 6.$$

Proof: If G does not contain a cycle, them G is a forest. By Corollary 5.1.6, $q \leq p - 1 \leq 3p - 6$ whenever $p \geq 3$.

If G contains a cycle, then by Lemma 7.5.1, every face boundary contains a cycle. Since each cycle in G has length at least three, each face has degree at least 3. By Lemma 7.5.2,

$$q \leq 3(p-2)/(3-2) = 3p-6.$$

∎

Theorem 7.5.3 gives an inequality that holds for all planar graphs. Therefore, if a graph does not satisfy the inequality, then it is not planar. We illustrate this idea below on K_5.

Corollary 7.5.4. *K_5 is a not planar.*

Proof: We have

$$|E(K_5)| = \binom{5}{2} = 10.$$

But $3p-6 = 15-6 = 9$, so for K_5 we have

$$q = 10 > 9 = 3p-6,$$

and the inequality $q \leq 3p-6$ does not hold. We conclude from Theorem 7.5.3 that K_5 is not a planar graph. ∎

Notice that Theorem 7.5.3 is only a necessary condition for a graph to be planar. If a graph satisfies $|E(G)| \leq 3|V(G)|-6$, it does **not** follow that it is planar. As an example, consider the graph of Figure 7.11. Since it has K_5 as a subgraph, it cannot be planar, but $|E(G)| = 11 < 12 = 3|V(G)|-6$.

Corollary 7.5.5. *A planar graph has a vertex of degree at most five.*

Proof: This is true if $|V(G)| \leq 2$. If $p = |V(G)| \geq 3$ and $q = |E(G)|$ then by Theorem 7.5.3,

$$q \leq 3p-6$$

and therefore

$$\frac{2q}{p} \leq 6 - \frac{12}{p}.$$

This shows that the average degree of a vertex in G is less than six, and therefore G contains a vertex of degree at most five. ∎

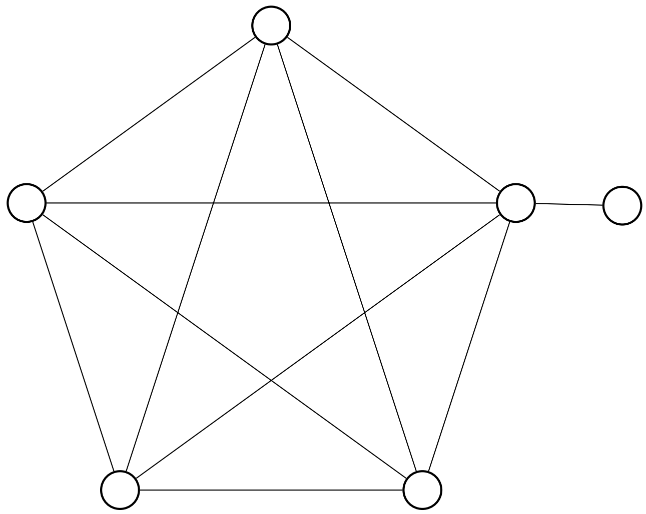


Figure 7.11: A nonplanar graph with $q \leq 3p-6$

After a few attempts to make a planar embedding of $K_{3,3}$, you will conclude that it also is not planar. However, neither Theorem 7.5.3 nor Corollary 7.5.5 implies that $K_{3,3}$ is not planar. (You should check this.) Nevertheless, one can repeat the proof of Theorem 7.5.3 with an additional observation to obtain a result strong enough to prove that $K_{3,3}$ is not planar.

Theorem 7.5.6. *In a bipartite planar graph G with $p \geq 3$ vertices and q edges, we have*

$$q \leq 2p-4.$$

Proof: If G does not contain a cycle, then G is a forest. By Corollary **??**, $q \leq p-1 \leq 2p-4$ whenever $p \geq 3$.

If G contains a cycle, then by Lemma 7.5.1, every face boundary contains a cycle. Since G is bipartite, it does not have cycles of length 3. Hence each cycle in G has length at least 4, and each face has degree at least 4. By Lemma 7.5.2,

$$q \leq 4(p-2)/(4-2) = 2p-4.$$

∎

Lemma 7.5.7. *$K_{3,3}$ is not planar.*

Proof: We have

$$|E(K_{3,3})| = 3 \cdot 3 = 9.$$

But $2p - 4 = 2 \cdot 6 - 4 = 8$, so for $K_{3,3}$ we have

$$q = 9 > 8 = 2p - 4$$

and the inequality $q \le 2p - 4$ does not hold. We conclude from Theorem 7.5.6 that $K_{3,3}$ is not a planar graph. ∎

7.6 Kuratowski's Theorem

We have been able to prove by counting arguments that two graphs, K_5 and $K_{3,3}$, are not planar. We are going to see how we can use graphs based on K_5 and $K_{3,3}$ to certify that a graph is not planar.

First we need some language to properly state our result.

An **edge subdivision** of a graph G is obtained by applying the following operation, independently, to each edge of G: replace the edge by a path of length 1 or more; if the path has length $m > 1$, then there are $m - 1$ new vertices and $m - 1$ new edges created; if the path has length $m = 1$, then the edge is unchanged. For example, Figure 7.12 shows a graph H, and an edge subdivision G of H.

Note that the operation of edge subdivision does not change planarity: if G is a planar graph, then all edge subdivisions of G are planar; if G is nonplanar, then all edge subdivisions of G are nonplanar. Similarly, note that if a graph G has a nonplanar subgraph, then G is nonplanar.

From these observations, we can immediately conclude that if a graph G has a subgraph isomorphic to an edge subdivision of $K_{3,3}$ or K_5, then G is nonplanar. One of the most famous results of graph theory, known as **Kuratowski's Theorem**, establishes that the converse of this result is also true.

Theorem 7.6.1. *A graph is not planar if and only if it has a subgraph that is an edge subdivision of K_5 or $K_{3,3}$.*

(We omit the proof of this result as it is beyond the scope of our current study.)

Note that Kuratowski's Theorem has the following surprising consequence. Suppose we begin with a nonplanar graph G and do the following operation as long as it is possible. Delete a vertex v or an edge e whose deletion leaves a nonplanar graph. When this process ends, what will the final graph G' be?

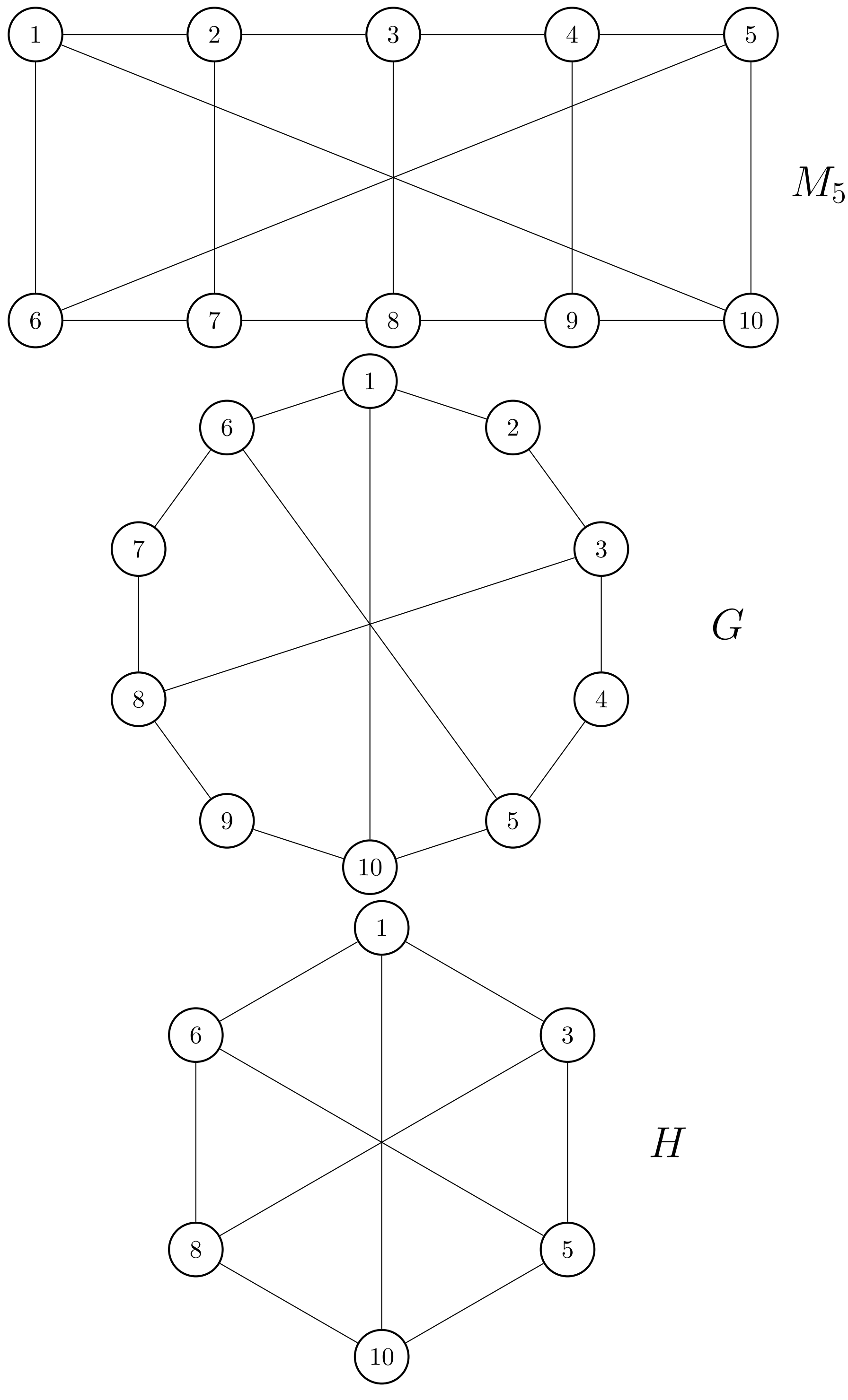


Figure 7.12: Edge subdivisions and an example of Kuratowski's Theorem

According to Kuratowski's Theorem, G' *must be* an edge subdivision of K_5 or $K_{3,3}$!

