trim

TEXTS AND READINGS
IN MATHEMATICS 55

A First Course in Graph Theory and Combinatorics

Sebastian M. Cioabă
and
M. Ram Murty

HINDUSTAN
BOOK AGENCY

TEXTS AND READINGS
IN MATHEMATICS **55**

A First Course in Graph Theory and Combinatorics

Texts and Readings in Mathematics

A First Course in Graph Theory and Combinatorics

Sebastian M. Cioabă
University of Delaware, USA
and
M. Ram Murty
Queen's University,Canada

HINDUSTAN
BOOK AGENCY

Published in India by

Hindustan Book Agency (India)
P 19 Green Park Extension
New Delhi 110 016
India

email: info@hindbook.com
http://www.hindbook.com

ISBN 978-81-85931-98-2 ISBN 978-93-86279-39-2 (eBook)
DOI 10.1007/978-93-86279-39-2

1	2	3	4	5	6	7	8	9	0
१	२	३	४	५	६	७	८	९	०

Nagari numerals around 11th century A.D.

PREFACE

The butterfly counts not months but moments, and has time enough.

Rabindranath Tagore

The concept of a graph is fundamental in mathematics since it conveniently encodes diverse relations and facilitates combinatorial analysis of many complicated counting problems. In this book, we have traced the origins of graph theory from its humble beginnings of recreational mathematics to its modern setting for modeling communication networks as is evidenced by the world wide web graph used by many internet search engines.

This book is an introduction to graph theory and combinatorial analysis. It is based on courses given by the second author at Queen's University at Kingston, Canada between 2002 and 2008. The courses were aimed at students in their final year of their undergraduate program. As such, we believe this text is very suitable for a first course on this topic.

Graph theory and combinatorics interact well with other branches of mathematics like number theory, algebraic topology, algebraic geometry and representation theory as well as other sciences. For instance, Ramanujan graphs and expander graphs have gained prominence with applications to the construction of optimal communication networks. Thus, we have included a chapter on this important emerging theme at the end of the book.

There are many books on graph theory and combinatorics. What makes this book unique is that we have tried to make it suitable for self-study. Students and non-experts should be able to work through the book at their own pace without an instructor. Hints to the exercises have also been provided to facilitate this study.

The book can also be used for a course at the college level. The material can easily be covered in two semesters. Instructors may find it easy to highlight the graph-theoretic aspects in one course, and the combinatorial aspects in another. For instance, Chapters 1, 3, 4, 5, 6, 8, 10, 11, 12 can be used for a one semester course in graph theory. Chapters 2, 3, 6, 7, and 9 can comprise a short semester course in combinatorics.

At the end of this book, we present a brief list of books and papers that give more details about some of the topics discussed here.

S.M. Cioabă and M. Ram Murty
April 2009

Contents

CHAPTER 1

Basic Notions of Graph Theory

1.1. The Königsberg Bridges Problem

Graph theory may be said to have begun in the 1736 paper by Leonhard Euler (1707-1783) devoted to the Königsberg bridge problem. In the town of Königsberg (now Kaliningrad in western Russia), there were two islands and seven bridges connected as shown in the figure below. The challenge was to leave home and to traverse each bridge exactly once and return home.

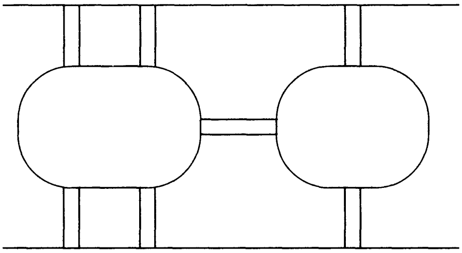


FIGURE 1.1. The bridges of Königsberg

Euler constructs a *graph* corresponding to the problem as follows (see Figure 1.2). The two sides of the river and the two islands are represented by *vertices* or *points* in the plane. They are joined if there is a bridge between them.

The resulting graph has *multiedges* according as the number of bridges between the two points. The Königsberg bridge problem reduces to a *circuit* through the graph which traverses each edge only once. Euler reasoned that if there is such a circuit in the graph, the *valence* of each vertex, or the number of edges coming out of any vertex must be even (see Figure 1.3).

In the Königsberg bridge graph, the valence of each vertex is odd and hence, no such circuit exists. This example illustrates many of the basic notions of graph theory which we take up in the next section.

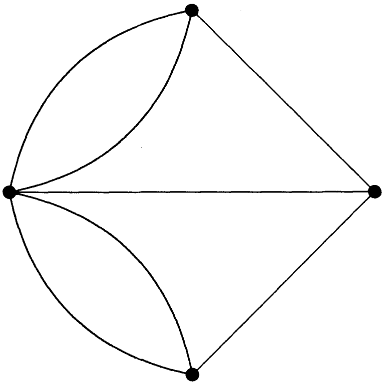


FIGURE 1.2. A graph representation of the bridges of Königsberg

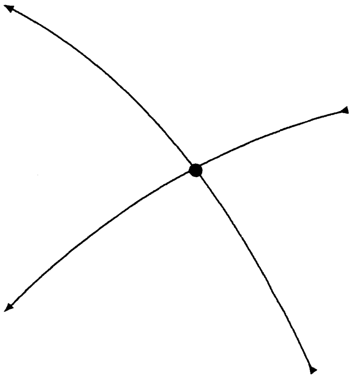


FIGURE 1.3. A vertex in an Eulerian cycle

1.2. What is a Graph?

A **graph** X is a pair (V, E) consisting of a set of **vertices** $V = V(X)$ and **edges** $E = E(X)$ that associates with each edge two vertices (not necessarily distinct) called its **endpoints**. A **loop** is an edge whose endpoints are equal. **Multiple edges** are edges having the same pair of endpoints. A graph is called **simple** if it has no loops or multiple edges. When u and v are endpoints of an edge, we say they are **adjacent** or are **neighbours**. The **valence** or **degree** of a vertex is the number of edges coming out of it. We denote the valence or the degree of the vertex x by $d(x)$. A vertex is said to be **odd** or **even** according as $d(x)$ is odd or even. A graph is said to be **finite** if the vertex and edge sets are finite. We will be treating only finite graphs here.

The graph in Figure 1.2 has multiple edges and thus, is not a simple graph. It has one vertex of valence 5 and three of valence 3. All of its vertices are odd. It has no loops. Our first theorem of graph theory is obvious.

THEOREM 1.2.1. *For a finite graph X,*

$$\sum_{x \in V} d(x) = 2|E(X)|.$$

COROLLARY 1.2.2. *In any finite graph, the number of odd vertices is even.*

An **independent set** or **stable set** in a graph is a subset of vertices no two of which are adjacent. The **complete graph** on n vertices is a simple graph in which any two distinct vertices are adjacent. We denote this graph by the notation K_n. A graph is called **bipartite** if the vertex set can be written as the union of two disjoint independent sets. The bipartite graph $K_{r,s}$ is the simple bipartite graph whose vertex set is a disjoint union of two independent sets of size r and s with every element in the first set adjacent to every element in the second set. The **n-cycle** denoted C_n is the graph on n vertices $v_1, ..., v_n$ with only the adjacency relation $(v_i, v_{i+1}) \in E(C_n)$ for $1 \leq i \leq n$ where we interpret v_{n+1} as v_1.

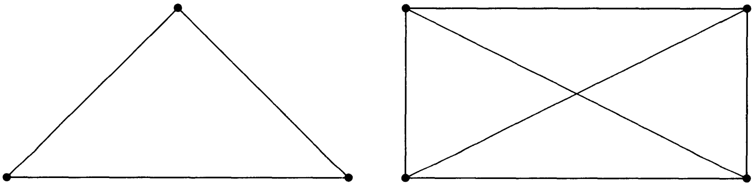


FIGURE 1.4. $K_3 = C_3$ and K_4

Until 1976, one of the most famous unsolved problems of mathematics was the four colour conjecture. This conjecture says that every map can be properly coloured using only four colours, where a proper colouring means that no two adjacent regions should be coloured the same. It was finally solved in 1976 by Kenneth Appel and Wolfgang Haken using extensive computer verification. For some, this is not satisfying and so the search is still on for a more conceptual and clearer solution.

The problem has a long history. It was first posed in a letter of October 23, 1852 from Augustus de Morgan (1806-1871) to William Rowan Hamilton (1805-1865). It was asked by one of de Morgan's students Frederick Guthrie who later attributed to his brother Francis

Guthrie. In 1878, Arthur Cayley (1821-1895) announced the problem to the London Mathematical Society and Alfred Bray Kempe (1849-1922) published a "proof" in 1879. In 1890, Percy John Heawood (1861-1955) indicated there was a gap in Kempe's proof and gave a simple proof that "five colours suffice". This is called the Five Colour Theorem which we will prove later in the book.

Graphs arise in diverse contexts and many of the "real world" problems can be formulated graph-theoretically. An important problem that arises in practice is the following scheduling one. Suppose we have n timetable slots in which to schedule r classes. We want a timetabling so that no student has a conflict. We can create a graph on r vertices, each vertex denoting a class. We join two vertices if they have a common student. We want to "colour" the graph using n colours so that no two adjacent vertices have the same colour. The **chromatic number** of a graph X, written $\chi(X)$, is the minimum number of colours needed to colour the vertices so that no two adjacent vertices have the same colour.

Bipartite graphs arise in job assignment questions. Suppose we have m jobs and n people, but not all people are qualified to do the job. Can we make job assignments so that all the jobs are done? Each job is filled by one person and each person can hold at most one job. Thus, we can create a bipartite graph consisting of n people and m jobs and join a person to a job if the person can do the respective job.

Sometimes, we can assign "weights" to edges and this facilitates discussion of "routing problems". Suppose we have a road network. The edges will correspond to road segments and the weights can be the distances between various points of the network. Questions concerning the shortest path from point a to point b can be formulated in terms of finding the graph geodesic between vertex a and vertex b.

1.3. Mathematical Induction and Graph Theory Proofs

In many proofs of theorems in graph theory and combinatorics, we will require the principle of **mathematical induction** which we recall below. Suppose we have a sequence of propositions $\{P_n\}$ indexed by the natural numbers that we would like to prove. We begin by verifying that P_1 is true. If we can prove that P_k for $k \leq n$ implies P_{n+1} for every n, then all of the propositions are established.

The simplest illustration of this is the following. Notice that

$$1^3 + 2^3 = 9 = 3^2$$

$$1^3 + 2^3 + 3^3 = 36 = 6^2$$

$$1^3 + 2^3 + 3^3 + 4^3 = 100 = 10^2$$

a pattern first noticed by Aryabhata in 5th century India. He showed that in general that

$$s_n := 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

and he did this essentially by the principle of mathematical induction. So the proposition P_n is that s_n is given by the formula above. For $n = 1$ it is clear. Assume we have proved it for each $k \leq n$. Then,

$$s_{n+1} = s_n + (n+1)^3$$

and by the induction hypothesis,

$$s_n = \left(\frac{n(n+1)}{2}\right)^2$$

so that we obtain

$$s_{n+1} = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = (n+1)^2\left(\frac{n^2}{4} + (n+1)\right)$$

$$= (n+1)^2\left(\frac{n^2+4n+4}{4}\right) = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

as required.

We derive two important theorems below by the method of mathematical induction. The first concerns parity of cycles in graphs. The second characterizes Eulerian graphs.

A **walk** in a graph is a sequence $v_0, e_1, v_1, ..., e_k, v_k$ of vertices v_i and edges e_i such that for $1 \leq i \leq k$, the edge e_i has endpoints v_{i-1} and v_i. We sometimes refer to the walk as a v_0, v_k walk to indicate the initial and final points of the walk. The **length** of a walk is the number of edges in it. We say a walk is **odd** or **even** according as the length of the walk is odd or even respectively. A **trail** is a walk with no repeated edge. A **path** is a walk with no repeated vertex. Thus, a path is also a trail. The **distance** $d(u, v)$ between vertices u and v equals the shortest length of a u, v path. A **circuit** is a closed trail. A **cycle** is a closed path. We speak of odd or even paths, trails, cycles, circuits according as their lengths are odd or even respectively.

A graph is said to be **connected** if any two of its vertices are joined by a path. Any graph can be partitioned into its connected components.

LEMMA 1.3.1. *Every closed odd walk contains an odd cycle.*

PROOF. We use induction on the length ℓ of the closed walk W. For $\ell = 1$, a closed walk of length one clearly is also a cycle of length one. So there is nothing to prove. Now suppose that the assertion has been established for odd walks of length $< \ell$. If W has no repeated vertices, then W itself is a closed cycle. Otherwise, we may suppose that a vertex v is repeated in W. We can think of the walk as starting from v and view W as two v, v walks W_1 and W_2 (say). The length of W is the sum of the lengths of W_1 and W_2. As the length of W is odd, one of W_1 or W_2 must have odd length which is necessarily smaller than the length of W. By induction, this odd walk must have an odd cycle. ∎

1.4. Eulerian Graphs

A graph is called **Eulerian** if it has a closed trail containing all edges. A beautiful theorem of Leonhard Euler is the following result.

THEOREM 1.4.1. *A graph is Eulerian if and only if it is connected and all vertices have even degree.*

REMARK 1.4.2. It seems that Euler did not give a complete proof in his 1741 paper. The first complete published proof was given by Karl Hierholzer (1840-1871) in a posthumous article in 1873. The graph we drew to model the problem did not appear in print until 1894.

Before we prove the previous theorem, we need the following lemma.

LEMMA 1.4.3. *If every vertex of a graph X has degree at least 2, then X contains a cycle.*

PROOF. Let P be a maximal path in X. Let u be an endpoint of P. Since P is maximal, every neighbour of u must already be a vertex of P otherwise, P can be extended. Since u has degree at least 2, it has a neighbour v in $V(P)$ via an edge not in P (see Figure 1.5). The edge uv completes a cycle with the portion of P from v to u. ∎

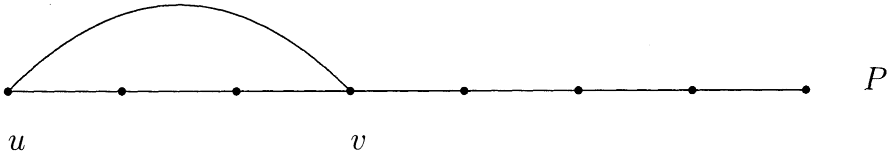


FIGURE 1.5

PROOF. (Theorem 1.4.1) The necessity is clear from what we have said before. We prove sufficiency by induction on the number of edges m of X. If $m = 0$, there is nothing to prove. Since X has even degrees, every vertex of X has degree at least 2. By Lemma 1.4.3, X contains a cycle C. Let X' be the graph obtained from X by deleting the edges of the cycle C. Since C has 0 or 2 edges at each vertex, each component of X' is a connected graph whose degrees are all even. By induction, each component of X' has an Eulerian circuit. We combine these circuits with C to get an Eulerian circuit of X as follows. We travel along C and when we encounter a component of X' for the first time, we go through the Eulerian circuit of that component. This completes the proof. ■

This theorem can be generalized to directed graphs (or **digraphs**). In this context, the theorem on the existence of an Eulerian circuit can be suitably generalized and has interesting algebraic and combinatorial applications (see Exercise 4.5.8).

1.5. Bipartite Graphs

We will use Lemma 1.3.1 to prove the following theorem of König (1936). Dénes König (1884-1944) studied at Budapest and Göttingen. His book *Theorie der endlichen und unendlichen Graphen* - "Theory of finite and infinite graphs" which appeared in 1936 is considered to be the first monograph in graph theory and contributed greatly to the growing interest in this subject.

THEOREM 1.5.1. *A graph X is bipartite if and only if it has no odd cycle.*

PROOF. We first show necessity. Every walk alternates between the two sets of a bipartition. So every return to the original partite set happens after an even number of steps. Hence, X has no odd cycle. For the converse, let X be a graph with no odd cycle. Let U be a non-trivial component of X and u a vertex in it. For each $v \in V(U)$ let $f(v)$ be the minimum length of a u, v-path. Since U is connected, $f(v)$ is defined of every $v \in V(U)$. Let

$$A = \{v \in V(U) : f(v) \,\text{is even}\}$$

and

$$B = \{v \in V(U) : f(v) \,\text{is odd}\}.$$

An edge v, v' within A or B would create a closed odd walk. By Lemma 1.3.1, X would contain an odd cycle, contrary to assumption. Thus, A and B are independent sets. Clearly, $X = A \cup B$ so X is bipartite. ■

We conclude this section with a simple result concerning the degrees of the vertices of a bipartite graph. The bipartite version of the Theorem 1.2.1 is the following result.

THEOREM 1.5.2. *If X is a bipartite graph with colour sets A and B, then*

$$\sum_{a\in A} d(a) = \sum_{b\in B} d(b) = |E(X)|.$$

PROOF. By counting the number of edges of X in two different ways, the result follows immediately. ∎

1.6. Exercises

EXERCISE 1.6.1. Is there a simple graph of 9 vertices with degree sequence

$$3, 3, 3, 3, 5, 6, 6, 6, 6?$$

EXERCISE 1.6.2. Is there a bipartite graph of 8 vertices with degrees

$$3, 3, 3, 5, 6, 6, 6, 6?$$

EXERCISE 1.6.3. In a simple graph with at least two vertices, show that there are at least two vertices with the same degree.

EXERCISE 1.6.4. Show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

and

$$1 + 3 + \cdots + (2n-1) = n^2.$$

EXERCISE 1.6.5. A **directed graph** (or **digraph**) is a graph X together with a function assigning to each edge, an **ordered** pair of vertices. The first vertex is called the **tail** of the edge and the second is called the **head**. To each vertex v, we let $d^+(v)$ be the number of edges for which v is the tail and $d^-(v)$ the number for which it is the head. We call $d^+(v)$ the **outdegree** and $d^-(v)$ the **indegree** of v. Prove that

$$\sum_{v} d^+(v) = \sum_{v} d^-(v) = \#E(X)$$

where the sum is over the vertex set of X.

EXERCISE 1.6.6. In any digraph, we define a **walk** as a sequence

$$v_0, e_1, v_1, e_2, ..., e_k, v_k$$

with v_{i-1} the tail of e_i and v_i its head. The analogous notions of trail, path, circuit and cycle are easily extended to digraphs in the obvious way. If X is a digraph such that the outdegree of every vertex is at least one, show that X contains a cycle.

EXERCISE 1.6.7. An **Eulerian trail** in a digraph is a trail containing all the edges. An **Eulerian circuit** is a closed trail containing all the edges. Show that a digraph X contains an Eulerian circuit if and only if $d^+(v) = d^-(v)$ for every vertex v and the underlying graph has at most one component.

EXERCISE 1.6.8. Determine for what values of $m \geq 1$ and $n \geq 1$ is $K_{m,n}$ Eulerian.

EXERCISE 1.6.9. What is the maximum number of edges in a connected, bipartite graph of order n ?

EXERCISE 1.6.10. How many 4-cycles are in $K_{m,n}$?

EXERCISE 1.6.11. Let Q_n be the **n-dimensional cube** graph. Its vertices are all the n-tuples of 0 and 1 with two vertices being adjacent if they differ in precisely one position. Show that Q_n is connected and bipartite.

EXERCISE 1.6.12. Show that Q_n has 2^n vertices and $n2^{n-1}$ edges.

EXERCISE 1.6.13. How many 4-cycles are in Q_n ?

EXERCISE 1.6.14. Does Q_n contain any copies of $K_{2,3}$?

EXERCISE 1.6.15. Show that every graph X contains a bipartite subgraph with at least half the number of edges of X.

EXERCISE 1.6.16. Let X be a graph in which every vertex has even degree. Show that it is possible to orient the edges of X such that the indegree equals the outdegree for each vertex.

EXERCISE 1.6.17. Show that a graph X is connected if and only if for any partition of its vertex set into two non-empty sets, there exists at least one edge between the two sets.

EXERCISE 1.6.18. Show that in a connected graph any two paths of maximum length have at least one common vertex.

EXERCISE 1.6.19. Let X be a graph with n vertices and e edges. Show that there exists at least one edge uv such that

$$d(u) + d(v) \geq \frac{4e}{n}.$$

EXERCISE 1.6.20. If X is a graph on n vertices containing no K_3's, then the number of edges of X is less than or equal to $\lfloor \frac{n^2}{4} \rfloor$ edges. Give an example of a graph on n vertices containing no K_3's with $\lfloor \frac{n^2}{4} \rfloor$ edges.

CHAPTER 2

Recurrence Relations

2.1. Binomial Coefficients

Combinatorics is the study of finite sets. To define finite sets, we need the notion of bijective function. Given two sets X and Y, a function $f : X \to Y$ is **injective** or **one-to-one** if $f(a) \neq f(b)$ for any $a, b \in X$ with $a \neq b$. A function $f : X \to Y$ is **surjective** or **onto** if for any $y \in Y$, there exist $x \in X$ such that $f(x) = y$. A function is **bijective** if it is injective and surjective. A function $f : X \to Y$ is **invertible** if there exists a function $g : Y \to X$ such that $f(x) = y$ if and only if $g(y) = x$. If g exists, it is called the **inverse** of f and it is usually denoted by f^{-1}. We leave as an exercise the fact that a function is bijective if and only if it is invertible.

We say that a set X is finite if there exists an positive integer n and a bijective function $f : X \to \{1, \ldots, n\}$. In this case, we say that X has n elements or it has cardinality n. Also, the empty set $\emptyset$ is the finite set of cardinality 0.

We usually denote a set with n elements by $[n] = \{1, 2, \ldots, n\}$. To a subset A of $[n]$, one can associate its **characteristic vector** $\chi_A \in \{0, 1\}^n$, where $\chi_A(i) = 1$ if $i \in A$ and 0, otherwise.

PROPOSITION 2.1.1. *The number of subsets of a set with n elements is 2^n.*

PROOF. The correspondence $A \to \chi_A$ is a bijection between the subsets of $[n]$ and the vectors in $\{0, 1\}^n$. The result follows easily since there are 2^n vectors in $\{0, 1\}^n$. ■

One can also use induction on n to prove the previous proposition (see Exercise 2.7.2).

A **permutation** of $[n]$ is a bijective function $f : [n] \to [n]$. The set of all permutations of $[n]$ is denoted by S_n. It is a group called the **symmetric group**. Since $f(1)$ can be chosen in n ways, $f(2)$ in $(n-1)$ ways, ..., $f(n-2)$ in 2 ways and $f(n-1)$ in one way, it follows that the number of permutations is $n(n-1)\ldots 2 \cdot 1$ which will be denoted by $n!$.

We call $i \in [n]$ a **fixed point** for a permutation σ if $\sigma(i) = i$. For $k \geq 2$, the **cycle** $(i_1, \dots, i_k)$ is the permutation $\pi \in S_n$ with $\pi(i_j) = i_{j+1}$ for $j \in [k]$ (here $i_{k+1} = i_1$) and any other $l \neq i_1, \dots, i_k$ is a fixed point of π.

Note that $(i_1, \dots, i_k) = (i_j, i_{j+1}, \dots, i_k, i_1, \dots, i_{j-1})$ for each $j \in [k]$. The **length** of the cycle π is k. A cycle of length 2 is also known as a **transposition**. The **parity** of a permutation $\sigma \in S_n$ equals parity of the number of pairs $1 \leq i < j \leq n$ such that $\sigma(i) > \sigma(j)$. The **signature** of σ is 1 if the parity of σ is even and -1 otherwise.

THEOREM 2.1.2. *Every permutation can be written as a product of disjoint cycles. The representation is unique modulo the order of the factors and the starting points of the cycles.*

PROOF. Let $\sigma \in S_n$. We prove the theorem by induction on the number k of points that are not fixed by the permutation σ.

If $k = 2$, then σ is a transposition which is a cycle of length 2 and we are done.

Assume that $k \geq 3$. Let $i \in [n]$ such that $\sigma(i) \neq i$. Denote by l the smallest integer such that $\sigma^l(i) = i$. Then, $\pi = (i, \sigma(i), \dots, \sigma^{l-1}(i))$ is a cycle of length l. We leave as an exercise for the reader to prove that the number of points that are not fixed by $\sigma\pi^{-1}$ is less than k. By applying the induction hypothesis to $\sigma\pi^{-1}$, the theorem follows. ■

For any integer k with $0 \leq k \leq n$, define the **binomial coefficient** $\binom{n}{k}$ as the number of subsets with k elements (or k-subsets) of $[n]$.

PROPOSITION 2.1.3.

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

PROOF. It is obvious that $\binom{n}{1} = n$ for each $n \geq 1$. Let us count the number of pairs (A, x), where $A \subseteq [n], |A| = k$ and $x \in A$. There are $\binom{n}{k}$ such A's and each has k elements. Thus, the answer is $k\binom{n}{k}$. On the other hand, if we count the x's first, we have n choices. For each x, there are $\binom{n-1}{k-1}$ subsets A such that $A \subseteq [n], x \in A$. This is because each such A is of the form $B \cup \{x\}$, where $B \subset [n] \setminus \{x\}$ and $|B| = k-1$. Thus, the answer we get now is $n\binom{n-1}{k-1}$. Hence, $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$.

Replacing n by $n-1, n-2, \dots, n-k+2$, we obtain

$$\binom{n-i}{k-i} = \frac{n-i}{k-i}\binom{n-i-1}{k-i-1}$$

for $i = 0, 1, \ldots, k-2$. Multiplying all these equations together, we get

$$\binom{n}{k}\prod_{i=1}^{k-2}\binom{n-i}{k-i} = \frac{n(n-1)\ldots(n-k+1)}{k!}\prod_{i=1}^{k-2}\binom{n-i}{k-i}.$$

Simplifying the previous equality, we obtain

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

as claimed. ■

When n is an integer, an easy to remember formula for $\binom{n}{k}$ is $\frac{n!}{k!(n-k)!}$. One can use these results to determine which binomial coefficient $\binom{n}{k}$ is the largest when $0 \leq k \leq n$ (see Exercise 2.7.1).

The originators of combinatorics came from the East and the main stimulus came from the Hindus. The formulae for the number of permutations on n elements and the number of k-subsets of $[n]$ were known to Bhaskara around 1150. Special cases of these formulae were found in texts dating back to the second century BC.

The following theorem is often attributed to Blaise Pascal (1623-1662) who knew this result as it appeared in a posthumous pamphlet published in 1665. It appears that the result was known to various mathematicians preceding Pascal such as the 3rd century Indian mathematician Pingala.

THEOREM 2.1.4 (Binomial Theorem). *For any positive integer n,*

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

PROOF. Writing $(x+a)^n$ as $(x+a)(x+a)\ldots(x+a)$, we notice that the number of times the term $x^k a^{n-k}$ appears, equals the number of ways of choosing k brackets (for x) from the n factors of the product. That is exactly $\binom{n}{k}$. ■

Sir Isaac Newton (1643-1727) was one of the greatest mathematicians of the world. His contributions in mathematics, physics and astronomy are deep and numerous. In 1676, Newton showed that a similar formula holds for real n. Newton's formula involves infinite series and it will be discussed in the Catalan number section.

If $f, g : \mathbb{N} \to \mathbb{R}$, we say $f(n) \sim g(n)$ if $\lim\limits_{n\to\infty}\dfrac{f(n)}{g(n)} = 1$. James Stirling (1692-1770) was a Scottish mathematician who showed that

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

This is usually called Stirling's formula. It appears in *Methodus Differentialis* which Stirling published in 1730. Abraham de Moivre (1667-1754) also knew this result around 1730.

2.2. Derangements

The term *reccurence* is due to Abraham de Moivre (1722). A sequence satisfies a recurrence relation when each term of the sequence is defined as a function of the preceding terms. In many counting questions, it is more expedient to obtain a recurrence relation for the combinatorial quantity in question. Depending on the nature of this recurrence, one is then able to determine in some cases, an explicit formula, and in other cases, where explicit formulas are lacking, some idea of the growth of the function. We will give several examples in this chapter.

We begin with the problem of counting the number of permutations σ of S_n without any fixed points. These are permutations with the property that $\sigma(i) \neq i$ for all $1 \leq i \leq n$. Such permutations are called **derangements**. The first appearance of this problem is in 1708 in a book on games of chance *Essay d'Analyse sur les Jeux de Hazard* by Pierre Rémond de Montmort (1678-1719).

Let d_n be the number of derangements on $[n]$. We will obtain a recurrence relation for it as follows. For such a derangement, we know that $\sigma(n) = i$ for some $1 \leq i \leq n-1$. We fix such an i and count the number of derangements with $\sigma(n) = i$. Since there are $n-1$ choices for i, the final tally is obtained by multiplying this number by $n-1$. If σ is a derangement with $\sigma(n) = i$, we consider two cases. If $\sigma(i) = n$, then σ restricted to

$$\{1, 2, ..., n\} \backslash \{i, n\}$$

is a derangement on $n-2$ letters and the number of such is d_{n-2}. If $\sigma(i) \neq n$, let j be such that $\sigma(j) = n$, with $i \neq j$. Thus, if we define σ' by setting

$$\sigma'(k) = \sigma(k), \quad \text{for } 1 \leq k \leq n-1,\ k \neq j$$

and $\sigma'(j) = i$, we see that σ' is a derangement on $n-1$ letters. Conversely, if σ' is a derangement on $n-1$ letters and $\sigma'(j) = i$, we can extend it to a derangement on n letters by setting $\sigma(j) = n$ and $\sigma(n) = i$. Thus, we get the recurrence

THEOREM 2.2.1.

$$d_n = (n-1)(d_{n-1} + d_{n-2}).$$

Now we will prove by induction that:

THEOREM 2.2.2. *For $n \geq 1$,*

$$d_n = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}.$$

PROOF. Indeed, if $n = 1$, it is clear that $d_1 = 0$ and for $n = 2$, $d_2 = 1$. If we let $f(n)$ denote the right hand side of the above equation, we will show that $f(n)$ satisfies the same recursion as d_n with the same initial conditions, thereby establishing the result. Thus, $(n-1)(f(n-1) + f(n-2))$ equals

$$\begin{aligned}
&(n-1)! \sum_{j=0}^{n-2} \frac{(-1)^j}{j!} \left((n-1) \left(1 + \frac{(-1)^{n-1}}{(n-1)!} \right) + 1 \right) \\
&= n! \sum_{j=0}^{n-2} \frac{(-1)^j}{j!} + \frac{(-1)^{n-1}}{(n-1)!} (n-1) \\
&= f(n)
\end{aligned}$$

as desired. ■

Let us observe that

$$\lim_{n \to \infty} \frac{d_n}{n!} = \frac{1}{e}.$$

In fact, we can make this more precise. As the series is alternating we begin by noting that if a_n is a decreasing sequence of positive real numbers tending to zero, then,

$$|\sum_{j=0}^{\infty} (-1)^j a_j - \sum_{j=0}^{n} (-1)^j a_j| \leq |a_{n+1} - (a_{n+2} - a_{n+3}) - \cdots | \leq a_{n+1}.$$

Thus,

$$\left| e^{-1} - \frac{d_n}{n!} \right| < \frac{1}{(n+1)!}.$$

Denoting by $\lfloor x \rfloor$ the largest integer less than or equal to x, the previous equation implies the following result.

THEOREM 2.2.3. *For $n \geq 1$,*

$$d_n = \lfloor n!/e + 1/2 \rfloor.$$

PROOF. By our remarks above,

$$|d_n - n!/e| \leq \frac{1}{n+1} < \frac{1}{2}$$

for $n \geq 1$. As d_n is a non-negative integer, it is uniquely determined by this inequality as the nearest integer to $n!/e$.

We leave as an easy exercise for the reader to show that the nearest integer to x is $[x+1/2]$. ■

This result means that the probability that a random permutation in S_n is a derangement is about $\frac{1}{e}$. We give a different proof of the formula for the number of derangements using inclusion and exclusion in Chapter 3.

2.3. Involutions

We now want to count the number of elements of order 2 in the symmetric group S_n. Such an element is called an **involution**. Recall that any permutation is a product of disjoint cycles and the order of the permutation is the least common multiple of the cycle lengths. Thus, if the permutation has order 2, then all the cycles must be of length 1 or 2. Let $s(n)$ be the number of such involutions. We partition these involutions into two groups: those that fix n and those that do not. The number fixing n is clearly $s(n-1)$. If σ is an involution not fixing n, then $\sigma(n) = i$ (say) for some $1 \le i \le n-1$. But then we must necessarily have $\sigma(i) = n$ as σ is a product of 1-cycles or 2-cycles (transpositions). Thus, σ restricted to

$$\{1, 2, ..., n-1\} \backslash \{i\}$$

is an involution on $n-1$ letters. There are $s(n-2)$ such elements and $n-1$ choices for i, so we get the recurrence

THEOREM 2.3.1. *Let $s(n)$ be the number of involutions in S_n. Then*

$$s(n) = s(n-1) + (n-1)s(n-2).$$

We can derive a modest amount of information from this recurrence, though our results will not be as sharp as what we obtained for d_n, the number of derangements in S_n. We have:

THEOREM 2.3.2. (1) *$s(n)$ is even for all $n > 1$.*
(2) *$s(n) > \sqrt{n!}$ for all $n > 1$.*

PROOF. Clearly, $s(1) = 1$ and $s(2) = 2$ and the assertion is true for $n = 2$. From the recurrence (or directly) we see that $s(3) = 4$. Consequently, applying induction to the recurrence, one can show easily that $s(n)$ is even. We will also apply induction to prove the second part of the theorem. Again, for $n = 2$ and $n = 3$, the inequality is clear. Suppose we have established the inequality for numbers $< n$. Then, by induction,

$$s(n) > \sqrt{(n-1)!} + (n-1)\sqrt{(n-2)!} \ge (\sqrt{(n-1)!})(1 + \sqrt{n-1}).$$

To complete the proof, we need to show

$$1+\sqrt{n-1} \geq \sqrt{n}.$$

But this is clear by squaring both sides of the inequality. ■

2.4. Fibonacci Numbers

The **Fibonacci numbers** are defined recursively as follows. $F_0 = 1$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The following problem led Fibonacci to consider these numbers. Suppose we start with a pair of rabbits, one male and one female. At the end of each month, every female produces one new pair of rabbits (one male and one female). The question that Leonardo Pisano Fibonacci (1170-1250) asked was: how many pairs will there be in one year ? This problem appears in 1202 in his book *Liber abaci* which also introduced the use of Arabic numerals into Europe.

It is easy to see that the number of pairs after n months will be exactly F_n. How can we find a formula for F_n ?

The Fibonacci numbers satisfy a **linear recurrence relation with constant coefficients**. These are recurrence relations of the following form:

$$y_n = a_1 y_{n-1} + a_2 y_{n-2} + \cdots + a_k y_{n-k}$$

where $k \geq 1$ is a fixed integer and $a_1, a_2, \ldots, a_k$ are all constant (they do not depend on n).

To find a general formula for y_n, we must solve the characteristic equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k.$$

If this equation has distinct solutions, then y_n is going to be a linear combination of the n-th powers of these solutions. Using the initial k values of the sequence $(y_n)_n$, one can find the exact formula for y_n.

If the previous equation has multiple solutions, a formula for y_n can be determined as follows. If α is a solution with multiplicity r, then one can check $\alpha^n, n\alpha^n, \ldots, n^{r-1}\alpha^n$ are all solutions of the characteristic equation. We can write y_n as a linear combination of such solutions and use the initial values of the sequence $(y_n)_n$ to determine a precise formula.

Let us try to use this method to find a formula for F_n. Since the recurrence relation is $F_n = F_{n-1}+F_{n-2}$, it follows that the characteristic equation is $x^2 = x+1$. The solutions of this equation are $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. We obtain that $F_n = c\alpha^n + d\beta^n$, where c and d are constants to be determined.

Since $1 = F_0 = c+d$ and $1 = F_1 = c\alpha + d\beta$, we obtain that $c = \frac{\sqrt{5}+1}{2\sqrt{5}}$ and $d = \frac{\sqrt{5}-1}{2\sqrt{5}}$. We deduce that

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

2.5. Catalan Numbers

Eugéne Charles Catalan (1814-1894) was born in Bruges, Belgium. He defined the numbers which bear his name today, while counting the number of ways of decomposing a convex n-gon into triangles by $n-2$ non-intersecting diagonals. Around the same time, the Catalan numbers were also studied by Johann Andreas von Segner (1704-1777), Leonhard Euler (1707-1783) and Jacques Binet (1786-1856).

The Catalan numbers have many combinatorial interpretations and arise in branches of mathematics and computer science. There are at least 66 combinatorial interpretations of Catalan numbers (see Exercise 6.19 in Richard Stanley's *Enumerative Combinatorics, Volume 2*).

Here we will define the Catalan number C_n as the number of ways we can bracket a sum of n elements so that it can be calculated by adding two terms at a time. For example, for $n = 3$, we have

$$((a+b)+c) \quad \text{and} \quad (a+(b+c)).$$

Thus, $C_3 = 2$.

For $n = 4$, we have $C_4 = 5$ since there are five ways of bracketing a sum with 4 terms:

$$\begin{gathered}(((a+b)+c)+d),\\ ((a+(b+c))+d),\\ (a+((b+c)+d)),\\ (a+(b+(c+d))),\\ ((a+b)+(c+d)).\end{gathered}$$

We can obtain a recurrence for C_n as follows. Any bracketed expression is of the form

$$E_1 + E_2$$

where E_1 is a bracketed expression containing i terms (say) and E_2 is a bracketed expression containing $n-i$ terms. By our definition, there are C_i choices for E_1 and C_{n-i} choices for E_2, so we get

$$C_n = \sum_{i=1}^{n-1} C_i C_{n-i}.$$

It may be that Segner was the first to notice this recurrence relation and Euler was the first to solve it (see Chapter 6 in *Enumerative Combinatorics, Volume 2* by Richard Stanley). Notice that this recurrence is more complicated than the one for d_n or $s(n)$ derived in the previous sections in that the recurrence uses all of the previous C_i's for its determination.

In order to determine a nice formula for the Catalan numbers, we use the theory of generating functions. To an infinite sequence $(a_n)_{n\geq 0}$ we associate the following **formal power series**:

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

We regard such series as algebraic objects without any interest in their convergence. We say two series are equal if their coefficient sequences are identical. We define addition and subtraction as follows

$$\sum_{n\geq 0}(a_n \pm b_n)t^n = \sum_{n\geq 0} a_n t^n \pm \sum_{n\geq 0} b_n t^n.$$

The multiplication is defined similarly to the one for polynomials.

$$\sum_{n\geq 0} a_n t^n \cdot \sum_{n\geq 0} b_n t^n = \sum_{n\geq 0} c_n t^n$$

where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. We can also differentiate formal power series the same way as one would do for polynomials.

$$\left(\sum_{n\geq 0} a_n t^n\right)' = \sum_{n\geq 1} n a_n t^{n-1}.$$

The standard functions of analysis are defined as formal power series by their usual Taylor series. For example,

$$e^t = \sum_{n\geq 0} \frac{t^n}{n!}.$$

The following equation is a definition of $(1+t)^\alpha$

$$(1+t)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} t^n$$

where $\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}$ for any real number α. If α is a nonnegative integer, then this is just Theorem 2.1.4 since $\binom{\alpha}{n} = 0$ for $n > \alpha$. For α real, the equation above will be regarded here as a definition. An alternative approach would be to define $(1+t)^\alpha$ for any rational α by using the exponent laws (which hold for power series) and then prove that its Taylor series has the claimed form. This was done by Newton.

We encode the recurrence for the Catalan numbers in a **generating function** as follows. Let

$$F(t) = \sum_{n=0}^{\infty} C_n t^n$$

where we set $C_0 = 0$ and $C_1 = 1$. Let us compute the coefficient of t^n in $F(t)^2$ for $n \geq 2$. It is equal to

$$\sum_{i=1}^{n-1} C_i C_{n-i} = C_n$$

since $C_0 = 0$. Thus,

$$F(t)^2 = F(t) - t.$$

This is a quadratic equation in $F(t)$ which we can solve using the familiar formula for solving quadratic equations:

$$F(t) = \frac{1 \pm \sqrt{1-4t}}{2}.$$

We must determine which "sign" will give us the correct solution for $F(t)$. We choose the minus sign because $F(0) = 0$. Thus,

$$F(t) = \frac{1 - \sqrt{1-4t}}{2}.$$

We can use the binomial theorem to determine the C_n's explicitly. Indeed, the coefficient of t^n on the right hand side of the above expression for $F(t)$ is easily seen to be

$$-\frac{1}{2}\binom{1/2}{n}(-4)^n$$

which simplifies to the following result.

THEOREM 2.5.1.

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

We can use Stirling's formula to determine the asymptotic behaviour of C_{n+1}. Indeed, by Stirling's formula,

$$n! \sim \sqrt{2\pi n}(n/e)^n,$$

so that

$$C_{n+1} \sim \frac{2^{2n}}{(n+1)\sqrt{\pi n}},$$

from which we see that it has exponential growth.

2.6. Bell Numbers

Eric Temple Bell (1883-1960) was born in Aberdeen, Scotland. He was the president of the Mathematical Association of America between 1931 and 1933.