For example, in Figure 7.12, the graph M_5 has subgraph G, and G is an edge subdivision of H. Also, H is actually $K_{3,3}$, where the vertices in the two vertex classes are $\{1,5,8\}$ and $\{3,6,10\}$. Thus we conclude from Kuratowski's Theorem that M_5 is nonplanar. Figure 7.12 illustrates one convenient strategy when looking for an edge subdivision of $K_{3,3}$ or K_5: first find a long cycle in the graph – in this case the cycle has 10 vertices; then find edges or paths (subdivided edges) across the cycle – in this case edges {1, 10} and {5, 6}, together with any one of edges $\{2,7\},\{3,8\},\{4,9\}$, would create an edge subdivision of $K_{3,3}$.

Note that M_5 has 10 vertices, 15 edges and girth 4, so our counting results are not strong enough to prove that M_5 is not planar.

Problem Set 7.6

1. For each of the graphs in Figure 7.13, determine if it is planar. Prove your conclusion in each case.

2. Let G be a connected planar graph with p vertices and q edges and girth k. Show that
$$q \leq \frac{k(p-2)}{k-2}.$$
Show also that if equality holds, all faces of G have degree k.

3. Prove that the Petersen graph is nonplanar, without using any form of Kuratowski's theorem.

4. (a) Prove that the Petersen graph is nonplanar by Kuratowski's Theorem, finding a subgraph that is an edge subdivision of $K_{3,3}$.
   (b) Show that there exist two edges of the Petersen graph whose deletion leaves a planar graph.

5. Prove that the n-cube is not planar when $n \geq 4$, without using any form of Kuratowski's theorem.

6. (a) Prove that the 4-cube is nonplanar by Kuratowski's Theorem, finding a subgraph that is an edge subdivision of $K_{3,3}$.
   (b) Show that there exist four edges of the 4-cube whose deletion leaves a planar graph.

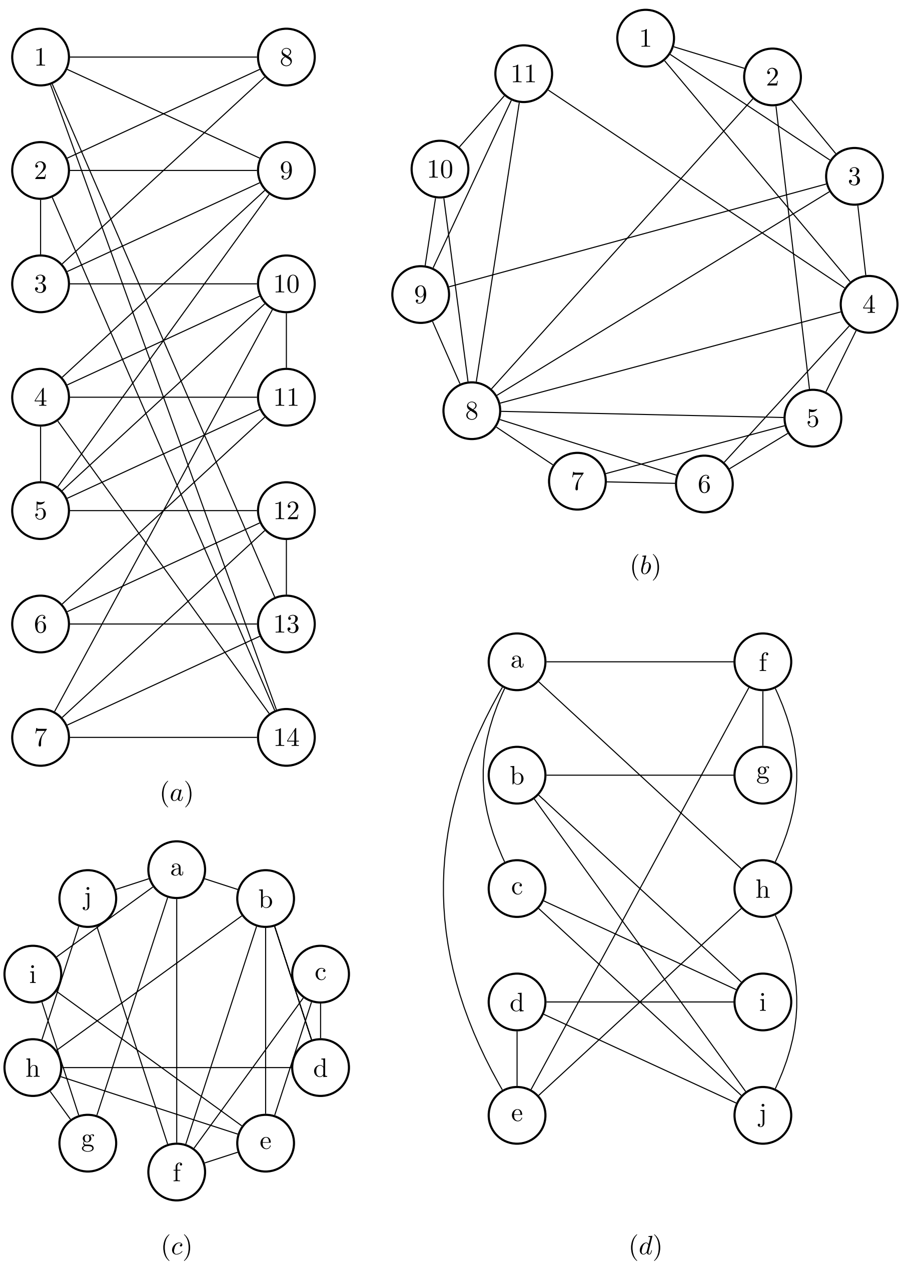


Figure 7.13:

(c) Show that no matter which 3 edges are deleted from a 4-cube, the resulting graph is not planar.

7. Consider the graph G_n with $V(G_n) = \{3, 4, \ldots, n\}$ and $\{u, v\} \in E(G_n)$ if and only if $u|v$ or $v|u$.

   (a) Find the largest value k such that G_k is planar and give a planar embedding of G_k.

   (b) Prove that G_{k+1} is not planar using Kuratowski's Theorem.

   (c) Find $n < 50$ so that G_n has K_5 as a subgraph.

   (d) Find $n < 40$ so that G_n has $K_{3,3}$ as a subgraph.

8. Consider the prime graph B_n defined in Problem 11 of Problem Set 4.4.

   (a) Prove that B_8 is planar.

   (b) Using Kuratowski's Theorem, prove that B_9 is not planar.

9. Prove that every planar bipartite graph G has a vertex of degree at most three.

10. Let G denote the graph below. (You may assume, without proof, that G has girth six.)

    (a) Let H be any graph obtained from G by deleting two edges. Prove that H is not planar.

    (b) Prove that there exist three edges that can be deleted from G so that the resulting graph is planar.

11. Prove that every planar graph having girth at least six has a vertex of degree at most two. Prove that this is false if the girth is five.

12. Prove that if G is a planar graph in which every vertex has degree at least five, then $|V(G)| \geq 12$. Find such a graph with $|V(G)| = 12$.

13. (a) Prove that the complement of the 3-cube is nonplanar.

    (b) Prove that if G has $p \geq 11$ vertices, then at least one of G and $\bar{G}$ is nonplanar.

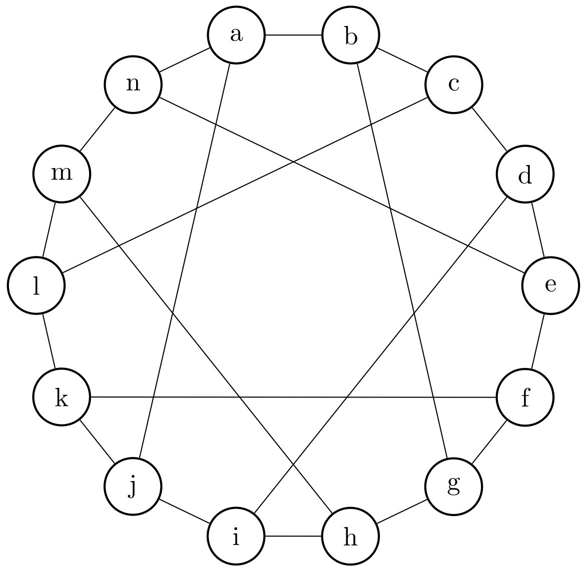


Figure 7.14: Planarity exercise.

7.7 Colouring and Planar Graphs

Definition 7.7.1. *A k-**colouring** of a graph G is a function from $V(G)$ to a set of size k (whose elements are called **colours**), so that adjacent vertices always have different colours. A graph with a k-colouring is called a k-**colourable** graph.*

For example, Figure 7.15 gives a 4-colouring of a graph. The colours in this case are the integers $1, 2, 3, 4$, and the colour assigned (by the function) to each vertex is written beside the vertex in the diagram.

Theorem 7.7.2. *A graph is 2-colourable if and only if it is bipartite.*

Proof: If a graph has bipartition (A, B), then we obtain a 2-colouring by assigning one colour to all vertices in A, and the second colour to all vertices in B; no edge joins two vertices of the same colour since (A, B) is a bipartition (so all edges join a vertex in A to a vertex in B).

Conversely, if a graph has a 2-colouring, then let the vertices of one colour be set A, and the vertices of the second colour be set B. Then (A, B) is a bipartition since all edges join vertices of different colours. ∎

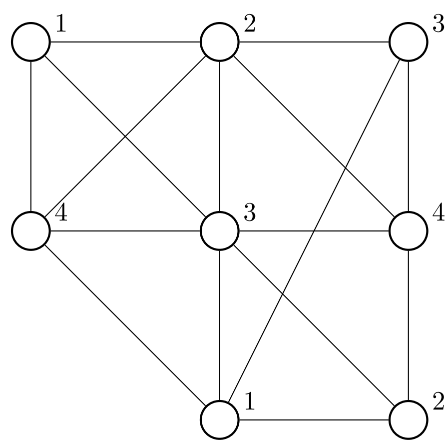


Figure 7.15: A 4-colouring of a graph

It follows that we have a description of all the 2-colourable graphs — they are precisely the graphs in which all cycles have even length. However, 3-colourable graphs are not well understood. There is no simple description known, and graph theorists believe that none exists.

Similarly, whereas there is an efficient algorithm to determine whether a graph is 2-colourable (Theorem 5.5.1), graph theorists believe that no efficient algorithm exists to determine whether a graph is 3-colourable.

Theorem 7.7.3. *K_n is n-colourable, and not k-colourable for any $k < n$.*

Proof: Any graph on n vertices is n-colourable; assign different colours to the vertices, so no two vertices have the same colour. K_n is not k-colourable for any $k < n$, since such a colouring would assign the same colour to some pair of vertices. But all pairs of vertices are adjacent in K_n, so we would have assigned the same colour to adjacent vertices. Thus K_n has no k-colouring for $k < n$. ▌

Theorem 7.7.4. *Every planar graph is 6-colourable.*

Proof: The proof is by induction on the number p of vertices. First note that all graphs on one vertex are 6-colourable, so the result is true for $p = 1$.

For the induction hypothesis, assume the result is true for all planar graphs on $p \leq k$ vertices, where $k \geq 1$.

Now consider a planar graph G on $p = k + 1$ vertices. From Corollary 7.5.5, G has a vertex v with $\deg(v) \leq 5$. Suppose we remove vertex v, and all edges incident to v, from G, and call the resulting graph G'. Then G' has k vertices, and is a planar graph (all subgraphs of a planar graph are planar). Thus we can apply the induction hypothesis to G', so G' is 6-colourable. Now find a 6-colouring of G'. There are at most 5 vertices in G' that are adjacent to v in G, so these vertices are assigned at most 5 different colours in the 6-colouring of G'. Thus there is at least one of the 6 colours remaining. Assign one of these remaining colours to v, so that v has a different colour from all of its adjacent vertices in G. Thus we have a 6-colouring of G, and the result is true for $p = k+1$. We have now proved that the result is true by mathematical induction. ▌

Let us proceed to the Five-Colour Theorem. The proof relies on the notion of edge-contraction which we now define.

Definition 7.7.5. *Let G be a graph and let $e = \{x, y\}$ be an edge of G. The graph G/e obtained from G by* **contracting** *the edge e is the graph with vertex set $V(G) \setminus \{x, y\} \cup \{z\}$, where z is a new vertex, and edge set*

$$\{\{u, v\} \in E(G) : \{u, v\} \cap \{x, y\} = \emptyset\} \cup \{\{u, z\} : u \notin \{x, y\}, \{u, w\} \in E(G) \text{ for some } w \in \{x, y\}\}.$$

Intuitively, we can think of the operation of contracting e as allowing the "length" of e to decrease to 0, so that the vertices x and y are identified into a new vertex z. Any other vertex that was adjacent to one (or both) of x and y is adjacent to z in the new graph G/e. See Figure 7.16 for an example.

If G has p vertices and q edges then G/e has $p-1$ vertices and at most $q-1$ edges.

Remark: G/e is planar whenever G is.

The converse of this remark is not true; G/e may be planar when G is non-planar. See Figure 7.7 for an example.

Now we are ready to prove the Five-Colour Theorem.

Theorem 7.7.6. *Every planar graph is 5-colourable.*

Proof: The proof is by mathematical induction on the number of vertices p of a planar graph.

For any graph G having one vertex, G is 5-colourable.

Induction Hypothesis: Assume that every planar graph on $p \leq k$ vertices is 5-colourable, where $k \geq 1$.

Let G be any planar graph on $p = k+1$ vertices.

*Case 1: Graph **G** has a vertex of degree 4 or less.*

Proceeding as in the 6-colour theorem above, it can be shown that G is 5-colourable.

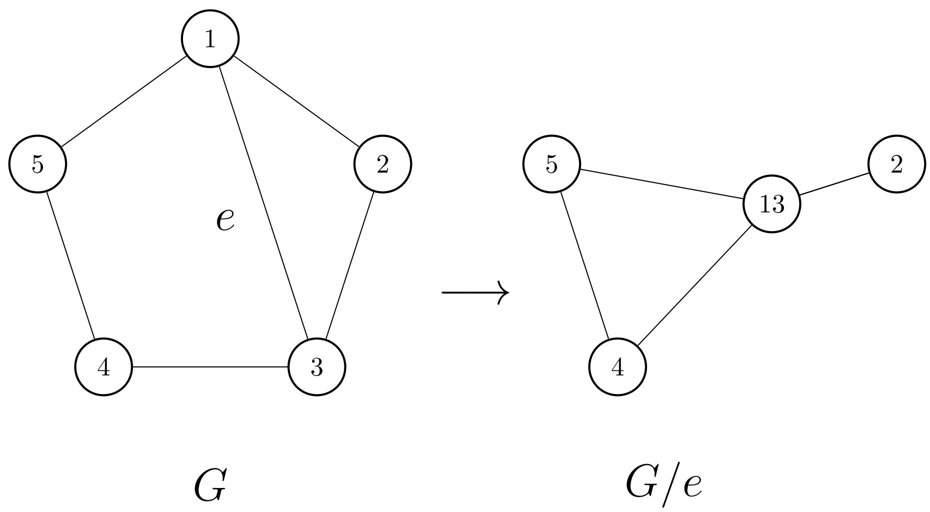


Figure 7.16: Contraction

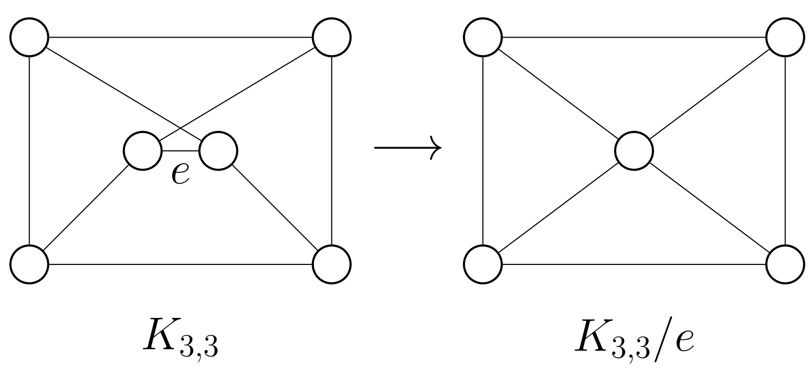


Figure 7.17: Contraction

*Case 2: Graph **G** has no vertex of degree 4 or less.*
Then, by Corollary 7.5.5, G has a vertex, say v, of degree 5.

If the 5 vertices joined to v are mutually adjacent, then G has a subgraph isomorphic to K_5. This is impossible since G is planar by hypothesis. Hence, at least 2 neighbours of v are not adjacent, say a and b.

Contract edge $e = \{a, v\}$ to get graph $H = G/e$, and label the new vertex v. Contract edge $f = \{b, v\}$ of H to get graph $K = H/f$, and label the new vertex v. Since G is planar, so are H and K; furthermore, K has $k-1$ vertices. Therefore K is 5-colourable by the induction hypothesis.

Use the 5-colouring of K to colour all the vertices of G except for a, b, and v. Since a and b are not adjacent in G, they can both accept the same colour. Colour both vertices a and b with the colour assigned to vertex v in K. Hence, at most four distinct colours appear on the five neighbours of v. Colour v with one of the absent colours. Then we have a valid 5-colouring of G.

In both cases, G has a 5-colouring.

Therefore, by mathematical induction it follows that every planar graph has a 5-colouring. ∎

The most famous result of graph theory is the "**Four colour theorem**". The known proofs are by mathematical induction, but involve many hundreds of cases, and use computer verification for cases. Its statement is as follows.

Theorem 7.7.7. *Every planar graph is* 4*-colourable.*

It is important to note that the converse of this result does not hold. For example, from Theorem 7.7.3 we know that K_5 is not 4-colourable, so it is correct to deduce from the Four Colour Theorem that K_5 is not planar. However, from Theorem 7.7.2 we know that $K_{3,3}$ is 2-colourable (and thus 4-colourable), but we know already from Corollary 7.5.7 that $K_{3,3}$ is not planar.

7.8 Dual Planar Maps

Note that our colourings are colourings of vertices, with the restriction that vertices joined by an edge have different colours. However, most descriptions of the Four Colour Theorem refer to colouring of regions, say countries in a map, with the restriction that regions with a common boundary have different colours.

In fact, these are completely equivalent results, as we show now. Given a connected planar embedding G, the **dual** G^* is a planar embedding constructed as follows: G^* has one vertex for each face of G. Two vertices of G^* are joined by an edge whenever the corresponding faces of G have an edge in common (one side for each face), and the edge in G^* is drawn to cross this common boundary edge in G. For example, Figure 7.18 illustrates the construction of G^* from a planar embedding G. Note that the faces of G^* now correspond to the vertices of G.

There are a number of things to note about the relationship between G and G^*. First, a face of degree k in G becomes a vertex of degree k in G^*, and a vertex of degree j in G becomes a face of degree j in G^*. Thus, Theorems 4.3.1 and 7.1.2 are the same result for planar embeddings, since Theorem 4.3.1 for G becomes Theorem 7.1.2 for G^* and vice versa. This connection between G and G^* is even stronger, since $(G^*)^*$ and G are the same graph.

Note that a bridge in G gives an edge in G^* between a vertex and itself (such an edge is called a loop), and more than one edge between two faces in G gives more than one edge between a pair of vertices (these are called, together, a multiple edge). Thus G^* may be a multigraph rather than a graph.

These complications aside, it is now clear that the Four Colour Theorem for colouring vertices in planar graphs is equivalent to the Four Colour Theorem for colouring faces in planar embeddings, via duality.

Problem Set 7.8

1. (a) Prove that every planar graph without a triangle (that is, a cycle of length three) has a vertex of degree three or less.

   (b) Without using Theorem 7.7.7, prove that every planar graph without a triangle is 4-colourable.

2. Prove that if G is a planar graph with girth at least six, then G is 3-colourable. (You may use the result of Problem 11 in Problem Set 7.6.)

3. Let G be a connected planar embedding with p vertices and q edges, and suppose that the dual graph G^* is isomorphic to G.

   (a) Prove that $q = 2p - 2$.

   (b) Give an example of such a graph with six vertices.