The n-th Bell number, denoted by B_n, is the number of partitions of an n-element set. A partition of $[n]$ is a collection of pairwise disjoint non-empty subsets $B_1, \ldots, B_k$ (called blocks) whose union is $[n]$. By convention, $B_0 = 1$. The partitions of $[2]$ are $\{1\} \cup \{2\}$ and $\{1,2\}$. The partitions of $[3]$ are $\{1\} \cup \{2\} \cup \{3\}, \{1,2\} \cup \{3\}, \{1,3\} \cup \{2\}, \{2,3\} \cup \{1\}$ and $\{1,2,3\}$. Thus, $B_1 = 1$, $B_2 = 2$ and $B_3 = 5$. We will derive a recurrence relation for the Bell numbers. Of the partitions of $[n]$, we consider the block to which n belongs. Clearly, such a block can be written as $\{n\} \cup Y$ for some subset Y of $\{1, 2, ..., (n-1)\}$. If this block has k elements, then Y is a subset of $k-1$ elements. The number of ways of choosing Y is $\binom{n-1}{k-1}$. The remaining elements can be partitioned in B_{n-k} ways. Thus, we obtain

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}.$$

We can use this recurrence to write down an **exponential generating function**:

$$G(t) = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

Then,

$$G'(t) = \sum_{n=1}^{\infty} \frac{B_n}{(n-1)!} t^{n-1} = \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{t^{k-1}}{(k-1)!} \frac{B_{n-k} t^{n-k}}{(n-k)!}.$$

The sum on the right hand side is easily seen to be

$$e^t G(t).$$

Thus,

$$G(t) = Ae^{e^t}$$

for some constant A. Since $G(0) = 1$, we must have $A = e^{-1}$. This proves:

THEOREM 2.6.1.

$$\sum_{n=0}^{\infty} \frac{B_n t^n}{n!} = e^{e^t - 1}.$$

We can use this theorem to derive an explicit formula for B_n as follows. The right hand side of the above equation can be expanded as

$$\frac{1}{e}\sum_{j=0}^{\infty}\sum_{n=0}^{\infty}\frac{j^n t^n}{n!j!}$$

and on comparing the coefficients of t^n we obtain:

THEOREM 2.6.2.

$$B_n = \frac{1}{e}\sum_{j=0}^{\infty}\frac{j^n}{j!}.$$

2.7. Exercises

EXERCISE 2.7.1. If $0 \leq k \leq \lfloor \frac{n}{2} \rfloor$, show that

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

EXERCISE 2.7.2. Prove by induction on n that $[n]$ has 2^n subsets.

EXERCISE 2.7.3. Show that

$$1 \cdot 1! + 2 \cdot 2! + \ldots n \cdot n! = (n+1)! - 1.$$

EXERCISE 2.7.4. Show that

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

for each $n \geq k \geq l \geq 0$.

EXERCISE 2.7.5. Show that

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

EXERCISE 2.7.6. Show that

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

EXERCISE 2.7.7. Show that

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

EXERCISE 2.7.8. Show that

$$\frac{2^{2n}}{2n+1} < \binom{2n}{n} < 2^{2n}$$

and use Stirling's formula to prove that

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}}.$$

EXERCISE 2.7.9. Give a solution using binomial coefficients and a direct combinatorial solution to the following question: How many pairs (A, B) of subsets of $[n]$ are there such that $A \cap B = \emptyset$?

EXERCISE 2.7.10. Show that the number of even subsets of $[n]$ equals the number of odd subsets of $[n]$. Give two proofs, one using binomial formula, and one using a direct bijection. Calculate the sum of the sizes of all even (odd) subsets of $[n]$.

EXERCISE 2.7.11. Let n be an integer, $n \geq 1$. Let s_i denote the number of subsets of $[n]$ whose order is congruent to $i \pmod 3$ for $i \in \{0, 1, 2\}$. Determine s_0, s_1, s_2 in terms of n.

EXERCISE 2.7.12. Prove by mathematical induction that

$$\sqrt{5}F_n = \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

for $n \geq 0$.

EXERCISE 2.7.13. Show that the number of distinct ways of triangulating a convex n-gon by $n-2$ nonintersecting diagonals equals C_{n-1}.

EXERCISE 2.7.14. Show that the number of solutions of the equation

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

in positive integers ($x_i > 0$ for each i) is $\binom{n-1}{k-1}$.

EXERCISE 2.7.15. Show that for each n and $k, 1 \leq k \leq n$

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} < \left(\frac{en}{k}\right)^k.$$

EXERCISE 2.7.16. Calculate

$$\sum_{A \subseteq [n]} |A|^2.$$

EXERCISE 2.7.17. Calculate

$$\lim_{n\to\infty} \sqrt[n]{\sum_{k=0}^{n} \binom{n}{k}^t}$$

when t is a real number.

EXERCISE 2.7.18. Let k be a non-negative integer number. Show that any non-negative integer number n can be written uniquely as

$$n = \binom{x_k}{k} + \binom{x_{k-1}}{k-1} + \cdots + \binom{x_2}{2} + \binom{x_1}{1}$$

where $0 \leq x_1 < x_2 < \cdots < x_k$.

EXERCISE 2.7.19. Let B_n denote the n-th Bell number. Show that $B_n < n!$ for each $n \geq 3$.

EXERCISE 2.7.20. Determine the number of ways of writing a positive integer n as a sum of ones and twos.

CHAPTER 3

The Principle of Inclusion and Exclusion

3.1. The Main Theorem

The principle of inclusion-exclusion was used by De Moivre in 1718 to calculate the number of derangements on n elements.

Let A be a finite set and for each $i \in \{1, 2, ..., n\}$, let A_i be a subset of A. We would like to know how many elements there are in the set

$$A \setminus \cup_{i=1}^{n} A_i.$$

That is, we would like to know the number of elements remaining in A after we have removed the elements of A_i for each $i = 1, 2, ..., n$. To this end, we define for each subset I of $[n] = \{1, 2, ..., n\}$,

$$A_I = \cap_{i \in I} A_i.$$

That is, A_I consists of elements belonging to all A_i, $i \in I$. If I is the empty set $\emptyset$, we make the convention $A_\emptyset = A$. The principle of inclusion and exclusion is contained in the following theorem.

THEOREM 3.1.1. *The number of elements not belonging to any A_i, $1 \leq i \leq n$ is given by*

$$\sum_{I \subseteq [n]} (-1)^{|I|} |A_I|.$$

PROOF. The sum is equal to

$$\sum_{I \subseteq [n]} (-1)^{|I|} \sum_{a \in A_I} 1 = \sum_{a \in A} \sum_{I : I \subseteq [n], a \in A_I} (-1)^{|I|}.$$

Let S_a be the set of indices i such that $a \in A_i$. Then, the inner sum is over all subsets of S_a. If S_a is empty, this sum is 1. Otherwise, by the Binomial Theorem, it is equal to

$$\sum_{j=0}^{|S_a|} (-1)^j \binom{|S_a|}{j} = (1 - 1)^{|S_a|} = 0,$$

when S_a is non-empty. Hence, the sum is equal to the number of elements a for which S_a is empty. Since the number of elements not belonging to any A_i is precisely the number of elements a for which S_a is empty, this completes the proof. ■

This simple principle is one of the most powerful in all of mathematics and has important consequences which we will present in the next sections.

3.2. Derangements Revisited

It will be recalled that in Chapter 2, we derived a recurrence relation for the number of derangements of a set with n elements. We then "guessed" a formula and proved it by induction. We now give a more credible approach to the derivation of this formula. Let A be the set $\{1, 2, ..., n\}$. The number d_n counts the number of permutations without any fixed points. For each i, $1 \leq i \leq n$, let A_i be the subset of permutations fixing i. Then, the number of derangements is the number of permutations not belonging to any of the A_i, $1 \leq i \leq n$. For each subset I of $\{1, 2, .., n\}$, the number of elements of A_I is clearly $(n - |I|)!$. By the inclusion-exclusion principle, we obtain the following result.

THEOREM 3.2.1.

$$d_n = \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)!.$$

This is precisely the formula we established by induction in the previous chapter. As noted earlier, this result has the curious consequence that if a group of 100 people each wrote their names on a card and these cards were then collected and shuffled and a card is handed back to each person, then the probability that a person would receive their own original card back is very close to $1 - 1/e$.

3.3. Counting Surjective Maps

Let us now count the number of surjective functions from an n-set to a k-set. The total number of functions from $[n]$ to $[k]$ is clearly k^n.

THEOREM 3.3.1. *The number of surjective functions* $f : [n] \rightarrow [k]$ *is*

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

PROOF. For each $1 \leq i \leq k$, let A_i be the set of functions from an n-set to a k-set that do not have i in their range. Then, A_I has cardinality $(k - |I|)^n$. By the inclusion-exclusion principle, the result is now immediate. ■

COROLLARY 3.3.2. *If k and n are nonnegative integers, then*

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n=\begin{cases}0 & \text{if } k<n;\\ n! & \text{if } k=n.\end{cases}$$

PROOF. If $n<k$, there are no surjective functions from an n-set to a k-set. The number of surjective maps from an n-set to another n-set is clearly $n!$. The result now follows from the previous theorem. ∎

3.4. Stirling Numbers of the First Kind

We now introduce **Stirling numbers of the first kind**, denoted $s(n,k)$. The Stirling numbers of first kind and of second kind (which will be defined in the next section) are named after James Stirling whose formula for $n!$ is contained in the previous chapter. Recall that every permutation has a unique decomposition (up to rearrangement) as a product of disjoint cycles. We define $s(n,k)$ by the rule that $(-1)^{n-k}s(n,k)$ is the number of permutations of S_n which can be written as a product of k-disjoint cycles. Clearly, $s(n,n)=1$ since the only permutation that has n disjoint cycles in its cycle decomposition is the identity permutation. It is also clear that

$$\sum_{k=1}^{n}(-1)^{n-k}s(n,k)=\sum_{k=1}^{n}|s(n,k)|=n!.$$

We now establish a recurrence for $s(n,k)$.

THEOREM 3.4.1.

$$s(n+1,k)=-ns(n,k)+s(n,k-1).$$

PROOF. Of the permutations of S_{n+1} with k disjoint cycles, we consider those in which $(n+1)$ appears as a one cycle and those in which it does not. The number in the first group is clearly $(-1)^{n-(k-1)}s(n,k-1)$. For the number in the second group, we may view the elements as permutations of S_n with k disjoint cycles into which we have inserted $(n+1)$. For a cycle of S_n of length j, there are j places into which we can insert $(n+1)$ giving j new permutations. Now if σ is a permutation of S_n with k-cycles of lengths $j_1,...,j_k$, we can interpolate $(n+1)$ into this in $j_1+\cdots+j_k=n$ ways. Thus, the number of elements in the second group is $n(-1)^{n-k}s(n,k)$.

Thus,

$$(-1)^{n+1-k}s(n+1,k)=(-1)^{n-(k-1)}s(n,k-1)+n(-1)^{n-k}s(n,k).$$

This simplifies to give the stated recurrence. ∎

For $t \in \mathbb{R}$, we denote $(t)_n = t(t-1)\dots(t-n+1)$. Using the previous result, we can prove the following:

THEOREM 3.4.2.

$$(t)_n = \sum_{k=1}^{n} s(n,k)t^k.$$

PROOF. Again, we use induction on n. For $n = 1$, the result is clear. Assume that the result is established for $n \leq m$. Then,

$$(t)_{m+1} = (t)_m(t-m) = \left(\sum_{k=1}^{m} s(m,k)t^k\right) \cdot (t-m).$$

The coefficient of t^k on the right is

$$s(m,k-1) - ms(m,k)$$

which is precisely $s(m+1,k)$ by the previous theorem. This completes the proof. ∎

3.5. Stirling Numbers of the Second Kind

We denote by $S(n,k)$ the number of partitions of an n-set into k-blocks. These numbers are called the **Stirling numbers of the second kind**. We will try to relate these numbers to the discussion of the surjective functions. Observe that if we have a surjective map f from an n-set to a k-set, the "fibers", namely $f^{-1}(j) := \{i : i \in [n], f(i) = j\}$, for $1 \leq j \leq k$ form a partition of the n-set into k-blocks. Conversely, given a partition of a n-set into k-blocks, there are clearly $k!S(n,k)$ ways of defining a surjective map from the n-set to a k-set because we can view each block as the fiber of the image of such a map and there are $k!$ ways of assigning the image. Putting this together with Theorem 3.3.1 gives the following result.

THEOREM 3.5.1.

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

We again see how one can deduce Corollary 3.3.2. Indeed, if $k > n$, there are no ways of partitioning an n-set into k-blocks as each block must contain at least one element. For $k = n$, we clearly have $S(n,n) = 1$.

This formula also allows us in yet another way to deduce the generating function for the Bell numbers B_n which we derived in the previous chapter. Indeed, we clearly have

$$B_n = \sum_{k=0}^{n} S(n,k).$$

On the other hand, notice that

$$\sum_{n=0}^{\infty} \frac{S(n,k)t^n}{n!} = \frac{1}{k!}\sum_{n=0}^{\infty}\frac{t^n}{n!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n.$$

Upon interchanging the summation, we get that this equals

$$\frac{1}{k!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}e^{(k-j)t}.$$

Using the binomial theorem, we can simplify the right hand side and deduce:

THEOREM 3.5.2.

$$\sum_{n=0}^{\infty}\frac{S(n,k)t^n}{n!} = \frac{1}{k!}(e^t-1)^k.$$

Combining this fact with the formula relating B_n with the Stirling numbers of the second kind easily gives us again the generating function

$$\sum_{n=0}^{\infty}\frac{B_nt^n}{n!} = e^{e^t-1}.$$

Even though we have an explicit formula for the $S(n,k)$'s, it will be useful to derive the following recurrence relation.

THEOREM 3.5.3.

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

PROOF. In partitioning the n-set $\{1,2,...,n\}$ into k blocks, we have two possibilities. Either n is in a singleton block by itself or it is not. In the first case, the number of such decompositions clearly corresponds to $S(n-1,k-1)$. In the second case, we take the decomposition of an $(n-1)$-set into k-blocks, and we now have k choices into which we may place n. This gives the recursion. ■

We may use this recursion to give another 'generating form' for the numbers $S(n,k)$ for n fixed and varying k. To this end, we recall the notation $(t)_n = t(t-1)(t-2)...(t-n+1)$.

THEOREM 3.5.4.

$$t^n = \sum_{k=1}^{n} S(n,k)(t)_k.$$

PROOF. The proof is by induction on n. For $n = 1$, the result is clear. Suppose that we have proved the formula for $n \leq m$. Then, we write

$$t^{m+1} = t^m \cdot t = \sum_{k=1}^{m} S(m,k)(t)_k((t-k)+k)$$

by the induction hypothesis. Because $(t)_k(t-k) = (t)_{k+1}$, we deduce that

$$t^{m+1} = \sum_{k=1}^{m} S(m,k)(t)_{k+1} + \sum_{k=1}^{m} kS(m,k)(t)_k.$$

By changing variables on the first sum, and noting that $S(m, m+1) = 0$, we may write the right hand side as

$$\sum_{k=1}^{m+1} \{S(m,k-1) + kS(m,k)\}(t)_k = \sum_{k=1}^{m+1} S(m+1,k)(t)_k$$

by the recursion of Theorem 3.5.3. This completes the proof. ∎

COROLLARY 3.5.5. *If A and B are the $n \times n$ matrices whose (i,j)-th entries are given by $s(i,j)$ and $S(i,j)$ respectively, then $B = A^{-1}$.*

PROOF. Let V be the vector space of polynomials of degree $\leq n$, with constant term zero. Then A and B are the transition matrices from the two bases:

(1) $t, t^2, ..., t^n$;
(2) $(t)_1, (t)_2, ..., (t)_n$.

The result now follows from linear algebra. ∎

COROLLARY 3.5.6. *The following are equivalent:*

(1) $g_n = \sum_{k=1}^{n} S(n,k) f_k$;
(2) $f_n = \sum_{k=1}^{n} s(n,k) g_k$.

PROOF. This is immediate from matrix inversion. ∎

If we define f_0 and g_0 so that $f_0 = g_0$, and

$$F(t) = \sum_{n=0}^{\infty} \frac{f_n t^n}{n!}$$

and

$$G(t) = \sum_{n=0}^{\infty} \frac{g_n t^n}{n!}$$

where g_n and f_n are related as in Corollary 3.5.6, then we can determine the relationship between these two generating functions as follows.

$$G(t) = f_0 + \sum_{n=1}^{\infty}\sum_{k=1}^{n} S(n,k) f_k \frac{t^n}{n!}.$$

Interchanging summation, we deduce

$$G(t) = f_0 + \sum_{k=1}^{\infty} f_k \frac{(e^t-1)^k}{k!} = F(e^t - 1).$$

which implies the following result.

COROLLARY 3.5.7. *If f_n and g_n are related as in Corollary 3.5.6, then*

$$G(t) = F(e^t - 1).$$

This allows us to deduce the generating function for Stirling numbers of the first kind. Let $g_k = 1$ and $g_n = 0$ for $n \neq k$. Then, $f_n = s(n,k)$. By Corollary 3.5.7, we get

$$\frac{t^k}{k!} = F(e^t - 1).$$

Putting $x = e^t - 1$ gives

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

3.6. Exercises

EXERCISE 3.6.1. There are 13 students taking math, 17 students taking physics and 18 students taking chemistry. We know there are 5 students taking both math and physics, 6 students taking physics and chemistry and 4 students taking chemistry and math. Only 2 students out of the total of 50 students are taking math, physics and chemistry. How many students are not taking any courses at all ?

EXERCISE 3.6.2. The **greatest common divisor** $\gcd(a,b)$ of two natural number a and b is the largest natural number that divides both a and b. If n is a natural number, denote by $\phi(n)$ the number of integers k with $1 \leq k \leq n$ and $\gcd(n,k) = 1$. Show that if p is a prime, then $\phi(p) = p-1$ and that if $p \neq q$ are two primes, then $\phi(pq) = (p-1)(q-1)$.

EXERCISE 3.6.3. If $n = p_1^{a_1} \dots p_r^{a_r}$ with p_i distinct primes, then show that

$$\phi(n) = n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$

EXERCISE 3.6.4. How many integers less than n are not divisible by any of $2, 3$ and 5 ?

EXERCISE 3.6.5. How many 7 digit phone numbers contain at least 3 odd digits ?

EXERCISE 3.6.6. If $A_1, A_2, \dots, A_n$ are finite sets, show that

$$\sum_{i=1}^{n} |A_i| - \sum_{i\neq j} |A_i \cap A_j| \leq | \cup_{i=1}^{n} A_i| \leq \sum_{i=1}^{n} |A_i|.$$

When does equality happen ?

EXERCISE 3.6.7. If n and r are non-negative integers with $0 \leq r \leq n$, denote by $f(n,r)$ the number of permutations of S_n with exactly r fixed points. Show that

$$\lim_{n\to\infty} \frac{f(n,r)}{n!} = \frac{1}{er!}.$$

EXERCISE 3.6.8. Show that

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^{n+1} = \binom{n+1}{2} n!.$$

EXERCISE 3.6.9. Let $s(n,k)$ denote the Stirling numbers of the first kind. Show that

$$x(x+1)\dots(x+n-1) = \sum_{k=0}^{n} |s(n,k)| x^k.$$

EXERCISE 3.6.10. Using the previous identity, prove that the number of permutations with an even number of cycles (in their decomposition as a product of disjoint cycles) is equal to the number of permutations with an odd number of cycles.

EXERCISE 3.6.11. Let $S(n,k)$ denote the Stirling numbers of second kind. Show that

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

EXERCISE 3.6.12. Prove that

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

EXERCISE 3.6.13. Show that

$$|s(n,1)| = (n-1)!.$$

Give two proofs.

EXERCISE 3.6.14. Prove that $S(n,1) = S(n,n) = 1$ and $S(n,2) = 2^{n-1} - 1$.

EXERCISE 3.6.15. Show that $S(n,n-1) = \binom{n}{2}$.

EXERCISE 3.6.16. Let $s(n)$ be the number of involutions in the symmetric group S_n. Show that

$$f(t) := \sum_{n\geq 0} \frac{s(n)t^n}{n!} = e^{t+\frac{t^2}{2}}.$$

EXERCISE 3.6.17. The Bernoulli numbers b_n are defined by the recurrence relation

$$\sum_{k=0}^{n} \binom{n+1}{k} b_k = 0$$

for $n \geq 1$ and $b_0 = 1$. Prove that

$$g(t) := \sum_{n\geq 0} \frac{b_n t^n}{n!} = \frac{t}{e^t - 1}.$$

These numbers were first studied by Jakob Bernoulli (1654-1705) in 1713.

EXERCISE 3.6.18. Show that $g(t) + \frac{t}{2}$ is an even function of t, where $g(t)$ is defined in the previous exercise.

EXERCISE 3.6.19. Show that $b_n = 0$ for each odd number $n \geq 3$.

EXERCISE 3.6.20. Let $(f_n)_{n\geq 0}$ and $(g_n)_{n\geq 0}$ be sequences, with exponential generating functions $F(X)$ and $G(X)$. Show that the following the statements

$$g_n = \sum_{k=0}^{n} \binom{n}{k} f_k$$

and

$$G(X) = e^X f(X)$$

are equivalent.

CHAPTER 4

Matrices and Graphs

4.1. Adjacency and Incidence Matrices

Given a graph X, we associate two matrices to encode its information. The first is the **adjacency matrix** A or sometimes denoted A_X or $A(X)$. If n is the number of vertices of X, then A is an $n \times n$ matrix whose (i, j)-th entry is the number of edges between i and j. In case X is a simple graph, this is simply a $(0, 1)$ matrix whose i, j-th entry is 1 or 0 according as i is joined to j.

THEOREM 4.1.1. *The (i, j)-th entry of A^m is the number of walks of length m from i to j.*

PROOF. We prove this by induction. For $m = 1$, this is clear from the definition. Suppose we have proved it for A^j for $j \leq m - 1$. Write $A^r = (a_{i,j}^{(r)})$. Since $A^m = A^{m-1} \cdot A$, we have

$$a_{ij}^{(m)} = \sum_{k=1}^{n} a_{ik}^{(m-1)} a_{kj}.$$

Clearly, the number of paths from i to j of length m is

$$\sum_{k=1}^{n} (\#\text{of paths from } i \text{ to } k \text{ of length } m-1)\, a_{kj}.$$

By induction, the number of paths from i to k of length $m - 1$ is $a_{ik}^{(m-1)}$ which proves the theorem. ∎

There is another matrix M called the **incidence matrix** of the graph. If X has n vertices and e edges, then M is a an $n \times e$ matrix defined as follows. The (i, j)-th entry is 1 if the vertex v_i is incident to the edge e_j, and 0 otherwise. The relationship between this matrix and the adjacency matrix is given by the easily verified equation

$$MM^t = D + A$$

where D is the diagonal matrix consisting of the vertex degrees.

4.2. Graph Isomorphism

An **isomorphism** between two graphs X and Y is a bijection f between the vertex set of X and the vertex set of Y such that uv is an edge of X if and only if $f(u)f(v)$ is an edge of Y. The reader is invited to show that the graphs in Figure 4.1 are isomorphic. We will usually study isomorphism in the context of simple graphs. A moment's reflection shows that applying a permutation to both the rows and columns of the adjacency matrix of a graph X has the effect of reordering the vertices of X. A **permutation matrix** is a square 0, 1 matrix which has precisely one entry 1 in each row and each column and 0's elsewhere.

THEOREM 4.2.1. *The graphs X and Y are isomorphic if and only if there is a permutation matrix P such that*

$$PA_XP^{-1} = A_Y.$$

We begin by reviewing some elementary facts from linear algebra about matrices and their characteristic polynomials. Given a square matrix A, its **characteristic polynomial** is $\det(\lambda I - A)$. The roots of this polynomial are called **eigenvalues** of A. If λ is an eigenvalue and v is an eigenvector so that $Av = \lambda v$, then v is called an **eigenvector** corresponding to λ. Thus, for two graphs to be isomorphic, it is necessary that their adjacency matrices have the same eigenvalues. However, this is not a sufficient condition for isomorphism. Consider the graph obtained from C_4 by adding an isolated vertex. This graph has the same eigenvalues as $K_{1,4}$, but it is obviously not isomorphic to $K_{1,4}$. See also Exercise 4.5.15 and Exercise 4.5.16.

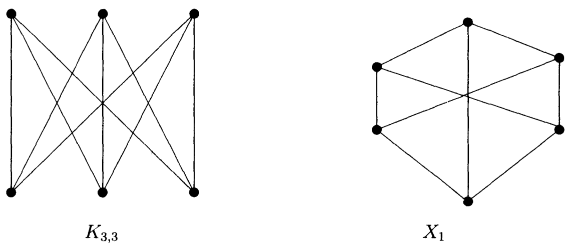


FIGURE 4.1

EXAMPLE 4.2.2. Let us compute the characteristic polynomial of the n by n matrix J whose i,j-th entry is 1 for all $1 \leq i, j \leq n$. Clearly, it is a singular matrix (that is, its determinant is zero because the rows are linearly dependent). Any eigenvector $v = (x_1, ..., x_n)$ with eigenvalue λ satisfies $Jv = \lambda v$ so that

$$x_1 + \cdots + x_n = \lambda x_i,$$

for all $1 \leq i \leq n$. Clearly, $\lambda = n$ is an eigenvalue and $v = (1, 1, ..., 1)$ is a corresponding eigenvector. On the other hand, the subspace of vectors $v = (x_1, ..., x_n)$ satisfying the equation

$$x_1 + \cdots + x_n = 0$$

has dimension $n - 1$ and these vectors correspond to eigenvalue zero. Thus, the characteristic polynomial is $(\lambda - n)\lambda^{n-1}$.

EXAMPLE 4.2.3. Let us determine the characteristic polynomial of the complete graph K_n. The adjacency matrix of K_n is $J - I$ with J as in Example 4.2.2 and I is the identity matrix of order n. Now let us recall that if A has eigenvalue μ then $\mu + c$ is an eigenvalue of $A + cI$ because $\det(\lambda I - (A + cI)) = \det((\lambda - c)I - A)$. Thus, the eigenvalues of $J - I$ are $n - 1$ and -1 with multiplicity 1 and $n - 1$ respectively. Therefore, the characteristic polynomial of the complete graph on n vertices is $[\lambda - (n - 1)](\lambda + 1)^{n-1}$.

EXAMPLE 4.2.4. Let us determine the characteristic polynomial of the bipartite graph $K_{r,s}$. Since the adjacency matrix has form

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

it has rank 2. Recall now that the **rank** of a square matrix is equal to the number of non-zero eigenvalues counted with multiplicity. As our matrix has trace zero and this is also equal to the sum of the eigenvalues, we deduce that $A_{m,n}$ has only two non-zero eigenvalues λ_1, λ_2 with $\lambda_1 = -\lambda_2 = b$ (say). Moreover, each of these has multiplicity 1. Thus, the characteristic polynomial is (with $n = r + s$)

$$\lambda^{n-2}(\lambda^2 - b^2).$$

We can actually determine b more precisely. If we look at the definition of the characteristic polynomial as $\det(\lambda I - A_{r,s})$, we see that the coefficient of λ^{n-2} can be arrived at as follows. From the determinant expression, we must choose $(n - 2)$ diagonal entries and the other two entries must come from non-zero entries in order to contribute to the coefficient. This can also be seen from the formula for the determinant. The permutations that contribute must necessarily fix $(n-2)$ letters and thus correspond to transpositions. The remaining positions contribute $-a_{i,j}$ and $-a_{j,i}$ for some i, j. Since the graph is bipartite, there are rs non-zero contributions of this form. This means b^2 must be rs. Thus, the characteristic polynomial is

$$\lambda^{n-2}(\lambda - \sqrt{rs})(\lambda + \sqrt{rs}).$$

This can also be deduced in another (simpler) way. As we observed, the number of closed walks of length 2 is equal to the trace of the square of the adjacency matrix. In our bipartite case, this is clearly $2rs$, which must necessarily equal the sum of the squares of the eigenvalues, which is $2b^2$. Thus, $b^2 = rs$.

4.3. Bipartite Graphs and Matrices

The eigenvalues of bipartite graphs have the following interesting property.

THEOREM 4.3.1. *If X is bipartite, and λ is an eigenvalue with multiplicity m, then $-\lambda$ is also an eigenvalue of multiplicity m.*

PROOF. Since X is bipartite, we may arrange our rows and columns of $A = A_X$ according to the partite sets so that A has the following form

$$A = \begin{pmatrix} O & B \\ B^t & O \end{pmatrix}$$

where B is a 0, 1 matrix. If λ is an eigenvalue with eigenvector

$$v = \begin{pmatrix} x \\ y \end{pmatrix},$$

partitioned according to the partite sets. We have

$$\lambda v = Av = \begin{pmatrix} By \\ B^t x \end{pmatrix} = \lambda \begin{pmatrix} x \\ y \end{pmatrix}$$

so that $By = \lambda x$ and $B^t x = \lambda y$. Let

$$v' = \begin{pmatrix} x \\ -y \end{pmatrix}.$$

Then

$$Av' = \begin{pmatrix} -By \\ B^t x \end{pmatrix} = \begin{pmatrix} -\lambda x \\ \lambda y \end{pmatrix} = -\lambda \begin{pmatrix} x \\ -y \end{pmatrix} = -\lambda v'.$$

Thus, v' is an eigenvector with eigenvalue $-\lambda$. Also, m independent eigenvectors corresponding to λ give m independent eigenvectors corresponding to $-\lambda$. This completes the proof. ∎

We can now characterize bipartite graphs by the shape of the characteristic polynomial.

THEOREM 4.3.2. *The following statements are equivalent.*

(1) *X is bipartite;*
(2) *The eigenvalues of X occur in pairs λ_i, λ_j such that $\lambda_i = -\lambda_j$;*
(3) *The characteristic polynomial of X is a polynomial in λ^2;*
(4) *for any positive integer t, $\sum_{i=1}^{n} \lambda_i^{2t-1} = 0$ where the sum is over the eigenvalues (with multiplicity) of A_X.*

PROOF. The fact that (1) implies (2) was done in the previous theorem. The equivalence of (2) and (3) is clear since $(\lambda - \lambda_i)(\lambda - \lambda_j) = (\lambda^2 - a)$ with $a = \lambda_i^2$. It is also clear that (2) implies (4) since the eigenvalues occur in pairs with opposite signs and so they cancel each other in the sum in (4). To see that (4) implies (1), we recall that the (i, j)-th entry of A_X^{2t-1} counts the number of paths of length $2t - 1$ from vertex i to vertex j. In particular, the diagonal entries count the number of closed walks of this length. But the sum of the diagonal entries is the total number of closed paths of this length and (4) says this sum is zero. Thus, X has no closed paths of odd length. By Theorem 1.5.1, X is bipartite. ∎

4.4. Diameter and Eigenvalues

Recall from linear algebra the notion of a **minimal polynomial** of a matrix. By the Cayley-Hamilton theorem (or by the fact that $1, A, A^2, ..., A^{n^2}$ are linearly dependent via dimension considerations) we deduce that A satisfies some monic polynomial equation. Among all, there is one of minimal degree which is necessarily unique (by the division algorithm). The degree of this minimal polynomial is equal to the number of distinct eigenvalues of A.

Indeed, this is easy to see in the case of real symmetric matrices that we are dealing with. By the **spectral theorem** all the eigenvalues of a real symmetric matrix are real and there is a basis of eigenvectors. If we let

$$g(\lambda) = \prod_{i=1}^{r} (\lambda - \lambda_i)$$

where the λ_i range over the distinct eigenvalues of A, then $g(A) = 0$. To see this, it suffices to see how $g(A)$ operates on set of basis vectors.

We take the basis of eigenvectors and see that this is immediate (as the various factors commute) and we may write

$$g(A) = \prod_{i=1}^{r}(A - \lambda_i I).$$

If there were a polynomial h of smaller degree with $h(A) = 0$, we see that it must divide the polynomial $g(\lambda)$ and must consist of a product of terms of the form $\lambda - \lambda_i$ for some proper subset of subscripts. But then, the eigenvector v_j corresponding to an eigenvalue λ_j that is omitted in the product will not be annihilated by $h(A)$.

Recall that the distance $d(u, v)$ between vertices u, v equals the shortest length of a path connecting u and v. Now we define the **diameter** of a graph X as

$$\operatorname{diam}(X) = \max_{u,v \in V(X)} d(u, v)$$

where the maximum is over all possible pairs of vertices.

THEOREM 4.4.1. *If* $\operatorname{diam}(X) < \infty$, *then the diameter is strictly less than the number of distinct eigenvalues of* X.

PROOF. Let A be the adjacency matrix of X. Then A satisfies a polynomial of degree r if and only if some non-zero linear combination of $A^0, A^1, ..., A^r$ is zero. Since the number of distinct eigenvalues is equal to the degree of the minimal polynomial, we need only show that $A^0, A^1, ..., A^k$ are linearly independent when $k \leq \operatorname{diam}(X)$. Let $k = \operatorname{diam}(X)$ and choose v_i, v_j so that the distance between v_i and v_j equals k. By counting walks from v_i to v_j we see that the i, j-th entry of A^k is not zero. But the (i, j)-th entry of A^t for $t < k$ is zero because $d(v_i, v_j) = k$. Therefore, A^k is not a linear combination of A^t for $t < k$. Hence, the degree of the minimal polynomial is strictly greater than $\operatorname{diam}(X)$. ∎

The examples of previous section show that this result is sharp. For instance, in the case of the complete graph K_n, the diameter is equal to 1 and the number of distinct eigenvalues is 2. In the case of the bipartite graph $K_{r,s}$, we have diameter 2 and the number of distinct eigenvalues is 3. There are many other classes of graphs X whose number of distinct eigenvalues equals $1 + \operatorname{diam}(X)$.

4.5. Exercises

EXERCISE 4.5.1. Determine the eigenvalues of P_4 and C_5.

EXERCISE 4.5.2. Show that a graph X with n vertices is connected if and only if $(A+I_n)^{n-1}$ has no zero entries, where A is the adjacency matrix of X.

EXERCISE 4.5.3. For a simple graph X with e edges, t_3 triangles and adjacency matrix A, show that

$$\operatorname{tr}(A) = 0, \quad \operatorname{tr}(A^2) = 2e, \quad \operatorname{tr}(A^3) = 6t_3.$$

EXERCISE 4.5.4. If X is a bipartite graph with e edges and λ is an eigenvalue of X, show that

$$|\lambda| \leq \sqrt{e}.$$

EXERCISE 4.5.5. Let X be a simple graph with n vertices and e edges. If λ is an eigenvalue of the adjacency matrix A of X, show that

$$|\lambda| \leq \sqrt{\frac{2e(n-1)}{n}}.$$

EXERCISE 4.5.6. If two non-adjacent vertices of a graph X are adjacent to the same set of vertices, show that its adjacency matrix has eigenvalue 0.

EXERCISE 4.5.7. The **eccentricity** of a vertex u in a graph X is the maximum of $d(u,v)$ as v ranges over the vertices of X. The minimum of all the possible eccentricities is called the **radius**, denoted $\mathbf{rad}(X)$, of the graph X. Show that if X is connected, then

$$\operatorname{rad}(X) \leq \operatorname{diam}(X) \leq 2\operatorname{rad}(X).$$

EXERCISE 4.5.8. Let R be a commutative ring and $A_1, ..., A_k$ be $n \times n$ matrices. We define a **generalized commutator** as

$$[A_1, ..., A_k] = \sum_{\sigma \in S_k} (\operatorname{sgn} \sigma) A_{\sigma(1)} ... A_{\sigma(k)}.$$

When $k = 2n$, show that

$$[A_1, ..., A_k] = 0.$$

This is a classical theorem of Shimson Avraham Amitsur (1921-1994) that can be proved using Euler circuits in digraphs.

EXERCISE 4.5.9. Show that the graphs in Figure 4.1 are isomorphic by presenting an explicit isomorphism.

EXERCISE 4.5.10. Let M be the incidence matrix of a simple graph X. Prove that

$$MM^t = D + A$$

where A is the adjacency matrix of X and D is a diagonal matrix consisting of the degrees of the vertices of X.

EXERCISE 4.5.11. In a simple graph X, we choose an **orientation** by assigning a direction to each edge. The modified incidence matrix N is defined as follows. Its rows are parameterized by the vertices v_i and the columns by the edges e_j, as before. The i, j-th entry of N is $+1$ if v_i is the tail of e_j, -1 if it is the head and zero otherwise. Prove that

$$NN^t = D - A_X.$$

EXERCISE 4.5.12. The **Laplacian matrix** of a graph X is $D - A$. Show that the smallest eigenvalue of the Laplacian is 0. If X is connected, then 0 has multiplicity 1 for the Laplacian.

EXERCISE 4.5.13. If X is k-regular, then λ is an eigenvalue of the its adjacency matrix if and only if $k - \lambda$ is an eigenvalue of its Laplacian matrix.

EXERCISE 4.5.14. Prove that $\lambda^4 + \lambda^3 + 2\lambda^2 + \lambda + 1$ cannot be the characteristic polynomial of an adjacency matrix of any graph.

EXERCISE 4.5.15. Determine the characteristic polynomial of the cycle C_4.

EXERCISE 4.5.16. Let Y denote the graph obtained from a graph X by adding an isolated vertex. Show that $P_Y(\lambda) = \lambda P_X(\lambda)$. If $X = C_4$, compare P_Y with $P_{K_{1,4}}$.

EXERCISE 4.5.17. The **odd girth** of a graph X is the shortest length of an odd cycle. If X and Y have the same eigenvalues, then they have the same odd girth.

EXERCISE 4.5.18. The **line graph** $L(X)$ (see also Chapter 11)of a graph X the edges of X as vertices, two edges e and f of X being adjacent in $L(X)$ if they have common endpoint in X. Show that if N is the incidence matrix of X, then the adjacency matrix of $L(X)$ is $N^tN - 2I_m$, where m is the number of edges of X.

EXERCISE 4.5.19. If X is k-regular and λ is an eigenvalue of the adjacency matrix of X, then $k + \lambda - 2$ is an eigenvalue of the line graph of X.

EXERCISE 4.5.20. Any eigenvalue of a line graph is greater than or equal to -2.

CHAPTER 5

Trees

5.1. Forests, Trees and Leaves

A **forest** is an acyclic graph (that is, a graph with no cycles). The connected components of a forest are called **trees**. Therefore, a **tree** is a connected acyclic graph. In particular, any tree is a bipartite graph. A **leaf** is a vertex of degree one. In the figure below, we have a tree with seven leaves.

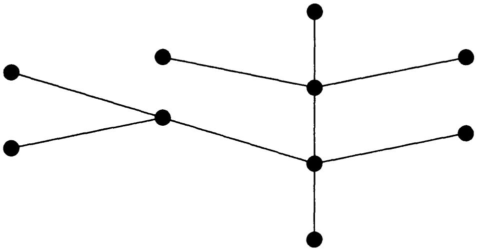


FIGURE 5.1

Given a graph X and a vertex v, we denote by $X - v$ the graph obtained by deleting the vertex v and any edges incident with v. We begin by proving the following:

LEMMA 5.1.1. *Every tree with $n \geq 2$ vertices has at least two leaves. Deleting a leaf from an n-vertex tree gives a tree with $n - 1$ vertices.*

PROOF. A connected graph with at least two vertices has at least one edge. Let us consider a maximal path in the graph joining u and v (say). Every neighbour of u or v must be member of the path for otherwise, this would violate maximality of the path. If u or v had two neighbours, we would get cycle. Thus, u and v must be leaves. Now let v be a leaf. We will show that $X' = X - v$ is a tree. Clearly, $X - v$ is acyclic because deleting a vertex is not going to increase the number of cycles. We must show it is connected. Given two vertices in X', let P be a path joining them in X which exists because X is connected.

This path cannot involve v for otherwise v will have degree at least two. Therefore, X' is connected. ∎

We now give the following characterization of trees.

THEOREM 5.1.2. *Let X be a graph on n vertices. The following are equivalent.*

(1) *X is a tree.*
(2) *X is connected and has $n-1$ edges.*
(3) *X has $n-1$ edges and no cycles.*
(4) *For any $u, v \in V(X)$, there is a unique path joining them.*

PROOF. To prove (1) implies (2), we use induction. By the previous lemma, let v be a leaf and consider the tree $X' = X - v$ with $n-1$ vertices. By induction, it has $n-2$ edges and together with the edge joining X' to v, we get a total of $n-1$ edges. The same argument shows that (1) implies (3). To prove that (2) implies (3), let us suppose X has a cycle. We may delete edges from any cycle until we get a graph X' which is acyclic and has n vertices. But then, X' is a tree and so has $n-1$ edges. Thus, no edges were deleted from X and X has no cycles. We can also show that (3) implies (1) as follows. Let $X_1, ..., X_k$ be the connected components of X. Since every vertex appears in one component, we have that

$$\sum_{i=1}^{k} |V(X_i)| = n.$$

As X has no cycles, each component is a tree so that $|E(X_i)| = |V(X_i)| - 1$ for each i. Thus, the number of edges of X is $n-k$. But as X has $n-1$ edges, $k=1$ and so X has only one connected component. Therefore, X is a tree. Finally, we must show the equivalence of (1) and (4). Clearly, (1) implies (4) for otherwise X would have a cycle. Conversely, if any two points have a unique path joining them, there are no cycles in the graph and moreover, X is connected. This completes the proof. ∎

5.2. Counting Labeled Trees

Arthur Cayley (1821-1895) spent 14 years as a lawyer during which he published 250 mathematical papers. In total, he published over 900 papers and notes covering almost every aspect of mathematics.

A classical result of Cayley states that the number of labeled trees on n vertices is n^{n-2}. Despite its simplicity, it is remarkable that there is no simple proof of this formula. We apply an inductive argument to deduce it.

Let $G(n, m)$ be the number of connected graphs on n labeled vertices and m edges. Let $F(n, m)$ denote the number of such graphs that have no vertices of degree 1. Let A be the set of connected graphs on n labeled vertices having m edges. Let A_i be the subset of A of connected graphs with vertex v_i of degree 1. Thus,

$$F(n, m) = |A \backslash \cup_i A_i|.$$

Let us observe that $|A_i| = G(n-1, m-1)(n-1)$ and generally

$$|A_I| = G(n - |I|, m - |I|)(n - |I|)^{|I|}.$$

Then, by the inclusion-exclusion principle, we have

$$F(n, m) = \sum_{I \subseteq V} (-1)^{|I|} G(n - |I|, m - |I|)(n - |I|)^{|I|}.$$

By collecting subsets of the same cardinality in the sum on the right, we obtain the following result.

THEOREM 5.2.1.

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

Theorem 5.1.2 tells us that any connected graph on n vertices and $n-1$ edges is necessarily a tree. Thus, $G(n, n-1)$ is the number of labeled trees on n vertices. Since every tree has a leaf, we have that $F(n, n-1) = 0$.

THEOREM 5.2.2. *If T_n denotes the number of labeled trees on n vertices, then*

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

Now we are ready to prove Cayley's formula.