4. Let G be a connected planar embedding in which every face has even degree. Prove that G is a bipartite graph.

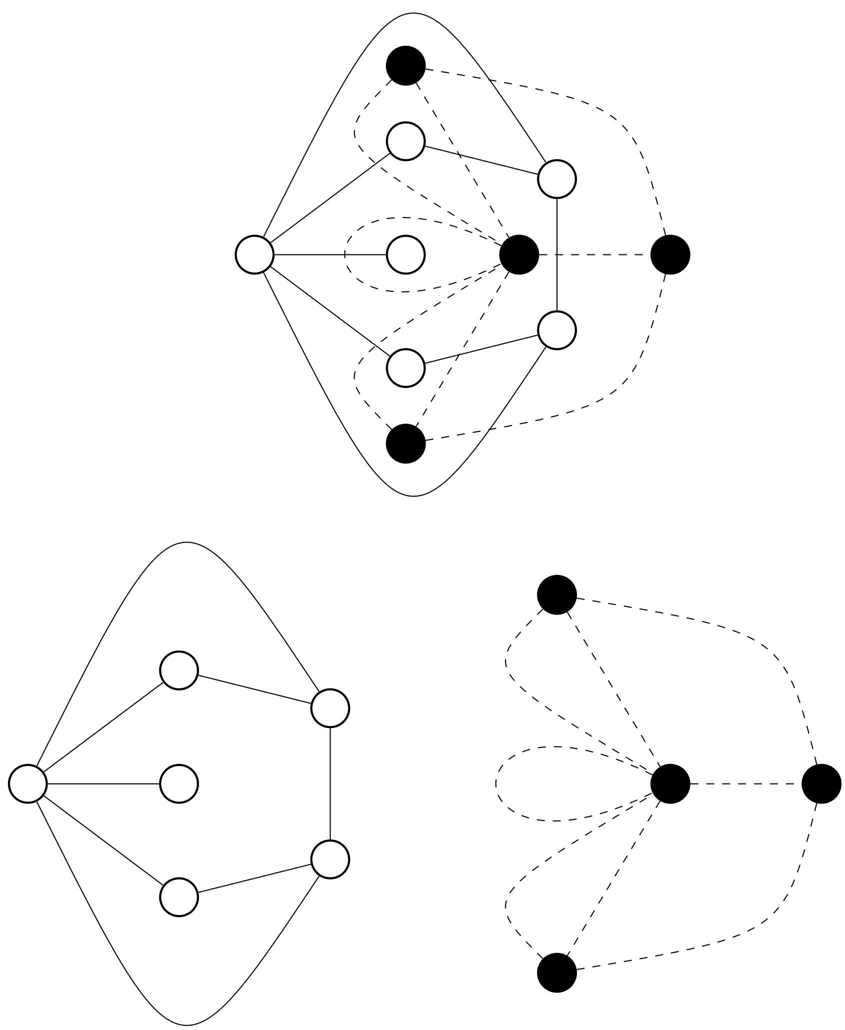


Figure 7.18: The dual of a planar embedding

5. Find a planar bipartite 3-regular graph with 14 vertices.

6. Show that a planar graph with $p > 2$ vertices and $2p-3$ edges is not 2-colourable.

7. Show that a graph with $2m$ vertices and $m^2 + 1$ edges is not 2-colourable.

8. Show that K_5 can be obtained by contracting five edges of the Petersen graph. Hence deduce from the nonplanarity of K_5 and the remark following the definition of edge-contraction, that the Petersen graph is nonplanar.

Chapter 8

Matchings

8.1 Matching

A **matching** in a graph G is a set M of edges of G such that no two edges in M have a common end. (Another way to express the condition is that in the spanning subgraph of G with edge set M, every vertex has degree at most 1.) So M *matches* certain pairs of adjacent vertices—hence the name. The thick edges in Figure 8.1 form a matching. We say that a vertex v of G is **saturated** by M, or that M **saturates** v, if v is incident with an edge in M. Of course, every graph has a matching; for example the empty set $\emptyset$ is always a matching. The question we will be most interested in is to find a largest matching in G, called a **maximum matching** of G. In Figure 8.1 the matching M indicated there has size 3, and therefore is not a maximum matching, since it is easy to find a matching of size 4. A special kind of maximum matching is one having size $p/2$, that is, one that saturates every vertex, called a **perfect matching**. Of course, not every graph has a perfect matching.

We will be concentrating on matching problems for bipartite graphs. Here is a way to restate the problem in case G is bipartite.

Job assignment problem. We are given a set A of workers and a set B of jobs, and for each job, the set of workers capable of doing the job. We want to assign as many jobs as possible to workers able to do them, but each worker is to be assigned to at most one job, and each job is to be assigned to at most one worker.

For example, suppose that $A = \{a, b, c, d, e, f\}$ and $B = \{g, h, i, j, k, l\}$, and the lists of workers that can do the jobs are:

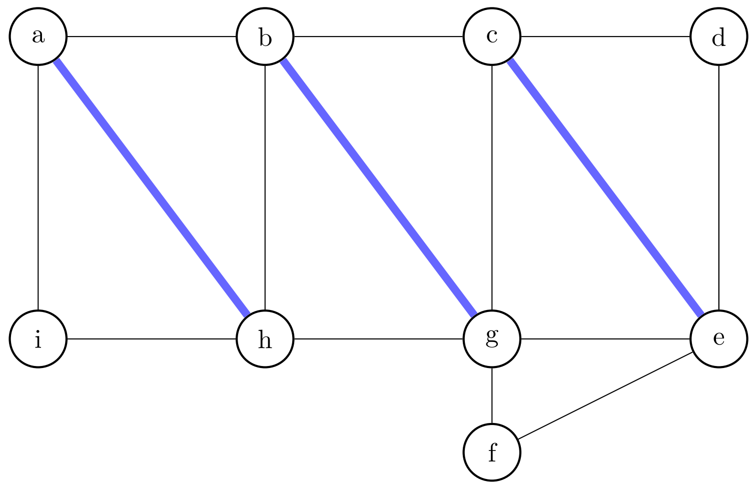


Figure 8.1: G with matching M

For $g:\ c, e$
For $h:\ a, c$
For $i:\ a, b, c, d, f$
For $j:\ c, e$
For $k:\ c, e$
For $l:\ b, d, f$

Why is the job assignment problem equivalent to the maximum matching problem of bipartite graphs? From the data of the job assignment problem we can construct a bipartite graph G with vertex set $A \cup B$ and with $u \in A$ adjacent to $v \in B$ if and only if worker u can do job v. (The graph corresponding to the sample data above is shown in Figure 8.2.) Conversely, given a bipartite graph with bipartition A, B we make a worker for each element of A and a job for each element of B and declare worker u to be able to do job v if and only if $\{u, v\} \in E(G)$. The condition that jobs be assigned to workers that can do them, means that an assignment is a set of edges. The condition that each worker be assigned to at most one job and that each job be assigned to at most one worker, corresponds to the condition that the assigned edges form a matching.

If we have a matching M of G, certain kinds of paths are useful for obtaining a larger matching. We say that a path $v_0 v_1 v_2 \ldots v_n$ is an **alternating path** with respect to M if one of the following is true:

$\{v_i, v_{i+1}\} \in M$ if i is even and $\{v_i, v_{i+1}\} \notin M$ if i is odd
$\{v_i, v_{i+1}\} \notin M$ if i is even and $\{v_i, v_{i+1}\} \in M$ if i is odd.

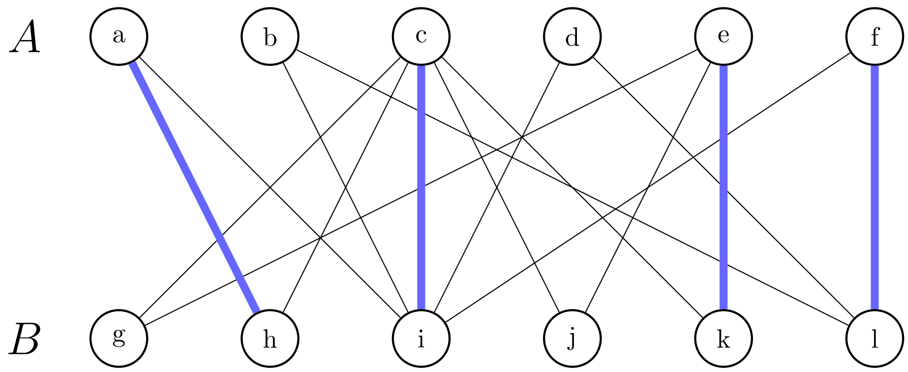


Figure 8.2: A bipartite example

That is, edges of the path are alternately in and not in M. In the graph of Figure 8.1, with respect to the matching indicated there, the following are examples of alternating paths: (i) $ahbg$, (ii) $iahgb$, (iii) $iahbgf$. An **augmenting path** with respect to M is an alternating path joining two distinct vertices neither of which is saturated by M. The path (iii) above is an augmenting path in Figure 8.1. Note that augmenting paths have odd length because they begin and end with nonmatching edges.

Lemma 8.1.1. *If M has an augmenting path, it is not a maximum matching.*

Proof: Let P be an augmenting path $v_0 v_1 v_2 \ldots v_n$. Then $\{v_i, v_{i+1}\} \in M$ if i is odd, and $\{v_i, v_{i+1}\} \notin M$ if i is even. Moreover, n must be odd. So there are fewer edges of P in M than not in M. If we replace the edges of M that are in P by the other edges of P, we get a matching M' that is larger than M. ▌

8.2 Covers

A **cover** of a graph G is a set C of vertices such that every edge of G has at least one end in C. In Figure 8.1 $\{a, h, g, c, e\}$ is a cover. It is easy to find large covers, just as it is easy to find small matchings. For example, in any graph G, $V(G)$ is a cover. Also, if G is bipartite with bipartition A, B, then A is a cover, and so is B. A very useful observation about matchings and covers is the following.

Lemma 8.2.1. *If M is a matching of G and C is a cover of G, then $|M| \leq |C|$.*

Proof: For each edge $\{u, v\}$ of M, u or v is in C. Moreover, for two different edges of M, any vertices of C they saturate must be different, since M is a matching. Therefore, $|M| \le |C|$. ▮

Sometimes we can use a cover to prove that a matching is maximum.

Lemma 8.2.2. *If M is matching and C is a cover and $|M| = |C|$, then M is a maximum matching and C is a minimum cover.*

Proof: Let M' be any matching. Then by Lemma 8.2.1

$$|M'| \le |C| = |M|.$$

It follows that M is a maximum matching. Now let C' be any cover. Then by Lemma 8.2.1

$$|C'| \ge |M| = |C|.$$

It follows that C is a minimum cover. ▮

We will show that if G is bipartite, then it is always possible to find such M and C, that is, that the maximum size of a matching is the minimum size of a cover. This is *König's Theorem*, the subject of the next section.

Problem Set 8.2

1. Show that a tree has at most one perfect matching.

2. How many perfect matchings are there in K_n? How many in $K_{m,n}$?

3. How many perfect matchings has the graph L_n of Figure 8.3? (There are n vertical edges.) (Hint: where a_n denotes the number of perfect matchings of L_n, find a recurrence relation for a_n.)

4. Show that for $n \ge 1$, the n-cube has a perfect matching.

5. Show that the 64 squares of a chessboard can be covered with 32 dominoes, each of which covers two adjacent squares.

6. Show that if two opposite corner squares of a chessboard are removed, then the resulting board cannot be covered with 31 dominoes.

7. Let G be a graph with even number of vertices. Prove that if G has a Hamilton cycle, then G has a perfect matching.

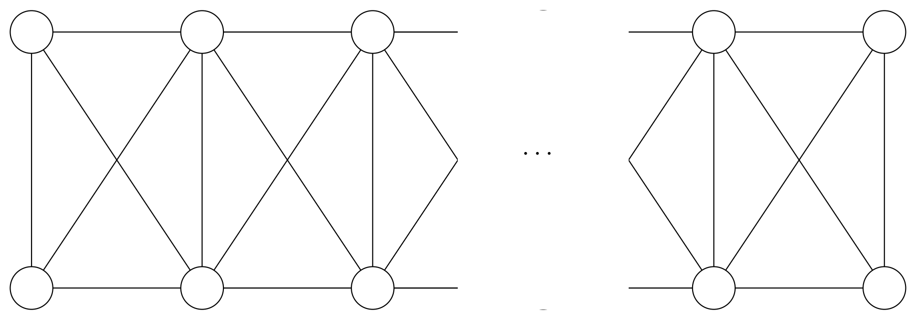


Figure 8.3: L_n

8. In the previous problem, suppose in addition that G is bipartite, with bipartition A, B. Let $u \in A$, $v \in B$, and let H denote the graph obtained from G by deleting u and v and their incident edges. Prove that H has a perfect matching.

9. Show that if two squares of the chessboard having opposite colours are removed, then the resulting board can be covered by 31 dominoes. Hint: Use the previous exercise.

10. Consider the prime graph B_n introduced in Problem 11 of Problem Set 4.4. Use induction on n to show that, if n is even, B_n has a perfect matching. You may use without proof the fact that there is a prime number between k and $2k$ for $k \geq 2$.

11. Prove that C is a cover of G if and only if $V(G) \setminus C$ is a set of pairwise nonadjacent vertices.

12. Show that it is not always true that there exist a matching M and a cover C of the same size.

13. Let N be a matrix. We want to find a largest set of non-zero entries of N such that no two are in the same row or in the same column. Formulate this problem as one of finding a maximum matching in a bipartite graph.

14. In the previous problem interpret the meaning of a cover of the bipartite graph in terms of the matrix N.

15. Find a bipartite graph G with bipartition A, B where $|A| = |B| = 5$, and having the following properties. Every vertex has degree at least 2, the total number

of edges is 16, and G has no perfect matching. Why does your graph not have a perfect matching?

16. Suppose that for some $n \geq 1$, graph G with p vertices satisfies $p = 2n$ and $deg(v) \geq n$ for every vertex v. Prove that G has a perfect matching. (Hint: Prove that if M is a matching that is not perfect, then there exists an augmenting path of length 1 or 3.)

17. Suppose that M is a matching of G that is not contained in any larger matching, and that M' is a maximum matching of G. Prove that $|M'| \leq 2|M|$.

8.3 König's Theorem

The main result about matching in bipartite graphs is the following theorem of König.

Theorem 8.3.1. *(König's Theorem) In a bipartite graph the maximum size of a matching is the minimum size of a cover.*

Though minimum covers have the same size as maximum matchings in bipartite graphs, this is not true in general. For example, a minimum cover in K_p has size $p-1$ and a maximum matching has size $\lfloor \frac{p}{2} \rfloor$.

Let A, B be a bipartition of G, and let M be a matching of G. In the following **XY-construction** we use alternating paths to define sets X, Y, and show that they have certain properties. This will allow us to prove König's Theorem, and also to give an efficient algorithm to find a maximum matching.

Let X_0 be the set of vertices in A not saturated by M and let Z denote the set of vertices in G that are joined by to a vertex in X_0 by an alternating path. If $v \in Z$ we use $P(v)$ to denote an alternating path that joins v to X_0. Now define:

(a) $X = A \cap Z$.

(b) $Y = B \cap Z$.

For example, in the graph of Figure 8.2 we have

$$X_0 = \{b, d\}, \quad X = \{a, b, c, d, e, f\}, \quad Y = \{g, h, i, j, k, l\}.$$

As a second example, consider the same graph but with a different matching, shown in Figure 8.4. Then we have

$$X_0 = \{d\}, \quad X = \{d, b, f\}, \quad Y = \{i, l\}.$$

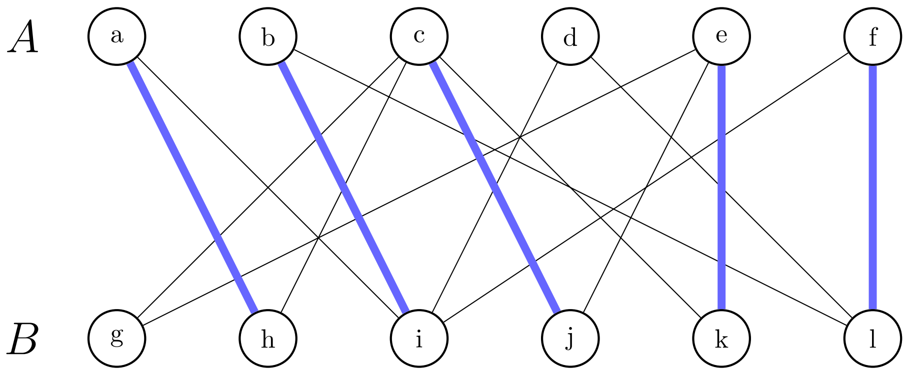


Figure 8.4: A second bipartite example

Notice that any alternating path $P(v)$ has even length if $v \in X$ and odd length if $v \in Y$. Since the first edge of any alternating path beginning at a vertex in X_0 is not a matching edge, and every second edge is a matching edge, it follows that

- If $v \in X$, then the last edge of $P(v)$ is in M (this is true vacuously if $v \in X_0$).
- If $v \in Y$, then the last edge of $P(v)$ is not in M.

One more easy observation: If w is a vertex of an alternating path $P(v)$ from X_0 to $v \in Z$, then $w \in Z$.

Lemma 8.3.2. *Let M be a matching of bipartite graph G with bipartition A, B, and let X and Y be as defined above. Then:*

(a) There is no edge of G from X to $B \setminus Y$;

(b) $C = Y \cup (A \setminus X)$ is a cover of G;

(c) There is no edge of M from Y to $A \setminus X$;

(d) $|M| = |C| - |U|$ where U is the set of unsaturated vertices in Y;

(e) There is an augmenting path to each vertex in U.

Proof: Suppose that (a) is false, and let $u \in X$, $v \in B \setminus Y$, $\{u, v\} \in E(G)$. Then adding v to the even-length alternating path $P(u)$ from X_0 to u, gives us an odd-length alternating path to v, which implies that $v \in Y$, a contradiction.

For (b), the only edges of G that are not incident with an element of C are those from X to $B \setminus Y$. However, no such edges exist by part (a), so C is a cover.

Now suppose that (c) is false, and let $u \in Y$, $v \in A \setminus X$, $\{u, v\} \in M$. Then adding v to the odd-length alternating path $P(u)$ from X_0 to u, gives us an even-length alternating path to v, which implies that $v \in X$, a contradiction.

For (d), from part (c), every edge of M joins a vertex in Y to a vertex in X, or joins a vertex in $A \setminus X$ to a vertex in $B \setminus Y$. The number of edges of the first type is $|Y| - |U|$. Also, by the fact that $X_0 \subseteq X$, every vertex in $A \setminus X$ is saturated by M, so the number of edges of the second type is $|A \setminus X|$. It follows that

$$|M| = |Y| - |U| + |A \setminus X| = |C| - |U|.$$

Finally, (e) is easy—if such a vertex v exists, then $P(v)$ is an augmenting path. ▮

We can check that the conclusions of Lemma 8.3.2 are satisfied in the two examples above. Notice in particular, that in Figure 8.2 we have $U = \{g, j\}$, and, for example, augmenting paths to g and j are given by $bicg$ and $bicj$. If we use the latter path to get a larger matching, then we get the matching of Figure 8.4. In Figure 8.4, there are no unsaturated vertices in Y, so $U = \emptyset$.

Proof of Theorem 8.3.1: Let M be a maximum matching of G. Then from Lemma 8.1.1 and part (e) of Lemma 8.3.2, U must be the empty set, so $|U| = 0$. Therefore, from parts (b) and (d) of Lemma 8.3.2, $C = Y \cup (A \setminus X)$ is a cover of G with $|C| = |M|$, and the result follows immediately from Lemma 8.2.2. ▮

Notice in the example of Figure 8.4 that there is no unsaturated vertex in Y. The construction of the proof of König's Theorem then gives the cover $C = Y \cup (A \setminus X) = \{a, c, e, i, l\}$. It has size 5, and therefore shows that the matching shown there is maximum.

Problem 8.3.3. *Let G be a bipartite graph with bipartition A, B, where $|A| = |B| = n$. Prove that if G has q edges, then G has a matching of size at least q/n.*

Solution: Notice that what is needed, is to prove that the maximum size of a matching is at least q/n. By König's Theorem, it is enough to show that the minimum size of a cover is at least q/n. Suppose that C is a cover of G. There can be at most n edges incident to any element of C, so there can be at most $n|C|$ edges incident with one or more elements of C. But C is a cover, so *every* edge must be incident with one or more elements of C. Therefore, $n|C| \geq q$, or $|C| \geq q/n$. Since every cover contains at least q/n vertices, therefore, the minimum size of a cover is at least q/n, and we are done. ▮

An algorithm for maximum matching in bipartite graphs

The XY-construction and Lemma 8.3.2 essentially provides an algorithm to find a maximum matching:

Step 1. Begin with any matching M.
Step 2. Construct X and Y.
Step 3. If there is an unsaturated vertex v in Y, find an augmenting path $P(v)$ ending at v, use it to construct a larger matching M', and replace M by M'. Then go to Step 2.
Step 4. If every vertex in Y is saturated, stop. M is a maximum matching, and $C = Y \cup (A \setminus X)$ is a cover of minimum size.