THEOREM 5.2.3 (Cayley, 1889). *For $n \geq 2$,*

$$T_n = n^{n-2}.$$

PROOF. We prove the theorem by induction on n. For $n = 2$, the formula is clear. By induction, $T_{n-i} = (n-i)^{n-i-2}$ for $i \geq 1$. Using Theorem 5.2.2, we obtain that

$$T_n + \sum_{i=1}^{n} (-1)^i \binom{n}{i} (n-i)^{n-2} = 0.$$

By Theorem 3.3.1, the latter sum is $-n^{n-2}$ from which we deduce the theorem. ■

5.3. Spanning Subgraphs

A **spanning subgraph** of a graph X is a subgraph with vertex set $V(X)$. A **spanning tree** is a spanning subgraph which is a tree. Given a graph X, we let $\tau(X)$ denote the number of spanning trees of X.

In a graph X, the graph obtained by deleting an edge e is denoted $X-e$. In this case, let us note that the vertices of e still belong to $X-e$. It may happen that this process increases the number of components of the graph, in which case we call e a **cut edge** or a **bridge**. The **contraction** of X by an edge e with endpoints u and v is the graph obtained by replacing u and v by a single vertex whose incident edges are the edges other than e that were incident to u or v. The resulting graph, denoted X/e has one less edge than X.

THEOREM 5.3.1. *If $\tau(X)$ is the number of spanning trees in X and $e \in E(X)$ is not a loop, then*

$$\tau(X) = \tau(X-e) + \tau(X/e).$$

PROOF. The spanning trees of X that omit e are counted by $\tau(X-e)$. The spanning trees that contain e are in one-to-one correspondence with the spanning trees of X/e. To see this, note that when we contract e in a spanning tree that contains e, we obtain a spanning tree of X/e because the resulting subgraph of X/e is spanning, connected and has the right number of edges. Since the other edges maintain their identity under contraction, no two trees are mapped to the same spanning tree of X/e by this operation. Also, each spanning tree of X arises in this way and so the function is a bijection. ∎

Recall that the Laplacian of a graph X is the matrix

$$L = D - A,$$

where A is the adjacency matrix of X and D is the diagonal matrix whose (i,i)-th entry equals the degree of vertex i.

Gustav Robert Kirchhoff (1824-1887) is perhaps best known for the Kirchhoff's laws in electrical circuits. These were announced in 1845 and extended previous work of Georg Simon Ohm (1789-1854).

A celebrated theorem of Kirchhoff from 1847 gives the number $\tau(X)$ via a determinant formula. This results is also known as the Matrix-Tree Theorem.

THEOREM 5.3.2 (Matrix-Tree Theorem). *For any loopless graph X, the number of spanning trees $\tau(X)$ equals $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the i-th row and j-th column of the Laplacian matrix L.*

We will not prove this theorem since it involves detailed linear algebra. We pause to remark that Cayley's theorem can be deduced easily from this more general result as follows. The number of trees on a vertex set $v_1, ..., v_n$ is the number spanning trees of the complete graph K_n. The adjacency matrix of K_n is $J - I$ with notation of the previous chapter. Thus, the Laplacian of the complete graph is

$$(n-1)I - (J - I)$$

and any cofactor is the determinant of $(n-1)I_{n-1} - (J_{n-1} - I_{n-1})$ where we have written the subscript to indicate the size of our matrix. By Example 4.2.3 in Chapter 4, we see that this determinant is the characteristic polynomial of the graph K_{n-1} evaluated at $\lambda = n - 1$ which is

$$[\lambda - (n-2)](\lambda + 1)^{n-2} = n^{n-2}$$

and thus, we recover Cayley's formula.

Theorem 5.3.2 can be stated in more succinct terms. Recall that the **classical adjoint** of a matrix A, denoted $\mathrm{adj}(A)$, is the transpose of the matrix whose i,j-th entry is $(-1)^{i+j}$ times the determinant of the matrix obtained from A by deleting the i-th row and j-th column. If J denotes (as before) the matrix all of whose entries are equal to 1, then Theorem 5.3.2 is equivalent to the assertion that

$$\mathrm{adj}(L) = \tau(X)J.$$

For example, Cayley's formula can be restated as

$$\mathrm{adj}(nI - J) = n^{n-2}J.$$

It is not hard to see that

$$J^2 = nJ, \qquad JL = LJ = 0.$$

These equations imply that $(nI - J)(J + L) = nJ - J^2 + nL - JL = nL$. Thus,

$$\mathrm{adj}(J + L)\mathrm{adj}(nI - J) = \mathrm{adj}((nI - J)(J + L)) = \mathrm{adj}(nL).$$

Cayley's formula implies $\mathrm{adj}(nI - J) = n^{n-2}J$. Also, $\mathrm{adj}(nL) = n^{n-1}\mathrm{adj}(L$ because in the adjoint the entries are formed by taking $(n-1) \times (n-1)$ determinants. We therefore deduce that

$$[\mathrm{adj}(J + L)]J = n\mathrm{adj}(L).$$

By Theorem 5.3.2,

$$\mathrm{adj}(L) = \tau(X)J$$

so we obtain

$$[\mathrm{adj}(J + L)]J = n\tau(X)J.$$

Multiplying both sides of the equation by $(J+L)$ on the left gives

$$[\det(J+L)]J = n\tau(X)(J+L)J.$$

Because $(J+L)J = J^2 + LJ = nJ$, we therefore deduce the next result.

THEOREM 5.3.3. *Let X be a simple graph whose Laplacian matrix is L. The number of spanning trees in X is given by*

$$\tau(X) = n^{-2}\det(J+L).$$

In the case X is a connected k-regular graph, we can derive a nicer formula. Recall that the adjacency matrix of X has eigenvalue k. Since X is connected, the multiplicity of this eigenvalue is 1. To see this, let $v = (x_1, ..., x_n)$ be an eigenvector corresponding to the eigenvalue k. The equation

$$A_X v = kv$$

implies that

$$\sum_{j=1}^{n} a_{ij}x_j = kx_i.$$

Without any loss of generality suppose that $x_1 > 0$ and that $x_1 = \max_{1\le i\le n} x_i$. If for some i, $x_i < x_1$, then

$$kx_1 = \sum_{j=1}^{n} a_{1j}x_j < kx_1$$

which is a contradiction. Thus, all the x_i are equal and so every eigenvector must be a multiple of $(1, 1, ..., 1)$. If X is not connected, the multiplicity of the eigenvalue is easily seen to be the number of connected components. By Theorem 5.3.3, we must compute the determinant

$$\det(J + kI - A)$$

which is just the characteristic polynomial of $A - J$ evaluated at k. The eigenvalues of $A - J$ are easily determined. Let $v_1, ..., v_n$ be a orthogonal basis of eigenvectors of A, with v_1 a multiple of $(1, 1, ..., 1)$ corresponding to the eigenvalue k. Then, for $2 \le i \le n$,

$$(A - J)v_i = \lambda_i v_i$$

as $Jv_i = 0$. This is true because v_1 is orthogonal to the v_i. Also,

$$(A - J)v_1 = (k - n)v_1$$

so this determines all the eigenvalues of $A - J$ and their multiplicity. The characteristic polynomial of $A - J$ is

$$(\lambda - (k - n))\prod_{i=2}^{n}(\lambda - \lambda_i).$$

Putting this together with Theorem 5.3.3 gives

THEOREM 5.3.4. *If X is a connected k-regular graph, then the number of spanning trees of X is given by*

$$\frac{\prod_{i=2}^{n}(k-\lambda_i)}{n},$$

where the product is over the eigenvalues unequal to k.

This theorem can, for instance, be used to compute the number of spanning trees of the bipartite graph $K_{n,n}$ (see Exercise 5.5.11).

5.4. Minimum Spanning Trees and Kruskal's Algorithm

In many contexts in which graph theory is applied, we consider **weighted graphs**. That is, we suppose we have a graph X together with a "weight" function $w : E(X) \rightarrow \mathbb{R}_+$ that assigns to each edge a positive weight. For example, our graph could be a network of cities, and the weight function could be the cost of putting a communication network between the two cities. We will be interested in finding a connected subgraph so that its total "cost", i.e., the sum of the weights of the edges in the subgraph, is minimal. Clearly, if there is a cycle, we can delete a 'costly' edge from the cycle and so, what we are searching is a spanning tree whose 'cost' is minimal. We call such a tree a **minimum spanning tree**. Of course, it need not be unique.

There is a fundamental algorithm, called **Kruskal's algorithm** which determines a minimum spanning tree of any connected graph in a 'greedy' fashion. It can be described as follows. Choose an edge e_1 of X with $w(e_1)$ minimal. Eliminate it from the list. Inductively choose $e_2, ..., e_{n-1}$ in the same manner subject to the constraint that the newly chosen edge does not form a cycle with previously chosen edges. The required spanning tree is the subgraph with these edges. Before we prove that this **greedy algorithm** actually works, we illustrate this with an example.

Consider the following weighted adjacency matrix giving the cost of building a road from one city to another. An infinite entry indicates there is a mountain in the way and a road cannot be built. The question is to determine the least cost of making all the cities reachable from each other. This amounts to finding a spanning tree with minimum “length”.

$$\begin{array}{c|ccccc} & A & B & C & D & E \\ A & 0 & 3 & 5 & 11 & 9 \\ B & 3 & 0 & 3 & 9 & 8 \\ C & 5 & 3 & 0 & \infty & 10 \\ D & 11 & 9 & \infty & 0 & 7 \\ E & 9 & 8 & 10 & 7 & 0 \end{array}.$$

The algorithm proceeds first by finding an edge of minimum weight, AB say. It then deletes this edge. In the next step, the algorithm finds the next smallest entry, BC say. The algorithm continues in this way and whenever an edge is chosen which produces a cycle, the algorithm does not select it. Thus, in the example below, AC is the next smallest entry but we would not choose it for it produces a cycle with AB and BC.

Thus the next entry to choose is DE followed by BE. Thus the minimum spanning tree is given in Figure 5.2. The minimum ‘cost’ is 21.

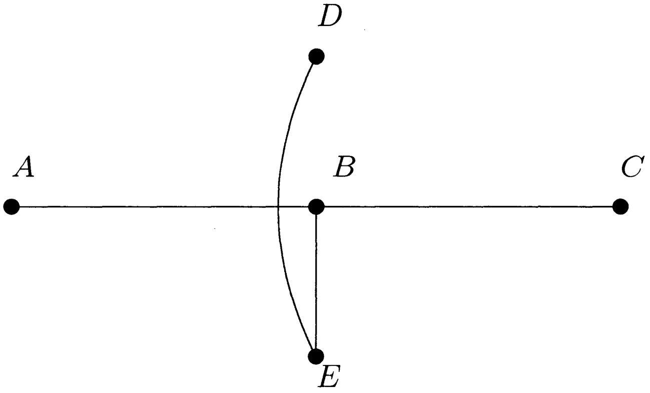


FIGURE 5.2. A minimum spanning tree of weight 21

THEOREM 5.4.1. *In a weighted connected graph X, Kruskal's algorithm constructs a minimum weight spanning tree.*

PROOF. Kruskal's algorithm produces a tree since it selects $n - 1$ edges which do not form cycles from a connected graph on n vertices. Let T be the tree produced by the algorithm and let T^* be a minimum weight spanning tree. If $T = T^*$, we are done. If not, let e be the first edge chosen for T that is not in T^*. Adding e to T^* creates a cycle C

since T^* is a spanning tree. Because T contains no cycles, we deduce that the cycle C must contain at least one edge e' not in $E(T)$. Now consider the subgraph $T^* + e - e'$ of X obtained from T^* by adding the edge e and removing the edge e'. The subgraph $T^* + e - e'$ is actually a spanning tree of X because it has $n - 1$ edges and contains no cycles. Since T^* contains e' and all the edges of T chosen before e, it means that both e' and e are available when the algorithm chooses e and therefore, $w(e) \leq w(e')$. Thus, $T^* + e - e'$ is a spanning tree with weight at most that of T^* (actually with the same weight as T^* since T^* is a minimum weight spanning tree) that agrees with T for a longer initial list of edges than T^* does. Repeating this process, we deduce that the tree created by Kruksal's algorithm has the same weight as T^* which finishes the proof. ■

5.5. Exercises

EXERCISE 5.5.1. Prove that in any tree, every edge is a bridge.

EXERCISE 5.5.2. Let X be a connected graph on n vertices. Show that X has exactly one cycle if and only if X has n edges. Prove that a graph with n vertices and e edges contains at least $e - n + 1$ cycles.

EXERCISE 5.5.3. Let $d_1, d_2, ..., d_n$ be positive integers. Show that there exists a tree on n vertices with vertex degrees $d_1, d_2, ..., d_n$ if and only if

$$\sum_{i=1}^{n} d_i = 2n - 2.$$

EXERCISE 5.5.4. The number of trees with degree sequence $d_1, \ldots, d_n$ with $d_1 + \cdots + d_n = 2n - 2$ is

$$\binom{n-2}{d_1 - 1, \ldots, d_n - 1} = \frac{(n-2)!}{(d_1 - 1)! \ldots (d_n - 1)!}.$$

EXERCISE 5.5.5. Show that if X is a tree on n labeled vertices, then each element of $\{X - e : e \in E(X)\}$ is a forest of two trees.

EXERCISE 5.5.6. Let T and T' be two distinct trees on the same set of n vertices. Show that for each edge $e \in E(T) \setminus E(T')$, there exists $e' \in E(T') \setminus E(T)$ such that $T \setminus \{e\} \cup \{e'\}$ is a tree.

EXERCISE 5.5.7. Let T_n be the number of trees on n labeled vertices. Prove that

$$2(n-1)T_n = \sum_{i=1}^{n-1} \binom{n}{i} T_i T_{n-i} i(n-i).$$

Exercise 5.5.8. Show that

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

Exercise 5.5.9. Let $G(r,s;m)$ be the number of connected bipartite graphs with partite sets of size r and s having m edges, and let $F(r,s;m)$ be the number of such graphs not containing any vertices of degree 1. Prove that

$$F(r,s;m) = \sum_{i,j} \binom{r}{i}\binom{s}{j}(-1)^{i+j}G(r-i,s-j;m-i-j)(s-j)^i(r-i)^j.$$

Exercise 5.5.10. Putting $m = r+s-1$ in the previous exercise, notice that $G(r,s;r+s-1)$ counts the number $T(r,s)$ (say) of spanning trees in the bipartite graph $K_{r,s}$. Deduce that

$$0 = \sum_{i,j} \genfrac{}{}{0pt}{}{r}{i} \binom{s}{j}(-1)^{i+j}T(r-i,s-j)(s-j)^i(r-i)^j$$

and that $T(r,s) = r^{s-1}s^{r-1}$.

Exercise 5.5.11. Show that the number of spanning trees of the bipartite graph $K_{n,n}$ is n^{2n-2}.

Exercise 5.5.12. The **Wiener index** of a graph X is $W(X) = \sum_{u,v \in V(X)} d(u,v)$, where $d(u,v)$ denotes the distance from u to v. Show that if X is a tree on n vertices, then

$$W(K_{1,n-1}) \le W(X) \le W(P_n).$$

Exercise 5.5.13. A communication link is desired between five universities in Canada: Queen's, Toronto, Waterloo, McGill and UBC. With obvious notation, the matrix below gives the cost (in thousands of dollars) of building such a connection between any two of the universities.

$$\begin{array}{c} \\ Q \\ T \\ W \\ M \\ U \end{array}
\begin{array}{c}
\begin{array}{ccccc} Q & T & W & M & U \end{array} \\
\begin{pmatrix}
- & 350 & 400 & 300 & 1200 \\
350 & - & 100 & 600 & 1300 \\
400 & 100 & - & 700 & 1400 \\
300 & 600 & 700 & - & 1600 \\
1200 & 1300 & 1400 & 1600 & -
\end{pmatrix}
\end{array}.$$

Use the greedy algorithm to determine the minimal cost so that all universities are connected.

EXERCISE 5.5.14. Every tree with maximum degree d has at least d leaves. Construct a tree with n vertices and maximum degree d for each $n > d \geq 2$.

EXERCISE 5.5.15. Let X be a graph on $n \geq 3$ vertices such that by deleting any vertex of X, we obtain a tree. Find X.

EXERCISE 5.5.16. Show that every connected graph X contains at least two vertices u with the property that $X \setminus \{u\}$ is connected. What are the trees on n vertices that contain exactly two vertices with this property ?

EXERCISE 5.5.17. Show that the graph obtained from K_n by removing one edge has $(n-2)n^{n-3}$ spanning trees.

EXERCISE 5.5.18. Let G_n be the graph obtained from the path P_n by adding one vertex adjacent to all the vertices of the path P_n. Determine the number of spanning trees of G_n.

EXERCISE 5.5.19. If G is a graph on n vertices having maximum degree $k \geq 2$ and diameter D, show that

$$n \leq \begin{cases} 2D+1, \text{ if } k=2 \\ \frac{k[(k-1)^D-1]}{k-2}+1, \text{ otherwise.} \end{cases}$$

EXERCISE 5.5.20. The **center** of a graph X is the subgraph induced by the vertices of minimum eccentricity. Show that the center of a tree is a vertex or an edge.

CHAPTER 6

Möbius Inversion and Graph Colouring

6.1. Posets and Möbius Functions

August Ferdinand Möbius (1790-1868) introduced the function which bears his name in 1831 and proved the well-known inversion formula. He was an assistant to Carl Friedrich Gauss (1777-1855) and made important contributions in geometry and topology. The Möbius function is very important tool not only in combinatorics, but also in algebra and number theory.

A **poset** is a pair $(P, \leq)$ with P a set and $\leq$ a relation on P (that is, a subset of $P \times P$) satisfying

(1) $x \leq x$ for all $x \in P$ (reflexive property);
(2) $x \leq y$ and $y \leq x$ implies $x = y$ (antisymmetric property);
(3) $x \leq y$, $y \leq z$ implies $x \leq z$ (transitive property).

We call $\leq$ a **partial order** on P. If $x \leq y$ and $x \neq y$, we sometimes write $x < y$. An **interval** $[x, z]$ consists of elements of $y \in P$ satisfying $x \leq y \leq z$. A poset P is called **locally finite** if every interval is finite. We say y **covers** x if $x \leq y$ and the interval $[x, y]$ consists of only two elements, namely, x and y. The **Hasse diagram** of $(P, \leq)$ is given by representing elements of P as points in the Euclidean plane, joining x and y by a line whenever y covers x and putting y "higher" than x on the plane.

Here are some examples of posets.

(1) If S is a finite set and we consider the collection $P(S)$ of all subsets of S, partially ordered by set inclusion, is a locally finite poset.
(2) If $\mathbb{N}$ is the set of natural numbers, we can definite a partial order by divisibility. Thus, $a \leq b$ if and only if $a|b$. It is easily verified that this is a partial order.
(3) If S is a finite set we consider $\Pi(S)$, the collection of partitions of S. Given two partitions α and β we say $\alpha \leq \beta$, if every block of α is contained in a block of β. We sometimes refer to α as a **refinement** of β.

(4) If $V(n, q)$ is the n-dimensional vector space over the finite field of order q, we can consider the poset of its subspaces partially ordered by inclusion.

(5) We can define a partial order on the elements of the symmetric groups S_n as follows. Let $\sigma \in S_n$. A permutation $\tau \in S_n$ is said to be a **reduction** of σ if $\tau(k) = \sigma(k)$ for all k except for $k = i, j$ where we have $\sigma(i) > \sigma(j)$ with $i < j$. We will write $\eta \leq \sigma$ if we can obtain η by a sequence of reductions from σ. This is called the **Bruhat order** on the symmetric group which makes S_n into a poset.

Given two posets $(P_1, \leq_1)$ and $(P_2, \leq_2)$, we can define their **direct product** as $(P_1 \times P_2, \leq)$, with partial order

$$(x_1, y_1) \leq (x_2, y_2) \quad \text{if} \quad x_1 \leq_1 x_2, \quad \text{and} \quad y_1 \leq_2 y_2.$$

If x and y are not comparable in P, we sometimes write $x \not\leq y$. Let F be a field and denote by $I(P)$ the set of intervals of P. The **incidence algebra** $I(P, F)$ is the F-algebra of functions

$$f : I(P) \to F$$

where we define multiplication (or convolution) by

$$(fg)(x, y) = \sum_{x \leq z \leq y} f(x, z) g(z, y).$$

Here we are writing $f(x, z)$ for $f([x, z])$. Given a locally finite poset P, its **Möbius function** μ is a map

$$\mu : P \times P \to \mathbf{Z}$$

defined recursively as follows. We set $\mu(x, y) = 0$ if $x \not\leq y$. Otherwise, we define it by the recursion

$$\sum_{x \leq z \leq y} \mu(x, z) = \delta(x, y)$$

where $\delta(x, y) = 1$ if $x = y$ and 0 otherwise. Observe that this equation can be written in "matrix form" as follows.

Define the **zeta function** of P by $\zeta(x, y) = 1$ if $x \leq y$ and zero otherwise. If for the moment, we assume P is finite, and we list our elements in some sequence $z_1, ..., z_n$ say. The matrix Z whose (i, j)-th entry is $\zeta(z_i, z_j)$ and the matrix M whose (i, j)-th entry is $\mu(z_i, z_j)$ satisfy $MZ = I$. This follows from the above recursion for μ. Thus, M is the inverse of the matrix Z. Since the inverse is both a left inverse as well as a right inverse, we deduce that $ZM = I$ which means

$$\sum_{x\le z\le y} \mu(z,y) = \delta(x,y).$$

THEOREM 6.1.1 (Möbius Inversion for Posets, Version 1). *Let* $(P,\le)$ *be a locally finite poset and suppose that* $f : P \to \mathbf{R}$ *is given by*

$$f(x) = \sum_{y\le x} g(y).$$

Then

$$g(x) = \sum_{y\le x} \mu(y,x)f(y),$$

and conversely.

PROOF. We have that

$$\sum_{y\le x}\mu(y,x)\sum_{z\le y} g(z) = \sum_{z\le x} g(z) \sum_{z\le y\le x} \mu(y,x) = g(x)$$

as required. The converse is left as an exercise. ∎

THEOREM 6.1.2 (Möbius Inversion for Posets, Version 2). *Let* $(P,\le)$ *be a locally finite poset and suppose that*

$$f(x) = \sum_{y\ge x} g(y).$$

Then,

$$g(x) = \sum_{y\ge x} \mu(x,y)f(y),$$

and conversely.

PROOF. As before,

$$\sum_{y\ge x}\mu(x,y)\sum_{z\ge y} g(z) = \sum_{z\ge x} g(z) \sum_{x\le y\le z} \mu(x,y) = g(x),$$

as required. The converse is left as an exercise. ∎

6.2. Lattices

Given a poset $(P,\le)$, we say z is a **lower bound** of x and y if $z\le x$ and $z \le y$. Any maximal element of the set of lower bounds for x and y is called a **greatest lower bound**. Such elements need not be unique as simple examples can show. The notions of **upper bound** and **least upper bound** are similarly defined. A **lattice** L is a pair $(L,\le)$ such that $(L,\le)$ is a poset and the greatest lower bound and least upper bound exist for any pair of elements x and y. We denote the greatest lower bound of x and y by $x \wedge y$ and least upper bound by $x \vee y$. For example, in the poset of the reals with the usual ordering, $x \wedge y$ is $\min(x, y)$ and $x \vee y$ is $\max(x, y)$. In the poset of the natural numbers partially ordered by divisibility, $x \wedge y$ is $\gcd(x, y)$, the greatest common divisor of x and y and $x \vee y$ is $\operatorname{lcm}(x, y)$, the least common multiple of x and y. In the poset of subsets of a set S partially ordered by set inclusion, $x \wedge y$ is $x \cap y$ and $x \vee y$ is $x \cup y$.

Two posets $(P_1, \leq_1)$ and $(P_2, \leq_2)$ are said to be **isomorphic** if there is a one-to-one and onto map $f : P_1 \to P_2$ such that $x \leq_1 y$ if and only if $f(x) \leq_2 f(y)$.

Let S be a set of n elements and consider the poset $P(S)$ of subsets of S. Let $I = \{0, 1\}$ be the two element poset defined by $0 < 1$. One can show easily that $P(S)$ and I^n are isomorphic. For each subset A of S we define $f(A)$ to be the characteristic vector of A. It is then easily verified that this is the required isomorphism.

This observation allows us to compute the Möbius function of $P(S)$ very easily. Indeed, it is not hard to verify that if $(P_1, \leq_1)$ and $(P_2, \leq_2)$ are two locally finite posets, then the Möbius function of $P_1 \times P_2$ is given by

$$\mu((x_1, x_2), (y_1, y_2)) = \mu(x_1, y_1)\mu(x_2, y_2).$$

Now, the Möbius function for I is easily seen to be given by

$$\mu(x, y) = (-1)^{y-x}.$$

Thus, the Möbius function for I^n is given by

$$\mu((x_1, .., x_n), (y_1, ..., y_n)) = (-1)^{\sum_i (y_i - x_i)},$$

and using the isomorphism between $P(S)$ and I^n given above, we deduce that

$$\mu(A, B) = (-1)^{|B|-|A|}.$$

The Möbius inversion formula for sets now reads as:

THEOREM 6.2.1. *If*

$$F(A) = \sum_{A \subseteq B} G(B),$$

then

$$G(A) = \sum_{A \subseteq B} (-1)^{|B|-|A|} F(B),$$

and conversely.

We can specialize this to deduce the inclusion-exclusion principle. Indeed, suppose we have a set A with subsets A_i with $i \in I$. We would like to derive a formula for the size of

$$A \backslash \cup_i A_i.$$

For each subset J of I, we let $F(J)$ be the number of elements of A which belong to every A_i for $i \in J$. Let $G(J)$ be those elements which belong to every A_i for $i \in J$ and to no other A_i for $i \notin J$. Clearly,

$$F(K) = \sum_{J \supseteq K} G(J).$$

By Möbius inversion, we obtain

$$G(K) = \sum_{J \supseteq K} \mu(K, J) F(J).$$

What we seek is $G(\emptyset)$. Because $F(J) = |\cap_{i \in J} A_i|$, we retrieve the principle of inclusion and exclusion. Thus, the Möbius inversion formula is a vast generalization of this important principle.

6.3. The Classical Möbius Function

Let us consider the lattice $D(n)$ of divisors of a natural number n. By the unique factorization theorem, we see that if

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

with p_i's being distinct primes, then

$$D(n) \simeq D(p_1^{\alpha_1}) \cdots D(p_k^{\alpha_k}).$$

Thus, in order to determine the Möbius function of $D(n)$, it suffices to determine for $D(p^a)$ for primes p. We observe that $\mu(p^i, p^j)$ is 1 if $i = j$, is -1 if $i = j - 1$ and 0 otherwise. By the product theorem, the Möbius function for $D(n)$ is easily computed: $\mu(a, b) = 0$ unless $a|b$ in which case it is the classical Möbius function $\mu(b/a)$ defined as follows: $\mu(n)$ is zero unless n is square-free in which case it is $(-1)^k$, where k is the number of prime factors of n. The Möbius inversion formula for the lattice of natural numbers partially ordered by divisibility is now seen as an immediate consequence of the general inversion formula.

One immediate application of the Möbius inversion formula is to count the number $\phi(n)$ of natural numbers less than n which are coprime to n. We see immediately that

$$\phi(n) = \sum_{d|n} \mu(d) n/d.$$

There are many applications of the inversion formula in counting problems. For instance, let us look at the following celebrated example. If we have an infinite supply of beads of λ colours, in how many ways can we make a necklace of n beads? Clearly, any necklace can be thought of as a sequence $(a_1, ..., a_n)$, where we identify any cyclic permutation of the sequence as giving rise to the same necklace. We will say that a necklace is **primitive** of length n if for no divisor $d < n$ it is not obtained by repeating n/d times a necklace of length d. We say a necklace has **period** d if it is obtained by repeating $\frac{n}{d}$ times a primitive necklace of length d. With these notions, we can count first the number of sequences to be λ^n. On the other hand, each sequence corresponds to some primitive necklace of period d which must necessarily divide n. If we let $M(d)$ be the number of primitive necklaces of length d, we have d places from which to start the sequence and so we obtain

$$\lambda^n = \sum_{d|n} dM(d).$$

By Möbius inversion, we get

$$M(n) = \frac{1}{n}\sum_{d|n} \mu(d)\lambda^{n/d}.$$

Now the total number of necklaces is

$$\sum_{d|n} M(d).$$

This can be simplified further. We have

$$\sum_{de=n}\sum_{ab=d} \frac{1}{d}\mu(a)\lambda^b = \sum_{abe=n} \frac{\lambda^b}{b}\frac{\mu(a)}{a} = \sum_{b|n}\frac{\lambda^b}{b}\sum_{ae=n/b} \mu(a)/a.$$

The inner sum is easily seen to be $\phi(n/b)/(n/b)$. Thus, the final formula is

$$\frac{1}{n}\sum_{b|n} \phi(n/b)\lambda^b.$$

6.4. The Lattice of Partitions

Let S be a finite set and $\Pi(S)$ the collection of its partitions. We make $\Pi(S)$ into a poset as follows. Recall that the components of a partition are called blocks (or equivalence classes). We say $\alpha \leq \beta$ if β refines the α. That is, each block of α is a union of blocks of β. For example,

$$\alpha = \{1, 2\}\{3, 4, 5\} \leq \{1\}\{2\}\{3, 5\}\{4\} = \beta.$$

It is easy to verify that this poset is a lattice with minimal element 0 given by the partition consisting of one block containing all the elements of S. The maximal element 1 is given by the partition consisting of singleton sets. Thus, the "greater" the partition, the larger the number of blocks.

We would like to determine the Möbius function of this lattice. To this end, let us define $b(\alpha)$ to be the number of blocks of the partition α. Let us fix a partition β with m blocks. If $\alpha \leq \beta$, then every block of α is a union of blocks of β and it is then clear that if we view β as a set of its blocks, then

$$[0, \beta] \simeq \Pi(\beta),$$

which will be useful in the computation of the Möbius function.

Let x be an indeterminate. For each partition α define $g(\alpha)$ to be the polynomial $(x)_{b(\alpha)}$. Then,

$$\sum_{\alpha \leq \beta} g(\alpha) = \sum_{\alpha \leq \beta} (x)_{b(\alpha)} = \sum_{k=1}^{m} S(m,k)(x)_k = x^m = x^{b(\beta)}$$

by a calculation from Chapter 2. By Möbius inversion,

$$g(\beta) = (x)_m = \sum_{\alpha \leq \beta} \mu(\alpha, \beta) x^{b(\alpha)} = \sum_{k=1}^{m} s(m,k) x^k,$$

by a calculation done (again) in the Chapter 2. Identifying the coefficients of x^k of both sides of the identity above gives

$$s(m,k) = \sum_{\alpha \leq \beta, b(\alpha)=k} \mu(\alpha, \beta).$$

Taking $k = 1$ gives

$$s(m,1) = \mu(0, \beta).$$

Thus, the value of the Möbius function $\mu(0, \beta)$ depends only the number of blocks in β, namely $b(\beta)$. But recall that $(-1)^{m-1} s(m,1)$ is the number of permutations of S_m with exactly one cycle in their disjoint cycle decomposition. The number of such permutations is $(m-1)!$. Thus, we have proved that:

THEOREM 6.4.1. *For the lattice of partitions $\Pi(S)$ of an n element set, we have*

$$\mu(0,1) = (-1)^{n-1}(n-1)!.$$

We will now count the number of connected labeled graphs on n vertices. To this end, let us observe that any graph induces partition on the vertices given by its connected components. For each partition β of the n vertices, let $g(\beta)$ be the number of graphs whose partition of connected components is finer than β. Let $f(\beta)$ be the number of graphs whose partition of connected components is equal to β. Clearly,

$$g(\beta) = \sum_{\alpha \geq \beta} f(\alpha).$$

By Möbius inversion, we get

$$f(\beta) = \sum_{\alpha \geq \beta} \mu(\beta, \alpha) g(\alpha).$$

What we want to determine is $f(0)$. But this is

$$f(0) = \sum_{\alpha} \mu(0, \alpha) g(\alpha).$$

If $\alpha = \{B_1, ..., B_k\}$, then clearly

$$g(\alpha) = \sum_{\alpha} (-1)^{b(\alpha)-1}(b(\alpha)-1)! 2^{\binom{|B_1|}{2}} \cdots 2^{\binom{|B_k|}{2}}.$$

6.5. Colouring Graphs

Graph colouring is one of the main topics in graph theory. We describe here some connections between this subject and Möbius inversion. More details regarding graph colouring will appear in Chapter 10 and Chapter 11.

Given a map M in the plane, let $p_M(\lambda)$ be the number of ways of colouring M properly using λ colours. We say that a colouring is **proper** if no two adjacent regions receive the same colouring. If $r(M)$ is the number of regions of the map, then the number of arbitrary colourings using λ colours is clearly $\lambda^{r(M)}$. Given any such colouring, we may "refine" it to get a proper colouring of a unique "submap" obtained by deleting the common boundary between the regions with the same colour. It is also clear that we may define a partial ordering on the set of "submaps" of M in the obvious way. Thus, we obtain

$$\lambda^{r(M)} = \sum_{A \subseteq M} p_A(\lambda).$$

By applying Möbius inversion on this poset of submaps, we obtain

$$p_M(\lambda) = \sum_{A \subseteq M} \mu(A, M) \lambda^{r(A)}.$$

This remarkable formula also shows that the number of ways of colouring the map M using only λ colours is given by a polynomial in λ of degree equal to the number of regions. This is not at all an obvious fact and yet by the theory of Möbius inversion, we were able to deduce it immediately.

The same result can be derived for colouring graphs. If X is a graph and $p_X(\lambda)$ is the number of properly colouring the vertices of X using λ colours, then we may derive a similar formula as follows. If X has $n(X)$ vertices, the number of arbitrary colourings of X using λ colours is $\lambda^{n(X)}$. Any such colouring can be refined to give a proper colouring of a subgraph obtained by contracting any two adjacent vertices that received the same colouring. The collection of subgraphs is a poset in the obvious way and thus, by Möbius inversion we see that

$$p_X(\lambda) = \sum_{A \subseteq X} \mu(A, X)\lambda^{n(A)},$$

which is again a polynomial in λ of degree equal to the number of vertices of the graph.

The **scheduling problem** is really a colouring problem. Suppose in a university we are to schedule exams so that no student has a time conflict. We construct a graph whose vertices are the courses for which we must schedule an exam. We join two vertices if the corresponding courses have a common student. The colours correspond to time slots and a proper colouring of the graph means that we assign time slots so that no student has a conflict.

Recall that given a graph X and an edge e by X/e we mean the contraction of X by e which means we create a new graph where the two vertices of e are identified.

THEOREM 6.5.1. *Let X be a simple graph and let $p_X(\lambda)$ be the number of ways of properly colouring X using λ colours. If e is an edge, then*

$$p_X(\lambda) = p_{X-e}(\lambda) - p_{X/e}(\lambda).$$

PROOF. Clearly, any proper colouring of X is also a proper colouring of $X - e$. Thus, we look at all proper colourings of $X - e$ and remove from this number those which are not proper colourings of X. This latter number corresponds to the situation where the two vertices of e get the same colour in $X - e$. But this corresponds to a proper colouring of X/e. ■

Since $X - e$ and X/e have at least one less edge than X, we see immediately by induction that $p_X(\lambda)$ is a polynomial in λ. However, a more precise theorem can be derived.

THEOREM 6.5.2. *The polynomial $p_X(\lambda)$ has degree $n = |V(X)|$ and integer coefficients alternating in sign and beginning as*

$$p_X(\lambda) = \lambda^n - |E(X)|\lambda^{n-1} + \cdots,$$

where $|E(X)|$ is the cardinality of the edge set.

PROOF. We prove this by induction on the number of edges of X. The claim holds trivially if $|E(X)| = 0$ for then $p_X(\lambda) = \lambda^n$. By induction, we may write

$$p_{X-e}(\lambda) = \lambda^n - (|E(X)| - 1)\lambda^{n-1} + a_2\lambda^{n-2} - \cdots$$

and

$$-p_{X/e}(\lambda) = \quad -\lambda^{n-1} + b_1\lambda^{n-2} - \cdots$$

where $a_2, ...$ and $b_1, ...$ are non-negative integers by the induction hypothesis. Adding these two equations gives

$$p_X(\lambda) = \lambda^n - |E(X)|\lambda^{n-1} + (a_2 + b_1)\lambda^{n-2} + \cdots$$

and the theorem is proved. ∎

Based on this result, we call $p_X(\lambda)$ the **chromatic polynomial** of X. This polynomial was introduced by George David Birkhoff (1884-1944) in 1912 as an attempt to attack the four-colour conjecture (now theorem). Showing that $p_X(4) > 0$ for any planar graph X is equivalent to the four-colour theorem.

For the complete graph K_n, the chromatic polynomial is easily seen to be

$$\lambda(\lambda - 1)(\lambda - 2) \cdots (\lambda - (n - 1)).$$

When we expand this as a polynomial in λ, we obtain

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

and the numbers $s(n, k)$ are the Stirling numbers of the first kind. From our theorem, we see that the $s(n, k)$ alternate in sign. Recall that $|s(n, k)|$ is the number of permutations of the symmetric group S_n with exactly k cycles in its unique factorization as a product of disjoint cycles.

The chromatic number $\chi(X)$ of the graph X is the smallest positive integer m so that $p_X(m) > 0$. The chromatic number of the complete graph K_n is clearly n. For the cycle graph C_n, the chromatic number is 2 or 3 according as n is even or odd. The four colour theorem is the assertion that the chromatic number of any graph obtained from a planar map is 4.

One can get a trivial bound for the chromatic number which is easily seen to be sharp in the cases of the complete graph and the odd cycles.

THEOREM 6.5.3. *Let $\Delta(X)$ denote the maximum degree of any vertex in a simple graph X. Then*

$$\chi(X) \leq 1 + \Delta(X).$$

PROOF. We use a *greedy* colouring by colouring the vertices in the order $1, 2, \ldots, n$ assigning to i the smallest-indexed colour not already used by its neighbours $j < i$.

Each vertex i will have at most Δ neighbours $j < i$ so this colouring will not use more than $\Delta + 1$ colours. ■

As our remarks indicate, this theorem is sharp. However, a famous theorem of Brooks, proved in 1941, states that these are the only two counterexamples and if we exclude them, we have a sharper bound.

THEOREM 6.5.4 (Brooks, 1941). *If X is connected and not a complete graph or an odd cycle, then*

$$\chi(X) \leq \Delta(X).$$

The proof of this theorem is rather complicated and we will skip it here.

6.6. Colouring Trees and Cycles

Theorem 6.5.1 can be used to determine the chromatic polynomial of trees. In fact, any tree T has a leaf v (say). Let e be the unique edge containing vertex v. We have that

$$p_T(\lambda) = p_{T-e}(\lambda) - p_{T/e}(\lambda).$$

Since $T - e$ has two connected components, namely an isolated vertex and a tree with one less edge than T, we see that an inductive argument easily shows:

THEOREM 6.6.1. *Let T be a tree with n vertices. Then*

$$p_T(\lambda) = \lambda(\lambda - 1)^{n-1}.$$

PROOF. We apply induction on n and note that in the remark preceding the statement of the theorem, T/e is a tree on $n - 1$ vertices. Thus, induction gives

$$p_X(\lambda) = \lambda\{\lambda(\lambda - 1)^{n-2}\} - \lambda(\lambda - 1)^{n-2} = \lambda(\lambda - 1)^{n-1}.$$

■

COROLLARY 6.6.2. *The chromatic number of a tree is 2.*

Theorems 6.5.1 and 6.6.1 can be used to determine the chromatic polynomial of the cycle C_n on n vertices. Deleting an edge from the cycle gives a tree on n vertices and contracting an edge gives a cycle on $n-1$ vertices. Thus, by an inductive argument we deduce:

THEOREM 6.6.3. *The chromatic polynomial of the cycle C_n is*

$$(\lambda-1)^n+(-1)^n(\lambda-1).$$

In particular, the chromatic number of C_n is 2 or 3 according as n is even or odd.

PROOF. For $n=3$, we verify the theorem directly:

$$\lambda(\lambda-1)(\lambda-2)=(\lambda-1)^3-(\lambda-1).$$

For the general case, by the remark preceding the theorem and the induction hypothesis, we get

$$\lambda(\lambda-1)^{n-1}-\{(\lambda-1)^{n-1}+(-1)^{n-1}(\lambda-1)\}$$

which is easily seen to be the stated expression. ■

It is rather remarkable that the converse of Theorem 6.6.1 also holds. That is, if X is a graph with chromatic polynomial $p_X(\lambda)=\lambda(\lambda-1)^{n-1}$, then X is a tree. To see this, first note that if X consists of connected components $X_1, X_2, ...$ then the chromatic polynomial of X is just the product of the chromatic polynomials of the connected components. Secondly, any chromatic polynomial has $\lambda=0$ as a root. This can be seen in several ways. An immediate way to see it is to say that the number of ways of colouring a map using zero colours is zero. Another way is to see it is via an inductive argument from the contraction deletion Theorem 6.5.1. Thus, the order of the zero at $\lambda=0$ is at least equal to the number of connected components. Since the zero is of order 1 in our case, the graph is connected. In addition, the number of edges is $n-1$ which can be seen from computing the coefficient of the second term. Thus, X is connected and has exactly $n-1$ edges and so by Theorem 5.1.2, X is a tree. This proves:

THEOREM 6.6.4. *If X has chromatic polynomial $\lambda(\lambda-1)^{n-1}$, then X is a tree on n vertices.*

There are other classes of graphs except trees that are not isomorphic but share the same chromatic polynomial. An easy way to construct such graphs is by using the following theorem.

THEOREM 6.6.5. *Let X and Y be two graphs whose intersection is a complete graph K_r. Then*

$$p_{X\cup Y}(\lambda) = \frac{p_X(\lambda)\cdot p_Y(\lambda)}{\lambda(\lambda-1)\dots(\lambda-r+1)}.$$

We leave the proof of this theorem as an exercise.