Now we give a more explicit way to construct X and Y and, at the same time, the alternating paths $P(v)$ that define them. It is very much like breadth-first search—we find the elements of X, Y in levels. We find first the vertices that are reachable by alternating paths beginning in X_0 and having 0 edges (this is just X_0, of course), then those that are reachable by alternating paths having 1 edge, then those reachable by alternating paths having 2 edges, et cetera. The vertices v in the next level are exactly those (whose level has not yet been assigned) that are joined by an edge to a vertex u in the previous level. The only additional rule is that, when we are creating an even level, that edge $\{u, v\}$ must be a matching edge. Just as in breadth-first search, when a vertex v is recognized as an element of X or of Y, we assign it a parent $\mathrm{pr}(v)$, which is the vertex u in the previous level from which we reached v. When we find an unsaturated vertex v in Y, then we can trace the path $v\mathrm{pr}(v)\mathrm{pr}^2(v)\ldots w$, where $w \in X_0$, and this is an augmenting path. There is no need to construct the rest of X and Y in this case—we can immediately use the augmenting path to get a bigger matching. Here is a statement of the resulting algorithm. In it, we use $\hat{X}$ to represent the set of elements of X that we have found so far, and similarly for $\hat{Y}$. Initially, $\hat{X} = X_0$ and $\hat{Y} = \emptyset$.

Bipartite matching algorithm

Step 0. Let M be any matching of G.
Step 1. Set $\hat{X} = \{v \in A : v \text{ is unsaturated}\}$, set $\hat{Y} = \emptyset$, and set $\mathrm{pr}(v)$ to be undefined for all $v \in V(G)$.
Step 2. For each vertex $v \in B \setminus \hat{Y}$ such that there is an edge $\{u, v\}$ with $u \in \hat{X}$, add v to $\hat{Y}$ and set $\mathrm{pr}(v) = u$.
Step 3. If Step 2 added no vertex to $\hat{Y}$, return the maximum matching M and the minimum cover $C = \hat{Y} \cup (A \setminus \hat{X})$, and stop.

Step 4. If Step 2 added an unsaturated vertex v to $\hat{Y}$, use pr values to trace an augmenting path from v to an unsaturated element of $\hat{X}$, use the path to produce a larger matching M', replace M by M', and go to Step 1.
Step 5. For each vertex $v \in A \setminus \hat{X}$ such that there is an edge $\{u, v\} \in M$ with $u \in \hat{Y}$, add v to $\hat{X}$ and set $\mathrm{pr}(v) = u$. Go to Step 2.

Here is an example of the application of the algorithm. Consider the graph of Figure 8.5 with the matching M indicated there. Take $A = \{1, 2, 3, 4\}$.

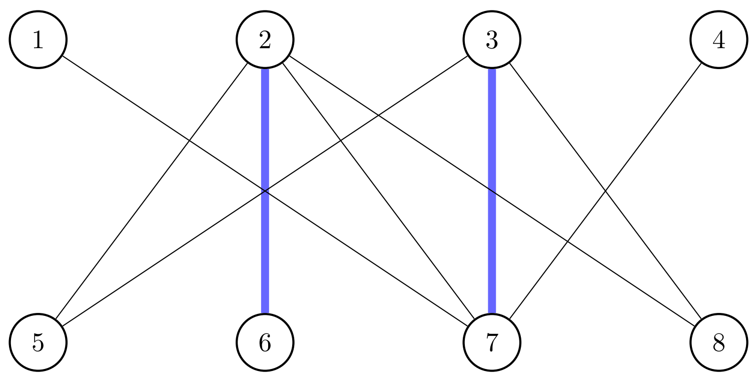


Figure 8.5: Example of the algorithm

Initially, $\hat{X} = \{1, 4\}$ and $\hat{Y} = \emptyset$. Then 7 is added to $\hat{Y}$ with $\mathrm{pr}(7) = 1$. Then 3 is added to $\hat{X}$ with $\mathrm{pr}(3) = 7$. Then 5 and 8 are added to $\hat{Y}$ with $\mathrm{pr}(5) = \mathrm{pr}(8) = 3$. Since 5 (for example) is unsaturated we have the augmenting path 5371. This gives the new matching $M = \{\{2, 6\}, \{3, 5\}, \{1, 7\}\}$.

Beginning again (with no parent values), we have $\hat{X} = \{4\}$, $\hat{Y} = \emptyset$. Then 7 is added to $\hat{Y}$ with $\mathrm{pr}(7) = 4$. Then 1 is added to $\hat{X}$ with $\mathrm{pr}(1) = 7$. Now nothing can be added to $\hat{Y}$ and so the algorithm terminates with the current matching M and the cover $C = (A \setminus \hat{X}) \cup \hat{Y} = \{2, 3, 7\}$.

Problem Set 8.3

1. Let G be a bipartite graph, and let Δ be the largest degree of any vertex of G. Prove that G has a matching of size at least q/Δ. Also, show that this is false in general if G is not bipartite.

2. Let n be a positive integer. Construct a bipartite graph with bipartition A, B, where $|A| = |B| = n$, for which the size of a maximum matching is less than

$(q+1)/n$. (In other words, show that the value q/n is the best possible in Problem 8.3.3.)

3. (Difficult) Let G be a bipartite graph with bipartition A, B, where $|A| = |B| = n$, and suppose that every vertex of G has degree at least $\delta < n$. Prove that G has a matching of size at least the minimum of n and $(q - \delta^2)/(n - \delta)$.

4. Construct a bipartite graph with bipartition A, B, where $|A| = |B| = 8$, and having minimum degree 2, for which the size of a maximum matching is less than $(q-3)/6$. (This shows that the value $(q - \delta^2)/(n - \delta)$ in the previous exercise, cannot be increased.)

5. Find a maximum matching and a minimum cover in the graph of Figure 8.6, by applying the algorithm, beginning with the matching indicated.

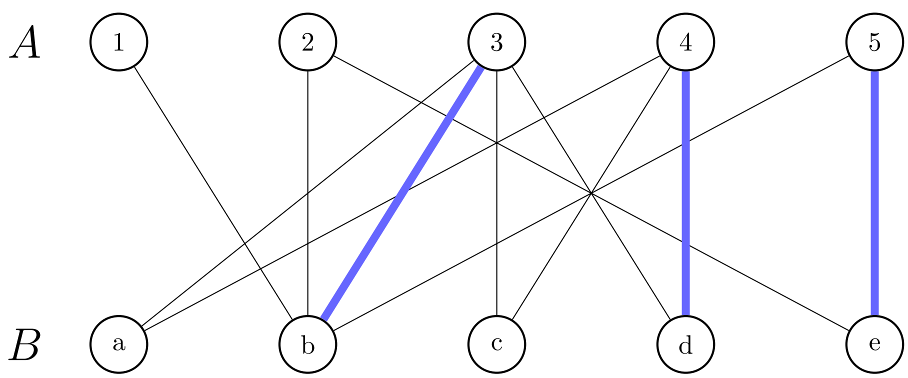


Figure 8.6: Matching exercise

6. Find a maximum matching and a minimum cover in the graph of Figure 8.7, by applying the algorithm, beginning with the matching indicated.

7. Find a maximum matching and a minimum cover in the graph of Figure 8.8, by applying the algorithm, beginning with the matching of size 18 consisting of all the edges oriented from northwest to southeast.

8. Let G be bipartite with bipartition A, B. Suppose that C and C' are both covers of G. Prove that $\hat{C} = (A \cap C \cap C') \cup (B \cap (C \cup C'))$ is also a cover of G.

9. In the previous exercise, prove that if C and C' are minimum covers, then so is $\hat{C}$.

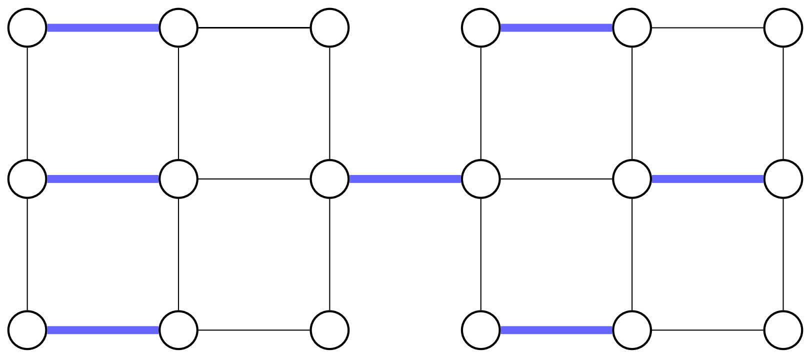


Figure 8.7: Matching exercise

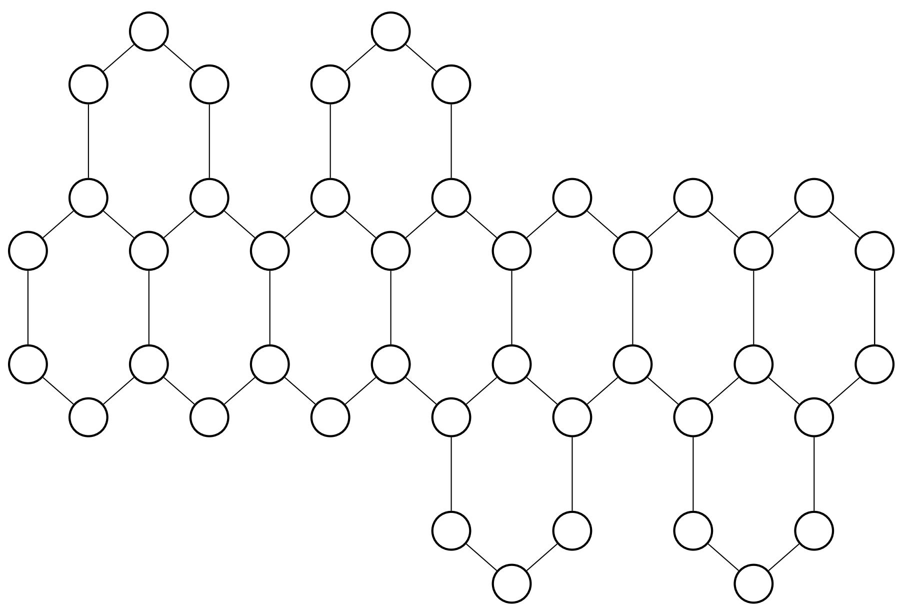


Figure 8.8: Matching exercise

8.4 Applications of König's Theorem

If A, B is a bipartition of G, no matching of G can have size bigger than $|A|$. It is interesting to determine whether there is one of exactly this size. (A perfect matching has this property, but if $|A| < |B|$, there will be no perfect matchings.) This problem was raised in a different context by Hall, and the resulting theorem (although it follows from König's Theorem) is called *Hall's Theorem*.