6.7. Sharper Bounds for the Chromatic Number

We will now connect eigenvalues of the adjacency matrix of a graph with its chromatic number. As preparation to this end, we will review the notion of **Rayleigh-Ritz quotient** or **ratio** from linear algebra.

Let A be a real symmetric matrix. If $x = (x_1, \dots, x_n)^t$ and $y = (y_1, \dots, y_n)^t$ are two n by 1 column vectors, then the inner product (x, y) is defined as $x_1y_1 + \dots + x_ny_n$. For any non-zero column vector v, we call $(Av, v)/(v, v)$ the **Rayleigh-Ritz quotient** of v and denote it by $R(A, v)$. Denote by λ_{max} and λ_{min} the largest and smallest eigenvalues of A respectively. Then

$$\lambda_{\text{max}} = \max_{v\neq 0} \frac{(Av, v)}{(v, v)}$$

and

$$\lambda_{\text{min}} = \min_{v\neq 0} \frac{(Av, v)}{(v, v)}.$$

To see this, observe that if U denotes the matrix whose columns form an orthonormal basis of eigenvectors of A, then we may write

$$A = UDU^t,$$

where D is a diagonal matrix whose diagonal entries are the eigenvalues of A. Thus,

$$(Av, v) = v^tAv = v^tUDU^tv = \sum_i \lambda_i |(U^tv)_i|^2.$$

As each of the terms $|(U^tv)_i|^2$ is non-negative,

$$\lambda_{\text{min}} \sum_i |(U^tv)_i|^2 \le v^tAv \le \lambda_{\text{max}} \sum_i |(U^tv)_i|^2.$$

Since U is an orthogonal matrix, we have

$$\sum_i |(U^tv)_i|^2 = \sum_i |v_i|^2 = v^tv.$$

Thus, if $v \neq 0$,

$$\lambda_{\text{min}} \le \frac{(Av, v)}{(v, v)} \le \lambda_{\text{max}}.$$

The inequalities are easily seen to be sharp by considering the eigenvectors corresponding to $\lambda_{\max}$ and $\lambda_{\min}$ respectively, which proves our assertion. This result is usually referred to as the Rayleigh-Ritz theorem in the literature.

If X is a graph, let us denote $\lambda_{\max}(X)$ and $\lambda_{\min}(X)$ to be the largest and smallest eigenvalues of the adjacency matrix A_X of X. We also say that X' is a **subgraph** of X if $V(X') \subseteq V(X)$ and $E(X') \subseteq E(X)$. We begin by proving:

THEOREM 6.7.1. *If X' is a subgraph of X, then*

$$\lambda_{\max}(X') \le \lambda_{\max}(X); \quad \lambda_{\min}(X') \ge \lambda_{\min}(X).$$

If $\Delta(X)$ and $\delta(X)$ denotes the maximal and minimal degrees of X, then

$$\delta(X) \le \lambda_{\max}(X) \le \Delta(X).$$

PROOF. The first part of the theorem is proved as follows. By relabeling the vertices, we may assume that the adjacency matrix A of X has a leading principal submatrix A_0 which is the adjacency matrix of X'. Let z_0 be chosen so that $A_0 z_0 = \lambda_{\max}(A_0) z_0$ and $(z_0, z_0) = 1$. Let z be the column vector with $|V(X)|$ rows formed by adjoining zero to entries of z_0. Then,

$$\lambda_{\max}(A_0) = R(A_0, z_0) = R(A, z) \le \lambda_{\max}(A).$$

Thus, $\lambda_{\max}(A_0) \le \lambda_{\max}(A)$. The other inequality is proved in a similar way. For the second part, let u be a column vector each of whose entries is 1. Then, if $n = |V(X)|$ and d_i is the degree of vertex v_i, we have

$$R(A, u) = \frac{1}{n} \sum_{i,j} a_{ij} = \frac{1}{n} \sum_i d_i \ge \delta(X).$$

But the Rayleigh quotient $R(A, u)$ is at most $\lambda_{\max}(A)$ and so

$$\lambda_{\max}(X) \ge \delta(X).$$

For the other inequality, let v be an eigenvector corresponding to the eigenvalue $\lambda_0 = \lambda_{\max}(X)$. Let x_j be the largest positive entry of v. Then,

$$\lambda_0 x_j = (\lambda_0 v)_j = \sum_i^{*} x_i \le \Delta(X) x_j$$

where the $*$ on the summation means we sum over the vertices adjacent to v_j. This proves the theorem. ∎

We will now relate the chromatic number to the largest eigenvalue of the adjacency matrix of X. To this end, we say a graph is **t-critical** if $\chi(X) = t$ and for all proper vertex subgraphs U of X, we have $\chi(U) < t$.

LEMMA 6.7.2. *Suppose X has chromatic number $t \geq 2$. Then X has a t-critical subgraph U such that every vertex of U has degree at least $t-1$ in U.*

PROOF. The set of all vertex subgraphs of X is non-empty and contains some graphs (for instance, X itself) that have chromatic number t. Let U be a vertex subgraph of X whose chromatic number is t which is minimal with respect to the number of vertices. Clearly, U is t-critical. Moreover, if $v \in V(U)$, then the vertex subgraph whose vertex set is $V(U)\backslash v$ is a vertex subgraph of U and has a vertex colouring with $t-1$ colours. If the valency of v in U were less than $t-1$, then, we could have extended this vertex colouring to U contradicting $\chi(U) = t$. ■

The previous lemma has the following important consequences.

THEOREM 6.7.3 (Szekeres-Wilf 1968). *If X is a graph, then*

$$\chi(X) \leq 1 + \max_{Y \subseteq X} \delta(Y).$$

PROOF. By Lemma 6.7.2, there is a vertex subgraph U of X whose chromatic number is $\chi(X)$ and $\delta(U) \geq \chi(X) - 1$. Thus, we have

$$\chi(X) \leq 1 + \delta(U) \leq 1 + \max_{Y \subseteq X} \delta(Y).$$

■

By a slight modification of the previous proof, we also get the following result.

THEOREM 6.7.4 (Wilf, 1967). *For any graph X, we have*

$$\chi(X) \leq 1 + \lambda_{\max}(X).$$

PROOF. As before, there is a vertex subgraph U of X whose chromatic number is $\chi(X)$ and $\delta(U) \geq \chi(X) - 1$. Thus, by Theorem 6.7.1, we have

$$\chi(X) \leq 1 + \delta(U) \leq 1 + \lambda_{\max}(U) \leq 1 + \lambda_{\max}(X),$$

as desired. ■

6.8. Sudoku Puzzles and Chromatic Polynomials

The Sudoku puzzle has become a very popular puzzle that many newspapers carry as a daily feature. The puzzle consists of a 9×9 square grid in which some of the entries of the grid have a number from 1 to 9. One is then required to complete the grid in such a way that every row, every column, and every one of the nine 3×3 sub-grids contain the digits from 1 to 9 exactly once. The sub-grids are shown below.

For anyone trying to solve a Sudoku puzzle, several questions arise naturally. For a given puzzle, does a solution exist ? If the solution exists, is it unique ? If it is not unique, how many solutions are there ? Moreover, is there a systematic way of determining all the solutions ? How many puzzles are there with a unique solution ? What is the minimum number of entries that can be specified in a single puzzle to ensure a unique solution ? For instance, the next figure shows that the minimum is at most 17. We leave it to the reader to show that the puzzle below has a unique solution. It is unknown if a puzzle with 16 specified entries exists that yields a unique solution.

							1	
4								
	2							
				5		4		7
		8				3		
		1		9				
3			4			2		
	5		1					
			8		6			

We reinterpret the Sudoku puzzle as a vertex colouring problem in graph theory. We associate a graph with the 9×9 Sudoku grid as follows. The graph will have 81 vertices with each vertex corresponding to a cell in a grid. Two distinct vertices will be adjacent if and only if the corresponding cells in the grid are either in the same row, or same column, or the same sub-grid. Each completed Sudoku square then corresponds to a proper colouring of this graph. We put this problem in a more general and formal context. Consider an $n^2 \times n^2$ grid. To each cell in a grid, we associate a vertex labeled (i, j) with $0 \leq i, j \leq n^2 - 1$. We will say that (i, j) and (i', j') are adjacent if $i = i'$ or $j = j'$ or

$\lfloor \frac{i}{n} \rfloor = \lfloor \frac{i'}{n} \rfloor$ and $\lfloor \frac{j}{n} \rfloor = \lfloor \frac{j'}{n} \rfloor$. Recall that $\lfloor x \rfloor$ is the largest integer less than or equal to a. We will denote this graph by X_n and call it the Sudoku graph of rank n. An easy computation shows that X_n is a regular graph having degree $3n^2 - 2n - 1$. In the case $n = 3$, X_3 is 20-regular and in case $n = 2$, X_2 is 7-regular.

A Sudoku square of rank n will be a proper coloring of this graph using n^2 colours.

THEOREM 6.8.1. *For every natural number n, the chromatic number of the Sudoku square X_n is n^2.*

PROOF. It is easy to see that we need at least n^2 colours because the n^2 vertices of the same row or column create a complete subgraph of order n^2. For $0 \leq i \leq n^2 - 1$, write $i = t_i n + d_i$, where $0 \leq t_i \leq n - 1$ and $0 \leq d_i \leq n - 1$. Colour the vertex corresponding to the cell (i, j) of the Sudoku square by the colour $d_i n + t_i + n t_j + d_j$, reduced modulo n^2. We leave it as an exercise for the reader to show that this is a proper colouring of X_n with n^2 colours. ■

A Sudoku puzzle corresponds to a partial colouring of X_n and the question is whether this partial colouring can be completed to a total proper colouring of the Sudoku graph X_n with n^2 colours. Given a partial proper colouring C of a graph G), one can show that the number of ways of completing this colouring to obtain a proper colouring with λ colours, is a polynomial in λ, provided that λ is greater than or equal to the number of colours used in C. We leave this as an exercise.

It is not obvious at the outset if a given puzzle has a solution. Also, it is always clear whether or not a puzzle has a unique solution. An obvious necessary condition to have a unique solution is that the partial Sudoku square must contain at least 8 distinct numbers from $\{1, \ldots, 9\}$. This is not sufficient as the square below has exactly two solutions. The proof of this fact is left as an exercise.

9		6		7		4		3
			4			2		
	7			2	3		1	
5						1		
	4		2		8		6	
		3						5
	3		7				5	
		7			5			
4		5		1		7		8

6.9. Exercises

EXERCISE 6.9.1. Show that the five examples from the first are actually posets.

EXERCISE 6.9.2. Draw the Hasse diagram for S_3 with the Bruhat order and determine completely the Möbius function of this poset.

EXERCISE 6.9.3. If

$$G(x) = \sum_{n \leq x} F(x/n)$$

prove that

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

EXERCISE 6.9.4. Show that

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

where $[x]$ denotes the greatest integer less than x.

EXERCISE 6.9.5. Let $(P_1, \leq_1)$ and $(P_2, \leq_2)$ be two locally finite posets. Show that

$$\mu((x_1, y_1), (x_2, y_2)) = \mu(x_1, y_1)\mu(x_2, y_2).$$

EXERCISE 6.9.6. Let $(P, \leq)$ be a finite poset. For $a \in P$, we will denote by $\downarrow a$ the set $\{x \in P : x \leq a\}$ and $\uparrow a$ the set $\{x \in P : a \leq x\}$. We say that P is **linearly ordered** if any two elements of P are comparable. Show that any partial ordering of P can be extended to a linear ordering as follows. View the poset $(P, \leq)$ as a subset R of $P \times P$ satisfying the axioms: (1) $(a, a) \in R$, (2) $(a, b) \in R$ and $(b, a) \in R$ implies $a = b$ and (3) $(a, b) \in R$, $(b, c) \in R$ implies $(a, c) \in R$. A linear order can be regarded as a subset R' of $P \times P$ which has the additional property that for any $a, b \in P$ either $(a, b) \in R'$ or $(b, a) \in R'$. Let now a, b be incomparable in $(P, \leq)$. Put $R' = R \cup (\downarrow a \times \uparrow b)$. Verify that R' is a partial order of P in which $(a, b) \in R'$. Deduce that any partial ordering of P can be extended to a linear ordering.

EXERCISE 6.9.7. Six different television stations are applying for channel frequencies and no two stations can use the same frequency if they are within 150 miles of each other. If the distances between the stations A, B, C, D, E and F are given by the matrix below, find the minimal number of frequencies needed.

$$\begin{array}{c|cccccc|}
 & A & B & C & D & E & F \\
A & - & 85 & 175 & 200 & 50 & 100 \\
B & 85 & - & 125 & 175 & 100 & 160 \\
C & 175 & 125 & - & 100 & 200 & 250 \\
D & 200 & 175 & 100 & - & 210 & 220 \\
E & 50 & 100 & 200 & 210 & - & 100 \\
F & 100 & 160 & 250 & 220 & 100 & -
\end{array}.$$

EXERCISE 6.9.8. Prove that the sum of the coefficients of the chromatic polynomial of a graph X is zero unless X has no edges. Show that the coefficients of $p_X(\lambda)$ alternate in sign.

EXERCISE 6.9.9. If $X_1, \dots, X_t$ are the components of X, then

$$p_X(\lambda) = \prod_{i=1}^{t} p_{X_i}(\lambda).$$

If $p_X(\lambda)$ is the chromatic polynomial of a graph X, show that we can write it as $\lambda^c f(\lambda)$ where $f(0) \neq 0$ and c is the number of connected components of X.

EXERCISE 6.9.10. The **join** of two graphs X and Y is defined as the graph obtained by joining every vertex of X to every vertex of Y. We denote this graph by $X \vee Y$. Show that $\chi(X \vee Y) = \chi(X) + \chi(Y)$.

EXERCISE 6.9.11. The wheel graph is $K_1 \vee C_n$. That is, the wheel graph is the cycle graph together with a vertex at the 'center' which is connected to all the vertices of C_n. Determine the chromatic polynomial of the wheel graph. Show also that

$$p_{K_{2,n}}(\lambda) = \lambda(\lambda-1)(\lambda-2)^n + \lambda(\lambda-1)^n.$$

EXERCISE 6.9.12. Let $p_X(\lambda)$ be the chromatic polynomial of a connected graph X of order n. Show that

$$|p_X(\lambda)| \leq \lambda(\lambda-1)^{n-1}$$

if $n \geq 3$.

EXERCISE 6.9.13. Compute the chromatic polynomial of the graph in Figure 6.1.

EXERCISE 6.9.14. Prove Theorem 6.6.5.

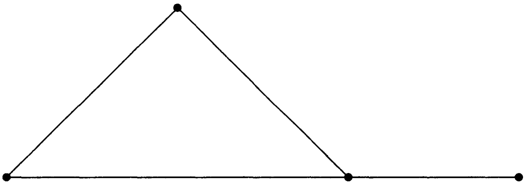


FIGURE 6.1

EXERCISE 6.9.15. Let X be a graph with n vertices, e edges and maximum degree Δ. Show that

$$\lambda_{max} \geq \max\left(\frac{2e}{n}, \sqrt{\Delta}\right).$$

When does equality occur ?

EXERCISE 6.9.16. Let G be a graph with n vertices and let C be a partial proper colouring of t vertices of G using k colours. If $p_{G,C}(\lambda)$ denotes the number of ways of completing this colouring using λ colours to a proper colouring of G, then prove that $p_{G,C}(\lambda)$ is a polynomial in λ with integer coefficients of degree $n-t$ for $\lambda \geq k$.

EXERCISE 6.9.17. Show that the chromatic number of a graph X satisfies

$$\chi(X) \leq \frac{1+\sqrt{8e+1}}{2}.$$

EXERCISE 6.9.18. Let G_n be the graph whose vertex set is $[2n] = \{1, 2, \ldots, 2n\}$ and where (i, j) is an edge if and only if i and j have a common prime divisor. Show that the chromatic number of X_n is at least n.

EXERCISE 6.9.19. The **Kneser graph** $K(n, k)$ is the graph whose vertices are all the k-element subsets of $[n]$. Two k-subsets are adjacent in $K(n, k)$ if and only if they are disjoint. Show that the Petersen graph (Figure 10.2) is isomorphic to $K(5, 2)$ and that $\chi(K(n, k)) \leq n-2k+2$. The chromatic number of $K(n, k)$ actually equals $n-2k+2$ as proved by László Lovász in 1978, but this is a more difficult result.

EXERCISE 6.9.20. Let $c(X)$ denote the number of components of the graph X and for $F \subseteq E(X)$, denote by $X[F]$ the spanning subgraph of X with edge set F. Show that

$$p_X(\lambda) = \sum_{F \subseteq E(X)} (-1)^{|F|} \lambda^{c(X[F])}.$$

CHAPTER 7

Enumeration under Group Action

7.1. The Orbit-Stabilizer Formula

Let G be a group and X a set. We say G **acts** on X if there is a map $G \times X \to X$ (usually denoted by $(g, x) \mapsto g \cdot x$) satisfying the following axioms for all $x \in X$:

(1) $1 \cdot x = x$, where 1 denotes the identity of G;
(2) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

Here are a few examples.

(1) If G is a group and H is a subgroup, let X be the set of left cosets of H in G. Then G acts on X via $g(aH) = (ga)H$.
(2) If G is a group and we let X be G itself, then G acts on itself via conjugation: $g \cdot x = gxg^{-1}$.
(3) Let p be prime and $G = \mathbf{Z}/p\mathbf{Z}$ be the additive group of residue classes $[a] \bmod p$. Let X be the set of all p-tuples $(x_1, x_2, ..., x_p)$ where $x_i \in \{1, 2, ..., n\}$. Since G is cyclic, it suffices to define how $[1]$ acts on X. We put

$$[1] \cdot (x_1, x_2, ..., x_p) = (x_p, x_1, ..., x_{p-1}).$$

In other words, $[1]$ acts like a shift operator, shifting the coordinates by one component.
(4) Let n be a natural number and $G = \mathbf{Z}/n\mathbf{Z}$. Let X be the set of all n-tuples $(x_1, ..., x_n)$ where $x_i \in \{1, 2, ..., \lambda\}$. We define

$$[1] \cdot (x_1, x_2, ..., x_n) = (x_n, x_1, ..., x_{n-1}).$$

We can view the set X as all the possible "necklaces" formed by using beads of λ colours. This perspective will be useful in later applications.

It will be convenient to simplify our notation slightly. Instead of writing $g \cdot x$, we will simply write gx, when it is clear that $g \in G$ and $x \in X$. An action of G on X determines an equivalence relation on X as follows. Namely, we will write $x \sim y$ if there is an element $g \in G$ such that $gx = y$. Thus, if $gx = y$ then $x = g^{-1}y$ and $y \sim x$. Since $1x = x$, this means that $x \sim x$. Also, it is easy to check that $x \sim y$ and

$y \sim z$ implies $x \sim z$. Therefore, $\sim$ defines an equivalence relation on X. Consequently, we can partition X into equivalence classes, which we call **orbits**. More precisely, if we use the notation Gx to signify the set

$$\{gx : g \in G\}$$

then it is clear that the equivalence classes consist of sets of the form Gx_i for various x_i's.

If G and X are finite, it is natural to ask how many elements are there in each orbit and how many equivalence classes there are. We begin with the first question. We begin by listing the $|G|$ elements

$$gx : \quad g \in G \tag{7.1.1}$$

and ask how many times an element gets repeated. Indeed, $gx = hx$ if and only if $h^{-1}gx = x$, that is if and only if $h^{-1}g$ fixes x.

This leads to the notion of the **stabilizer** of x, denoted G_x, and defined as the set of elements of G fixing x. It is easy to see that the stabilizer of x is a subgroup of G for any $x \in X$. In the context above, we see that $gx = hx$ if and only if $h^{-1}g$ lies in G_x. In other words, $gx = hx$ if and only if $gG_x = hG_x$. Thus, in the listing (7.1.1), each element is repeated the same number of times, namely $|G_x|$ times so that the number of distinct elements is $[G : G_x]$. As the set X is partitioned into its orbits, we see that there are elements x_i's so that

$$X = \uplus_{i=1}^{t} Gx_i.$$

For each subgroup H of G we define fix(H) to be the set of H-fixed points of X. That is

$$\text{fix}(H) = \{x \in X : \quad hx = x \quad \forall h \in H\}.$$

If $g \in G$, we simply write fix(g) for the set of elements fixed by the subgroup generated by g. From the above relation, we separate those x_i's for which Gx_i consists of singleton sets. In other words, we obtain:

THEOREM 7.1.1 (Orbit-Stabilizer formula). *If G is a finite group acting on a finite set X, we have*

$$|X| = |\text{fix}(G)| + \sum_{G_{x_i} \neq G} [G : G_{x_i}].$$

This formula is of central importance in mathematics and has numerous applications. For instance, in the case a group G acts on itself via conjugation, we get:

COROLLARY 7.1.2 (The class equation). *Let G act on itself via conjugation. Let $Z(G) = \{g : gx = xg, \forall x \in G\}$ denote its* **center** *and $C(x) = \{g \in G : gx = xg\}$ be the* **centralizer** *of x in G. Then,*

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : C(x)].$$

PROOF. We see immediately that x is a G-fixed point if and only if $x \in Z(G)$. Moreover, the stabilizer of any element x is $C(x)$. The formula is now immediate from the orbit-stabilizer formula applied to this specific case. ■

If we apply the orbit-stabilizer formula to Example 3 above, we see that on one hand, we have n^p elements in X and on the other, the set of fixed elements is easily seen to be of size n. Now every summand in the sum is p since $\mathbf{Z}/p\mathbf{Z}$ has no non-trivial subgroups. We recover the following result:

THEOREM 7.1.3 (Fermat's little theorem). *If p is a prime number, then p divides $n^p - n$ for each integer n.*

A less trivial application by considering the following situation. Let G be a group of order n and consider

$$X = \{(x_1, ..., x_p) : \quad x_1 \cdots x_p = 1, \quad x_i \in G\}.$$

The size of X is n^{p-1} since we may choose each of $x_1, ..., x_{p-1}$ in n ways, then x_p is uniquely determined by the equation

$$x_1 \cdots x_p = 1.$$

We let the additive group $\mathbf{Z}/p\mathbf{Z}$ act on X by setting

$$[1] \cdot (x_1, ..., x_p) = (x_p, x_1, ..., x_{p-1}).$$

Note that the set of fixed points consists of elements $(x, x, ..., x)$ with $x^p = 1$. If p is a prime divisor of n, the orbit-stabilizer formula immediately gives that the number of fixed points is divisible by p. Since $\text{fix}(G) \neq \emptyset$ (why?), it follows that G has an element of order p. This is usually referred to as Cauchy's theorem. We record this as:

COROLLARY 7.1.4 (Cauchy, 1845). *If G is a group of order n and p is a prime dividing n, then G has an element of order p.*

However, much more is true. Cauchy's theorem was generalized by Peter Ludwig Sylow (1832-1918) in 1872. Almost all work on finite groups use Sylow's theorems. The class equation enables us to deduce the first Sylow theorem, namely:

COROLLARY 7.1.5 (Sylow's First Theorem). *If G is a group of order n and p^k is a prime power dividing n, then G has a subgroup of order p^k.*

PROOF. We proceed by induction on $|G|$. If $|G| = 2$, the theorem is true.

Let $|G| = p^r m$, where $r \geq k$ and m and p are coprime. If $x \in G$ and p^k divides $|C(x)|$, then we are done by induction.

Otherwise, because every summand in the sum occurring in the class equation is divisible by p, we deduce that p divides the order of the center $Z(G)$. By Cauchy's theorem, $Z(G)$ has an element x of order p. The subgroup generated by x in G is normal since $x \in Z(G)$. The quotient $G/\langle x\rangle$ has order divisible by p^{k-1} and by induction has a subgroup $H/\langle x\rangle$ of order p^{k-1}. By the correspondence theorem, H is a subgroup of G of order p^k, as desired. ∎

We remark that all of the Sylow theorems can be derived by considering appropriate group action. Recall the notion of a p-Sylow subgroup. If p^k is the largest power of a prime number p dividing the order of G, and P is a subgroup of order p^k, we call P a **p-Sylow subgroup** of G. The **normalizer** of a subgroup H of G is $N(H) = \{g : g \in G, gHg^{-1} = H\}$.

COROLLARY 7.1.6 (Sylow's Second Theorem). *Let G be a finite group of order n and P a p-Sylow subgroup of G. Let X be the set of p-Sylow subgroups of G and let P act on X via conjugation. Then, P is the only fixed point under this action. Thus, the number of p-Sylow subgroups is $\equiv 1(\bmod p)$ and all of the p-Sylow subgroups are conjugates of P. Moreover, any p-subgroup of G is contained in some conjugate of P.*

PROOF. Suppose Q is another p-Sylow subgroup fixed by P. Then, $gQg^{-1} = Q$ for all $g \in P$. Take $x \in P\backslash Q$. Then, x is in the normalizer $N(Q)$. But $N(Q)$ contains Q and the coset xQ is not Q. As the quotient $N(Q)/Q$ has order coprime to p, the coset xQ has order k coprime to p. Thus, for some k, $x^k \in Q$ with $(k,p) = 1$. But x has order equal to some prime power p^b (say). So we can find integers u, v so that $ku + p^b v = 1$. Hence, $x = x^{ku+p^b v} \in Q$, contrary to hypothesis. As the set X is partitioned into orbits under the action of P, we deduce immediately that the number of elements of X is $\equiv 1 \pmod p$. Now let Y be the set of conjugates of P. Let H be a p-subgroup of G. Then H acts on Y. If H fixes an element Q of Y, then H is in the normalizer of Q. If H is not contained in Q, then the argument above gives us a contradiction. Thus every p-subgroup H is contained in some conjugate of P. In particular, if H is another p-Sylow subgroup, this means that it is conjugate to P. This completes the proof. ∎

A p-**group** is a group whose order is a power of p where p is a prime number. We remark that any p-group G has subgroups of all orders dividing $|G|$. Indeed, the class equation implies the non-triviality of the center. By Cauchy's theorem, we may take an element z in the center of order p and consider the quotient $G/\langle z\rangle$. By induction, this has subgroups of all orders dividing $|G|/p$ which by the correspondence theorem give subgroups of the required order in G. For an arbitrary group G, and any prime power p^t dividing $|G|$, we deduce that G has subgroups of order p^t. Moreover, one can show that the number of these subgroups is $\equiv 1(\mod p)$, but we leave this as an exercise.

Given a finite group G of order n, and a subgroup H of G, we can partition G into the cosets of H from which we see **Lagrange's theorem**, namely that the order of any subgroup is a divisor of the order of G. The converse is not true, as is seen by considering the alternating group A_4 on 4 letters. These are the even permutations of S_4 and one can list the elements:

$$(1),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3),(1\,2\,3),(1\,3\,2),(1\,2\,4),(1\,4\,2)$$

$$(2\,3\,4),(2\,4\,3),(3\,4\,1),(3\,1\,4).$$

If A_4 had a subgroup H of order 6, then this subgroup is necessarily normal which means that the square of any element of A_4 lies in H. In particular, the square of any 3-cycle g is in H. But $g = (g^2)^2$ lies in H so that all 3-cycles must lie in H, a contradiction since there are 8 3-cycles. The virtue of Sylow theory is that it shows that the converse of Lagrange's theorem holds for prime powers dividing the order of the group.

7.2. Burnside's Lemma

It is possible to derive a formula for the number of equivalence classes under a group action. This is called Burnside's lemma as William Burnside (1852-1927) wrote about it in 1900. The result was known before Burnside mentioned it as it appears in the works of Augustin Louis Cauchy (1789-1857) in 1845 and of Ferdinand Georg Frobenius (1849-1917) in 1887.

We will apply the next result to the problem of counting necklaces encountered in the previous chapter.

THEOREM 7.2.1 (Burnside's lemma). *If G is a finite group acting on a set X, the number of equivalence classes is*

$$\frac{1}{|G|}\sum_{g\in G}|\text{fix}(g)|.$$

In other words, the number of equivalence classes is the average number of fixed points.

PROOF. The equivalence class of an element x of X is the orbit of x. Thus, if $w(x)$ is $1/|Gx|$, we see that the number of equivalence classes is

$$\sum_{x\in X} w(x).$$

On the other hand, this is

$$\sum_{x\in X}\frac{1}{|G|}|G_x| = \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G_x} 1 = \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G:\, gx=x} 1.$$

By interchanging the sum, we find this is

$$\frac{1}{|G|}\sum_{g\in G}\sum_{x\in X: gx=x} 1 = \frac{1}{|G|}\sum_{g\in G}|\text{fix}(g)|.$$

This completes the proof. ■

COROLLARY 7.2.2. *The number of conjugacy classes in a group is*

$$\frac{1}{|G|}\sum_{g\in G}|C(g)|.$$

PROOF. The number of fixed points of $g \in G$ is precisely $|C(g)|$. ■

Let us apply this to the problem of counting necklaces. Each necklace of length n formed out of beads of λ colours can be viewed as a sequence $(a_1, ..., a_n)$ with $a_i \in \{1, 2, ...\lambda\}$. Two necklaces are considered the same if the two sequences representing them are the same after a shift. In other words, $\mathbf{Z}/n\mathbf{Z}$ acts on the sequences and the number of necklaces is precisely the number of equivalence classes under this action. Now, how many fixed points does an element r of $\mathbf{Z}/n\mathbf{Z}$ have? A sequence $(a_1, ..., a_n)$ is fixed r if and only if

$$a_{i+tr} = a_i$$

for all t and all i. In other words,

$$a_{i+u} = a_i$$

for all i and all u lying in the subgroup generated by r in $\mathbf{Z}/n\mathbf{Z}$. Since $\mathbf{Z}/n\mathbf{Z}$ is cyclic, any subgroup is also cyclic so the number of fixed points of r is $\lambda^{n/o(r)}$ where $o(r)$ is the order of r mod n. Recall that in any cyclic group of order n, the number of elements of order $d|n$ is precisely $\phi(d)$. Thus, the number of necklaces is

$$\frac{1}{n}\sum_{r}\lambda^{n/o(r)} = \frac{1}{n}\sum_{d|n}\phi(d)\lambda^{n/d} = \frac{1}{n}\sum_{d|n}\phi(n/d)\lambda^{d}.$$

7.3. Pólya Theory

George Pólya (1887-1985) was one of the most influential mathematicians of the 20th century.

The action of a group G on a set X can be viewed as a map

$$G \to \mathrm{Sym}(X)$$

where we send each element $g \in G$ to the permutation $x \mapsto gx$ since $gx = gy$ implies $x = y$ by the axioms of action. In this way, we may view each element of G as a permutation and so we can consider its cycle decomposition as a product of disjoint cycles. Suppose g has c_1 cycles of length 1, c_2 cycles of length 2 ..., c_n cycles of length n where $n = |X|$. The **cycle index** of g is defined to be the monomial

$$x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}$$

which we symbolically denote by x^g. The **cycle index** of G is defined to be the polynomial

$$P_G(x) = \frac{1}{|G|}\sum_{g\in G}x^g.$$

The situation can be looked at in another way. If G acts on X and we have a map $f : X \to Y$, we may view Y as a set of **colours**. Then, the action of G on X induces an action of G on $\mathrm{Map}(X;Y)$, the set of maps from X to Y as follows:

$$(g \cdot f)(x) = f(g^{-1}x).$$

It is important to check that this is indeed an action: we have for $x \in X$,

$$[(gh)f](x) = f((gh)^{-1}x) = f(h^{-1}g^{-1}x).$$

On the other hand,

$$[g(hf)](x) = (hf)(g^{-1}x) = f(h^{-1}g^{-1}x),$$

as desired. Burnside's lemma immediately implies the following.

THEOREM 7.3.1 (Pólya). *Let X and Y be finite sets and G act on X. The number of orbits of G on* $\mathrm{Map}(X;Y)$ *is*

$$\frac{1}{|G|}\sum_{k=1}^{\infty} c_k(G)|Y|^k,$$

where $c_k(G)$ is the number of elements of G with exactly k disjoint cycles in their cycle decomposition.

REMARK 7.3.2. Notice that this number is simply $P_G(|Y|,|Y|,...)$.

PROOF. To apply Burnside's lemma, we must count the number of fixed points of an element g on $\mathrm{Map}(X;Y)$. That is, we must count the number of maps $f : X \to Y$ such that $gf = f$. This means that f is constant on each orbit of g. The number of orbits is the number of disjoint cycles in the cycle decomposition of g. We may assign values of f arbitrarily on each orbit, so the final count is given as stated in the theorem. ∎

If we let Y denote the set of λ colours of beads, and X denotes the set $\{1,2,...,n\}$, then a sequence $(a_1,...,a_n)$ of length n can then be viewed as a map f from X to Y. As the group $\mathbf{Z}/n\mathbf{Z}$ acts on the co-ordinates in the obvious way by shifting, this induces an action on $\mathrm{Map}(X;Y)$. We see then that the maps that correspond to distinct necklaces are equivalence classes of maps under this induced action.

We can retrieve our result about the necklace count from the previous section in the following way. First, we must determine the cycle structure of a residue class r viewed as a permutation. Clearly, all orbits have the same length and if $o(r)$ denotes the order of r, then each orbit has size $o(r)$ and the number of disjoint cycles is $n/o(r)$. Hence, the number of elements of $\mathbf{Z}/n\mathbf{Z}$ with exactly k cycles is zero unless $k|n$, in which case it is the number of elements of order n/k. The number of such elements is $\phi(n/k)$, as we saw before.

Now suppose we have the dihedral group D_n acting on the necklace sequences. Thus, if we present D_n as

$$\langle r, f : r^n = 1, f^2 = 1, frf = r^{-1}\rangle.$$

We could try to count the number of equivalence classes by using Burnside's formula. To use Burnside's formula, we have to count the number of fixed points of each element of D_n. It is better to use the cycle index polynomial to determine the number of equivalence classes. We illustrate this as follows.

Firstly, let us have a geometric view of the dihedral group. It is to be viewed as the group of symmetries of a regular n-gon. If we fix any vertex, and bisect the interior angle subtended at that vertex, we can view the element f as the flip of the polygon about this axis. We can view the elements fr^j as flips about the axis determined by the other points. If n is odd, each of these elements fixes one vertex and transposes pairs of vertices which are mirror images about that axis. Thus, the cycle structure of fr^j is that it is a product of one one-cycle and $(n-1)/2$ transpositions. Thus, in the case of n odd, the cycle index polynomial is easily seen to be

$$\frac{1}{2n}\left(\sum_{d|n}\phi(d)x_d^{n/d}+nx_1x_2^{(n-1)/2}\right).$$

Now we consider the case n even. As noted above, there are two axes of symmetry. The elements fr^j with j odd correspond to flipping through an axis through a vertex. In this case, it is seen that the opposite vertex is also fixed. In this way, we see the cycle decomposition is a product of $(n-2)/2$ transpositions and 2 1-cycles. If j is even, there are no fixed points and the cycle decomposition of fr^j is simply a product of $n/2$ transpositions. In this case, the cycle index polynomial is

$$\frac{1}{2n}\left(\sum_{d|n}\phi(d)x_d^{n/d}+\frac{n}{2}x_1^2x_2^{(n-2)/2}+\frac{n}{2}x_2^{n/2}\right).$$

Pólya's theorem now tells us that the number of equivalence classes of maps is $P_G(\lambda,\lambda,...)$ where λ is the number of elements of Y. This shows:

THEOREM 7.3.3. *Under the action of the dihedral group, the number of distinct necklaces of length n formed using beads of λ colours is*

$$\frac{1}{2}\left(\sum_{d|n}\phi(n/d)\lambda^d+\lambda^{(n+1)/2}\right)$$

if n is odd and

$$\frac{1}{2}\left(\sum_{d|n}\phi(n/d)\lambda^d+\frac{1}{2}\lambda^{(n+2)/2}+\frac{1}{2}\lambda^{n/2}\right)$$

if n is even.

We conclude this section with one application of Pólya theory to chemistry. It seems that the historic origins of the theory are rooted in problems arising in chemistry.

The methane molecule has chemical composition CH_4 where C denotes a carbon atom and H is a hydrogen atom. This molecule has tetrahedral shape and the H_4 indicates that there are 4 atoms of hydrogen in the molecule positioned at the vertices of the tetrahedron, with the carbon atom at the centroid. The problem is to determine how many different molecules can be formed by replacing the hydrogen atoms with one of bromine, chlorine or fluorine. This question can be re-interpreted in the context of the colouring problems considered by Pólya theory.

Indeed, the group of symmetries of the regular tetrahedron is A_4, the alternating group on 4 letters. To see this, observe that we can rotate the tetrahedron about the center of any face and each of these correspond to 3-cycles, one for each face. This gives us a total of 8 3-cycles in the group of symmetries. There is one more symmetry given by a rotation by 180 degrees about the axis joining the center of opposite sides. This is easily seen to be a product of two transpositions and there are 3 such permutations. Together with the identity, we have the full group of symmetries.

It is now straightforward to write down the cycle index polynomial of the action of A_4 on the vertices of the regular tetrahedron. From the discussion above, we have

$$P_{A_4}(x_1, x_2, x_3, x_4) = \frac{1}{12}\left(x_1^4 + 8x_1x_3 + 3x_2^2\right).$$

The number of different molecules is then seen to be $P_{A_4}(3,3,3,3) = 15$. If the group of symmetries are not taken into account, we have $3^4 = 81$ ways of placing the atoms of bromine, chlorine or fluorine at the vertices of the tetrahedron. However, many of them clearly give the same molecule.

We make a few additional remarks concerning Pólya's theorem. In the special case that $G = S_n$ acting on the set $\{1, 2, ..., n\}$ in the usual way, the cycle index polynomial $P_{S_n}(\lambda, ...\lambda)$ is

$$\frac{1}{n!}\sum_{k=0}^{n} |s(n,k)|\lambda^k$$

where the $s(n,k)$'s denote the Stirling numbers of the first kind. This represents the number of ways of colouring n indistinguishable objects (or balls) using λ colours. This is related to a problem treated earlier by simpler methods. Indeed, this is the same as asking in how many ways we may put n indistinguishable balls into λ boxes. This is the same as the number of solutions of

$$x_1 + x_2 + \cdots + x_\lambda = n$$

with the x_i's non-negative integers. In either interpretation, it is easily seen that the number of ways is

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

Indeed, if we first consider a collection of n distinguishable balls and we throw into this collection $\lambda-1$ indistinguishable "sticks", then the number ways we can arrange these objects is clearly

$$(n+\lambda-1)!.$$

However, $\lambda-1$ of these objects are identical and can be permuted in $(\lambda-1)!$ ways and so we get our result. Now if we say the balls are also indistinguishable, then we can permute these among themselves in $n!$ ways. In this way, we retrieve an earlier formula, namely,

$$(\lambda+n-1)(\lambda+n-2)\cdots\lambda=\sum_{k=0}^{n}|s(n,k)|\lambda^k.$$

If we change λ to $-\lambda$, we get

$$(\lambda)_n=\sum_{k=0}^{n}s(n,k)\lambda^k.$$

Two further applications of the Pólya theory are amusing. The game of tic-tac-toe involves a 3×3 grid in which the players place alternately x or o until a row, column or diagonal of the same symbols are placed and the game is over. It is interesting to consider how many possible configurations can be seen at any given moment during a game. Or even, one may ask how many possible outcomes are there. This in its generality is too difficult to answer. We will consider a simpler problem. Namely, in how many ways can we colour a 3×3 grid using three colours. We can see that the cyclic group of order 4 operates by rotation on such a grid. If we label the grid as

1	2	3
6	5	4
7	8	9

then a clockwise rotation r is represented by the permutation

$$(1397)(2486)(5)$$

whereas r^2 is given by

$$(19)(28)(37)(64)(5).$$

Note that r^3 has the same cycle structure as r and so we easily see that the cycle index polynomial is

$$P(x_1, ..., x_9) = \frac{1}{4}\left(x_1^9 + 2x_1x_4^2 + x_1x_2^4\right).$$

A simple calculation shows that the number of colourings with three colours is 4995. Of course, some of these never can represent the final outcome or the shape of the grid during the game. For such a computation, one needs a finer Pólya theory with weights, which we do not consider here.

Let us now consider the problem of colouring the faces of the cube using λ colours. To do this, we begin by considering the group of symmetries of the cube. These can be classified as follows.

(1) the identity element;
(2) rotation by 90 degrees about the axis joining the center of two opposite faces;
(3) rotation by 180 degrees about the same axis;
(4) rotation by 180 degrees about the axis joining the midpoints of two diagonally opposite edges;
(5) rotation by 120 degrees about the axis determined by the diagonal of the cube.

If we think of these symmetries as acting on the faces, and write down the cycle structure, we obtain the following:

(1) 1 element of type 1^6;
(2) 6 elements of type $1^2 4^1$;
(3) 3 elements of type $1^2 2^2$;
(4) 6 elements of type 2^3;
(5) 8 elements of type 3^2.

Thus, we see the group of symmetries has order 24. One can easily see that this group is isomorphic to S_4. We can immediately write down the cycle index polynomial for S_4 acting on the faces of the cube from the above analysis:

$$P_{S_4}(x_1, ..., x_6) = \frac{1}{24}\left(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2\right).$$

By Pólya's theorem, the number of ways of colouring the faces of the cube using λ colours is

$$\frac{1}{24}\left(\lambda^6 + 12\lambda^3 + 3\lambda^4 + 8\lambda^2\right).$$

In particular, there are 10 ways of colouring the faces of the cube using 2 colours.

7.4. Exercises

EXERCISE 7.4.1. Show that the examples from the first section are actions of groups.

EXERCISE 7.4.2. Let G be a finite group acting on a finite set X. For each $g \in G$, define $\sigma_g(x) = g \cdot x$ for each $x \in X$. Show that σ_g is a permutation of X.

EXERCISE 7.4.3. Show that the map

$$g \mapsto \sigma_g$$

is a group homomorphism from G into $\mathrm{Sym}(X)$ which is the group of permutations of the set X.