Consider the subset D of A. If its elements are to be saturated by a matching, there must be at least $|D|$ distinct elements of B that are adjacent in G to at least one element in D, since the matching edges incident to the elements of D must have distinct ends. For example, in Figure 8.4, the subset $D = \{a, b, d, f\}$ of A is joined by edges of the graph only to the three vertices h, i, l of B. It follows that there can be no matching saturating all of D, and therefore there can be no matching saturating all of A. Let us define, for any subset D of vertices of a graph G the **neighbour set** $N(D)$ of D to be $\{v \in V(G) :$ there exists $u \in D$ with $\{u, v\} \in E(G)\}$. Then if there is a matching saturating A, we must have at least $|D|$ elements in $N(D)$. Hall proved that, if every subset D satisfies this condition, then there will exist such a matching. As we indicated above, we can prove this using König's Theorem.

Theorem 8.4.1. *(Hall's Theorem) A bipartite graph G with bipartition A, B has a matching saturating every vertex in A, if and only if every subset D of A satisfies*

$$|N(D)| \geq |D|.$$

Proof: First, suppose that G has a matching M saturating every vertex in A. Then for any subset D of A, $N(D)$ contains the other end of the edge of M incident with v for every $v \in D$, and these vertices must all be distinct, so $|N(D)| \geq |D|$.

We prove the contrapositive of the "if" part of Hall's Theorem; namely, if there is no matching that saturates every vertex of A, then $|N(D)| < |D|$ for some subset $D \subseteq A$.

By hypothesis, there is no matching that saturates every vertex of A. Then, by König's Theorem, there exist a maximum matching M and a minimum covering C such that $|C| = |M| < |A|$. The sets A, B, C partition the vertices of G into 4 subsets $A \cap C, A \setminus C, B \cap C, B \setminus C$ as shown in Figure 8.9. (Remark: some of these subsets may be empty; for example, if $C = B$, then $B \setminus C = A \cap C = \emptyset$.) Since C is a cover, no edge joins a vertex of $B \setminus C$ to a vertex of $A \setminus C$, so $N(A \setminus C) \subseteq B \cap C$.

Let $D = A \setminus C$. Then

$$|N(D)| \le |B \cap C| = |C| - |A \cap C| < |A| - |A \cap C| = |A \setminus C| = |D|.$$

This completes the proof of the “if” part of Hall’s Theorem ▮

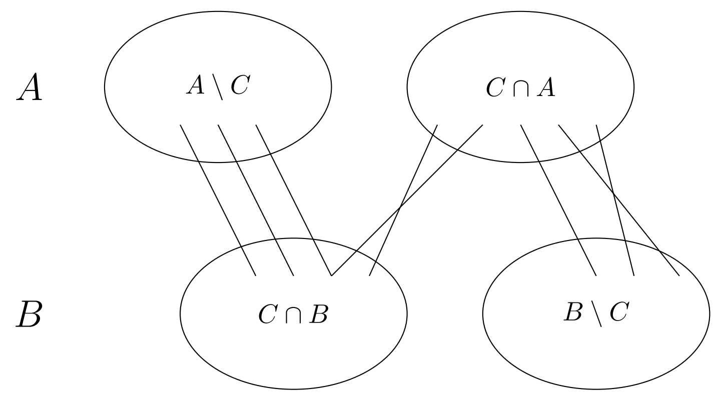


Figure 8.9: Proof of Hall’s Theorem

Note that, if there is no matching saturating all vertices in A, the maximum matching algorithm will find a set $D \subseteq A$ such that $|N(D)| < |D|$. Namely, at termination of the algorithm, we take $D = A \setminus C$, where C is the cover $Y \cup (A \setminus X)$. Therefore $D = X$ and $N(D) = Y$.

8.5 Systems of Distinct Representatives

The problem that led Hall to prove Theorem 8.4.1 can be described as follows. Suppose there are several interest groups in some population, for example, bridge players, socialists, football fans, and so on. We want to find a representative for each of these groups, perhaps to serve on some decision-making body. There are two rules, first, that a representative must belong to the group she represents, and second, that no one can represent two different groups. More formally, given a collection $Q_1, Q_2, \ldots, Q_n$ of subsets of a finite set Q, a **system of distinct representatives (SDR)** for the collection is a sequence (or n-tuple) $(q_1, q_2, \ldots, q_n)$ of n distinct elements of Q such that

$$q_i \in Q_i \text{ for } i = 1, 2, \ldots, n.$$

For example, suppose that $Q_1 = \{b, d\}$, $Q_2 = \{a, b, c, d\}$, $Q_3 = \{b, c\}$, $Q_4 = \{b, d\}$. Then we can choose $q_1 = b$, $q_2 = a$, $q_3 = c$, $q_4 = d$. As a second example, suppose that $Q_1 = \{b, d\}$, $Q_2 = \{a, b, c, d\}$, $Q_3 = \{b\}$, $Q_4 = \{b, d\}$. Then it is not hard to convince ourselves that there is no SDR. One way to do so, is to observe that the three subsets Q_1, Q_3, Q_4 have only 2 elements (b and d) among them, and yet an SDR would have to have 3 different elements from those 3 subsets. More generally, if we have a subcollection of the given collection of subsets, that have among them fewer elements than the number of subsets of the subcollection, then there cannot exist an SDR. Hall proved (see Corollary 8.5.1 below) that this is the only thing that can go wrong, that is, that if no such nasty subcollection exists, then there does exist an SDR.

What do SDR's have to do with matching? Given the collection $Q_1, Q_2, \ldots, Q_n$ of subsets of Q, we can construct the bipartite graph with bipartition $A = \{1, 2, \ldots, n\}$, $B = Q$ having the following adjacencies: vertices $k \in A$ and $b \in B$ are adjacent if and only if $b \in Q_k$. (For example, the graph associated with the first example above is shown in Figure 8.10.) Now, corresponding to each SDR $(q_1, q_2, \ldots, q_n)$, the edges $\{1, q_1\}$, $\{2, q_2\}, \ldots$, $\{n, q_n\}$ in G make up a matching saturating A. Conversely, for each matching of G saturating A, say $M = \{\{1, b_1\}, \{2, b_2\}, \ldots, \{n, b_n\}\}$, the sequence $(b_1, b_2, \ldots, b_n)$ is an SDR of $Q_1, Q_2, \ldots, Q_n$. In summary, the collection $Q_1, Q_2, \ldots, Q_n$ has an SDR if and only if graph G has a matching saturating every vertex in A.

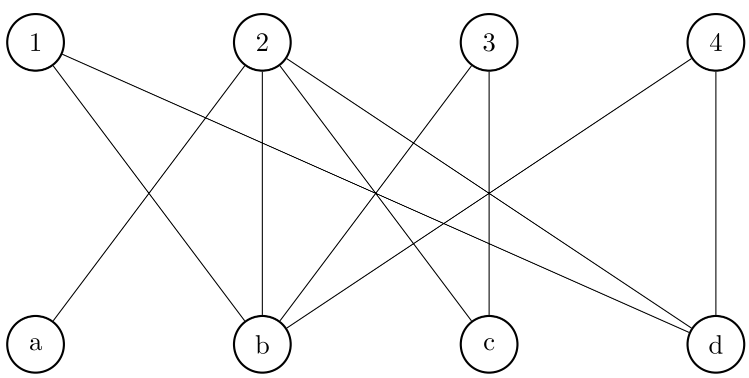


Figure 8.10: Graph constructed from first SDR example

Moreover, the condition described above for an SDR to exist, corresponds exactly to the requirement that in the graph, every subset D of A have $|N(D)| \geq |D|$. Thus the following theorem is nothing but a restatement of Theorem 8.4.1 in the language of SDR's.

Corollary 8.5.1. *(Hall's SDR Theorem) The collection $Q_1, Q_2, \ldots, Q_n$ of subsets of the finite set Q has an SDR if and only if, for every subset J of $\{1, 2, \ldots, n\}$, we have*

$$\left|\bigcup_{i \in J} Q_i\right| \geq |J|.$$

8.6 Perfect Matchings in Bipartite Graphs

We can use Hall's Theorem to obtain a condition for a bipartite graph to have a perfect matching.

Corollary 8.6.1. *A bipartite graph G with bipartition A, B has a perfect matching if and only if $|A| = |B|$ and every subset D of A satisfies*

$$|N(D)| \geq |D|.$$

Proof: Clearly, if $|A| \neq |B|$, then G has no perfect matching. On the other hand, if $|A| = |B|$, then G has a perfect matching if and only if it has a matching saturating every vertex in A, and then the result follows from Hall's Theorem. ∎

Another application is to regular bipartite graphs. We can show that these always have perfect matchings, since it is easy to show that they always satisfy the condition of Corollary 8.6.1. This result will be used in the next section, when we discuss edge-colouring.

Theorem 8.6.2. *If G is a k-regular bipartite graph with $k \geq 1$, then G has a perfect matching.*

Proof: Let A, B be a bipartition of G. Then since every edge has one end in A and the other in B, we have $\sum_{v \in A} deg(v) = \sum_{v \in B} deg(v)$. It follows that $k|A| = k|B|$, and therefore, since $k > 0$, that $|A| = |B|$. Now let $D \subseteq A$. Then since every edge incident with a vertex in D has its other end in $N(D)$, we have

$$\sum_{v \in D} deg(v) \leq \sum_{v \in N(D)} deg(v).$$

It follows that $k|D| \leq k|N(D)|$, and therefore (again, since $k > 0$) that $|N(D)| \geq |D|$. Now by Corollary 8.6.1, G has a perfect matching. ∎

Note: Theorem 8.6.2 works even if G contains multiple edges.