EXERCISE 7.4.4. Let G be a group acting on a set X and H a group acting on a set Y. Assume that X and Y are disjoint and let $U = X \cup Y$. For $g \in G, h \in H$, define

$$(g, h) \cdot x := g \cdot x \, \text{if} \, x \in X$$

and

$$(g, h) \cdot y := h \cdot y \, \text{if} \, y \in Y.$$

Show that this defines an action of $G \times H$ on U.

EXERCISE 7.4.5. Determine the number of ways in which four corners of a square can be coloured using two colours. It is permissible to use single colour on all four corners.

EXERCISE 7.4.6. In how many ways can you colour the four corners of a square using three colours ?

EXERCISE 7.4.7. If $X = [3]$, define an action of S_3 on X by $\sigma \cdot i = \sigma(i)$ for $i \in X$ and $\sigma \in S_3$. Calculate the cycle index polynomial $P_{S_3}(x_1, x_2, x_3)$.

EXERCISE 7.4.8. In how many ways can you colour the vertices of an equilateral triangle so that at least two colours are used ?

EXERCISE 7.4.9. What is the number of graphs on 4 vertices ? What is the number of nonisomorphic graphs on 4 vertices ?

EXERCISE 7.4.10. Let G and H be finite groups acting on finite sets X and Y. Assume that X and Y are disjoint. By Exercise 7.4.3, we can define an action of $G \times H$ on $X \cup Y$. If P_G and P_H indicate the cycle index polynomials of G acting on X and H acting on Y respectively, show that the cycle index polynomial of $G \times H$ acting on $X \cup Y$ is $P_G P_H$.

EXERCISE 7.4.11. How many striped flags are there having six stripes (of equal width) each of which can be coloured red, white or blue ?

EXERCISE 7.4.12. What if we change the number of stripes to n and the number of colours to q ?

EXERCISE 7.4.13. Let S_n acting on the set $X = [n]$ in the usual way (as in Exercise 7.4.1). Let P_{S_n} be the cycle index polynomial. Prove that P_{S_n} is the coefficient of z^n in the power series expansion of

$$\exp(zx_1 + z^2x_2/2 + z^3x_3/3 + \dots).$$

EXERCISE 7.4.14. We say that $\sigma \in S_n$ has cycle type $(c_1, \dots, c_n)$ if σ has precisely c_i cycles of length i in its unique decomposition as a product of disjoint cycles. Show that the number of permutations of type $(c_1, c_2, \dots, c_n)$ is

$$\frac{n!}{1^{c_1}c_1!2^{c_2}c_2!\dots n^{c_n}c_n!}.$$

EXERCISE 7.4.15. Let P_n denote the path on n vertices. What is the automorphism group $\mathrm{Aut}(P_n)$ of P_n ?

EXERCISE 7.4.16. What is the cycle index polynomial of $\mathrm{Aut}(P_n)$ acting on the vertex set of P_n ?

EXERCISE 7.4.17. In how many ways can we colour the vertices of P_n using λ colours, up to the symmetry of $\mathrm{Aut}(P_n)$?

EXERCISE 7.4.18. Consider the graph X on 5 vertices obtained from the complete graph K_5 by deleting two edges incident to the same vertex. What is the automorphism group $\mathrm{Aut}(X)$ of X ?

EXERCISE 7.4.19. Let X be the graph from Exercise 7.4.18. What is the cycle index polynomial of $\mathrm{Aut}(X)$ acting on the vertex set of X ?

EXERCISE 7.4.20. In how many ways can we colour the vertices of X using λ colours, up to the symmetry of $\mathrm{Aut}(X)$?

CHAPTER 8

Matching Theory

8.1. The Marriage Theorem

A **matching** of a graph X is a collection of edges of X which are pairwise disjoint. The vertices incident to the edges of a matching M are **saturated** by M. A **perfect matching** is a matching that saturates all the vertices of X.

Given a bipartite graph X with bipartite sets A and B, we would like to know when there is a matching such that each element of A is matched to an element of B uniquely, i.e., a matching that saturates A. Thus, a matching is a one-to-one map $f : A \rightarrow B$ such that $(a, f(a))$ is an edge of the bipartite graph X.

This question arises in many "real life" contexts: A could be a set of jobs a company would like to fill and B could be a set of candidates applying for the jobs. We would join $a \in A$ to $b \in B$ if b is qualified to do job a. Then the matching question is whether all the jobs can be filled. In another example, A could be a set of patients and B could be a set of drugs. Some patients being allergic to certain drugs, one would like to match each patient to a drug the patient is not allergic to such that each drug is taken by at most one subject.

This question was formulated in "matrimonial terms" and solved by Philip Hall (1904-1982) in 1935. His theorem goes under the appellation of the 'marriage theorem'. Suppose we have a set of n girls and n boys. We would like to match each girl to a boy she likes. Under what conditions can we match all the girls? We can encode this information as a bipartite graph X, with A being the set of girls, B the set of boys. We join vertex $a \in A$ to $b \in B$ if a likes b. Clearly, for a matching to be possible, each girl must like at least one boy. If we have a situation where two girls like only one boy, then we have a problem and the matching question cannot be solved.

More generally, a necessary condition is that for any subset S of A, if we let $N(S)$ be the set of boys liked by some girl in S, then we need $|N(S)| \geq |S|$. Hall's theorem is that this obvious necessary condition is also sufficient. This is one of the simplest, yet powerful, theorems in mathematics with far-reaching applications.

THEOREM 8.1.1 (Marriage Theorem). *Let X be a bipartite graph with partite sets A and B. There exists a matching that saturates A if and only if for every subset S of A, we have*

$$|N(S)| \geq |S|$$

where $N(S)$ is the set of neighbours of S.

PROOF. The proof is by induction on the number of vertices in A. The base case $|A| = 1$ is trivial since a matching that saturates A consists of one edge in this case. Assume now that $|A| \geq 2$.

First suppose that

$$|N(S)| \geq |S| + 1$$

for every proper subset S of A, i.e., a subset $S \subset A$ with $S \neq \emptyset$ and $S \neq A$. By deleting one edge ab of X with $a \in A, b \in B$ (together with the incident vertices a and b) we obtain a bipartite graph Y with parts $A' = A \setminus \{a\}$ and $B' = B \setminus \{b\}$. In this graph, our partite set $A' = A \setminus \{a\}$ has fewer elements than A. Every subset S of A' satisfies Hall's condition $|N(S)| \geq |S|$ and by induction there is a matching that saturates A' in Y. Together with the deleted edge xy, we obtain a matching in X that saturates A. This finishes the proof of this case.

If the condition

$$|N(S)| \geq |S| + 1$$

is not satisfied for all proper subsets of A, then for some proper subset S_0 of A, we have

$$|N(S_0)| = |S_0|.$$

The subgraph X_1 with partite sets S_0 and $N(S_0)$ satisfies Hall's condition and so by induction, we have a matching M_1 that saturates S_0 in X_1. The subgraph X_2 with partite sets $A \setminus S_0$ and $B \setminus N(S_0)$ also satisfies Hall's condition for if some subset $C \subseteq A \setminus S_0$ is such that

$$|N_{X_2}(C)| < |C|,$$

(where the notation $N_{X_2}(C)$ refers to the neighbours of C in X_2) then

$$|N_X(S_0 \cup C)| \leq |N_X(S_0)| + |N_{X_2}(C)| < |S_0| + |C|$$

contrary to Hall's condition. It follows that there is a matching M_2 that saturates $A \setminus S_0$ in X_2. We deduce that $M_1 \cup M_2$ is a matching of X that saturates A. This completes the proof. ∎

8.2. Systems of Distinct Representatives

Suppose S is a finite set and $A_1, ..., A_n$ are subsets. When is it possible to choose n distinct elements $a_1, ..., a_n$ with $a_i \in A_i$? The marriage theorem answers this question.

THEOREM 8.2.1. *A system of distinct representatives $a_1, ..., a_n$ with $a_i \in A_i$ can be chosen from a collection $A_1, ..., A_n$ of subsets of a set S if and only if*

$$|\cup_{i \in I} A_i| \geq |I|$$

for every subset I of $\{1, ..., n\}$.

PROOF. Consider the bipartite graph X with partite sets A and B. The vertices of A correspond to the subsets A_i $(1 \leq i \leq n)$ and the vertices of B are the elements of S. We join A_i in A to a vertex $a_j \in B$ if and only if $a_j \in A_i$. Choosing a set of distinct representatives is equivalent to finding a matching in X and the condition of the theorem is precisely Hall's condition. ∎

COROLLARY 8.2.2. *In a bipartite graph X with partite sets A and B there is a matching of A if for some k, we have* deg $(a) \geq k$ *for all $a \in A$ and* deg $(b) \leq k$ *for all $b \in B$.*

PROOF. We verify Hall's condition. For any subset S of A, at least $k|S|$ edges emanate from S. Since deg $(b) \leq k$ for all $b \in B$, these edges must be incident with at least

$$\frac{1}{k}(k|S|) = |S|$$

vertices of B. ∎

EXAMPLE 8.2.3. At a party, if every boy knows at least k girls and every girl knows at most k boys, then it is possible to match every boy with a girl he knows.

EXAMPLE 8.2.4. A **Latin square** is an $n \times n$ array on n symbols such that every symbol appears in each row and each column exactly once. For instance, the multiplication table for a finite group of order n would be an example of a Latin square. A $r \times n$ **Latin rectangle** is a $r \times n$ matrix on n symbols such that every symbol appears once in each row and at most once in each column. The first r rows of a Latin square form a $r \times n$ Latin rectangle.

A classical question is to determine if given a $r \times n$ Latin rectangle that uses the symbols $\{1, 2, ..., n\}$, it is possible to complete it to give a Latin square. The marriage theorem allows us to deduce that we can always do this. We construct a bipartite graph as follows. Let A_i

be the set of elements of $[n]$ **not** used in the i-th column. Choosing a system of distinct representatives for the A_i's would allow us to add one more row that can be inductively completed to produce a Latin square. This can be done if Hall's condition is satisfied. However, the bipartite graph with partite sets A consisting of the A_i's and B consisting of the elements of $[n]$ and we join A_i to $b \in B$ if and only if $b \in A_i$ has the property that deg $(A_i) = n - r$ for all i. Clearly, deg $(b) = n - r$ because each entry has been used exactly once for each row. By Corollary 8.2.2, we are done.

A pair of Latin squares (a_{ij}) and (b_{ij}) are called **orthogonal** if the n^2 pairs (a_{ij}, b_{ij}) are all distinct. For example, the two Latin squares on two elements

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

are not orthogonal since the pair matrix

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

is not a matrix of distinct entries.

In the 1780's, Euler showed how to construct $n \times n$ orthogonal Latin squares when n is odd or divisible by 4. He also conjectured that one cannot construct a pair of orthogonal Latin squares for all $n \equiv 2 \pmod 4$. The case $n = 6$ is also known as the **thirty-six officers problem**. It asks if it is possible to arrange 6 regiments of 6 officers each of different ranks in 6×6 square so that no rank or regiment will be repeated in a row or column. In 1900, Gaston Tarry (1843-1913) proved that this problem has no solution by checking all the possible arrangements of symbols.

In 1960, Raj Chandra Bose (1901-1987), Sharadchandra Shankar Shrikhande and Ernest Tilden Parker (1926-1991) showed that Euler's conjecture is false for $n > 6$. This means that $n \times n$ orthogonal Latin squares exist for all $n \geq 3$ except $n = 6$.

8.3. Systems of Common Representatives

Suppose we are given two collections of subsets $A_1, ..., A_n$ and $B_1, .., B_n$ of a set S. A set of elements $a_1, ..., a_n$ is said to be a **system of common representatives** if $\{a_1, ..., a_n\}$ is a system of distinct representatives for both $A_1, ..., A_n$ and $B_1, ..., B_n$. We consider the problem of when we can find a system of common representatives. In case one of the collections is a partition of S (or even a disjoint collection) this is an immediate consequence of the marriage theorem.

THEOREM 8.3.1. *A system of common representatives exists if and only if the union of any k of the sets A_i is not contained in the union of any $k-1$ of the sets B_j.*

PROOF. We construct a bipartite graph X in which the partite set A corresponds to the sets A_i and the set B correspond to the sets B_j. We join A_i to B_j if $A_i \cap B_j \neq \emptyset$. Clearly the existence of a complete matching is equivalent to the existence of a system of common representatives. The condition of the theorem is precisely Hall's condition. ∎

THEOREM 8.3.2. *Let G be a finite group, H and K subgroups of the same order. Then we can find elements $x_1, ..., x_r$ in G such that*

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_r = x_1K \cup x_2K \cup \cdots x_rK.$$

PROOF. We apply Theorem 8.3.1 with the A_i's being the right cosets of H and the B_j's being the left cosets of K. Since these cosets are disjoint, the condition of Theorem 8.3.1 is clearly satisfied simply by a cardinality count. Thus, it is possible to choose a system of common representatives and this is precisely the statement of the Theorem. ∎

COROLLARY 8.3.3. *If G is a finite group and H a subgroup, then it is possible to choose $x_1, ..., x_r$ so that $x_1H, ...x_rH$ is a complete set of left cosets of H and $Hx_1, ..., Hx_r$ is a complete set of right cosets of H.*

8.4. Doubly Stochastic Matrices

We now prove a famous theorem in the theory of doubly stochastic matrices using the marriage theorem. This result is the Birkhoff-von Neumann theorem that states that every doubly stochastic matrix is a convex combination of permutation matrices. Recall that a matrix $A = (a_{ij})$ is called **doubly stochastic** if every row sums to 1 and every column sums to 1. Such matrices arise naturally in probability theory. A **permutation matrix** is a doubly stochastic matrix in which a_{ij} is 0 or 1. Thus, every row and every column of a permutation matrix contains a single 1 and the rest of the entries are zero. The set of $n \times n$ permutation matrices forms a group isomorphic to the symmetric group on permutations on n letters.

THEOREM 8.4.1 (Birkhoff 1946, von Neumann 1953). *Every doubly stochastic matrix can be written as a linear combination of permutation matrices.*

PROOF. Let $M = (a_{ij})$ be a doubly stochastic matrix. We define a bipartite graph X with partite sets A and B. The vertices of A will be the rows R_i of A and the vertices of B will be the columns C_j of A. We join a row R_i to a column C_j if $a_{ij} \neq 0$. We claim that this bipartite graph satisfies Hall's condition. Indeed, suppose that $|N(S)| < |S|$ for some subset S of A. Let $|S| = s$. The previous inequality implies that there are s rows R_i with fewer than s neighbours. If we list our rows horizontally, the neighbours are precisely the columns in which the rows have non-zero entries. Adding up all the entries of each row gives a total of s. Doing the same column-wise gives us a sum of $< s$, which is a contradiction. Thus, Hall's condition is satisfied and there is a matching. The existence of a matching means we may select n non-zero entries of M in such a way that each row and each column contains exactly one of them. Of all these non-zero entries, let c_1 be one of least value. Thus, we can write

$$M = c_1 P_1 + R$$

where P_1 is a permutation matrix. Moreover, $(1 - c_1)^{-1} R$ is again a doubly stochastic matrix but with one less non-zero entry. Thus, the proof is completed by inducting on the number of non-zero entries. ■

8.5. Weighted Bipartite Matching

We now consider a weighted bipartite graph $K_{n,n}$ with non-negative weights w_{ij} corresponding to the edge (i, j). Our goal is to find a **maximal transversal**, that is, a matching so that the sum of the weights of the edges in the matching is maximal among all matchings. For the sake of simplicity, we assume that the weights are non-negative integers (which is usually not a restriction in practice). Let $W = (w_{ij})$ be the weight matrix.

The algorithm to find a maximal matching that we now describe is called the **Hungarian algorithm**. It was first discovered by Harold Kuhn in 1955 and later revised by James Munkres in 1957. The algorithm is based on the work of two Hungarian mathematicians Denes König (1884-1944) and Jenö Egervâry (1891-1958) and Kuhn named it the Hungarian algorithm in their honour.

The goal of finding a maximal matching is facilitated by supplementary "weights". We say a collection of numbers $u = (u_1, ..., u_n)$ and $v = (v_1, ..., v_n)$ is a **weighted cover** for W if

$$w_{ij} \leq u_i + v_j \qquad \forall 1 \leq i, j \leq n.$$

The **cost** of a cover is defined as

$$c(u, v) := \sum_i u_i + \sum_j v_j.$$

LEMMA 8.5.1. *For any matching M and any weighted cover, we have*

$$c(u,v) \geq w(M)$$

where $w(M)$ is defined as the sum of the weights of the edges in M. Moreover, $c(u,v) = w(M)$ if and only if M is a matching with maximal weight.

PROOF. The first part of the lemma is clear simply by summing over all the edges of the matching the inequality

$$w_{ij} \leq u_i + v_j.$$

Thus, there is no matching with weight greater than $c(u,v)$ for any cover and the maximal weight is at most the minimal cost of a cover. If $c(u,v) = w(M)$, then we must have the equality

$$w_{ij} = u_i + v_j$$

for all edges of the matching and this must be a matching of maximal weight. ∎

This lemma is the basis of the Hungarian algorithm. As we mentioned before, we suppose w_{ij} are non-negative integers and this is not any stringent restriction. We begin by choosing an arbitrary cover, which can easily be done simply by choosing u_i to be the largest weight in the i-th row and v_i to be zero. Clearly,

$$w_{ij} \leq u_i + v_j$$

is satisfied with this choice. Next, we form a bipartite graph $X_{u,v} = (A, B)$ where the vertices of A are the rows of the matrix W and the vertices of B are the columns. We join row i to column j if and only if $w_{ij} = u_i + v_j$. If we have a perfect matching in this graph, we are done by the lemma. Otherwise, Hall's condition is not satisfied and so there is a set of m rows "adjacent" to fewer than m columns. If for each of these rows, we decrease u_i by 1 and increase v_j by 1, and thus get a new sequence $u'_1, ..., u'_n$ and $v'_1, ..., v'_n$, the inequality

$$w_{ij} \leq u'_i + v'_j$$

is satisfied. To see this, note that if i, j are not related this is clear since we have the strict inequality $w_{ij} < u_i + v_j$. If i, j are related then the sum $u_i + v_j$ has not changed. We have thus obtained a new cover whose cost is smaller than the earlier one simply because Hall's condition is violated. The claim is that this converges to the minimal cost and thus the maximal weight transversal. This is clear since we must arrive at a matching for otherwise, we can lower the cost of the cover and this cannot go on endlessly.

To see how to work this algorithm in practice, it is best to use matrices. We illustrate this to determine a maximal transversal in the matrix

$$\begin{pmatrix} 4 & 1 & 6 & 2 & 3 \\ 5 & 0 & 3 & 7 & 6 \\ 2 & 3 & 4 & 5 & 8 \\ 3 & 4 & 6 & 3 & 4 \\ 4 & 6 & 5 & 8 & 6 \end{pmatrix}.$$

We will write the cost covers above the columns and along the rows. The initial cost cover is obtained by simply taking the largest weight in each row. We write the matrix whose entries are $u_i + v_j - w_{ij}$ alongside:

$$\begin{array}{c|ccccc} & 0 & 0 & 0 & 0 & 0 \\ \hline 6 & 2 & 5 & 0 & 4 & 3 \\ 7 & 2 & 7 & 4 & 0 & 1 \\ 8 & 6 & 5 & 4 & 3 & 0 \\ 6 & 3 & 2 & 0 & 3 & 2 \\ 8 & 4 & 2 & 3 & 0 & 2 \end{array}.$$

This gives rise to the "equality subgraph" :

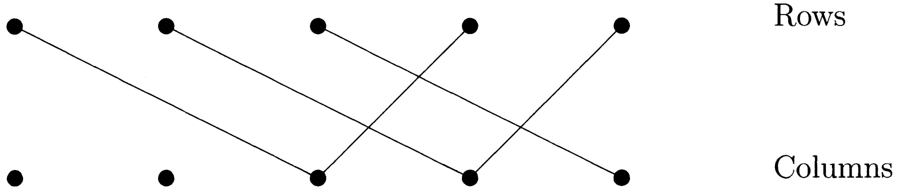


FIGURE 8.1

We can decrease u_i's by 1 and increase v_3, v_4, v_5 by 1 and re-write the matrix whose entries are $u_i + v_j - w_{ij}$ given by this new cover:

$$\begin{array}{c|ccccc} & 0 & 0 & 1 & 1 & 1 \\ \hline 5 & 1 & 4 & 0 & 4 & 3 \\ 6 & 1 & 6 & 4 & 0 & 1 \\ 7 & 5 & 4 & 4 & 3 & 0 \\ 5 & 2 & 1 & 0 & 3 & 2 \\ 7 & 3 & 1 & 3 & 0 & 2 \end{array}$$

and we draw the equality subgraph again getting the same graph as before. Thus, we can reduce all the u_i's by 1 and increase the v_3, v_4, v_5

by 1. Repeating the process once more gives:

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

where we have indicated a transversal by an asterisk. Since we have found a transversal, we can determine the cost as the sum of the u_i's and v_j's which we see to be 31.

If we were interested in a minimal transversal, all we need to do is to take the maximum M of all the entries and replace our weights w_{ij} by $M - w_{ij}$ and repeat the above algorithm.

8.6. Matchings in General Graphs

In a bipartite graph X with bipartite sets A and B, the marriage theorem gives a necessary and sufficient condition for the existence of a matching that saturates A. For general graphs, the following theorem gives a necessary and sufficient condition for the existence of a perfect matching. It was proved by William Tutte (1917-2002) in 1947. Tutte was one of the leading mathematicians in graph theory and combinatorics. In 1935, he began his studies at Cambridge in chemistry, but soon after he became interested in mathematics. During World War II, he worked at Bletchley Park as a code breaker and he was able to deduce the structure of a German encryption machine using only some intercepted encrypted messages.

An **odd component** of a graph H is a component of H with an odd number of vertices. Let $\mathrm{odd}(H)$ denote the number of odd components of H.

THEOREM 8.6.1 (Tutte 1947). *A graph X contains a perfect matching if and only if*

$$\mathrm{odd}(X \setminus S) \leq |S| \tag{8.6.1}$$

for each $S \subset V(X)$.

PROOF. If X has a perfect matching and S is a subset of vertices of X, then each odd component of $X \setminus S$ has a vertex adjacent to a vertex in S. This means $\mathrm{odd}(X \setminus S) \leq |S|$.

The proof of sufficiency is more complicated. We start it here and invite the reader to complete it.

Assume that condition (8.6.1) is satisfied for all $S \subset V(X)$. Note that by adding edges to X, condition (8.6.1) is preserved (Prove this).

The theorem is true unless there exists a graph X that has no perfect matchings and adding any missing edges would create a graph with a perfect matching.

Let X be such a graph. We will obtain a contradiction by showing that X actually contains a perfect matching.

Let C denote the set of vertices whose degree is $|V(X)| - 1$. If $X \setminus C$ is formed by disjoint complete graphs, then one can find a perfect matching easily. The case when $X \setminus C$ is not a union of disjoint cliques is left as an exercise. ∎

Tutte's theorem was later extended by Claude Berge (1926-2002) in 1958. Berge was one of the leading mathematicians in graph theory and combinatorics in the last century. His result gives a formula for $\nu(X)$ which is the size of a largest matching of a general graph. By size we mean the number of edges in the matching.

THEOREM 8.6.2 (Berge 1958). *For a graph X,*

$$\nu(X) = \frac{1}{2}\left(n - \max_{S \subset V(X)} (\mathrm{odd}(X \setminus S) - |S|)\right).$$

8.7. Connectivity

Recall that a graph X is called connected if any two of its vertices are connected by a path. A graph is **disconnected** if it is not connected. A component of X is a maximal connected subgraph of X. This notions can be extended as follows. The **vertex-connectivity** $\kappa(X)$ of X equals the minimum size of a subset of vertices of X whose deletion disconnects X. The **edge-connectivity** $\kappa'(X)$ of X equals the minimum size of a subset of edges of X whose deletion disconnects X. Thus, a graph is connected if and only if its (vertex- or edge-)connectivity is non-zero. By convention, $\kappa(K_n) = \kappa'(K_n) = n - 1$. In general, the following inequalities hold in any connected graph.

LEMMA 8.7.1. *If X is a connected graph, then*

$$1 \leq \kappa(X) \leq \kappa'(X) \leq \delta(X)$$

where $\delta(X)$ denotes the minimum degree of X.

PROOF. If X is connected, then obviously $\kappa(X) \geq 1$. Also, if x is a vertex of X whose degree equals $\delta(X)$, then deleting the $\delta(X)$ edges incident to x disconnects the graph X. Thus, $\kappa'(X) \leq \delta(X)$.

If $X = K_n$ or if $\kappa'(X) = 1$, then the inequality $\kappa(X) \leq \kappa'(X)$ holds as well. Assume that X is not a complete graph and $\kappa(X) \geq 2$. Let $x_1y_1, \ldots, x_ky_k$ be a set of $k = \kappa'(X)$ edges whose removal disconnects

X. If removing $\{x_1, \ldots, x_k\}$ disconnects X, then $\kappa(X) \leq k = \kappa'(X)$ and we are done. Otherwise, it means that the degree of each x_i is at most k which implies that $\kappa(X) \leq k$. ∎

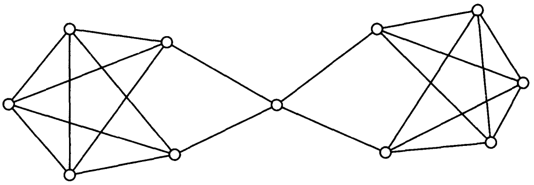


FIGURE 8.2. A 4-regular graph with $\kappa = 1$ and $\kappa' = 2$

A graph X is called k-connected if $\kappa(X) \geq k$. This means that the deletion of any $k-1$ vertices of X will not disconnect X. Similarly, X is called k-edge-connected if $\kappa'(X) \geq k$. Thus, a graph is 1-connected if and only if it is connected. The following result provides a necessary and sufficient condition 2-connectivity. We leave its proof as an exercise.

THEOREM 8.7.2. *A graph X is 2-connected if and only if any two vertices of X lie on a common cycle.*

The fundamental result involving graph connectivity was proved by Karl Menger (1902-1985) in 1927. Menger's theorem is an example of a min-max theorem. Given a graph X and two vertices $x \neq y$ of X, let $\kappa(x, y)$ denote the minimum number of vertices of X whose removal separates x from y. Also, two paths from x to y are called **independent** if they have only x and y in common.

THEOREM 8.7.3. *(a) Let x and y be two distinct nonadjacent vertices of a graph X. Then $\kappa(x, y)$ equals the minimum number of independent paths from x to y.*
(b) Let x and y be two vertices of X. Then the minimal number of edges whose removal separates x from y equals the minimum number of edge-disjoint paths from x to y.

PROOF. One inequality is obvious. If there are r independent paths from x to y, then deleting exactly one internal vertex from each path will separate x from y. The other inequality is left as an exercise. ∎

Menger's theorem gives the following necessary and sufficient for a graph to be k-connected or k-edge-connected.

COROLLARY 8.7.4. *(a) For $k \geq 2$, a graph X is k-connected if and only if it has at least two vertices and there are k independent paths between any two vertices.*
(b) For $k \geq 2$, a graph X is k-edge-connected if and only if it has at least two vertices and there are k edge-disjoint paths between any two vertices.

Menger's theorem is a very powerful result with many consequences in discrete mathematics. The interested reader may try to apply it to prove the Marriage Theorem for example.

8.8. Exercises

EXERCISE 8.8.1. A building contractor advertises for a bricklayer, a carpenter, a plumber and a toolmaker; he has five applicants - one for the job of bricklayer, one for the job of carpenter, one for the jobs of bricklayer and plumber, and two for the jobs of plumber and toolmaker. Can the jobs be filled? In how many ways?

EXERCISE 8.8.2. If in a party, every male knows at least k females and every female knows at most k males, show that it is possible to match every male with a female he knows.

EXERCISE 8.8.3. A **permutation matrix** is a $0, 1$ matrix having exactly one 1 in each row and column. Prove that a square matrix of non-negative integers can be expressed as a sum of k permutation matrices if and only if all row sums and column sums are equal to k.

EXERCISE 8.8.4. Let $X = (A, B)$ be a bipartite graph and suppose that A satisfies Hall's condition. Suppose further that each vertex of A is joined to at least t elements of B. Show that the number of matchings that saturate A is at least $t!$ if $t \leq |A|$.

EXERCISE 8.8.5. Show that there are at least $n!(n-1)! \cdots 2!1!$ Latin squares of order n. Show that this quantity is larger than $2^{(n-1)^2}$ for $n \geq 5$.

EXERCISE 8.8.6. There are rs couples in a party. The men are divided into r age groups with s men in each group. The women are divided into r height groups with s women in each group. Show that it is possible to select r couples so that all age groups and all height groups are represented.

EXERCISE 8.8.7. Find a minimum weight transversal in the matrix below.

$$\begin{pmatrix} 4 & 5 & 8 & 10 & 11 \\ 7 & 6 & 5 & 7 & 4 \\ 8 & 5 & 12 & 9 & 6 \\ 6 & 6 & 13 & 10 & 7 \\ 4 & 5 & 7 & 9 & 8 \end{pmatrix}.$$

EXERCISE 8.8.8. Determine whether or not the graph in Figure 8.3 has a perfect matching. If not, what is the size of a largest matching ?

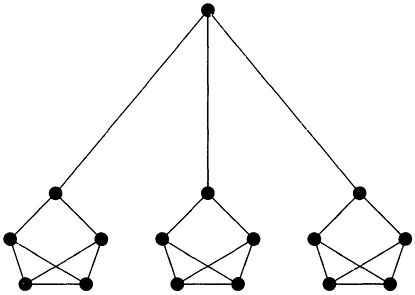


FIGURE 8.3

EXERCISE 8.8.9. For each $k \geq 2$, construct a k-regular graph on an even number vertices containing no perfect matchings. For each $k \geq 3$, construct k-regular graphs X such that $1 \leq \kappa(X) < \kappa'(X) < k$.

EXERCISE 8.8.10. Show that in the complete graph K_{2n} the number of perfect matchings is $(2n)!/2^n n!$.

EXERCISE 8.8.11. Let $W = (w_{ij})$ an $n \times n$ matrix of non-negative weights. Define a function f on the set of $n \times n$ doubly stochastic matrices by setting for $A = (a_{ij})$,

$$f(A) = \sum_{i,j} a_{ij} w_{ij}$$

where the summation is over all indices i, j. Show that f attains its maximum value at a permutation matrix.

EXERCISE 8.8.12. Let $t \geq 0$ be an integer. If X is bipartite graph with bipartite sets A and B such that $|N(S)| \geq |S| - t$ for each $S \subset A$, then X contains a matching that saturates $|A| - t$ vertices of A.

EXERCISE 8.8.13. Let $t \geq 1$ be an integer. If X is bipartite graph with bipartite sets A and B such that $|N(S)| \geq t \cdot |S|$ for each $S \subset A$, then each $a \in A$ has a set S_a of t neighbours in B with $S_a \cap S_{a'} = \emptyset$ for each $a \neq a' \in A$.

EXERCISE 8.8.14. Let A be a matrix with entries 0 or 1. Show that the minimum number of rows and columns that contain all the 1's of A equals the maximum number of 1's in A, no two on the same row or column.

EXERCISE 8.8.15. Finish the proof of Theorem 8.6.1.

EXERCISE 8.8.16. Show that any 3-regular graph with no bridges contains a perfect matching.

EXERCISE 8.8.17. Prove that every tree has at most one perfect matching.

EXERCISE 8.8.18. Show that a tree T has a perfect matching if and only if $\text{odd}(T \setminus x) = 1$ for any vertex x of T.

EXERCISE 8.8.19. Let X be a bipartite graph with bipartite sets A and B such that $|N(S)| > |S|$ for each $S \subset A$. Show that for any edge e of X, there exists a matching that contains e and saturates A.

EXERCISE 8.8.20. Let $V_1, \dots, V_n$ be subsets of a vector space V. Then $V_1, \dots, V_n$ has a linearly independent system of distinct representatives if and only if

$$\dim(\cup_{i \in I} V_i) \geq |I|$$

for each $I \subset [n]$.

CHAPTER 9

Block Designs

9.1. Gaussian Binomial Coefficients

Let V be an n-dimensional vector space over the finite field $\mathbf{F}_q$ of q elements. We would like to determine the number of subspaces of dimension k. For example, the number of 1-dimensional subspaces is easily found as these are subspaces spanned by one element. Such an element must be non-zero and there are $q^n - 1$ ways of choosing such an element. But for each choice, any non-zero scalar multiple of it will generate the same subspace as there are $q - 1$ such multiples for any fixed vector, we get a final tally of

$$\frac{q^n - 1}{q - 1}$$

for the number of 1-dimensional subspaces of V. This gives us a clue of how to determine the general formula.

Each subspace of dimension k has a basis of k elements. Let us first count in how many ways we can write down a basis for a k-dimensional subspace of V. For the first vector, we have $q^n - 1$ choices. For the second, we have $q^n - q$ choices since we must not pick any scalar multiple of the first vector chosen. For the third vector, we have $q^n - q^2$ such vectors since we should not pick any linear combination of the first two chosen. In this way, we see that the number of ways of writing down a basis for a k-dimensional subspace is

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1}).$$

On the other hand, any k-dimensional subspace is isomorphic to $\mathbf{F}_q^k$ and the number of bases it has correspond to the number of $k \times k$ non-singular matrices over $\mathbf{F}_q$. This number is easily seen to be

$$(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}).$$

Therefore, we obtain:

THEOREM 9.1.1. *Let V be a vector space of dimension n over $\mathbf{F}_q$. The number of k-dimensional subspaces in V is*

$$\binom{n}{k}_q := \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

REMARK 9.1.2. We refer to the numbers enumerated in the theorem as the q-binomial coefficients or sometimes as the Gaussian binomial coefficients. The reason for this will become apparent as we proceed. But for now, let us observe that if we think of q as a real number and take limits as $q \to 1^+$, we obtain by l'Hôspital's rule that

$$\lim_{q\to 1^+} \binom{n}{k}_q = \binom{n}{k},$$

and for this reason (and others), these numbers have properties similar to the binomial coefficients. This perspective has proved useful in trying to obtain q-analogs of classical binomial identities and to understand their meaning from the standpoint of these subspaces.

Let us observe that we could have done this count in another way. Indeed, to any ordered basis, we can associate a $k \times n$ matrix with the basis vectors being the rows. We can view our subspace of dimension k as the row span of this matrix. The row span is unchanged if we perform "row operations" on it as follows. We can multiply any row by a non-zero scalar. We can add one row to another. We can interchange rows. This allows us to speak about the reduced row echelon form of a matrix. This form is characterized by the fact that the first non-zero entry of each row is a 1. For any row, all the entries preceding the leading 1 are zero. If a column contains a leading 1, then all its other entries are zero. For example, if $n = 4$ and $k = 2$, the possible echelon forms are given by

$$\begin{pmatrix}1&0&*&*\\0&1&*&*\end{pmatrix},\quad \begin{pmatrix}1&*&0&*\\0&0&1&*\end{pmatrix},\quad \begin{pmatrix}1&*&*&0\\0&0&0&1\end{pmatrix},$$
$$\begin{pmatrix}0&1&0&*\\0&0&1&*\end{pmatrix},\quad \begin{pmatrix}0&1&*&0\\0&0&0&1\end{pmatrix},\quad \begin{pmatrix}0&0&1&0\\0&0&0&1\end{pmatrix},$$

where $*$ denotes any element of $\mathbf{F}_q$. It is clear that every subspace of dimension k has a unique echelon form. Thus, the number of subspaces of dimension k is equal to the number of echelon forms for a $k \times n$ matrix over $\mathbf{F}_q$. In the above example, this number is easily seen to be

$$q^4+q^3+2q^2+q+1 = \frac{(q^4-1)(q^4-q)}{(q^2-1)(q^2-q)}.$$

We now establish the q-analog of Pascal's triangle.

THEOREM 9.1.3.

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

PROOF. We prove this by counting the number of reduced row echelon forms. The left hand side is the number of reduced row echelon forms of a $k \times (n+1)$ matrix over $\mathbf{F}_q$. Such an echelon form either has a leading 1 in the $(k, n+1)$-entry or it does not. For those that do, we see that the $(k-1) \times n$ matrix formed by the first $k-1$ rows and first n columns is in echelon form and their number is

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

If the $(k, n+1)$ entry is not a leading 1, then the last column of such a reduced row echelon form has arbitrary entries. The $k \times n$ submatrix obtained by taking the first n columns is in reduced row echelon form and thus counts the number of subspaces of dimension k in an n-dimensional vector space. This number is

$$\binom{n}{k}_q .$$

As we have q^k choices for the last column, we obtain

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

This completes the proof. ■

Note that this reduces to the usual recurrence relation for binomial coefficients when $q = 1$.

THEOREM 9.1.4.

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

PROOF. This follows by observing that there is a bijection between the k-dimensional subspaces and the $n-k$-dimensional subspaces of the dual space. This can also be verified directly as follows. Note that

$$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)(q^{n-k}-1)(q^{n-k-1}-1)\cdots(q-1)}$$

which is clearly symmetric under the map $k \mapsto n-k$. ■

By applying Theorem 9.1.3, we deduce another recurrence:

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

We will use this to prove:

THEOREM 9.1.5 (The q-binomial theorem). *For $n \geq 1$,*

$$\prod_{i=0}^{n-1}(1+q^i t) = \sum_{k=0}^{n} \binom{n}{k}_q q^{\binom{k}{2}} t^k.$$

PROOF. We use induction on n. For $n = 1$, both sides of the equation at $1 + t$. Suppose that the result is true for n. Then,

$$\prod_{i=0}^{n}(1+q^i t) = (1+q^n t)\left(\sum_{k=0}^{n} \binom{n}{k}_q q^{\binom{k}{2}} t^k\right).$$

The coefficient of t^k on the right is

$$q^{\binom{k}{2}} \binom{n}{k}_q + q^{\binom{k-1}{2}} \binom{n}{k-1}_q q^n$$

which is equal to

$$q^{\binom{k}{2}} \left(\binom{n}{k}_q + q^{n-k+1} \binom{n}{k-1}_q\right) = q^{\binom{k}{2}} \binom{n+1}{k}_q,$$

as desired. ■

9.2. Introduction to Designs

Design theory has its origin in statistics where one must set up experiments or "clinical trials" to test the reliability of a product. Consider the following problem. Suppose that we have 7 volunteers to test 7 products. Each person is willing to test 3 products and each product should be tested by 3 people to ensure objectivity. Can we arrange the experiment so that any two people would have tested precisely one product in common?

Surprisingly, a solution is provided to this problem by the *Fano plane* (see Figure 9.1). This name honors Gino Fano (1871-1952) who was one of the pioneers of projective geometry. Consider the triangle of three points; we join each vertex to midpoint of the opposite side. The three midpoints are then joined by a circle. In this way, we have 7 points and 7 "lines". Each line would represent a product and the three vertices on a line would mark out three volunteers to test that particular product. Since any two points determine a unique line, we deduce that any two people test precisely one product in common. Observe that in this situation, we have by "duality" that any two products are simultaneously tested by precisely one person.

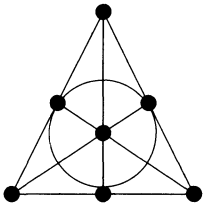


FIGURE 9.1. The Fano plane

Here is another famous problem, called Kirkman's schoolgirls problem. Thomas Kirkman (1806-1895) published this problem in *Lady's and Gentleman's Diary* in 1850. Fifteen schoolgirls walk home each day in five groups of three. Is it possible to arrange the walks over a one week period so that any two girls walk precisely once together in a group. Here is a solution. Consider the vector space $\mathbf{F}_2^4$ and remove the zero vector. We then have 15 vectors. Consider triples of vectors $\{x, y, z\}$ such that $x + y + z = 0$. The number of such vectors is 35 since we have 15 choices for x, 14 choices for y and then z is uniquely determined. Note that necessarily, these are distinct triples since if two of them were equal, we get the other vector must be zero, which we have removed. The number of ordered triples is 15×14 and we must divide this number by $3! = 6$ to get 35. Each triple corresponds to a 2-dimensional vector space of $\mathbf{F}_2^4$. It is now possible to arrange the solution vectors in 7 groups so that in each group, we have 5 triples and the union of the triples is the set of fifteen vectors. Thus, if we think each schoolgirl corresponding to a vector, this configuration gives us the solution.

To understand precisely what is behind this solution, we must understand the theory of combinatorial designs. It might be more illuminating to consider the following set up. Let X be a set of v volunteers, B a set of b products or "blocks" as they are called in the theory. We require that each volunteer test r products and each product should be tested by k people. In addition, we require that any pair of people together test precisely λ products. Can such an experiment be arranged?

We can represent this situation by a bipartite graph (X, B), where X consists of the set of v volunteers, B the set of b blocks. We join a vertex of X to a vertex of B if the corresponding person is to test that particular product. The conditions tell us that the degree of every vertex in X is r, and the degree of every vertex in B is k. The final condition tells us that any pair of vertices of X have precisely λ common neighbors. We can get immediately some necessary conditions for such a configuration to exist. Indeed, we can count the number of edges by going through the vertices of X or by going through the vertices of B. We deduce that

$$vr = bk.$$

Now let us construct another bipartite graph in which the vertices are pairs of vertices. We join a pair to a block if they occur in that block. This gives $v(v-1)\lambda/2$ edges. Since each block has k elements in it, there are $k(k-1)/2$ pairs that each block will be joined to and so we get

$$v(v-1)\lambda = k(k-1)b.$$

Since $vr = bk$, we obtain

$$(v-1)\lambda = (k-1)r.$$

These are obviously necessary conditions, but they are not sufficient, as we shall see. If there is a bipartite graph satisfying these properties, we call it a $2-(v,k,\lambda)$ design. Sometimes, the more cumbersome notation of a (b,v,r,k,λ) design is used, but since v, λ and k give us r and then b by the above relations, it is prudent to drop the extra parameters. Thus, we have proved:

THEOREM 9.2.1. *In any $2-(v,k,\lambda)$ design, with b blocks and each object appearing in r blocks, we must have*

$$vr = bk, \qquad \text{and} \qquad (v-1)\lambda = (k-1)r.$$

These conditions are necessary, but as we shall see below, they are not sufficient. For instance, it will be seen that there is no way to arrange 22 objects into 22 blocks with each object occurring in precisely 7 blocks and each block containing 7 objects so that any two distinct objects occur in precisely 2 blocks. This corresponds to $(v,b,r,k,\lambda) = (22,22,7,7,2)$ or a $2-(22,7,2)$ design.