Problem Set 8.6

1. For a bipartition A, B of the graph of Problem Set 8.3, #6, find a set $D \subseteq A$ such that $|N(D)| < |D|$.

2. In the graph of Problem Set 8.3, #7, find a set D of vertices such that $|N(D)| < |D|$.

3. Let G be a bipartite graph with bipartition A, B, let M be a matching of G, and let $D \subseteq A$. Prove that $|M| \leq |A| - |D| + |N(D)|$.

4. Let G be a bipartite graph with bipartition A, B. Prove that the maximum size of a matching of G is the minimum, over subsets D of A, of $|A| - |D| + |N(D)|$.

5. Let G be a bipartite graph with bipartition A, B such that $|A| = |B|$, and for every proper nonempty subset D of A, we have $|N(D)| > |D|$. Prove that for every edge $e \in E(G)$ there is a perfect matching containing e.

6. Check that the proof of Theorem 8.6.2 works even for bipartite multigraphs. (Note that a bipartite multigraph can have multiple edges, but is not allowed to have loops.)

7. A deck of playing cards is arranged in a rectangular array of four rows and thirteen columns. Prove that there exist thirteen cards, no two in the same column and no two of the same value.

8. Find a 3-regular graph having no perfect matching. (Such a graph must be nonbipartite.)

9. Show how to find in a bipartite graph, a largest set of mutually nonadjacent vertices.

10. Let N be a matrix. Let us define the *size* of a submatrix N' of N to be the number of rows of N' plus the number of columns of N'. How could one find a maximum size submatrix of N with the property that each of its entries is 0?

11. Prove Theorem 8.6.2 directly from König's Theorem.

12. Let G be a bipartite graph with bipartition A, B where $|A| = |B| = 2n$. Suppose that, for every subset $X \subseteq A$ and every subset $X \subseteq B$ such that $|X| \leq n$, $|N(X)| \geq |X|$. Prove that G has a perfect matching.

8.7 Edge-colouring

An **edge k-colouring** of a graph G is an assignment of one of a set of k colours to each edge of G so that two edges incident with the same vertex are assigned different colours. Consider the set of edges M that are assigned a particular colour. Then for any vertex v, there can be at most one edge of M incident with v. That is, M is a matching, and so an edge k-colouring of G amounts to a partitioning of the edges of G into k matchings. Figure 8.11 shows an edge 3-colouring of a graph, where the colours are indicated by different ways of drawing the edges.

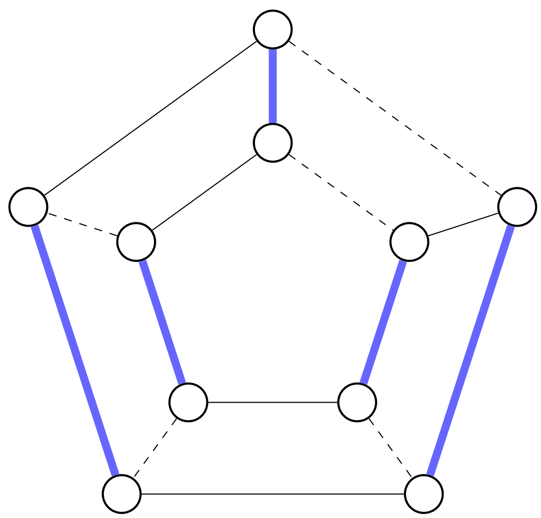


Figure 8.11: A graph with an edge 3-colouring

Obviously, we need at least $deg(v)$ different colours at each vertex v. Therefore, for G to have an edge k-colouring, we must have $k \geq \Delta$, where Δ denotes the maximum degree of vertices of G. The main result of this section is that for bipartite graphs this bound can be achieved.

Theorem 8.7.1. *A bipartite graph with maximum degree Δ has an edge Δ-colouring.*

Lemma 8.7.2. *Let G be a bipartite graph having at least one edge. Then G has a matching saturating each vertex of maximum degree.*

(Note that, in the special case of regular bipartite graphs, all of the vertices have maximum degree, and the lemma says that there must be a perfect matching. In fact, we already have seen this special case—it is Theorem 8.6.2.)

Proof: Let A, B be a bipartition of G and $K = \{v \in V : deg(v) = \Delta\}$. Let M be a maximum matching that leaves as few elements of K unsaturated as possible. If M saturates all elements of K, we are finished. Otherwise, we may assume, by interchanging A with B if necessary, that there is a vertex in $A \cap K$ that is not saturated by M. Apply the XY-construction, except that we define X_0 to consist only of the unsaturated vertices in $A \cap K$. Then Y contains no unsaturated vertex, since M is a maximum matching.

Suppose there is a vertex $w \in X$ having degree less than Δ. Consider the alternating path $P(w)$. It has even length. If we replace the edges of M that are in $P(w)$ by those that are not, we get another maximum matching, but one that leaves fewer elements of K unsaturated, a contradiction to the choice of M. So every vertex in X has degree Δ.

By the construction and the fact that M is maximum, for every $u \in Y$ there is an edge of M joining u to some vertex in X. Since X contains at least one unsaturated vertex, $|X| > |Y|$. Moreover, again by the construction, there is no edge from X to $B \setminus Y$, so $N(X) \subseteq Y$. Therefore,

$$\Delta|Y| < \Delta|X| = \sum_{v \in X} deg(v) \leq \sum_{v \in Y} deg(v) \leq \Delta|Y|,$$

a contradiction. Therefore, there are no vertices in K not saturated by M, and we are done. ▮

Proof of Theorem 8.7.1: The result can be proved by induction on Δ. First, if $\Delta = 0$, then G has no edges, and has an edge 0-colouring. Now suppose $m \geq 1$ and assume that every bipartite graph having $\Delta < m$ has an edge Δ-colouring. Let G be a bipartite graph with $\Delta = m$. By Lemma 8.7.2, G has a matching M saturating all the vertices of degree m. Delete M from G to obtain the graph H. Then H is bipartite and has $\Delta = m-1$, and so by the induction hypothesis, it has an edge $(m-1)$-colouring. If we use this colouring on G, and use one additional colour for the edges of M, then we have an edge m-colouring of G. The result is proved by induction. ▮

Note that the proof of Lemma 8.7.2 suggests a modification of the matching algorithm which will efficiently find a matching saturating all vertices of maximum degree. Therefore, since the proof of Theorem 8.7.1 just requires us to find and delete such a matching and repeat, there is an efficient algorithm for finding an edge Δ-colouring of a given bipartite graph.

8.8 An Application to Timetabling

We have sets of instructors and courses, and for each instructor, the list of courses she teaches. We need to schedule the courses into as few timetable slots as possible, so that no instructor is required to be in two places at the same time. We have the additional requirement that two sections of the same course cannot be given in the same slot. (This may be because we want courses to be available at several different times.)

Let us construct the bipartite graph G having a vertex for each instructor and a vertex for each course, with an edge joining a course vertex to an instructor-vertex if that instructor teaches that course. (If an instructor teaches more than one section of the same course, this would be a multigraph.) The set of edges of the graph corresponds to all of the classes that must be scheduled. Now suppose that we have arranged a schedule, and consider the set of classes taught in a particular slot. These cannot involve any instructor more than once, nor can they involve the same course more than once. That is, they correspond to a matching of G. If we take the slots to correspond to colours, then our problem is one of colouring the edges of G with the minimum number of colours.

Since G is bipartite, we know from Theorem 8.7.1 that the minimum number of slots needed is the maximum degree of the graph G constructed from the data. This is the largest number of sections of a single course, or the largest number of classes taught by a single instructor, whichever is larger. We also know how to solve the problem algorithmically, and actually find a schedule that achieves this minimum.

But suppose now that there is also a classroom limitation, so that at most m classes can be assigned to the same slot. Then of course we cannot find a schedule having fewer than q/m slots, where q is the total number of classes to be scheduled (and is the number of edges of the graph G above). Our problem now becomes:

Bounded edge-colouring problem: What is the smallest number of colours needed to edge-colour a bipartite graph G, given that no colour can be assigned to more than m edges?

The answer turns out to be the smallest integer that is at least q/m and also is at least Δ. This follows from the next result.

Theorem 8.8.1. *Let G be a graph with q edges, and suppose k, m are positive integers such that* *(a)* *G has an edge k-colouring;*

(b) $q \leq km$.

Then G has an edge k-colouring in which every colour is used at most m times.

Proof: Suppose that the colouring does not already have the desired property, so that some colour, say red, is used at least $m+1$ times. If every other colour is used at least m times, then

$$q \geq m+1+m(k-1) > km,$$

a contradiction. So there exists a second colour, say blue, that is used at most $m-1$ times.

Now the red edges and the blue edges form disjoint matchings M and M' of G. Consider the spanning subgraph H of G having edgeset $M \cup M'$. Then every vertex of this graph has degree 0 or 1 or 2. Therefore, each component of H consists of a path or a cycle with edges alternately in M and M'. Moreover, any cycle is even. Since $|M| > |M'|$, there must exist a component of H containing more edges of M than of M'. Such a component must consist of an augmenting path for M'. If we use that path to make M' larger by one and to make M smaller by one, then we have a new edge k-colouring of G such that red is used fewer times, and blue is still used at most m times. We can repeat this argument until we find a colouring with the desired property. ∎

Now we can solve the bounded edge-colouring problem for bipartite graphs by combining Theorems 8.7.1 and 8.8.1.

Corollary 8.8.2. *In a bipartite graph G, there is an edge k-colouring in which each colour is used at most m times if and only if*

(a) $\Delta \leq k$, *and*

(b) $q \leq km$.

Problem Set 8.8

1. Show that the number of colours required to edge-colour a nonbipartite graph G can exceed Δ.

2. Prove that every subgraph of an edge k-colourable graph is edge k-colourable.

3. Prove that a k-regular bipartite graph has an edge k-colouring, using Theorem 8.6.2.

4. Show that the Petersen graph cannot be edge 3-coloured.

5. Show that Theorem 8.8.1 does not work for vertex-colouring. That is, show that if a graph can be k-coloured and $mk \geq p$, it is not necessarily true that there is a k-colouring in which each colour is used at most m times.

6. An n by n *permutation matrix* is a matrix having one 1 and $n-1$ 0's in every row and in every column. Let N be an n by n matrix such that every row and every column contains k 1's and $n-k$ 0's. Prove that N is the sum of k permutation matrices.

7. State an algorithm for finding in a bipartite graph a matching saturating all vertices of maximum degree.

Index