More generally, one speaks of a $t-(v,k,\lambda_t)$ design if we insist that any t points are contained in precisely λ_t blocks. For example, in the design of statistical experiments, we may want any collection t people to simultaneously test precisely λ_t products. A $2-(v,3,1)$ design is often called a *Steiner triple system.* We present examples of designs in the following sections.

9.3. Incidence Matrices

A convenient way of encoding the information in a block design (X,B) is by the use of the **incidence matrix**. This is a $v \times b$ matrix A whose rows index the objects and the columns index the blocks. The (i,j)-th entry of A is 1 if the i-th object occurs in block j. Otherwise, it is zero. We immediately see that every row adds up to r and every column adds up to k. Also note that if we look at the $v \times v$ matrix AA^t, the (i,j)-th entry is precisely the number of common neighbors of objects i and j. By the conditions for the block design, this number is λ if $i \neq j$ and r if $i = j$. This we record as:

THEOREM 9.3.1. *Let A be the incidence matrix of the $2-(v,k,\lambda)$ block design (X,B). Let J be the $v \times v$ matrix all of whose entries are 1. Then,*

$$AA^t = \lambda J + (r-\lambda)I.$$

This relation allows us to obtain further necessary conditions for the existence of block designs. Indeed, we can compute the determinant of AA^t as

$$\begin{vmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{vmatrix} = \begin{vmatrix} r+(v-1)\lambda & r+(v-1)\lambda & \cdots & r+(v-1)\lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{vmatrix}$$

where we have simply added to the first row the sum of all the other rows. We can now factor $(r+(v-1)\lambda)$ from the determinant. Thus, the determinant is

$$(r+(v-1)\lambda)\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{vmatrix} = rk \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & r-\lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-\lambda \end{vmatrix}$$
$$= rk(r-\lambda)^{v-1},$$

where we have used Theorem 9.2.1 to replace $r+(v-1)\lambda$ with rk and in the determinant we have multiplied the first row by $-\lambda$ and added it to each of the other rows. This gives $rk(r-\lambda)^{v-1}$ as the value of the determinant.

COROLLARY 9.3.2 (Fisher's inequality). *In any $2-(v,k,\lambda)$ design, we must have $b \geq v$. That is, there must be at least as many blocks as points.*

PROOF. By the theorem, we see that the matrix AA^t is non-singular and thus has rank v. If $b < v$, then as the row rank of A is equal to the column rank of A, we see that A has rank at most b. Recall that for any two matrices A and B for which AB is defined, the row space of AB is contained in the row space of A. Thus, rank of AB is less than or equal to the rank of A. In our situation, we deduce that rank of AA^t is less than or equal to b which is strictly less than v, contradiction. ∎

Designs in which $b = v$ are called *symmetric designs.* In that case, we immediately deduce:

COROLLARY 9.3.3. *If in a symmetric* $2-(v,k,\lambda)$ *design, v is even, then $k-\lambda$ is a perfect square.*

PROOF. If $b = v$, the incidence matrix is a square matrix and from the theorem, we deduce that

$$(\det A)^2 = r^2(r-\lambda)^{v-1}.$$

The left hand side is a perfect square and so $(r-\lambda)^{v-1} = (k-\lambda)^{v-1}$ must also be a perfect square. As $v-1$ is odd, this forces $k-\lambda$ to be a perfect square. ■

Thus, in the example above, we see that there is no $2-(22,7,2)$ design because $7-2$ is not a perfect square. We will prove later the following important theorem in the theory of designs. This was proved in 1951 by Richard Hubert Bruck (1914-1991), Sarvadaman Chowla (1907-1995) and Herbert John Ryser (1923-1985).

THEOREM 9.3.4 (Bruck-Ryser-Chowla). *If (X,B) is a symmetric* $2-(v,k,\lambda)$ *design, and v is odd, then the equation*

$$(k-\lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2 = z^2$$

has a non-zero solution in integers.

As an application of this theorem, consider the existence of a $2-(29,8,2)$ design. That is, can we arrange 29 objects into 29 blocks with each object occurring in 8 blocks and any two objects occur in precisely 2 blocks. The theorem implies that if such a design exists then we can solve the diophantine equation

$$6x^2 + 2y^2 = z^2$$

with $(x,y,z) \neq (0,0,0)$. We may assume that $\gcd(x,y,z)=1$, for otherwise, we can cancel the common factor. From the equation, we see that 2 divides the left hand side and hence must divide the right hand side. So write $z = 2z_1$. We get

$$3x^2 + y^2 = 2z_1^2$$

has a non-trivial solution. If we reduce this mod 3, we get

$$2z_1^2 \equiv y^2 \pmod 3.$$

If z_1 is coprime to 3, we deduce that 2 is a square mod 3, which is not the case. Thus, 3 divides z_1, so write $z_1 = 3z_2$ to deduce that

$$3x^2 + y^2 = 18z_2^2$$

has a non-trivial solution. But now, 3 divides y and $9|3x^2$ implies $3|x$, contrary to the coprimality assumption at the outset. Hence, there is no such design.

9.4. Examples of Designs

If we consider a v element set X and consider the collection B of all k-element subsets of X, we see that any t-element set with $0 \leq t \leq k$, is contained in precisely

$$\binom{v-t}{k-t}$$

elements of B. This is an example of a

$$t - \left(v, k, \binom{v-t}{k-t}\right)$$

design.

We will now consider q-analogs of this construction. We begin with an important class of examples known as *projective planes*. For the elements of X we take all the 1-dimensional subspaces of $V = \mathbf{F}_q^3$. There are

$$\binom{3}{1}_q = \frac{q^3-1}{q-1} = q^2+q+1$$

such subspaces. For B we take the 2-dimensional subspaces and we will say a 1-dimensional subspace U is incident with a two dimensional subspace W if $U \subseteq W$. By the correspondence theorem, the number of such subspaces is the same as the number of 1-dimensional subspaces of the quotient V/U. As this quotient is isomorphic to $\mathbf{F}_q^2$, the number of times a subspace is replicated in the blocks is $(q^2-1)/(q-1) = q+1$. Moreover, any two distinct one-dimensional subspaces generate a unique two dimensional subspace so that this gives us $2-(q^2+q+1, q+1, 1)$ design for any prime power q. This is called a *projective plane* of order q. This has a visual metaphor. A projective plane of order n is a collection X of n^2+n+1 elements called "points" and a collection B of n^2+n+1 blocks called "lines". We require that each point is on precisely $n+1$ lines and each line has precisely $n+1$ points, and any two distinct points determine a unique line. Thus, a projective plane of order n is a $2-(n^2+n+1, n+1, 1)$ design. It is unknown if there are any projective planes of order n when n is not a prime power. We will address this question below using the Bruck-Ryser-Chowla theorem.

The *Fano plane* consisting of seven points and seven lines is the $2-(7,3,1)$ design constructed above using the finite field of two elements. This is usually represented by a triangle along with the midpoints of the three sides together with the centroid. The lines are the sides of the triangle, the lines joining the midpoints of the sides and finally the "line" joining the three midpoints usually drawn as a circle. This has the amusing application to the following problem. Arrange the luncheon engagements of seven people over a week long period in such a way that each day three people have lunch together and by the end of the week, any two of the people would have had lunch together precisely once. If we think of the Fano plane and view the vertices as the people, the lines representing the days of the week, the points on the line determine which of the three people should lunch together, then we have a visual resolution of the required arrangement.

We now prove the only non-existence theorem known in the theory of projective planes.

THEOREM 9.4.1. *If a projective plane of order n exists and $n \equiv 1$ or $2 \pmod 4$, then n can be expressed as a sum of two squares.*

PROOF. As observed earlier, we are asking for the existence of a $2-(n^2+n+1, n+1, 1)$ design. Notice that $v = n(n+1)+1$ is odd. Applying the Bruck-Ryser-Chowla theorem, we deduce that the Diophantine equation

$$nx^2 + (-1)^{n(n+1)/2}y^2 = z^2$$

has a non-trivial integral solution. If $n \equiv 1 \pmod 4$, then $n(n+1)/2$ is odd so the theorem says that we can solve

$$nx^2 = z^2 + y^2$$

in non-zero integers. The same implication occurs when $n \equiv 2 \pmod 4$. Thus n is the sum of two rational squares. To complete the proof, we need to show that n is in fact the sum of two integral squares. Now we need to use one more fact from number theory. Recall that an odd prime number p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$. From this, one can deduce that the numbers that can be expressed as a sum of two integer squares are precisely the numbers whose unique factorization into distinct prime powers does not admit a prime $\equiv 3 \pmod 4$ to an odd power. Thus, if n cannot be written as a sum of two squares, then there is a prime $p \equiv 3 \pmod 4$ an odd power p^{2a+1} (say) of which divides n exactly. Reducing the equation mod p^{2a+1}, we get

$$y^2 + z^2 \equiv 0 \pmod{p^{2a+1}}.$$

If y, z are coprime to p, this is already a contradiction for it says that -1 is a perfect square mod p. If y and z are not coprime to p, only an even power of p can divide each of them and hence both of them and after canceling it, we get a contradiction that completes the proof. ■

We can apply this result to show that there is no projective plane of order 6. Indeed, if there is, by the previous theorem, 6 can be written as a sum of two integral squares, which is clearly not the case. Thus, there is no $2-(43,7,1)$ design. In particular, there is no way to arrange 43 objects into 43 blocks such that each block contains 7 objects and any two objects occurring together in precisely one block.

For a long time, the first unresolved case was $n = 10$. The above theorem does not exclude this possibility as 10 can be written as $1+9$. In 1991, Clement Lam of Concordia University, Canada using the Cray 1 computer showed that there is no projective plane of order 10. Thus, we still have no conceptual proof of this fact. It is generally believed that projective planes can only exist when n is a prime power, but this has not yet been proved.

9.5. Proof of the Bruck-Ryser-Chowla Theorem

The proof of Theorem 9.3.4 requires the use of Lagrange's four square theorem. This theorem says that every natural number can be written as a sum of four squares of natural numbers. We prove it in four steps. As the identity

$$(|z|^2 + |w|^2)(|u|^2 + |w|^2) = |uz - \overline{w}v|^2 + |wu + \overline{z}v|^2$$

is easy to verify directly for all complex numbers u, v, w, z, we deduce from it, by putting $z = x_1 + ix_2$, $w = x_3 + ix_4$, $u = y_1 + iy_2$, $w = y_3 + iy_4$ that

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

where

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$$

$$z_3 = x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2$$

$$z_4 = x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1.$$

This means that if a can be written as a sum of four integral squares, and b can be written as a sum of four integral squares, so can ab and we have an explicit recipe for determining these squares if we know the ones for a and b respectively. As every number is a product of prime numbers, it therefore suffices to prove Lagrange's theorem for prime numbers.

The next step is to see that for any odd prime p, we can solve the congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

To see this, we consider the set of squares mod p, which has size $1+(p-1)/2 = (p+1)/2$. The same is true of the set of elements of the form $-1-y^2$. If these sets were disjoint, we would get at least $p+1$ residue classes mod p, a contradiction. Hence, there is a common element and this gives a solution to the congruence. Since the integers in the interval $[-(p-1)/2, (p-1)/2]$ forms a complete set of residue classes mod p, we may choose $|x| < p/2$ and $|y| < p/2$, we deduce that there are integers x, y so that

$$x^2 + y^2 + 1 = mp$$

with $m < p$.

The third step is to consider the smallest natural number m such that mp can be written as a sum of four squares. By the previous paragraph, the set is non-empty. Call the smallest such m, m_0. Then, $m_0 < p$. If $m_0 = 1$, we are done so let us suppose that $1 < m_0 < p$. Hence, we can write

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

If m_0 were even, then either all of the x_i's are even or all of them are odd, or precisely two of them, say, x_1, x_2 (without loss of generality) are even. In any of the cases, $x_1 - x_2, x_1 + x_2, x_3 - x_4, x_3 + x_4$ are even and we have

$$\frac{m_0}{2} p = \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2.$$

Thus $(m_0/2)p$ can be written as a sum of four squares and this is a contradiction to the minimality of m_0. So we may suppose m_0 is odd.

The final step involves choosing y_1, y_2, y_3, y_4 so that $y_i \equiv x_i \pmod{m_0}$ with $|y_i| \leq (m_0 - 1)/2$. Then,

$$m_0 m_1 = y_1^2 + y_2^2 + y_3^2 + y_4^2$$

with $m_1 < m_0$. By step 1, we see that $(m_0 p)(m_0 m_1)$ can be written as a sum of four squares:

$$z_1^2 + z_2^2 + z_3^2 + z_4^2$$

with the z_i's being given explicitly in terms of x_i's and the y_i's. From this explicit description, we see directly that $z_i \equiv 0 \pmod{m_0}$. Thus, we may divide out by m_0^2 and deduce that $m_1 p$ can be written as a sum of four squares. But this contradicts the minimality of m_0 as $m_1 < m_0$. This completes the proof of Lagrange's theorem.

Now we will sketch the proof of the Bruck-Ryser-Chowla theorem. Suppose that we have a symmetric (v, k, λ) design with v odd. Let $n = k - \lambda$ and suppose that $v \equiv 3 \pmod 4$. We want to show that

$$nx^2 = z^2 + \lambda y^2$$

has a non-trivial integral solution. It suffices to show that this has a non-trivial rational solution, since we can always clear denominators.

By Lagrange's theorem, we may write $n = a^2 + b^2 + c^2 + d^2$ and so let H be the 4×4 matrix:

$$\begin{pmatrix} -a & b & c & d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}.$$

Then, $HH^t = H^tH = nI$. Now let A be the incidence matrix of the symmetric block design. This is a $v \times v$ matrix. Now look at the $(v+1) \times (v+1)$ matrix B obtained by adding a 1 in the $(v+1, v+1)$-th position and zeros everywhere else in the last row and last column. Then,

$$B^tB = \begin{pmatrix} A^tA & 0 \\ 0 & 1 \end{pmatrix}.$$

As $4|v+1$, we may create the $(v+1) \times (v+1)$ matrix K which has $(v+1)/4$ diagonal blocks of the matrix H. Then, $K^tK = KK^t = nI$. Consider the quadratic form

$$\mathrm{x}^tB^tB\mathrm{x} = k(x_1^2 + \cdots + x_v^2) + x_{v+1}^2 + \lambda \sum_{i \neq j \leq v} x_ix_j.$$

If we put $\mathrm{z} = B\mathrm{x}$, then this is

$$\sum_i z_i^2.$$

We may "complete squares" and re-write this as

$$\lambda(x_1 + \cdots + x_v)^2 + x_{v+1}^2 + n(x_1^2 + \cdots + x_v^2).$$

Consider another change of co-ordinates: $\mathrm{z} = K\mathrm{y}$. Then

$$\mathrm{z}^tz = \mathrm{y}^tK^tK\mathrm{y}$$

which is

$$\sum_i z_i^2 = n \sum_i y_i^2.$$

Thus, $\mathrm{x} = (B^{-1}K)\mathrm{y}$ so that

$$n(y_1^2 + \cdots y_{v+1}^2) = \lambda(x_1 + \cdots + x_v)^2 + x_{v+1}^2 + n(x_1^2 + \cdots + x_v^2).$$

The idea now is to choose the x_i and y_i suitably so as to obtain the statement of the theorem. As the matrix $B^{-1}K$ is a rational matrix, we may write

$$x_i = \sum_{i\geq 1} a_i y_i$$

with a_i rational. If $a_1 \neq 1$, choose $x_1 = y_1$; otherwise, choose $x_1 = -y_1$. In either case, $x_1^2 = y_1^2$ and y_1 is a rational linear combination of $y_2, ..., y_{v+1}$. Thus, x_2 is a rational linear combination of $y_2, ..., y_{v+1}$:

$$x_2 = \sum_{i\geq 2} b_i y_i$$

with b_i rational. If $b_2 \neq 1$, choose $x_2 = y_2$; otherwise, choose $x_2 = -y_2$. In either case $x_2^2 = y_2^2$ and y_2 is now a rational linear combination of $y_3, ..., y_{v+1}$. We continue in this way for each $i \leq v$ so that $x_i^2 = y_i^2$ for each $i \leq v$ and y_v is a rational multiple of y_{v+1} and x_{v+1} is a rational multiple of y_{v+1}. Put $y_{v+1} = 1$. Then, x_{v+1} and y_v are uniquely determined rational numbers and working backwards, so are all the x_i's and the y_i's. Since $x_i^2 = y_i^2$ for $1 \leq i \leq v$, we get

$$n = ny_{v+1}^2 = \lambda(x_1 + \cdots + x_v)^2 + x_{v+1}^2$$

has a solution in rational numbers. Moreover, the solution is non-trivial since x_{v+1} and y_{v+1} are non-zero. This completes the proof in this case.

The case $v \equiv 1 \pmod 4$ is similar and we leave it as an exercise to the reader. The essential change in the above proof is that we use the matrix A instead of the matrix B and replace K by the $v \times v$ matrix obtained by putting H on the diagonal and adding a 1 in the (v, v) position and zeros elsewhere in the last row and column. Then, the proof proceeds as before and we leave it as an exercise to the reader.

9.6. Codes and Designs

The fundamental paper *A mathematical theory of communications* from 1948 of Claude Shannon (1916-2001) is considered to be the starting point of coding theory. Around the same time, Richard Wesley Hamming (1915-1998) and Marcel J.E. Golay (1902-1989) also contributed to the beginning of this subject.

A **code** is a subset of $\mathbf{F}_q^n$. A code is called **linear** if it is a subspace of $\mathbf{F}_q^n$. It is **binary** if $q = 2$. The vectors in the code are called **codewords.** The **weight** of a vector v, denoted $wt(v)$, is the number of non-zero coordinates of v. The **Hamming distance** between two vectors v and w is the weight of $v - w$, and is denoted $d(v, w)$. If C is a code, the minimum distance $d(C)$ is the minimum of $d(v, w)$ for v, w distinct elements of C.

A code is said to be e-**error correcting** if $d(C) \geq 2e+1$. The reason for this definition is given by the following theorem.

THEOREM 9.6.1. *A code is e-error correcting if and only if the Hamming spheres:*

$$B_e(c) := \{v : d(v,c) \leq e\}$$

are disjoint for all $c \in C$.

PROOF. If $B_e(c_1)$ and $B_e(c_2)$ are not disjoint for two distinct codes c_1, c_2, then let v be a common element of these two Hamming spheres. Then,

$$d(c_1,c_2) \leq d(c_1,v) + d(v,c_2) \leq 2e.$$

But $d(c_1,c_2) \geq 2e+1$ for any two distinct code words, so this is a contradiction.

Conversely, if all the Hamming spheres are disjoint, and C is not e-error correcting, then there are two codewords c_1, c_2 such that $d(c_1,c_2) = f \leq 2e$. This means that c_1 and c_2 do not agree in f positions. Now change the co-ordinates of c_1 in $\lfloor f/2 \rfloor$ of these positions to agree with c_2 and call this changed vector b. Because $f \leq 2e$, we have that

$$d(c_1,b) = \lfloor f/2 \rfloor \leq e, \quad d(c_2,b) = f - \lfloor f/2 \rfloor \leq e$$

so that b is an element of $B_e(c_1)$ and $B_e(c_2)$ which is a contradiction. ∎

The application of these ideas in communication networks is as follows. If C is an e-error correcting code, then these codewords are used to send signals over a "noisy channel". If a code word c is received as c' and e errors are made in the transmission, then $d(c,c') \leq e$. Thus c' lies in the Hamming sphere $B_e(c)$. By Theorem 9.6.1, this is the unique code word satisfying this inequality.

We can construct error correcting codes by taking the rows of the incidence matrix of a symmetric (v,k,λ)-design as code words. Any two words have λ 1's together in precisely λ places. Each code has precisely k 1's and $v-k$ 0's. If R_1 and R_2 are distinct rows, then the number of co-ordinates with entry 1 at which R_1 and R_2 agree is the dot product $R_1 \cdot R_2$ and this is λ. If J is the vector consisting of all 1's, then the number of co-ordinates with entry 0 at which R_1 and R_2 agree is the dot product $(J-R_1)\cdot(J-R_2)$ which is $v-2k+\lambda$. By the definition of the Hamming distance, we deduce that

$$d(R_1,R_2) = 2(k-\lambda).$$

Thus, the rows of a symmetric (v,k,λ) design give us a $(k-\lambda-1)$-error correcting code.

In 1971, the Mars Mariner spacecraft used the rows of a $(31, 15, 7)$ design as codewords to send back photographs of Mars back to Earth. This code corrects 7 errors. In later space missions, more sophisticated codes called Reed-Solomon codes have been used and these codes are capable of correcting a larger number of errors. They are based on the following simple idea. Given a code word $(a_0, a_1, ..., a_{m-1})$, construct a polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}.$$

Fix a primitive root g of $\mathbf{F}_q$. Instead of trying to send the code word, the spacecraft transmits the sequence $f(0), f(g), \ldots, f(g^N)$ where $N > m$. Since a polynomial of degree m is determined by $m + 1$ values, this is sufficient information to retrieve the original code word $(a_0, ..., a_{m-1})$ and this can be done algorithmically in an efficient way. One can prove that this method gives rise to a $(q + m)/2$-error correcting code.

9.7. Exercises

EXERCISE 9.7.1. Prove that

$$(q^k - 1)\binom{n}{k}_q = (q^n - 1)\binom{n-1}{k-1}_q.$$

EXERCISE 9.7.2. Prove that

$$\binom{n+1}{k}_q = \binom{n}{k-1}_q + \binom{n}{k}_q + (q^n - 1)\binom{n-1}{k-1}_q.$$

EXERCISE 9.7.3. Let $f_q(n)$ be the number of subspaces of $\mathbb{F}_q^n$. Show that

$$f_q(n+1) = 2f_q(n) + (q^n - 1)f_q(n-1).$$

EXERCISE 9.7.4. Let L be the lattice of subspaces of $\mathbb{F}_q^n$ partially ordered by inclusion. If W is a subspace of dimension k, show that

$$\mu(0, W) = (-1)^k q^{\binom{k}{2}}.$$

EXERCISE 9.7.5. 16 students decide to sign up for three fields each. Each trip accommodates precisely 6 students. The students would like to sign up in such a way that any two of them would be together on precisely one of the trips. Is such arrangement possible ? Explain.

EXERCISE 9.7.6. Construct explicitly a $2-(31, 3, 1)$ design. For any natural number $n \geq 1$, show that there exists a $2 - (2^n - 1, 3, 1)$ design.

EXERCISE 9.7.7. If A is a $v \times b$ matrix and B is a $b \times v$ matrix, show that

$$\text{rank}(AB) \leq \min(\text{rank}(A), \text{rank}(B)).$$

EXERCISE 9.7.8. In a symmetric $2-(v,k,\lambda)$ design with incidence matrix A, show that

$$\frac{1}{k-\lambda}\left(A+\sqrt{\frac{\lambda}{k}}J\right)$$

is the inverse of

$$A^t-\sqrt{\frac{\lambda}{v}}J.$$

Deduce that

$$A^tA=\lambda J+(r-\lambda)I.$$

Use this equation to prove that in any symmetric design, every pair of blocks has precisely λ elements in common.

EXERCISE 9.7.9. Show that there is no projective plane of order 14.

EXERCISE 9.7.10. If $p\equiv 3 \pmod 4$ is a prime, show that there is no $2-(v,p+1,1)$ design with $v\equiv 3 \pmod 4$.

EXERCISE 9.7.11. If C is a code in $\mathbb{F}_q^n$ with distance $d(C)\geq 2e+1$, then

$$|C|\cdot\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\leq q^n.$$

EXERCISE 9.7.12. If C is a code in $\mathbb{F}_q^n$ with distance $d(C)=d$, then

$$|C|\leq q^{n-d+1}.$$

EXERCISE 9.7.13. Label the points of the Fano plane by the elements of $\mathbb{Z}_7$ such that each block of the Fano plane has the form $\{x,x+1,x+3\}$ for $x\in\mathbb{Z}_7$.

EXERCISE 9.7.14. Consider the following incidence structure: the points are the edges of the complete graph K_6 and the blocks are all the sets of three edges that form a perfect matching or a triangle in K_6. Show that this is a Steiner triple system on 15 points.

EXERCISE 9.7.15. Show that if $x,y,z\in\mathbb{F}_q^n$, then

$$d(x,z)\leq d(x,y)+d(y,z).$$

EXERCISE 9.7.16. Show that if a $2-(v,3,1)$ design exists, then $v\equiv 1,3 \pmod 6$.

EXERCISE 9.7.17. Consider the design whose point set is $\mathbb{Z}_n\times\mathbb{Z}_3$. The blocks are the triples

$$\{(x,0),(x,1),(x,2)\}$$

for $x \in \mathbb{Z}_n$ and

$$\left\{(x,i),(y,i),\left(\frac{x+y}{2},i+1\right)\right\}$$

for $x \neq y \in \mathbb{Z}_n$ and $i \in \mathbb{Z}_3$. Show that this is a $2-(6t+3,3,1)$-design.

EXERCISE 9.7.18. Show that the number of blocks in a $t-(v,k,\lambda)$ design is

$$b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}.$$

EXERCISE 9.7.19. Show that in any $t-(v,k,1)$ design

$$v \geq (t+1)(k-t+1).$$

EXERCISE 9.7.20. Show that there are at most two disjoint Steiner triple systems on a set of 7 points.

CHAPTER 10

Planar Graphs

10.1. Euler's Formula

A graph is said to be **embedded** in the plane if it can be drawn on the plane so that no two edges intersect. Such a graph is called a **planar graph**. Graphs arising from maps are clearly planar. In fact, planar maps can be characterized as such. Any planar map cuts out the plane into **faces**. To be precise, a maximal region of the plane which does not contain in its interior a vertex of the graph is called a **face**. A finite plane graph has also one unbounded face called the **outer face**. The faces are pairwise disjoint. The basic relation for planar graphs is the following theorem due to Euler.

THEOREM 10.1.1 (Euler, 1758). *If X is a connected planar graph with v vertices, e edges and f faces, then*

$$v - e + f = 2.$$

PROOF. The proof will be by induction on the number of vertices. If $v = 1$, then X is a "bouquet" of loops. If in addition $e = 0$, then $f = 1$ and the formula is true in this case. Each added loop cuts the face into two faces and so increases the face count by 1. So the formula holds in case $v = 1$. For $v > 1$ and X connected, take an edge e_0 which is not a loop and the contraction of X by e_0 gives X/e_0. Contraction does not reduce the number of faces so X/e has $v - 1$ vertices, $e - 1$ edges, and f faces. Since X/e has fewer number of vertices, we can apply the induction hypothesis to get

$$(v-1) - (e-1) + f = 2 = v - e + f = 2$$

which is what we want to prove. ∎

If X is not connected, then Euler's formula fails. If X is a planar graph with c connected components, then

$$v - e + f = c + 1.$$

This is easily seen be adding $c-1$ edges (or "bridges") and then applying Euler's formula to this connected graph. Adding the bridges does not alter the face count. Thus, we get

$$v - (e + c - 1) + f = 2$$

from which the formula follows. Euler's formula has many applications. The first is that we can derive some necessary conditions for a graph to be planar.

THEOREM 10.1.2. *If X is a simple planar graph with at least 3 vertices, then $e \leq 3v - 6$. If X is triangle-free, then $e \leq 2v - 4$.*

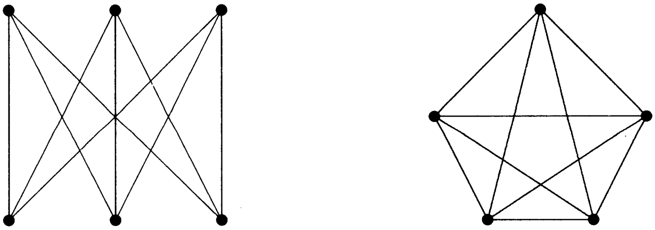
PROOF. It suffices to prove this for connected graphs. Every face must contribute at least three edges. But each edge appears in two faces. Thus, $3f \leq 2e$ and putting this into Euler's formula gives us

$$2 = v - e + f \leq v - e + \frac{2}{3}e$$

which gives the inequality

$$e \leq 3v - 6.$$

If X is triangle-free, then, each face contributes at least four edges. Since each edge appears in two faces, we get $2e \geq 4f$. Putting this back into Euler's formula gives the second inequality. ∎



$K_{3,3}$ K_5

FIGURE 10.1

COROLLARY 10.1.3. *The graphs, K_5 and $K_{3,3}$ are non-planar.*

PROOF. If K_5 were planar, then applying the theorem gives10 $\leq 15 - 6 = 9$, a contradiction. For $K_{3,3}$, we get $9 \leq 18 - 6 = 12$ which does not give a contradiction if we use the first inequality. However, the bipartite graph has no triangles and so, by the second inequality, we get $9 \leq 8$, which is a contradiction. ∎

A famous theorem of Kazimierz Kuratowski (1896-1980) proved in 1930 states that a graph is planar if and only if it can be (edge)-contracted to either K_5 or $K_{3,3}$. Thus, for example, as the Petersen graph (shown in Figure 10.2) can be contracted to K_5 by collapsing the edges connecting the "inside" cycle of 5 vertices to the outer five vertices, it is not planar.

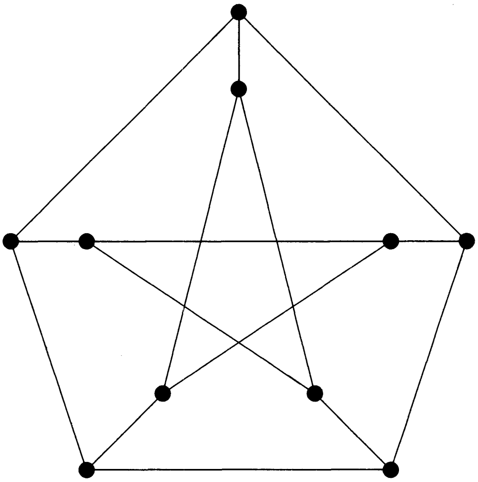


FIGURE 10.2. Petersen graph

THEOREM 10.1.4. *Every simple planar graph X contains a vertex of degree at most five.*

PROOF. If every vertex has degree at least six, then $2e \geq 6v$ which implies $e \geq 3v$. However, Theorem 10.1.2 implies $e \leq 3v - 6$ which is a contradiction. ■

Now, we can prove the six-colour theorem:

THEOREM 10.1.5 (The six colour theorem). *Every map can be properly coloured using six colours.*

PROOF. We proceed by induction on the number of vertices (or regions) of the planar graph associated with the map. Suppose that all planar graphs with fewer than $n - 1$ vertices are 6-colourable. By Theorem 10.1.4, X contains a vertex of degree 5 or less. By induction, $X - v$ is 6-colourable and as v has degree 5 or less, we can colour it with one of the six colours not used on any of its adjacent vertices. ■

10.2. The Five Colour Theorem

The four colour theorem has a colourful history! It states that any planar graph can be coloured using four colours. Since K_4 is planar, and has chromatic number 4, we see that four colours are necessary. To prove that this is sufficient is more difficult. The four colour conjecture was first formulated by Francis Guthrie on October 23, 1852. Guthrie was a student at University College London where he studied under Augustus de Morgan (1806-1871). When Guthrie asked de Morgan, he did not know how to prove it and wrote to Sir William Rowan Hamilton (1805-1865) in Dublin if he knew. It seems that Guthrie graduated and then studied law. After practicing as a barrister, he went to South Africa in 1861 as a professor of mathematics. After a few mathematical papers, he switched to the field of botany.

In the meanwhile, de Morgan circulated Guthrie's question to many mathematicians. Arthur Cayley, who learned of the question from de Morgan in 1878, posed it as a formal unsolved problem to the London Mathematical Society on 13 June, 1878. On 17 July 1879, Alfred Kempe (1849-1922), a London barrister and amateur mathematician announced in *Nature* that he had a proof. Kempe had studied under Cayley, and at Cayley's suggestion, submitted his paper to the *American Journal of Mathematics* in 1879. We will discuss Kempe's "proof" below. Apparently, Kempe received great acclaim for his work. He was elected Fellow of the Royal Society and served as its treasurer for many years. In 1912, he was knighted. The error in his "proof" was discovered in 1890 by Percy John Heawood (1861-1955), a lecturer in Durham, England. In his paper, Heawood showed how to salvage the proof and prove that every map is 5-colourable. We will now prove the following theorem due to Heawood.

THEOREM 10.2.1 (Heawood, 1890). *Any planar graph is* 5*-colourable.*

PROOF. We will prove the theorem by induction on the number of vertices. Let X be a planar graph on n vertices. The base case $n = 1$ is obvious. Assume $n \geq 2$. By Theorem 10.1.4, there is a vertex x of degree at most 5. The graph $Y = X \setminus \{x\}$ is also planar and by induction, Y can be coloured using at most 5 colours. If the degree of x is 4 or less, then x an be coloured with a colour not used for any of its adjacent vertices. This way, we can obtain a proper colouring of X with at most 5 colours. So we may suppose that x has degree 5. If any two of the neighbours of x get the same colour, then the previous argument shows how one can colour X with at most 5 colours. Let us label the neighbours of x as p, q, r, s, t and say that they are coloured in

Y with $1, 2, 3, 4, 5$ respectively, by the induction hypothesis. Denote by $X_{i,j}$ the subgraph of Y whose vertices are coloured with colour with i and j. Now consider $X_{1,3}$. Both p and r belong to $X_{1,3}$. If they lie in two distinct components, then, we may interchange colours 1 and 3 in the component containing r with the result that p and r are coloured using colour 1. Then, we can colour x using colour 3. If however, p and r lie in the same connected component of $X_{1,3}$, then this means there is a chain of vertices with alternating colours 1 and 3 from p to r. Now consider $X_{2,4}$. Both q and s belong to this subgraph. Again, if q and s lie in distinct connected components, we may interchange colours 2 and 4 in one of the components and free up one colour and use that to colour x. If q and s do not lie in the same connected component, then there is a path of alternating colours from q to s. But this path must cross the path from p to r and this would violate planarity. Thus, the second possibility cannot arise which means that we can use the same colour on q and s and thus, colour X with 5 colours. This finishes the proof. ■

Kempe's "proof" performed this colour reversal technique twice and this leads to difficulties as Heawood pointed out. Here is Kempe's argument. As before, we proceed by induction on the number of vertices. Let x be a vertex of degree at most 5. If the degree of x is at most 4, then an argument as in Heawood's proof can be applied (and we leave this as an exercise to the reader). However, the proof breaks down when degree of x is 5 for the following reasons. Label the vertices adjacent to x as p, q, r, s, t and let us suppose that induction gave the colouring of vertices as shown in Figure 10.3. If there is no $2, 3$ colour chain between q and s, we can carry a colour reversal to free the colour 2 (say) for vertex x. If there is no $2, 4$ colour chain between q and t, we can carry out a colour reversal to free the colour 2 for vertex x. It looks as if we therefore have a situation indicated in Figure 10.4. Since there cannot be a $1, 3$ colour chain between p and s, a colour reversal can paint the

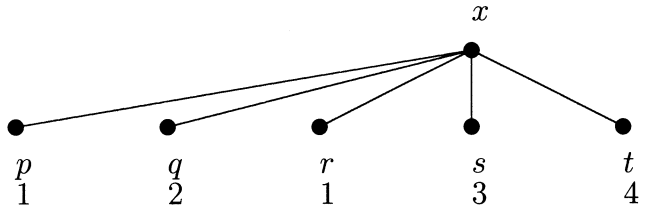


FIGURE 10.3

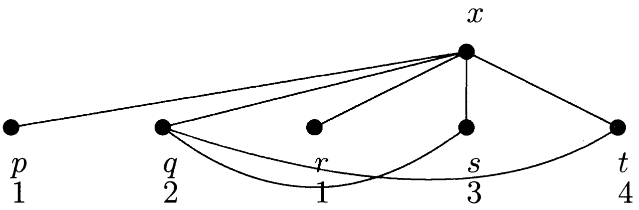


FIGURE 10.4

vertex p with colour 3. Since there cannot be a 1, 4 colour chain between r and t a colour reversal will paint the vertex r with colour 4. So it looks as if colour 1 is freed and we can use it to colour x. However, there is a gap in the reasoning. In the figure below, carrying out the reversals as indicated above will paint p and r with colour 1. Indeed,

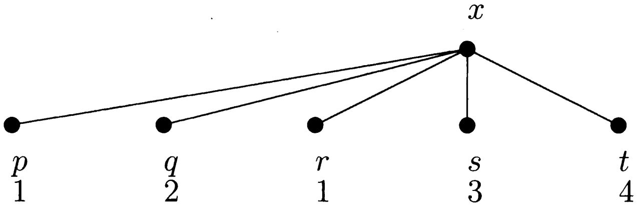


FIGURE 10.5

the colour reversal argument is valid for changing the colour of p and the colour of r. However, simultaneously changing the colour of p and r leads to difficulties. This is essentially what Heawood observed as the gap in Kempe's proof. He was able to salvage the argument to deduce the five colour theorem as we indicated above.

10.3. Colouring Maps on Surfaces of Higher Genus

As we mentioned earlier, $K_{3,3}$ is not a planar graph since we cannot draw it on the plane without intersecting edges. If however, we tried to draw it on a torus, then it is possible to draw the graph without crossing of edges as it can be verified easily. A celebrated theorem of Möbius (1870) is that any compact (orientable) surface is homeomorphic to a sphere with g handles. The **genus** of the surface is denoted g. A torus, for example, has genus one since it is homeomorphic to a sphere with one handle.

One can show that any graph X can be embedded in some compact orientable surface. The minimal genus of the surface for which this can be done is called the **genus of the graph**. For example, the genus of $K_{3,3}$ is 1.

For graphs embedded on a surface of genus g, Euler's formula generalizes as follows. A **face** is defined as before, as a maximal region cut out by the graph which contains no vertex of the graph in its interior. We state without proof the following result.

THEOREM 10.3.1 (Euler's formula). *If G is a connected graph of genus g, then*

$$v - e + f = 2 - 2g.$$

Using Euler's formula, we can prove as before that any simple graph of genus g has at most $3(v-2+2g)$ edges. This is the analogue that a planar graph has at most $3(v-2)$ edges. As before, summing up the degrees gives

$$2e \leq 6(v-2+2g)$$

so that there has to be at least one vertex of degree

$$\leq \frac{6(v-2+2g)}{v}.$$

This is the analog of the result for planar graphs which says there is at least one vertex of degree at most five. Now we can prove:

THEOREM 10.3.2 (Heawood, 1890). *Any graph X of genus g can be coloured with*

$$\left\lceil \frac{7+\sqrt{1+48g}}{2} \right\rceil$$

colours provided $g > 0$. Here $\lceil x \rceil$ denotes the smallest integer larger than or equal to x.

REMARK 10.3.3. Notice that if $g = 0$ were allowed in the formula, then we deduce the four colour theorem.

PROOF. Let

$$c = \left\lceil \frac{7+\sqrt{1+48g}}{2} \right\rceil.$$

If X has at most c vertices, we are done. So suppose that $v > c$. If we can show that every simple graph of genus g has a vertex of degree at most $c-1$, then we can use an induction argument as before to complete the proof. Notice that

$$c^2 - 7c + (12 - 12g) \geq 0$$

so that

$$c - 1 \geq 6 + \frac{12(g-1)}{c}.$$

Thus, from the remark before the statement of the theorem, we have that X has a vertex of degree at most

$$6+\frac{12(g-1)}{v}\leq 6+\frac{12(g-1)}{c}\leq c-1$$

as desired. ∎

REMARK 10.3.4. Notice that $g \geq 1$ is used in a crucial way in the inequalities at the end of the proof.

For a long time, it was an outstanding problem to determine the genus of the complete graph. The **complete graph conjecture**, proved in 1968 by Gerhard Ringel and J.W.T. Youngs, states that the genus of K_n is

$$\left\lceil\frac{(n-3)(n-4)}{12}\right\rceil.$$

10.4. Exercises

EXERCISE 10.4.1. The **girth** of a graph is the length of its shortest cycle (that is, closed path). Use Euler's formula to show that if X is a planar graph with girth γ, and v vertices, then the number of edges e of X satisfies the inequality

$$e\leq\frac{\gamma}{\gamma-2}(v-2).$$

EXERCISE 10.4.2. Determine the girth of the Petersen graph (Figure 10.2) and use the previous question to deduce that it is not a planar graph.

EXERCISE 10.4.3. Let X be a graph with chromatic number $\chi(X) > 3$. Show that the genus $g(X)$ of a graph X satisfies the inequality

$$g(X)\geq\frac{1}{12}\left(\chi(X)^2-7\chi(X)+12\right).$$

Deduce that for $n \geq 5$, the genus of the complete graph K_n is at least

$$\left\lceil\frac{(n-3)(n-4)}{12}\right\rceil.$$

EXERCISE 10.4.4. Determine all r, s such that $K_{r,s}$ is a planar graph.

EXERCISE 10.4.5. Show that $K_5 \setminus e$ is planar for any edge e of K_5.

EXERCISE 10.4.6. Show that $K_{3,3} \setminus f$ is planar for any edge f of $K_{3,3} \setminus f$.

EXERCISE 10.4.7. Let G be the graph obtained from $K_{4,4}$ by deleting a perfect matching. Is G planar ?

EXERCISE 10.4.8. Let S be a set of n points in the plane such that the distance between any two of them is at least 1. Show that there are at most $3n-6$ pairs x, y such that the distance between x and y is 1.

EXERCISE 10.4.9. The **crossing number** of a graph X is the minimum number of crossings in a drawing of X in the plane. What are the crossing numbers of K_5 and $K_{3,3}$?

EXERCISE 10.4.10. Let X be a graph with n vertices and e edges. If k is the maximum number of edges in a planar subgraph of X, show that the crossing number of X is at least $e-k$. Prove that the crossing number of X is at least $e-3n+6$. If X has no triangles, then the crossing number is at least $e-2n+4$.

EXERCISE 10.4.11. Show that the crossing number of K_6 is 3.

EXERCISE 10.4.12. A planar graph X is **outerplanar** if it has a drawing with every vertex on the boundary of the unbounded face. Show that any cycle is outerplanar. Show that K_4 is planar, but not outerplanar.

EXERCISE 10.4.13. Show that $K_{2,3}$ is planar, but not outerplanar.

EXERCISE 10.4.14. Any outerplanar graph is 3-colourable.

EXERCISE 10.4.15. An art gallery is represented by a polygon with n sides. Show that it is possible to place $\lfloor \frac{n}{3} \rfloor$ guards such that every point interior to the polygon is visible to some guard. Construct a polygon that can be guarded by precisely $\lfloor \frac{n}{3} \rfloor$ guards.

EXERCISE 10.4.16. What is the crossing number of the Petersen graph ?

EXERCISE 10.4.17. Prove that every outerplanar graph has a vertex of degree at most 2.

EXERCISE 10.4.18. Show that every planar graph decomposes into two bipartite graphs.

EXERCISE 10.4.19. For any $n \geq 4$, construct a planar graph with n vertices and chromatic number 4.

EXERCISE 10.4.20. Let X be a planar graph with a Hamiltonian cycle C. If X has f_i' faces of length i inside C and f_i'' faces of length i outside C, then

$$\sum_i (i-2)(f_i' - f_i'') = 0.$$

CHAPTER 11

Edges and Cycles

11.1. Edge Colourings

In the previous chapters, we have been considering vertex colourings. Now we will look at edge colourings of a graph. We will say that two edges are **adjacent** if they have a common vertex. We would like to colour the edges "properly" in the sense that no two adjacent edges receive the same colour. Given a graph X, we define the **edge chromatic number** denoted $\chi_e(X)$ to be the minimum number of colours needed to properly colour the edges.

The question of edge colourings occurs in many contexts. Suppose that in a school we have n teachers $T_1, ..., T_n$ to teach m classes $C_1, ..., C_m$ and teacher T_i must teach class C_j for p_{ij} class periods. Is it possible to schedule this in such a way that a minimum number of time slots are used? To study this question, we would construct a bipartite graph whose vertices consist of vertices T_i and the classes C_j. We will join T_i to C_j with p_{ij} edges and an edge colouring of this graph corresponds to a timetabling for the school. It will turn out that the edge chromatic number for this graph is p which is the maximum of the values of p_{ij}.

Clearly, if X is a graph whose maximal vertex degree is $\Delta(X)$, then we will need at least $\Delta(X)$ colours to properly edge colour X. It is a remarkable theorem proved independently by Gupta and Vizing, that in fact $\chi_e(X) \leq \Delta(X) + 1$. Thus, the edge chromatic number of a graph is either $\Delta(X)$ or $\Delta(X) + 1$ and at present, there is no convenient criterion to determine which one occurs.

In some cases, it is possible to determine which one of these occurs as the edge chromatic number. For instance, we have the following:

THEOREM 11.1.1. *Let X be a graph with an odd number of vertices n. Suppose further that X is k-regular, that is, the degree of each vertex is k. Then, $\chi_e(X) > k$.*

REMARK 11.1.2. By the theorem of Gupta-Vizing, we can conclude that $\chi_e(X) = k + 1$.

PROOF. In any proper edge colouring, no two edges meeting at the same vertex can be coloured the same colour. Thus, if we partition the edges according to colour, each vertex is incident with at most one element from each class. Thus, the number of vertices gives an upper bound for the number of edges in each colour class. But taking into account that an edge joins two vertices, we see that the number of edges in a colour class is at most $n/2$. Since n is odd, this can be sharpened to $(n-1)/2$. As our graph is regular, it has a total of $kn/2$ edges. Hence, the number of colours is at least

$$\frac{kn/2}{(n-1)/2} > k.$$

This completes the proof. ∎

We can apply this result to determine the edge chromatic number of the complete graph.

THEOREM 11.1.3. *The edge chromatic number of K_n is $n-1$ if n is even and n if n is odd.*

PROOF. First suppose n is odd. As K_n is $(n-1)$-regular, we can apply the previous theorem, to deduce that we will need at least n colours. We can represent K_n as follows. Draw the regular n-gon in the plane and use the vertices of the n-gon as the vertices of K_n. This is best visualized in the complex plane where we identify the vertices of the n-gon with the n roots of unity. If θ denotes the interior angle subtended at each vertex, then one can easily determine θ as follows. By connecting that particular vertex to every other vertex, we decompose the n-gon into $n-2$ triangles. Each triangle contributes π radians, and so $n\theta = (n-2)\pi$ implying $\theta = (n-2)\pi/n$. To form the complete graph, we simply rotate by π/n the line determined by the edge at the vertex of the n-gon. This shows that each of the edges of the complete graph is parallel to one of the sides of the n-gon. Now, draw in the edges as indicated above. First colour each of the edges of the n-gon a different colour. It is not difficult to see that any remaining edge is parallel to one of the outer edges. Then colour the remaining edges the colour of the edge of the n-gon which is parallel to it. This gives the desired colouring. In the case n is even, observe that $K_n = K_1 \vee K_{n-1}$. As $n-1$ is odd, we can properly edge colour K_{n-1} using $n-1$ colours. In this colouring, one colour is missing at each vertex of K_{n-1}. Use that colour to colour the edge joining it to K_1. This completes the proof. ∎

Thus, K_n with n odd requires one more colour than the maximal degree. Another class of graphs with this property is the cycle graph

C_n whose edge chromatic number is easily seen to be 3 if n is odd and 2 if n is even.

The edge colouring problem can be transformed into a vertex colouring problem in the following way. Given a graph X, we consider the **line graph** of X, denoted $L(X)$ whose vertices represent the edges of X. Two vertices of $L(X)$ are adjacent if the corresponding edges in X meet in a vertex. The edge chromatic number of X is then the chromatic number of $L(X)$. We can therefore apply some of our earlier results to the question of edge colouring. For example, what is the maximal degree of a vertex in $L(X)$? This boils down to asking how many edges are adjacent to a given edge in X. Since an edge has two endpoints, we easily find that the maximal degree is $\leq 2(\Delta(X)-1)$. Thus, by the theorem of Brooks on the chromatic number of a graph, we obtain

THEOREM 11.1.4. *The edge chromatic number satisfies the inequalities:*

$$\Delta(X) \leq \chi_e(X) \leq 2\Delta(X) - 1.$$

If $\Delta(X) \geq 3$, then the upper bound can be sharpened to $2\Delta(X) - 2$ by the theorem of Brooks.

PROOF. We only need to explain the last statement. The theorem of Brooks tells us that the chromatic number is bounded by the maximal degree unless the graph is C_n with n odd or the complete graph K_n. If $\Delta(X) \geq 3$, the first case cannot arise. In the second case, the result is true since the previous theorem determined the edge chromatic number of the complete graph. ∎

We can determine the edge chromatic number of bipartite graphs by a celebrated theorem of König. The method of proof resembles the five colour theorem.

THEOREM 11.1.5. *Let X be a bipartite graph with maximal degree Δ. Then, $\chi_e(X) = \Delta$.*

PROOF. We will induct on the number of edges of X. Let U and V be the partite sets of X. Remove an edge e that joins $u \in U$ and $v \in V$ (say) from X. The resulting graph X' is still bipartite. The highest vertex degree in X' is still Δ or less. By induction, we can edge colour X' using Δ colours or less. If we used at most $\Delta - 1$ colours, then we can use the remaining colour for the edge e. So assume we used Δ colours to colour the edges of X'. If one of the colours is missing from both the edges incident to u and the edges incident to v, then we can use that colour to colour e. So assume otherwise. Since the degree of u in X' is less than Δ, there is a colour c (say) missing at u which is used at v and similarly, a colour c' is missing at v which is used at u. Now consider the subgraph of X' which is coloured with either c or c'. In particular, consider the component which contains u. This component consists of a path of alternating colours, between c' and c. This path cannot end at v for that would be a path of odd length and the last edge would have colour c' which is not used at v. Now we can perform a colour reversal in this component and still have a proper edge colouring of X' with now c used at u which frees up c'. As c' is missing from v, we can use that colour to colour the edge e. This completes the proof. ∎

COROLLARY 11.1.6. $\chi_e(K_{r,s}) = \max(r, s)$.

A **decomposition** of a graph is a list of subgraphs such that each edge appears in exactly one subgraph in the list. An edge colouring of the graph gives rise to a decomposition of the edges into colour classes. A **k-factor** of a graph is a spanning subgraph which is a k-regular graph. Thus, a 1-factor is a matching. If we edge colour a k-regular graph using only k colours, then the colour classes give us a decomposition of the graph into 1-factors. Thus, for instance, if the Petersen graph were 3-colourable, removing a colour class leaves us a 2-regular graph which consists of odd cycles and cannot be decomposed as 1-factors.

An important application of Theorem 11.1.5 is to the problem of scheduling. Suppose that members of a hiring committee are to interview a number of candidates for a job. If each member interviews at most m candidates and each candidate is interviewed by at most n members individually, then Theorem 11.1.5 tells us that $\max(m, n)$ time slots are needed for this purpose. The precise timetabling of the candidates corresponds to matchings, which we can effectively determine using the Hungarian algorithm.

11.2. Hamiltonian Cycles

A **Hamiltonian cycle** in a graph is a closed path that visits each vertex exactly once (apart from the initial point and the end point). This is reminiscent of the Euler cycle discussed in Chapter 2. However, no simple criterion is known that characterizes graphs that contain a Hamiltonian cycle. In a practical context, this arises as the famous traveling salesman problem. The question is to visit each of the cities in a circuit exactly once and minimizing the cost of such a tour. No algorithm is known for finding such a tour and it represents one of the major unsolved problems in graph theory.

Despite being studied first by Kirkman, Hamilton cycles are named for Sir William Rowan Hamilton (1805-1865). In 1856, Kirkman asked if given the graph of a polyhedron, does there exist a cycle passing through every vertex ? In 1857, Hamilton invented the Icosian game which is the problem of finding a Hamilton cycle in a **dodecahedron** (seen in the Figure below). The game was actually sold as a pegboard with holes at the nodes of the dodecahedron. In 1859, Hamilton sold the game to a London game dealer for 25 pounds who marketed under the name *Around the world.*

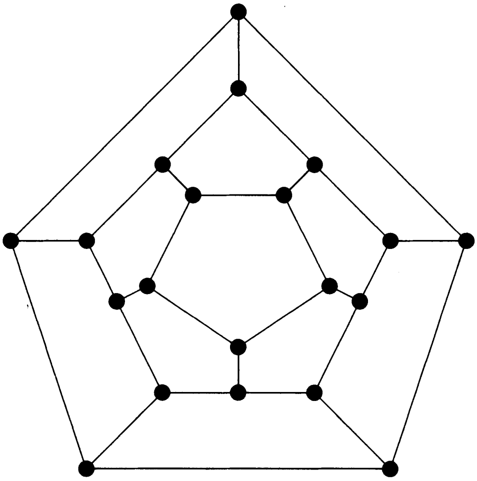


FIGURE 11.1. The dodecahedron graph

There is also the famous problem of the 'knight's tour' which asks if the knight on the chessboard can visit each of the squares exactly once and return to the starting point. This problem was first solved by Euler in 1759.

There are many theorems which provide sufficient conditions for the existence of a Hamiltonian cycle. We give one such theorem, due to Oystein Ore (1899-1968), below.

THEOREM 11.2.1. *Let X be a simple graph with v vertices. Suppose that $v \geq 3$ and that* $\deg(x) + \deg(y) \geq v$ *for any pair of non-adjacent vertices x and y. Then X has a Hamiltonian cycle.*

PROOF. Suppose that the theorem is false for some graph with $v \geq 3$ vertices. Add as many edges as possible to this graph without producing a Hamiltonian cycle. Call this new graph X'. X' cannot be the complete graph and so there is a pair of non-adjacent vertices x, y (say). By the construction of X', any addition of an edge will create a Hamiltonian cycle. In particular, adding the edge xy will create a Hamiltonian cycle.

Thus, X' has a path from x to y which visits all the vertices. Of these vertices, put a circle around the ones which are adjacent to x and put a square around the vertices before the adjacent ones in the Hamiltonian path. A number of deg (x) of the $v-1$ vertices are circled and deg (x) of the $v-1$ vertices are also squared. Thus, $v-1-\deg(x)$ are not squared. Since $\deg(y) \geq v - \deg(x) > v-1-\deg(x)$, there is a vertex z (say) adjacent (see Figure 11.2) to y which has been squared. Thus, we have a Hamiltonian cycle from x to the vertex "next" to z and then moving to y and then to z and back to x. This is a contradiction that X' has a Hamiltonian cycle. ■

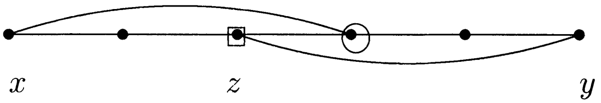


FIGURE 11.2

We have the following theorem due to Gabriel Andrew Dirac (1925-1984).

COROLLARY 11.2.2. *If X is a graph with v vertices such that every vertex has degree $\geq v/2$, then X has a Hamiltonian cycle.*

The Petersen graph is a 3-regular graph with edge chromatic number 4 (see Exercise 11.4.3). One can show that any 3-regular graph with a Hamiltonian cycle has edge chromatic number 3 and therefore, we conclude that the Petersen graph is not Hamiltonian (see Exercise 11.4.2 and Exercise 11.4.4).

The following is a necessary condition for a graph to have a Hamiltonian cycle.

THEOREM 11.2.3. *If X has a Hamiltonian cycle, then for each $S \subset V(X)$, the graph $X \setminus S$ has at most $|S|$ components.*

PROOF. Let C be a Hamiltonian cycle in X and $S \subset V(X)$ be a subset of vertices of X. When C leaves a component of $X \setminus S$, it must return to S. These returns to S must use different vertices of S. This proves the theorem. ■

This result can be useful when trying to show that a graph is not Hamiltonian. The graph below is such an example. The reader can easily construct examples which show that the above condition is not sufficient for the existence of a Hamiltonian cycle.

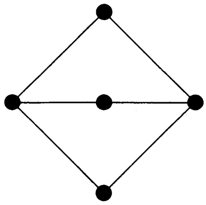


FIGURE 11.3. A graph that has no Hamiltonian cycle

A directed complete graph is called a **tournament** since it can be used to record the outcome of a round robin tournament (where every contestant is matched against every other contestant). The arrows on the edges would indicate the win-loss record.

THEOREM 11.2.4. *A directed complete graph always contains a Hamiltonian path.*

PROOF. Take a path of longest length in which each of the vertices are visited exactly once. The claim is that all the vertices of the graph are included. Suppose that $(x_1, ..., x_m)$ is our path and say that x_0 is not included in this. If (x_0, x_1) is an edge, then we can add this to or path and get a longer path in which all the vertices are distinct. Thus, (x_1, x_0) is in the graph. If (x_0, x_2) were in the graph, we can create the longer path $(x_1, x_0, x_2, ...)$ contrary to our choice. In this way, we deduce that (x_m, x_0) is in the graph which means we could have added it at the end of the path, which is again a contradiction. ∎

Theorem 11.2.4 has applications to the job-sequencing problem where we must arrange jobs to be performed in a sequence so as no time is wasted. For instance, suppose n books are to be printed and then bound. There is one printing machine and one binding machine. Let p_i denote the printing time of the i-th book and b_i the binding time for the i-th book. For any two books, i and j, we know that either $p_i \leq b_j$ or $p_j \leq b_i$. Theorem 11.2.4 tells us that it is possible to specify the order in which the books are printed and then bound so that the binding machine will be kept busy until all the books are bound once the first book is printed. Thus, the total time for completing the task is

$$p_k + \sum_{i=1}^{n} b_i$$

for some k. Indeed, we construct a directed complete graph on n vertices; there is a directed edge from i to j if and only if $b_i \geq p_j$. A

Hamiltonian path is an ordering of the books satisfying the above condition.

11.3. Ramsey Theory

The pigeonhole principle is a fundamental tool in mathematics. It basically says that if we have n pigeonholes and $n+1$ objects are placed in these pigeonholes, then there is at least one pigeonhole with two objects. Though this sounds like a simple principle, its mode of application can be very ingenious at times leading to striking results. For instance, in any simple graph, there are two vertices of the same degree. To see this, suppose there are n vertices. Then, the degrees are elements of the set $\{0, 1, ..., n-1\}$. If no two vertices have the same degree, then the vertex degrees must hit every value in this set. In particular, one must have degree $n-1$. But then, this means there is no vertex of degree 0. This is an instance of the pigeonhole principle. To give another example, in any $n+1$ numbers chosen from the natural numbers less than or equal to $2n$, two of them must be consecutive. By the same principle, one can deduce that there are two numbers, one which divides the other.

A generalization of the pigeonhole principle is the averaging argument. This says that given any numbers $x_1, ..., x_n$, one of these numbers is at least as large as the average $(x_1 + ... + x_n)/n$. Again, this simple principle has surprising consequences. For one thing, it generalizes the pigeonhole principle in the following way. If we put $kn+1$ objects into n pigeonholes, then one of the pigeonholes contains at least $k+1$ objects. Indeed, if x_i denotes the number of objects in the i-th pigeonhole, then the average of the x_i's is $k + 1/n$ and so at least one x_i is greater than $k + 1/n$. But as x_i is an integer, this must be at least $k+1$.

A vast generalization of the pigeonhole principle falls under the name of Ramsey theory. Frank Plumpton Ramsey (1906-1930) wrote on logic, mathematics and philosophy. The basic idea of Ramsey theory can be summarized by the words of Theodore Samuel Motzkin (1908-1970): "Complete disorder is impossible".

It can be illustrated by the following amusing fact. In any group of six people, there are either three mutual friends or three mutual strangers. This can be stated in graph-theoretic terms as follows. Take the complete graph K_6 whose vertices represent the six people. Colour the edge red if the two people know each other, otherwise, colour it blue. We claim that there must be a monochromatic triangle. To see this, note that each vertex has degree 5 and so there must be three edges of the same colour emanating from every vertex. Select one, and suppose without loss of generality, these edges are red connecting these vertices. If any one of the edges connecting these three vertices is red, we are done. If not, then we have a blue triangle and we are done. It is not hard to see that such a result cannot be inferred if we had K_5. Thus, 6 is the minimal number which ensures a monochromatic triangle from any random colouring of its edges.

Ramsey's generalization of this fact can be stated as follows:

THEOREM 11.3.1 (Ramsey, 1930). *Let $a, b \geq 2$ be integers and let*

$$n = \binom{a+b-2}{a-1}.$$

Then, any edge colouring of K_n with red and blue contains a red K_a or a blue K_b.

REMARK 11.3.2. The case discussed above is $a = b = 3$ and $n = 6$.

PROOF. The proof proceeds by induction on $a + b$. The case $a = b = 2$ is trivial. So assume $a > 2$ and $b > 2$ and that we have established the theorem for lower $a + b$. In particular, if

$$n_1 = \binom{a+(b-1)-2}{a-1}$$

and the edges of K_{n_1} are coloured using red and blue, then there is bound to be a red K_a or a blue K_{b-1}. Again, by induction, if

$$n_2 = \binom{(a-1)+b-2}{(a-1)-1}$$

then, there is bound to be a red K_{a-1} or a blue K_b. Now, to deduce the result for a, b, let n be as stated in the theorem and suppose we have randomly coloured the edges of K_n with red and blue. Consider one vertex v and look at its incident edges. There are $n - 1$ of them. By the recurrence for the binomial coefficients,

$$n-1 = \binom{a+b-2}{a-1} - 1 = \binom{a+b-3}{a-1} + \binom{a+b-3}{a-2} - 1$$
$$= n_1 + n_2 - 1 > (n_1 - 1) + (n_2 - 1).$$

Thus, these $n-1$ edges incident at v must contain at least n_1 blue edges or n_2 red edges (for otherwise, we would have $\leq n_1 - 1$ blue edges and $\leq n_2 - 1$ red edges which give us a total of $< n - 1$ edges incident at v). We consider only the first case since the other case is similar. In this case, the complete graph K_{n_1} vertices formed by the n_1 vertices incident with the above blue edges, contains a red K_a or a blue K_{b-1}. If the former is the case, we are done. If the latter, then together with the vertex v, we have the required K_b. This completes the proof. ∎

If we define the **Ramsey number** $R(a, b)$ to be the smallest value of n such that any 2-colouring of K_n contains a monochromatic K_a or K_b, then our remark above shows that $R(3, 3) \leq 6$. It is not difficult to see that K_5 can be 2-coloured in such a way there is no monochromatic triangle. Simply colour the 'outer' edges of K_5 one colour and the 'inner' edges another colour. Thus, $R(3, 3) = 6$. Our theorem above shows that in general

$$R(a, b) \leq \binom{a+b-2}{a-1}.$$

The precise determination of these numbers is still a major unsolved problem in this area.

There are several ways in which the theorem has been generalized. One way is to extend it to more colourings than just 2 colours. Thus, if K_n is edge coloured using r colours, and we specify positive integers $a_1, ..., a_r$, then how large must n be so that we are sure to have a subgraph K_{a_i} with the i-th colour. Does such an n even exist. This is established by the following:

THEOREM 11.3.3. *Let positive integers $a_1, ..., a_r$ be given. Then, there exists an n such that if K_n is edge coloured using r colours, then there is some K_{a_i} with the i-th colour.*

PROOF. We induct on r. We have already proved the case $r = 2$. Suppose then $r > 2$. By induction, there is an n_0 such that if we edge colour K_{n_0} using $r - 1$ colours, then there is some K_{a_i} with the i-th colour. Thus, we have applied the induction process with $r - 1$ and $a_2, ..., a_{r-1}$. Now let $n = R(a_1, n_0)$. By Theorem 11.3.1, any 2-colouring of K_n contains either K_{a_1} with the first colour or a K_{n_0} with the other colour. If the former, we are done. If the latter, by induction, the proof is complete. ∎

As can be seen, Ramsey theory is a merging of the induction technique with the pigeonhole principle. Its application in many problems can sometimes be quite subtle.

Here are two applications. In any sequence $a_1, \ldots, a_m$ of $m = R(n+1, n+1)$ distinct numbers, there is a monotonic subsequence of length $n+1$. Paul Erdös (1913-1996) and George Szekeres (1911-2005) proved this to hold for any sequence of n^2+1 numbers. See also Exercise 11.4.8. We take $m = R(n+1, n+1)$ and represent the numbers by the vertices of K_m. If $a_i < a_j$, we colour the edge i, j red; otherwise we colour it blue. Then, the result follows from Ramsey's theorem.

A famous theorem of Robert Palmer Dilworth (1914-1993) from 1955 says that any partial ordering of $ab + 1$ elements contains a chain of length $a+1$ or an antichain of length $b+1$ (where by an antichain, we mean a subset no two of which are comparable). For example, if we have $n+1$ natural numbers partially ordered by divisibility, then either there are two elements, one which divides the other, or all the numbers are incomparable. If we replace $ab+1$ by $R(a+1, b+1)$, then this is an immediate consequence of Ramsey's theorem since again, we can represent the vertices of K_n with $n = R(a+1, b+1)$ by the elements. We colour a pair x, y red if x and y are comparable and blue otherwise. Ramsey's theorem yields a red K_{a+1} or a blue K_{b+1} from which we deduce the result. See also Exercise 11.4.20.

In 1916, Issai Schur (1875-1941) applied Theorem to show that for any prime p sufficiently large, the "Fermat equation" mod p always has a solution. That is, $a^m + b^m \equiv c^m \pmod{p}$ can be solved provided $p > f(m)$ for some number $f(m)$. Schur shows that $f(m) = m!e + 1$ works.

In fact, Schur's theorem is based on the following result.

THEOREM 11.3.4. *Suppose m is a positive integer. Then there is an M such that if the positive integers $\{1, 2, ..., M-1\}$ are partitioned into m sets, the equation $x + y = z$ has a solution in at least one of the sets.*

PROOF. By Ramsey's Theorem 11.3.3, there is an M such that if the edges of K_M are coloured using m colours, then there is a monochromatic triangle. Let us assign a colour to each block of the given partition of $\{1, 2, ..., M-1\}$. Now colour the edge (i, j) with the colour assigned to the block in which $|i-j|$ appears. Since there is a monochromatic triangle, there are elements $1 \leq i < j < k \leq M$ such that $|i-j| = j-i, |j-k| = k-j$ and $|i-k| = k-i$ have the same colour, that is, lie in the same block. Then $x = j-i, y = k-j, z = k-i$ lie in the same block and we have $x + y = z$. ∎

COROLLARY 11.3.5. *There is an $f(m)$ such that for any prime $p > f(m)$, the equation $a^m + b^m \equiv c^m \pmod{p}$ always has a non-zero solution.*

PROOF. Let $f(m) = M$ as in Theorem 11.3.4. For any prime $p > M$, we consider the cosets of $\mathbf{F}_p^{*m} := \{u^m : u \in \mathbf{F}_p \setminus \{0\}\}$ in $\mathbf{F}_p$. There are m such cosets. Pick m distinct colours corresponding to each of the cosets. We now colour the elements of $\{1, 2, ..., M-1\}$ with the m colours according as the coset they lie in. By Theorem 11.3.4, we can solve $x + y = z$ in one of the cosets. Since the cosets are of the form $u\mathbf{F}_p^{*m}$ for some $u \neq 0$, we may write $x = ua^m, y = ub^m, z = uc^m$ and the theorem is now clear after canceling the u, which we can do since $u \neq 0$.

Moreover, a, b, c are all non-zero since they lie in $\mathbf{F}_p^*$. This completes the proof. ■

We conclude our discussion of Ramsey theory with an exponential lower bound for the Ramsey number $R(a, a)$. The next theorem uses the probabilistic method, a very powerful tool in combinatorics.

THEOREM 11.3.6 (Erdös, 1947). *The Ramsey number $R(a, a)$ satisfies the inequalities*

$$2^{a/2} \leq R(a, a) \leq 2^{2a}.$$

PROOF. The second inequality follows from Theorem 11.3.1 because

$$\binom{2a-2}{a-1} \leq 2^{2a-2} < 2^{2a}.$$

For the lower bound, we apply a "probabilistic" method as follows. Let us count the number of colourings on n vertices which contain a "red" K_a or a "blue" K_a. From the n vertices, we choose a vertices and make a "red" complete graph on a vertices. The number of ways of completing this graph is clearly

$$2^{\binom{n}{2} - \binom{a}{2}}.$$

Since we can do this construction for either of the two colours, the number of graphs on n vertices which contain a red K_a or a blue K_a is at most

$$2\binom{n}{a} 2^{\binom{n}{2} - \binom{a}{2}}.$$

If this quantity is strictly less than $2^{\binom{n}{2}}$ then there are graphs on n vertices whose 2-colouring of the edges do not contain a monochromatic K_a. Thus, we can conclude $R(a, a) > n$. Now we estimate n. Notice that we have

$$2\binom{n}{a} < 2^{\binom{a}{2}}.$$

Since

$$\binom{n}{a} < \frac{n^a}{a!}$$

we can ensure this condition if

$$\frac{2n^a}{a!} < 2^{\binom{a}{2}}.$$

Taking logarithms, we find upon using the trivial inequality $\log a! \leq a \log a$, we get

$$\log n < \frac{a-1}{2} \log 2 + \log a - \frac{\log 2}{a}$$

which is satisfied if $n = 2^{a/2}$. ■

11.4. Exercises

EXERCISE 11.4.1. Draw the line graph of $K_{3,3}$ and determine its chromatic number.

EXERCISE 11.4.2. Show that the Petersen graph (Figure 10.2) has no Hamiltonian cycles.

EXERCISE 11.4.3. Show that the edge-chromatic number of the Petersen graph is 4.

EXERCISE 11.4.4. If X is a 3-regular graph with a Hamiltonian cycle, show that $\chi_e(X) = 3$.

EXERCISE 11.4.5. Show that $K_{r,s}$ has no Hamiltonian cycle unless $r = s$.

EXERCISE 11.4.6. Show that $K_{s,s}$ contains $\frac{s!(s-1)!}{2}$ Hamiltonian cycles.

EXERCISE 11.4.7. Show that every path of 5 vertices lies in the dodecahedron lies in a Hamiltonian cycle.

EXERCISE 11.4.8. If X has a Hamiltonian path, then for each $S \subset V(X)$, the number of components of $X \setminus S$ is at most $|S| + 1$.

EXERCISE 11.4.9. Every set of n integers contains a nonempty subset whose sum is divisible by n. Show that there are sets of $n-1$ integers with no such subset.

EXERCISE 11.4.10. Show that every sequence of $mn+1$ real numbers contains either an increasing subsequence of length at least $m + 1$ or a decreasing subsequence of length at least $n + 1$. Show that there are sequences of mn real numbers for which the above conclusion fails.

EXERCISE 11.4.11. Let $a_1, \dots, a_n$ be nonnegative integers whose sum is k. If $k \leq 2n + 1$, show that for any $m \in [k]$, there exists $I \subset [n]$ such that

$$\sum_{i \in I} a_i = m.$$

For $k = 2n + 2$, describe a set of n nonnegative integers for which the statement above fails.

EXERCISE 11.4.12. Let S be a subset of the set of natural numbers $\leq 2n$. If $|S| = n + 1$, show that

(1) there are two elements in S which are coprime.
(2) there are two elements in S, one of which divides the other.

Describe a subset of n natural numbers less than $2n$ where each of the previous conclusions does not hold.

EXERCISE 11.4.13. Show that for any red-blue colouring of the edges of K_6, there exists a monochromatic cycle on 4 vertices. Show that this is not true for K_5.

EXERCISE 11.4.14. Show that the maximum number of edges in a non-Hamiltonian graph on n vertices is $\binom{n-1}{2} + 1$.

EXERCISE 11.4.15. Among five points in plane with no three collinear, show there are four that determine a convex quadrilateral.

EXERCISE 11.4.16. Among nine points in plane with no three collinear, show there are five that determine a convex pentagon.

EXERCISE 11.4.17. Let $n \geq 3$ be an integer number. Show that every set of $\binom{2n-4}{n-2} + 1$ points in the plane with no three collinear contains an n-subset forming a convex polygon.

EXERCISE 11.4.18. Consider a cycle on 8 vertices in which we join the opposite vertices. Show that the 3-regular graph obtained contains no triangles and its independence number is at most 4.

EXERCISE 11.4.19. Show that $R(3,4) = 9$.

EXERCISE 11.4.20. Recall that a poset P is a set P and a binary relation $\leq$ that is reflexive, transitive and antisymmetric. A **chain** is a sequence $a_1 < a_2 < \cdots < a_k$. An **anti-chain** is a subset of pairwise incomparable elements. If P is a finite poset, show that the minimum number of chains that cover P equals the maximum size of an antichain.

CHAPTER 12

Regular Graphs

12.1. Eigenvalues of Regular Graphs

Recall that a k-regular graph is one in which every vertex has degree k. Thus, every row sum (and hence every column sum) of its adjacency matrix A is k. We have seen (see Exercise 4.5.1) that k is an eigenvalue of A. Moreover, it is easy to see that all the eigenvalues λ satisfy $|\lambda| \leq k$. Indeed, let $v = (x_1, ..., x_n)^t$ be an eigenvector with eigenvalue λ. Then

$$\lambda v = Av$$

implies that

$$\lambda x_i = \sum_{(i,j)\in E} x_j.$$

Without loss of generality, we may suppose $|x_1| = \max_i |x_i|$. Then,

$$|\lambda||x_1| \leq k|x_1|,$$

from which we infer $|\lambda| \leq k$. A similar argument shows that if X is connected, then the multiplicity of $\lambda_0 = k$ is one. In fact, the same argument shows that the multiplicity of $\lambda_0 = k$ is the number of connected components of X. To see this, let $v = (x_1, ..., x_n)^t$ be an eigenvector corresponding to the eigenvalue k and without loss of generality, suppose $|x_1|$ is maximal as before. We may also suppose $x_1 > 0$. Then,

$$kx_1 = \sum_{(1,j)\in E} x_j \leq kx_1$$

which means that there is no cancelation in the sum and all the x_j's are equal to x_1.

Thus, if X is a connected k-regular graph, we may arrange the eigenvalues as

$$k = \lambda_0(X) > \lambda_1(X) > \cdots > \lambda_n(X) \geq -k.$$

It is not difficult to show that $-k$ is an eigenvalue of X if and only if X is bipartite, in which case, its multiplicity is again equal to the number of connected components.

Indeed, we have already observed (see Theorem 4.3.1) that the eigenvalues of the adjacency matrix of a bipartite graph occur in pairs λ_i, λ_j with $\lambda_i = -\lambda_j$. To show that if $-k$ is an eigenvalue of a connected k-regular graph X, that X must be bipartite, we let $(x_1, ..., x_n)$ be an eigenvector corresponding to $-k$. Then,

$$-kx_i = \sum_{j=1}^{n} a_{ij}x_j$$

implies

$$k|x_i| \leq \sum_{j=1}^{n} a_{ij}|x_j| \leq k|x_i|$$

if i is an index such that $|x_i|$ is maximal among the absolute values of the components of $(x_1, ..., x_n)$. The above inequality implies that we must have $|x_i| = |x_j|$ for any j adjacent to i. Since the graph is connected, this must be true of every component. Since the eigenvector is non-zero, each component must be strictly positive or strictly negative. Now let A be the vertices i such that $x_i > 0$ and B the vertices where $x_i < 0$. We can now show that A and B are independent sets. Indeed, if $x_i > 0$, then the relation

$$-kx_i = \sum_{j=1}^{n} a_{ij}x_j$$

shows that if we let a_i be the number of vertices in A adjacent to i and b_i the number of vertices adjacent to i in B, then

$$a_i - b_i = -k.$$

But $a_i + b_i = k$ so we deduce $2a_i = 0$. Hence, if $-k$ is an eigenvalue of a k-regular graph, then X is bipartite.

Any eigenvalue $\lambda_i \neq \pm k$ is referred to as a non-trivial eigenvalue. We denote by $\lambda(X)$ the maximum of the absolute values of all the non-trivial eigenvalues. We will see in the next sections that $\lambda(X)$ has closed connections with the structure of X.

12.2. Diameter of Regular Graphs

Recall that we defined a metric on a connected graph by defining the distance $d(x, y)$ for $x, y \in V$ as the minimal length amongst all the paths from x to y. The **diameter** of a connected graph was then the maximum value of the distance function. We begin by deriving an estimate for the diameter involving $\lambda(X)$ due to Fan Chung. If A is the adjacency matrix, then the (x, y)-th entry of A^r is the number of paths from x to y of length r. Hence, if m is the diameter of X, then every entry of A^m is strictly positive.

Let $n = |V|$ and $u_0, u_1, ..., u_{n-1}$ be an orthonormal basis of eigenvectors of A with corresponding eigenvalues $\lambda_0, ..., \lambda_{n-1}$ respectively. We may take $u_0 = u/\sqrt{n}$ where $u = (1, 1, ..., 1)$ as defined earlier. We can write

$$A = \sum_{i=0}^{n-1} \lambda_i u_i u_i^t.$$

More generally,

$$A^r = \sum_{i=0}^{n-1} \lambda_i^r u_i u_i^t.$$

In particular, we see that the (x, y)-th entry of A^m is

$$= \sum_i \lambda_i^m (u_i u_i^t)_{x,y}$$

which is

$$\geq \frac{k^m}{n} - \left| \sum_{i \geq 1} \lambda_i^m (u_i)_x (u_i)_y \right|.$$

Let us assume that X is not bipartite (so that $-k$ is not an eigenvalue. Then, by the Cauchy-Schwarz inequality,

$$\left| \sum_{i \geq 1} \lambda_i^m (u_i)_x (u_i)_y \right| \leq \lambda(X)^m \left(\sum_{i \geq 1} (u_i)_x^2 \right)^{1/2} \left(\sum_{i \geq 1} (u_i)_y^2 \right)^{1/2},$$

which is easily seen to be

$$\leq \lambda(X)^m (1 - (u_0)_x^2)^{1/2} (1 - (u_0)_y^2)^{1/2} \leq \lambda_1^m (1 - 1/n).$$

Thus, (x, y)-th entry of A^m is always positive if

$$\frac{k^m}{\lambda(X)^m} > n - 1.$$

If X is bipartite, it is easy to see that we get

$$\frac{2k^m}{\lambda(X)^m} > n - 1.$$

In other words, we have proved

THEOREM 12.2.1. *Let X be a k-regular graph with n vertices and diameter m. If X is not bipartite, then*

$$m < \frac{\log(n-1)}{\log(k/\lambda(X))}.$$

If X is bipartite, then we have the sharper inequality

$$m < \frac{\log[(n-1)/2]}{\log(k/\lambda(X))}.$$

This inequality also shows that regular graphs with small $\lambda(X)$, have small diameter. In communication theory, one requires the network to have small diameter for efficient operation. Note that the diameter of a connected, k-regular graph X on n vertices is always at least $\frac{\log(n-1)-2}{\log k}$ (see Exercise 5.5.20). The best upper bound obtained from the previous result is about twice as large as this lower bound.

At this point, a natural question is how small can $\lambda(X)$ be ? The following elementary observation about the eigenvalue $\lambda(X)$ is worth making. Observe that the eigenvalues of A^2 are simply the squares of the eigenvalues of A. On the other hand, the trace of A^2 is simply kn for a k-regular graph X. Thus, if X is not bipartite,

$$k^2 + (n-1)\lambda(X)^2 \geq kn$$

which gives the inequality

$$\lambda(X) \geq \left(\frac{n-k}{n-1}\right)^{1/2} \sqrt{k}.$$

If X is bipartite, then

$$2k^2 + (n-2)\lambda(X)^2 \geq nk,$$

in which case

$$\lambda(X) \geq \left(\frac{n-2k}{n-2}\right)^{1/2} \sqrt{k}.$$

If we think of k as fixed and $n \to \infty$, then we see that

$$\lim_{n\to\infty} \lambda(X) \geq \sqrt{k}.$$

An asymptotic version of a theorem of Alon and Bopanna from 1986 asserts that

$$\operatorname{liminf}_{n\to\infty}\lambda(X_{n,k}) \geq 2\sqrt{k-1} \tag{12.2.1}$$

where the limit is taken over k-regular graphs with n going to infinity. Several proofs of this result exist in the literature. A sharper version was derived by Nilli in 1991.

THEOREM 12.2.2. *Suppose that X is a k-regular graph. Assume that the diameter of X is $\geq 2b+2 \geq 4$. Then*

$$\lambda_1(X) \geq 2\sqrt{k-1} - \frac{2\sqrt{k-1}-1}{b}.$$

Let us make the following observation. If $m = d(u, v)$ is the diameter of X, then the number of paths from u of length m is $\leq k^m$ and as each such path has $m + 1$ vertices, we deduce that the number of vertices n satisfies the inequality

$$n \leq (m+1)k^m.$$

Thus, if k is fixed and $n \to \infty$, then the diameter also tends to infinity. In particular, Theorem 12.2.2 implies inequality (12.2.1) since $\lambda(X) \geq \lambda_1(X)$.

We preface our proof of Theorem 12.2.2 by recalling the Rayleigh-Ritz Theorem from Chapter 6, Section 6.8. Let A be a symmetric matrix (a similar analysis applies to Hermitian matrices). Let $\lambda_{\max}$ and λ_{min} be the largest and smallest eigenvalues of A respectively. Then, we have

$$\lambda_{\max} = \max_{v \neq 0} \frac{(Av, v)}{(v, v)}$$

and

$$\lambda_{\min} = \min_{v \neq 0} \frac{(Av, v)}{(v, v)}.$$

Now let $L(X)$ denote the space of real-valued functions on X. We can equip the vector space $L(X)$ with an inner product by defining

$$(f, g) = \sum_{x \in X} f(x) g(x).$$

We can view the adjacency matrix as acting on $L(X)$ via the formula

$$(Af)(x) = \sum_{(x,y) \in E(X)} f(y).$$

For a connected k-regular graph, $\lambda_0 = k$ is an eigenvalue of multiplicity 1 and the corresponding eigenspace is the set of constant functions. Hence, we can decompose our space as

$$L(X) = \mathbf{R} f_0 \oplus L_0(X)$$

where $f_0 \equiv 1$ and $L_0(X)$ is the space of functions orthogonal to f_0. Thus, we can consider A as operating on $L_0(X)$. By the Rayleigh-Ritz theorem,

$$\lambda_1(X) = \max_{\substack{f \neq 0 \\ (f, f_0) = 0}} \frac{(Af, f)}{(f, f)}.$$

Since we want a lower bound for $\lambda_1(X)$, it is natural to consider the matrix $\Delta = kI - A$ whose eigenvalues are easily seen to be $k - \lambda_i$

$(0 \leq i \leq n-1)$. (Δ is a discrete analogue of the classical Laplace operator.) Thus,

$$k - \lambda_1(X) = \min_{\substack{f \neq 0 \\ (f, f_0)=0}} \frac{(\Delta f, f)}{(f, f)}.$$

The strategy now is to find an appropriate function f, obtain an upper bound for (f, f) and a lower bound for $(\Delta f, f)$. We can now prove Theorem 12.2.2.

PROOF. Let $u, v \in G$ be such that $d(u, v) \geq 2b+2$. For $i \geq 0$, define sets

$$U_i = \{x \in G : d(x, u) = i\}$$
$$V_i = \{x \in G : d(x, v) = i\}.$$

Then, the sets $U_0, U_1, ..., U_b, V_0, V_1, ..., V_b$ are disjoint, for otherwise, by the triangle inequality we get $d(u, v) \leq 2b$ which is a contradiction. Moreover, no vertex of

$$U = \cup_{i=0}^{b} U_i$$

is adjacent to

$$V = \cup_{i=0}^{b} V_i$$

for otherwise $d(u, v) \leq 2b+1$ which is a contradiction. For each vertex in U_i, at least one lies in U_{i-1} and at most $q = k-1$ lie in U_{i+1} (for $i \geq 1$). Thus,

$$|U_{i+1}| \leq q|U_i|.$$

By the same logic, $|V_{i+1}| \leq q|V_i|$. By induction, we see that $|U_b| \leq q^{(b-i)}|U_i|$ and $|V_b| \leq q^{(b-i)}|V_i|$. We will set $f(x) = f_i$ for $x \in U_i$, $f(x) = g_i$ for $x \in V_i$ and zero otherwise, with the f_i and g_i to be chosen later. Now,

$$(f, f) = A + B$$

where

$$A = \sum_{i=0}^{b} f_i^2 |U_i|$$

and

$$B = \sum_{i=0}^{b} g_i^2 |V_i|.$$

By the inequalities derived above, we get

$$(f, f) \geq \sum_{i=0}^{b} f_i^2 q^{-(b-i)} |U_b| + \sum_{i=0}^{b} g_i^2 q^{-(b-i)} |V_b|.$$

We now choose $f_0 = \alpha$, $g_0 = \beta$, $f_i = \alpha q^{-(i-1)/2}$ and $g_i = \beta q^{-(i-1)/2}$ for $i \geq 1$. Thus,

$$(f, f) \geq (\alpha^2 + \beta^2)\left(1 + b\frac{|V_b|}{q^{b-1}}\right).$$

We choose α and β so that $(f, f_0) = 0$.

Now we derive an upper bound for $(\Delta f, f)$. Note that

$$\frac{1}{2}\sum_{(x,y)\in E}(f(x) - f(y))^2 = k(f, f) - (Af, f) = (\Delta f, f)$$

by an easy calculation. Let A_U denote the sum

$$\frac{1}{2}\sum_{\substack{(x,y)\in E\\ x \text{ or } y\in U}}(f(x) - f(y))^2$$

and let A_V be defined similarly. If we partition according to the contribution from each U_i and keep in mind that each $x \in U_i$ has at most $q = k - 1$ neighbours in U_{i+1}, we obtain

$$A_U \leq \sum_{i=1}^{b-1}|U_i|q\left(q^{-(i-1)/2} - q^{-i/2}\right)^2\alpha^2 + |U_b|q \cdot q^{-(b-1)}\alpha^2.$$

This is easily computed to be

$$= (\sqrt{q} - 1)^2\left(|U_1| + |U_2|q^{-1} + \cdots + |U_{b-1}|q^{-(b-2)} + |U_b|q^{-(b-1)}\right)\alpha^2$$
$$+\alpha^2(2\sqrt{q} - 1)|U_b|q^{-(b-1)}.$$

Consequently,

$$A_U \leq (\sqrt{q} - 1)^2(A - \alpha^2) + (2\sqrt{q} - 1)\frac{A - \alpha^2}{b}$$

which is less than

$$\left(1 + q - 2\sqrt{q} + \frac{2\sqrt{q} - 1}{b}\right)A.$$

Similarly,

$$A_V < \left(1 + q - 2\sqrt{q} + \frac{2\sqrt{q} - 1}{b}\right)B.$$

Combining these inequalities gives

$$k - \lambda_1(X) < 1 + q - 2\sqrt{q} + \frac{2\sqrt{q} - 1}{b}$$

which proves the theorem. ■

12.3. Ramanujan Graphs

The previous theorem motivates the definition of a **Ramanujan graph**. A k-regular graph is said to be **Ramanujan** if

$$\lambda(X) \leq 2\sqrt{k-1}.$$

This notion was introduced by Lubotzky, Phillips and Sarnak in a fundamental paper from 1986 in which they constructed infinite families of k-regular Ramanujan graphs whenever $k-1$ is a prime power. The graphs were named after Srinivasan Ramanujan (1887-1920) because the construction obtained by Lubotzky, Phillips and Sarnak and independently by Margulis, used deep number theoretic results related a conjecture of Ramanujan.

In view of the Alon-Bopanna theorem, these graphs are extremal with respect to the property of trying to minimize $\lambda(X)$ in the class of all k-regular graphs. Given $k \geq 3$, the explicit construction of an infinite family of k-regular Ramanujan graphs is still a major unsolved problem for any given k. So far, such constructions have been possible using deep results from algebraic geometry and number theory and only when $k-1$ is a prime power. For example, no one has been able to construct an infinite family of 7-regular Ramanujan graphs.

The complete graph K_n is an $(n-1)$-regular Ramanujan graph. Also, the cycle graph C_n is a 2-regular Ramanujan graph.

In section 4, we will construct a family of regular graphs using group theory and determine explicitly the eigenvalues of the adjacency matrix in terms of group characters. This will allow us to construct some explicit examples of Ramanujan graphs.

12.4. Basic Facts about Groups and Characters

A group G is a set together with a binary operation $*$ (say) satisfying the following axioms:

(1) $a, b \in G$ implies $a * b \in G$ (closure);
(2) $a, b, c \in G$ implies $(a * b) * c = a * (b * c)$ (associativity);
(3) there is an element called the **identity** $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (identity element);
(4) for any $a \in G$, there is a $b \in G$ so that $a * b = b * a = e$ (inverses); we write a^{-1} to denote the inverse of a.

If in addition to this, $a * b = b * a$ for all $a, b \in G$, we say that G is abelian or commutative. When G is finite, we call the size of G the **order** of G. Note also that in a group, we have the **cancelation law**: $a * b = a * c$ implies $b = c$ since we can multiply both sides on the left by a^{-1}. Warning: if $a * b = c * a$, we cannot necessarily conclude that $b = c$.

See example 6 below. The cancelation law also shows that the identity element is unique because if there were two e, e' say, then $a = ae = ae'$ and we deduce $e = e'$.

The reason for studying groups in the abstract is that many scientific discoveries can be formulated in the language of group theory. In addition, the fundamental particles in the heart of the atom seem to know everything about non-abelian groups! In fact, the character theory of certain subgroups of the group $GL_2(\mathbf{C})$ (see example 6 below) led to the discovery of new sub-atomic particles in the early 20th century.

Here are some examples of groups.

(1) $\mathbf{Z}$ under addition.

(2) $\mathbf{Z}$ under multiplication is not a group since there are no inverses.

(3) $\mathbf{R}^*$, non-zero reals under multiplication.

(4) $\mathbf{C}^*$, non-zero complex numbers under multiplication.

(5) $\mathbf{C}$ and $\mathbf{R}$ under addition.

All of these are examples of infinite abelian groups.

(6) $GL_2(\mathbf{R})$, or $GL_2(\mathbf{C})$ the collection of 2×2 invertible matrices with entries in $\mathbf{R}$ or $\mathbf{C}$ is a group under multiplication.

These are infinite non-abelian groups. Notice that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

We **cannot** cancel the matrix

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

from both sides of the equation!

(7) $\mathbf{Z}/n\mathbf{Z}$ under addition consists of residue classes modulo n. This is a finite abelian group of order n.

(8) $\mathbf{Z}/6\mathbf{Z}$ with multiplication is not a group since the residue class 2 does not have an inverse.

(9) $(\mathbf{Z}/p\mathbf{Z})^*$ is the set of coprime residue classes mod p, with p prime. This is a finite abelian group of order $p - 1$.

To indicate $a * b$ we sometimes drop the $*$ and simply write ab with no cause for confusion. There is a general tendency to use the multiplicative notation for writing the group law although there is non universal convention about this. Part of the reason for this is to emphasize that the groups we are dealing with need not be abelian. There is also a tendency to use the symbol 1 to denote the identity element (and 0 when we write the group additively).

(10) The symmetries of the equilateral triangle, namely rotation by 60 degrees denoted r and a flip about the vertical axis f generates a non-abelian group of order 6. This group is isomorphic to the group of permutations on 3 letters.

THEOREM 12.4.1. *If G is a finite abelian group of order n, then $g^n = 1$ for any element $g \in G$.*

PROOF. Let $g_1, ..., g_n$ be the distinct elements of G. The elements

$$gg_1, gg_2, ..., gg_n$$

are also distinct and therefore must be all of the elements of the group. Thus,

$$g_1 \cdots g_n = gg_1 \cdots gg_n = g^n(g_1 \cdots g_n)$$

and canceling by $(g_1 \cdots g_n)$, we deduce the result. ∎

This theorem can be thought of as a generalization of Fermat's little theorem which says that if p is prime and a is coprime to p, then

$$a^{p-1} \equiv 1(\bmod p).$$

Theorem 1 is true for non-abelian groups also and is due to Lagrange.

A group is called **cyclic** if there is an element g_0 such that every element of the group is of the form g_0^m for some integer m. For instance, $\mathbf{Z}$ is a cyclic group under addition with generator 1. As any cyclic group is countable, the group of non-zero reals under multiplication and the group of additive reals are not cyclic groups. The group of residue classes mod n under addition, is a cyclic group with generator being the residue class 1. Any coprime residue class will also serve as a generator.

A character χ of a group G is a map

$$\chi : G \rightarrow \mathbf{C}^*$$

such that $\chi(ab) = \chi(a)\chi(b)$. It is an example of a **homomorphism**. The character that sends every element to the element 1 is called the **trivial character**. Notice that any character of a group must take the identity element to 1 because $\chi(1^2) = \chi(1) = \chi(1)^2$ and the only non-zero complex number z satisfying $z^2 = z$ is $z = 1$. Another thing to notice is that $\chi(a^{-1}) = \chi(a)^{-1}$ since $1 = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$ from which the result is immediate. By Theorem 1, we deduce that if G is a finite group of order n,then $\chi(g)$ must be an n-th root of unity since $1 = \chi(g^n) = \chi(g)^n$.

The basic idea of character theory is that to understand the abstract group G, we map into something concrete like the multiplicative group of complex numbers and see how the image looks like to deduce what G looks like. It turns out that if G is a finite abelian group of order n, then there are exactly n distinct characters that one can construct. The set of characters in turn forms a group under multiplication of characters. Indeed, we define for two characters χ and ψ, the product character

$$(\chi\psi)(a) := \chi(a)\psi(a).$$

We call this the character group of G and denote it by $\hat{G}$. The identity element of $\hat{G}$ is the trivial character. The character inverse to χ is χ^{-1} defined by

$$\chi^{-1}(a) = \chi(a)^{-1}.$$

In the case of the additive group of residue classes mod n, all of the characters are given by

$$\chi_j(a) = e^{2\pi i j a/n}, \quad j = 0, 1, 2, ..., (n-1).$$

Notice that χ_0 is the trivial character.

12.5. Cayley Graphs

There is a simple procedure to constructing k-regular graphs using group theory. This can be described as follows. Let G be a finite group and S a k-element subset of G. We suppose that S is *symmetric* in the sense that $s \in S$ implies $s^{-1} \in S$. Now construct the graph $X(G, S)$ by having the vertex set to be the elements of G the (x, y) is an edge if and only if $xy^{-1} \in S$.

The eigenvalues of the Cayley graph are easily determined as follows. The cognoscenti will recognize that it is the classical calculation of the Dedekind determinant in number theory.

THEOREM 12.5.1. *Let G be a finite abelian group and S a symmetric subset of G of size k. Then the eigenvalues of the adjacency matrix of $X(G, S)$ are given by*

$$\lambda_\chi = \sum_{s \in S} \chi(s)$$

as χ ranges over all the irreducible characters of G.

REMARK 12.5.2. Notice that for the trivial character, we have $\lambda_1 = k$. If we have for all $\chi \neq 1$

$$\left| \sum_{s \in S} \chi(s) \right| < k$$

then the graph is connected by our earlier remarks. Thus, to construct Ramanujan graphs, we require

$$\left| \sum_{s \in S} \chi(s) \right| \leq 2\sqrt{k-1}$$

for every non-trivial irreducible character χ of G. This is the strategy employed in many of the explicit construction of Ramanujan graphs.

PROOF. For each irreducible character χ, let v_χ denote the vector $(\chi(g) : g \in G)$. Let $\delta_S(g)$ equal 1 if $g \in S$ and zero otherwise and denote by A the adjacency matrix of $X(G, S)$. Then,

$$(Av_\chi)_x = \sum_{g \in S} \delta_S(xg^{-1})\chi(g).$$

By replacing xg^{-1} by s, and using the fact that S is symmetric, we obtain

$$(Av_\chi)_x = \chi(x) \left(\sum_{s \in S} \chi(s) \right)$$

which shows that v_χ is an eigenvector with eigenvalue

$$\sum_{s \in S} \chi(s)$$

which completes the proof. ■

As mentioned above, this calculation is reminiscent of the Dedekind determinant formula in number theory. Recall that this formula computes $\det A$ where A is the matrix whose (i, j)-th entry is $f(ij^{-1})$ for any function f defined on the finite abelian group G of order n. The determinant is

$$\prod_{\chi} \left(\sum_{g \in G} f(g)\chi(g) \right).$$

The proof is analogous to the calculation in the proof of Theorem 3 and we leave it to the reader. As an application, it allows us to compute the determinant of a circulant matrix. For instance, we can compute the characteristic polynomial of the complete graph. Indeed, it is not hard to see that by taking the additive cyclic group of order n and setting $f(0) = -\lambda$, $f(a) = 1$ for $a \neq 0$, we obtain that the characteristic polynomial is

$$(-1)^n(\lambda - (n-1))(\lambda - 1)^{n-1}$$

by the Dedekind determinant formula. As the complete graph of order n is an $(n-1)$-regular graph, we see immediately from the above calculation that it is a Ramanujan graph.

If G is an abelian group and S is a subset of G, we can define another set of graphs $Y(G, S)$ called *sum graphs* as follows. The vertices consist of elements of G and (x, y) is an edge if $xy \in S$. Arguing as before, we can show

THEOREM 12.5.3. *Let G be an abelian group. For each character χ of G, the eigenvalues of $Y(G, S)$ are given as follows. Define*

$$e_\chi = \sum_{s \in S} \chi(s).$$

If $e_\chi = 0$, then v_χ and v_χ^{-1} are both eigenvectors with eigenvalues zero. If $e_\chi \neq 0$, then

$$|e_\chi| v_\chi \pm e_\chi v_{\chi^{-1}}$$

are two eigenvectors with eigenvalues $\pm|e_\chi|$.

Using this theorem, Winnie Li constructed Ramanujan graphs in the following way. Let $\mathbf{F}_q$ denote the finite field of q elements. Let $G = \mathbf{F}_{q^2}$ and take for S the elements of G of norm 1. This is a symmetric subset of G and the Cayley graph $X(G, S)$ turns out to be Ramanujan. The latter is a consequence of a theorem of Deligne estimating Kloosterman sums.

These results allow us to construct Ramanujan graphs by estimating character sums.

There is a generalization of these results to the non-abelian context. This is essentially contained in a paper by Diaconis and Shahshahani. Using their results, one can easily generalize the Dedekind determinant formula as follows (and which does not seem to be widely known). Let G be a finite group and f a class function on G. Then the determinant of the matrix A whose rows (and columns) are indexed by the elements of G and whose (i, j)-th entry is $f(ij^{-1})$ is given by

$$\prod_\chi \left(\frac{1}{\chi(1)} \sum_{g \in G} f(g)\chi(g) \right)^{\chi(1)}$$

with the product over the distinct irreducible characters of G.

The following theorem is due to Diaconis and Shahshahani.

THEOREM 12.5.4. *Let G be a finite group and S a subset which is stable under conjugation. Let A be the adjacency matrix of the graph $X(G, S)$ (where $u, v \in G$ are adjacent if and only if $uv^{-1} \in S$). Then the eigenvalues of A are given by*

$$\lambda_\chi = \frac{1}{\chi(1)} \sum_{s \in S} \chi(s)$$

as χ ranges over all irreducible characters of G. Moreover, the multiplicity of λ_χ is $\chi(1)^2$.

We remark that the λ_χ in the above theorem need not be all distinct. For example, if there is a non-trivial character χ which is trivial on S, then the multiplicity of the eigenvalue $|S|$ is at least $1 + \chi(1)^2$.

PROOF. We essentially modify the proof of Diaconis and Shahshahani to suit our context. We consider the group algebra $\mathbf{C}[G]$ with basis vectors e_g with $g \in G$ and multiplication defined as usual by $e_g e_h = e_{gh}$. We define the linear operator Q by

$$Q = \sum_{s \in S} e_s = \sum_{g \in G} \delta_S(g) e_g$$

which acts on $\mathbf{C}[G]$ by left multiplication. The matrix representation of Q with respect to the basis vectors e_g with $g \in G$ is precisely the adjacency matrix of $X(G, S)$ as is easily checked. If r denotes the left regular representation of G on $\mathbf{C}[G]$, we find that the action of

$$r(A) = \sum_{s \in S} r(s)$$

on $\mathbf{C}[G]$ is identical to Q. Moreover, $\mathbf{C}[G]$ decomposes as

$$\mathbf{C}[G] = \oplus_\rho V_\rho$$

where the direct sum is over non-equivalent irreducible representations of G and the subspace V_ρ is a direct sum of deg ρ copies of the subspace W_ρ corresponding to the irreducible representation ρ. The result is now clear from basic facts of linear algebra. ■

12.6. Expanders

For any subset A of the vertex set of a graph X, we may define the **edge-boundary** of A, denoted ∂A by

$$\partial A = \{xy \in E(X) : x \in A, y \notin A\}.$$

That is, the edge-boundary of A consists of the edges which are incident to precisely one vertex of A. The **edge-expansion** $h(X)$ of X equals the minimum of $\frac{|\partial A|}{|A|}$, where the minimum is taken over all subsets A of the vertex set of X of order at most $\frac{|V(X)|}{2}$. As many combinatorial invariants, the edge-expansion of a graph is hard to compute.

Let c be positive real number. A k-regular graph X with n vertices is called a c-**expander** if

$$h(X) \geq c. \qquad (12.6.1)$$

A very important problem is constructing infinite families of k-regular c-expanders for fixed $k \geq 3$ and some $c > 0$. Expander graphs play an important role in computer science and the theory of communication networks. These graphs arise in questions about designing networks that connect many users while using only a small number of switches. Our interest in them lies in the fact the theory of c-expanders can be related to the eigenvalue questions of the previous section. This is done in the next theorem.

THEOREM 12.6.1 (Alon-Milman, Dodziuk). *Let X be a k-regular graph. Then*

$$\frac{k-\lambda_1(X)}{2} \leq h(X) \leq \sqrt{2k(k-\lambda_1(X))}.$$

PROOF. We prove only the first inequality, the second inequality is slightly more complicated.

The idea is to apply the Rayleigh-Ritz ratio in the following way. As observed in the previous section, let f be a function defined on $V(X)$ that is orthogonal to the constant function f_0. If $L = kI - A$ is the Laplacian matrix of X, then

$$\frac{(Lf,f)}{(f,f)} \geq k - \lambda_1(X)$$

by Rayleigh-Ritz inequality.

Let A be a subset of $V(X)$ of size at most $\frac{|V(X)|}{2}$. If we set

$$f(x) = \begin{cases} |V(X) \setminus A| & \text{if } x \in A \\ -|A| & \text{if } x \notin A \end{cases}$$

then it is easily seen that $(f, f_0) = 0$. On the other hand, a direct calculation shows that

$$(f,f) = |V(X)||A||V(X) \setminus A|.$$

By using the formula

$$(Lf,f) = \frac{1}{2} \sum_{(x,y)\in E} (f(x) - f(y))^2$$

we easily check that

$$(Lf,f) = |X|^2|\partial A|$$

so that by the previous we obtain

$$\frac{|\partial A|}{|A|} \geq (k - \lambda_1(X))\frac{|V(X) \setminus A|}{|A|} \geq \frac{k-\lambda_1(X)}{2}.$$

Since this inequality holds for each $A \subset V(X)$ of size at most $\frac{|V(X)|}{2}$, it follows that $h(X) \geq \frac{k-\lambda_1(X)}{2}$. ∎

The previous theorem shows that making λ_1 as small as possible gives us good expander graphs. By the Alon-Bopanna theorem, we cannot do better than

$$\lambda(X) \leq 2\sqrt{k-1}.$$

Thus, Ramanujan graphs make excellent expanders.

In 1973, Margulis gave the first explicit construction of an infinite family of 8-regular graphs. Given an nonnegative integer m, consider the graph G_m whose vertex set is $\mathbb{Z}_m \times \mathbb{Z}_m$. Each vertex (x, y) of G_m is adjacent exactly to $(x+y, y), (x-y, y), (x, y+x), (x, y-x), (x+y+1, y), (x-y+1, y), (x, y+x+1), (x, y-x+1)$ where all the operations are done modulo m. Varying m produces an infinite family of 8-regular graphs. Margulis showed these graphs are expanders by using results from group representations. In 1981, Gabber and Galil used harmonic analysis to show that any non-trivial eigenvalue of G_m has absolute value at most $5\sqrt{2} \approx 7.05 < 8$.

12.7. Counting Paths in Regular Graphs

If A is the adjacency matrix of X, it is clear that the (x,y)-th coordinate of A^r enumerates the number of paths of length r from x to y. We will be interested in proper paths, that is paths which do not have back-tracking. We are interested in counting the number of proper paths of length r in a k-regular graph. Let A_r denote the matrix whose (x, y)-th entry will be the number of proper paths from x to y. Then, $A_0 = I$ and $A_1 = A$ and clearly

$$A^2 = A_2 + kI$$

since A_2 encodes the number of proper paths of length 2.

Inductively, it is clear that

$$A_1 A_r = A_{r+1} + (k-1)A_{r-1},$$

since the left hand side enumerates paths of length $r+1$ which are extended from proper paths of length r and the right side enumerates first the proper paths of length $r+1$ and proper paths of length $r-1$ which are extended to 'improper' paths of length r.

This recursion allows us to deduce the following identity of formal power series:

PROPOSITION 12.7.1.

$$\left(\sum_{r=0}^{\infty} A_r t^r\right)\left(I - At + (k-1)t^2\right) = (1-t^2)I.$$

12.8. The Ihara Zeta Function of a Graph

Let X be a k-regular graph and set $q = k - 1$. Motivated by the theory of the Selberg zeta function, Ihara was led to make the following definitions and construct the graph-theoretic analogue of it as follows. A proper path whose endpoints are equal is called a *closed geodesic.* If γ is a closed geodesic, we denote by γ^r the closed geodesic obtained by repeating the path γ r times. A closed geodesic which is not the power of another one is called a *prime geodesic.* We define an equivalence relation on the closed geodesics $(x_0, ..., x_n)$ and $(y_0, ..., y_m)$ if and only if $m = n$ and there is a d such that $y_i = x_{i+d}$ for all i (and the subscripts are interpreted modulo n. An equivalence class of a prime geodesic is called a *prime geodesic cycle.* Ihara then defines the zeta function

$$Z_X(s) = \prod_p \left(1 - q^{-s\ell(p)}\right)^{-1}$$

where the product is over all prime geodesic cycles and $\ell(p)$ is the length of p.

Ihara proves the following theorem:

THEOREM 12.8.1. *For $g = (q-1)|X|/2$, we have*

$$Z_X(s) = (1-u^2)^{-g} \det(I - Au + qu^2)^{-1}, \quad u = q^{-s}.$$

Moreover, $Z_X(s)$ satisfies the "Riemann hypothesis" (that is, all the singular points lie on $Re(s) = 1/2$) if and only if X is a Ramanujan graph.

PROOF. (Sketch) We assume that the zeta function has the shape given and show that it satisfies the Riemann hypothesis if and only if X is Ramanujan. Let $\phi(z) = \det(zI - A)$ be the characteristic polynomial of A. If we set $z = (1 + qu^2)/u$, then the singular points of the $Z_X(s)$ arise from the zeros of $\phi(z)$. Since

$$u = \frac{z \pm \sqrt{z^2 - 4q}}{2q}$$

and any zero of ϕ is real (because A is symmetric), we deduce that

$$\frac{z\overline{u}}{\overline{u}} = \frac{(1+qu^2)\overline{u}}{u\overline{u}} = \frac{\overline{u} + q|u|^2 u}{|u|^2}$$

is also real. Thus, the numerator is real and so, we must have

$$q|u|^2 = 1,$$

which is equivalent to the assertion of the theorem. ∎

12.9. Exercises

EXERCISE 12.9.1. If X is a k-regular graph with eigenvalues $k = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$, determine the eigenvalues of the complement of X.

EXERCISE 12.9.2. A graph X is regular and connected if and only if J is a linear combination of powers of the adjacency matrix A of X.

EXERCISE 12.9.3. Let $k = \lambda_0 > \lambda_1 > \cdots > \lambda_{s-1}$ be the distinct eigenvalues of the adjacency matrix A of a k-regular connected graph X with n vertices. Show that

$$J = \frac{n}{\prod_{i=1}^{s-1}(k-\lambda_i)} \cdot \prod_{i=1}^{s-1}(A - \lambda_i I_n).$$

EXERCISE 12.9.4. A graph X is **strongly regular** with **parameters** (n, k, a, c) if it is k-regular, every pair of adjacent vertices has a common neighbours and every pair of non-adjacent vertices has c common neighbours. Show that the adjacency matrix A of a strongly regular graph X with parameters (n, k, a, c) satisfies the equation

$$A^2 - (a-c)A - (k-c)I = cJ.$$

EXERCISE 12.9.5. Calculate the eigenvalues of a strongly regular graph X with parameters (n, k, a, c).

EXERCISE 12.9.6. Let $q \equiv 1 \pmod 4$ be a power of a prime. The **Paley graph** $\mathbb{P}_q$ has vertices the elements of the field $\mathbb{F}_q$ with x adjacent to y if $x - y$ is a square in $\mathbb{F}_q$. Show that $\mathbb{P}_5 = C_5$ and that $\mathbb{P}_q$ is a strongly regular graph with parameters $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right)$.

EXERCISE 12.9.7. Calculate the eigenvalues of the line graph $L(K_n)$ of the complete graph K_n.

EXERCISE 12.9.8. Calculate the eigenvalues of the complement of the line graph of K_n.

EXERCISE 12.9.9. An $n \times n$ matrix C is called a **circulant matrix** if row i of C is obtained from the first row of C by a cyclic shift of $i-1$ steps for each $i \in [n]$. Let Z be the $n \times n$ circulant matrix whose first row is $[0, 1, 0, \ldots, 0]$. Show that the eigenvalues of Z are $1, \omega, \omega^2, \ldots, \omega^{n-1}$, where $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$.

EXERCISE 12.9.10. Show that the Petersen graph is isomorphic to the complement of the line graph of K_5.

EXERCISE 12.9.11. Calculate the eigenvalues of the Petersen graph.

EXERCISE 12.9.12. Let C be an $n \times n$ circulant matrix whose first row is $[c_1, c_2, \ldots, c_n]$. Show that

$$C = \sum_{i=1}^{n} c_i Z^{i-1},$$

where Z is the $n \times n$ circulant matrix whose first row is $[0, 1, 0, \ldots, 0]$.

EXERCISE 12.9.13. A **circulant graph** is a graph X whose adjacency matrix is a circulant matrix. Show that a circulant graph is regular.

EXERCISE 12.9.14. If $[0, c_2, \ldots, c_n]$ is the first row of the adjacency matrix C of a circulant graph X, show that the eigenvalues of C are

$$\lambda_s = \sum_{i=2}^{n} a_i \omega^{(i-1)s},$$

for $s \in \{0, 1, \ldots, n-1\}$ and $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$.

EXERCISE 12.9.15. Show that the cycle C_n with n vertices is a circulant graph.

EXERCISE 12.9.16. Calculate the eigenvalues of the cycle C_n.

EXERCISE 12.9.17. The **Möbius ladder** M_{2n} is the 3-regular graph on $2n$ vertices which is obtained from the cycle C_{2n} by joining each pair of opposite vertices. Show that the Möbius ladder is a circulant graph.

EXERCISE 12.9.18. Show that the eigenvalues of the Möbius ladder M_{2n} are

$$\lambda_s = 2\cos\left(\frac{\pi s}{n}\right) + (-1)^s,$$

for $s \in \{0, 1, \ldots, 2n-1\}$.

EXERCISE 12.9.19. Determine which of the graphs $L(K_n), \overline{L(K_n)}$ and M_{2n} are Ramanujan.

EXERCISE 12.9.20. Let X be a graph with n vertices and let $w_{i,j}(r)$ denote the number of walks of length r between the vertices i and j of X. If W is the matrix whose (i,j)-th entry is

$$W_{i,j} = \sum_{r=1}^{\infty} w_{i,j}(r) x^r$$

show that

$$W(I_n - xA) = I_n,$$

where A is the adjacency matrix of X.

CHAPTER 13

Hints

Chapter 1. Basic Notions of Graph Theory

1.6.1 Use Corollary 1.2.2.

1.6.2 Use Theorem 1.5.2.

1.6.3 The degree of a vertex in a connected graph with n vertices is between 1 and $n-1$.

1.6.4 Use induction on n.

1.6.5 Use the idea from Theorem 1.5.2.

1.6.6 Consider a path of maximum length.

1.6.7 Modify the proof of Theorem 1.4.1.

1.6.8 The endpoints of each edge have different colours.

1.6.9 Find the maximum number of edges in $K_{a,b}$, when $a+b=n$.

1.6.10 Each C_4 must have two vertices of each colour.

1.6.11 If $x, y \in \{0,1\}^n$, show that the distance between x and y equals the number of positions in which x and y differ. For $x \in \{0,1\}^n$, let $w(x)$ denote the number of 1's in x. Partition the vertices of Q_n according to the parity of $w(x)$.

1.6.12 Use induction on n to calculate the number of vertices. For a vertex $x \in \{0,1\}^n$, calculate its degree.

1.6.13 Use induction on n or for each $x \neq y \in \{0,1\}^n$, count the common neighbours of x and y.

1.6.14 Use the previous hint.

1.6.15 Start with an arbitrary bipartite subgraph with two nonempty colour classes. For each vertex x, if the number of neighbors of x which are contained in its colour class is greater than the number of neighbors of x which are contained in the other colour class, then move x to the other colour class.

1.6.16 Use Theorem 1.4.1.

1.6.17 Prove by contradiction.

1.6.18 Prove by contradiction.

1.6.19 Show first that $\sum\limits_{uv \in E(X)} (d(u)+d(v)) = \sum\limits_{u \in V(X)} d^2(x)$ and use Cauchy-Schwarz inequality.

1.6.20 Use 1.6.19 to show that if a graph has n vertices and at least $\lfloor \frac{n^2}{4} \rfloor$ edges, then it contains a K_3.

Chapter 2. Recurrence Relations

2.7.1 Calculate $\frac{\binom{n}{k+1}}{\binom{n}{k}}$.

2.7.2 Count the subsets containing n and the ones not containing n separately.

2.7.3 Use the relation $(k+1)! - k! = k! \cdot k$

2.7.4 Use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ or count the number of pairs $\{(K, L) : K \subset [n], |K| = k, L \subset K, |L| = l\}$ in two ways.

2.7.5 Use the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ or count the number of k-subsets of $[n]$ depending on whether or not they contain n.

2.7.6 Use 2.7.5.

2.7.7 Count the number of k-subsets of $[m+n]$ in two ways.

2.7.8 Use the formula $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ and Stirling's formula for $n!$ and $(2n)!$.

2.7.9 With binomial coefficients, if $|A| = k$, then there are 2^{n-k} subsets B with $A \cap B = \emptyset$. Combinatorially, consider the matrix whose rows are the characteristic vectors of A and B.

2.7.10 The number of even subsets is $\binom{n}{0} + \binom{n}{2} + \ldots$ and the number of odd subsets is $\binom{n}{1} + \binom{n}{3} + \ldots$. Use Newton's binomial formula. For a bijective proof, if n is odd, consider the function $A \to A^c$. If n is even, use the fact that $n-1$ is odd.

2.7.11 If $\omega = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$, calculate $(1+\omega)^n$ in two different ways.

2.7.12 Use $F_n = F_{n-1} + F_{n-2}$.

2.7.13 Label $n-1$ sides of a convex n-gon with distinct labels. Construct a bijective function between to the triangulations of the convex n-gon by $n-2$ nonintersecting diagonals and the ways of bracketing the sum of $n-1$ terms corresponding to the labeled sides.

2.7.14 Write $n = 1 + 1 + \cdots + 1$ and construct a bijection between the solutions of the given equation and the $(k-1)$-subsets of a set with $n-1$ elements.

2.7.15 Use the formula of $\binom{n}{k}$ for the first inequality. Use induction on n for the second inequality.

2.7.16 Use binomial formula or count in two ways the number of triples (A, x, y) where $A \subset [n]$ and $x, y \in A$.

2.7.17 Use Stirling's formula.

2.7.18 Let $x_k = \max\{x : \binom{x}{k} \le n\}$.

2.7.19 Use the recurrence relation for the Bell numbers.

2.7.20 Find a recurrence formula using the fact the last term of the sum can be 1 or 2.

Chapter 3. The Principle of Inclusion and Exclusion

3.6.1 Use Theorem 3.1.1.

3.6.2 For $k \leq pq$, if $\gcd(k, pq) \neq 1$, then $\gcd(k, p) \neq 1$ or $\gcd(k, q) \neq 1$.

3.6.3 For $i \in [r]$, let $A_i = \{x : x \leq n, p_i | x\}$. Then use Theorem 3.1.1.

3.6.4 Use Theorem 3.1.1.

3.6.5 Use Theorem 3.1.1.

3.6.6 Use induction on n.

3.6.7 Use Theorem 3.2.1.

3.6.8 Use Theorem 3.3.1.

3.6.9 Use Theorem 3.4.2.

3.6.10 The number of permutations with an even number of cycles is $|s(n,2)| + |s(n,4)| + \ldots$. The number of permutations with an odd number of cycles is $|s(n,1)| + |s(n,3)| + \ldots$.

3.6.11 Use the counting idea from the proof of Theorem 3.5.3.

3.6.12 Use inclusion and exclusion. If you have m red cards and n blue cards, how many k-elements subsets are there consisting only of red cards.

3.6.13 $|s(n,1)|$ equals the number of permutations with exactly one cycle or use the recurrence relation.

3.6.14 Use the definition of $S(n, k)$.

3.6.15 Use the definition of $S(n, k)$.

3.6.16 Consider $f'(t)$ and use the recurrence relation $s(n) = s(n-1) + (n-1)s(n-2)$.

3.6.17 Calculate $(e^t - 1)g(t)$.

3.6.18 Use 3.6.17.

3.6.19 Use 3.6.17 and 3.6.18.

3.6.20 Calculate $e^X f(X)$.

Chapter 4. Matrices and Graphs

4.5.1 Determine the characteristic polynomials of P_4 and C_5.

4.5.2 Recall that $A^k_{i,j}$ equals the number of walks of length k from i to j and use the binomial theorem.

4.5.3 Use Theorem 4.1.1.

4.5.4 Use Theorem 4.1.1.

4.5.5 Use Exercise 4.5.3 and the Cauchy-Schwarz inequality.

4.5.6 Consider the rows corresponding to the two vertices.

4.5.7 For any three vertices i, j, k, $d(i, k) \leq d(i, j) + d(j, k)$, where $d(x, y)$ is the length of a shortest path from x to y.

4.5.8 Use the directed version of Theorem 1.4.1 to prove the result for matrices having all entries equal to 0 except one entry which equals 1.

4.5.9 Use induction on n.

4.5.10 Use the definition of M and A.

4.5.11 Use the definition of N and A.

4.5.12 Multiply the Laplacian matrix by the all one vector and use 4.5.11.

4.5.13 Use the definition of the Laplacian matrix.

4.5.14 Look at the coefficient of λ^3.

4.5.15 Calculate the eigenvalues of C_4.

4.5.16 Consider the adjacency matrix of Y.

4.5.17 If the odd girth of X is $2r+1$, then calculate in two ways the number of closed cycles of length $2s+1$ for $s \leq r-1$.

4.5.18 For any two edges e, f of X, calculate the (e, f)-entry of the matrix N^tN.

4.5.19 If μ is an eigenvalue of NN^t, then μ is an eigenvalue of N^tN.

4.5.20 Show that any eigenvalue of NN^t is positive.

Chapter 5. Trees

5.5.1 A tree has no cycles.

5.5.2 A connected graph has no cycles if and only if it has $n-1$ edges.

5.5.3 Use induction on n.

5.5.4 Use induction on n.

5.5.5 Use 5.5.1.

5.5.6 Use 5.5.1.

5.5.7 Use 5.5.6.

5.5.8 Use 5.5.7.

5.5.9 Use the principle of inclusion and exclusion.

5.5.10 Use 5.5.9.

5.5.11 Use the matrix-tree theorem.

5.5.12 Use induction on n.

5.5.13 Use Kruskal's algorithm.

5.5.14 If i has degree d and j is adjacent to i, consider the furthest point k from j such that $d(i, k) = d(j, k) + 1$.

5.5.15 Show that the maximum degree is 2.

5.5.16 Consider a spanning tree of X.

5.5.17 Use the matrix-tree theorem.

5.5.18 Use the matrix-tree theorem.

5.5.19 The number of vertices is less than the number of vertices of a k-regular tree of height D.

5.5.20 Consider a path of maximum length in the tree.

Chapter 6. Möbius Inversion and Graph Colouring

6.9.1 Use the definition of a poset.

6.9.2 Use the definition of the Hasse diagram.

6.9.3 Use Theorem 6.1.1.

6.9.4 Use 6.9.1.

6.9.5 Use the definition of the Möbius function.

6.9.6 Use the definition of a linear ordering.

6.9.7 Construct a graph whose vertices are stations with two stations adjacent if their distance is less than 150 miles.

6.9.8 The sum of the coefficients is related to the value of the chromatic polynomial at 1. Use induction for the second part.

6.9.9 Use the definition of the chromatic polynomial.

6.9.10 Colour $X \vee Y$ using the colourings of X and Y.

6.9.11 Use induction on n and Theorem 6.5.1.

6.9.12 Every connected graph has a spanning tree.

6.9.13 The vertex of degree 3 can be coloured in λ ways, then the vertex of degree 1 can be coloured with $\lambda - 1$ colours.

6.9.14 Use the definition of the chromatic polynomial.

6.9.15 Use the Rayleigh-Ritz theorem.

6.9.16 Use ideas from the proof of Theorem 6.5.1.

6.9.17 Partition the vertex set into $\chi(X)$ independent sets and count the edges between them.

6.9.18 Use the definition of the chromatic number.

6.9.19 Let A_i denote the family of k-subsets whose smallest element is i.

6.9.20 Use the principle of inclusion and exclusion.

Chapter 7. Enumeration under Group Action

7.4.1 Use the definition of a group action.

7.4.2 Use the definition of a group action.

7.4.3 Use the definition of a group homomorphism.

7.4.4 Use the definition of a group action.

7.4.5 Use Pólya's Theorem.

7.4.6 Use Pólya's Theorem.

7.4.7 Use the definition of the cycle index polynomial.

7.4.8 Use Pólya's Theorem.

7.4.9 A graph on n vertices has at most $\binom{n}{2}$ edges.

7.4.10 Use the definition of the cycle index polynomial.

7.4.11 Use the results in the last section.

7.4.12 Use the results in the last section.

7.4.13 Use the definition of the cycle index polynomial.

7.4.14 Use the results in the last section.

7.4.15 Remember that an automorphism of P_n is a bijection function $f : V(P_n) \to V(P_n)$ such that $xy \in E(P_n)$ if and only if $f(x)f(y) \in E(P_n)$.

7.4.16 Use the definition of the cycle index polynomial.

7.4.17 Use Pólya's Theorem.

7.4.18 Remember that an automorphism of a graph X is a bijection function $f : V(X) \to V(X)$ such that $xy \in E(X)$ if and only if $f(x)f(y) \in E(X)$.

7.4.19 Use the definition of the cycle index polynomial.

7.4.20 Use Pólya's Theorem.

Chapter 8. Matching Theory

8.8.1 Use Hall's Theorem 8.1.1.

8.8.2 Use Hall's Theorem 8.1.1.

8.8.3 Use Hall's Theorem 8.1.1.

8.8.4 Use induction on t.

8.8.5 Use Exercise 8.8.4 and induction on n.

8.8.6 Use Theorem 8.3.1.

8.8.7 Use the Hungarian algorithm.

8.8.8 Use Tutte's Theorem 8.6.1.

8.8.9 Use Tutte's Theorem 8.6.1.

8.8.10 Use induction on n

8.8.11 Use Birkhoff-von Neumann Theorem 8.4.1.

8.8.12 Add a proper number of vertices to A , join them to B and use Hall's Theorem 8.1.1.

8.8.13 Replace each vertex in A by an independent set of proper size and use Hall's Theorem 8.1.1.

8.8.14 Use Hall's Theorem 8.1.1.

8.8.15 If $X \backslash C$ is not a disjoint union of clique, then there are vertices x, y, z, w such that xy, xz are edges and yz and xw are not edges of X. Use the perfect matchings of $X \cup yz$ and $X \cup xw$ to construct a perfect matching for X.

8.8.16 Use Tutte's Theorem 8.6.1.

8.8.17 Consider the symmetric difference of two perfect matchings.

8.8.18 Use Tutte's Theorem 8.6.1.

8.8.19 Use Hall's Theorem 8.1.1.

8.8.20 Follow the proof of Hall's Theorem 8.1.1.

Chapter 9. Block Designs

9.7.1 Use the results in the first section.

9.7.2 Use the results in the first section.

9.7.3 Use the results in the first section.

9.7.4 Use the definition of the Möbius function.

9.7.5 Consider a design whose points are the students.

9.7.6 Generalize the construction from the second section.

9.7.7 The rank is the maximum number of independent rows or columns.

9.7.8 Use Theorem 9.3.1.

9.7.9 Use Theorem 9.4.1.

9.7.10 Use Theorem 9.3.4.

9.7.11 Use Theorem 9.6.1.

9.7.12 Remove the last $d-1$ entries from each codeword.

9.7.13 Use the definition of the Fano plane and Figure 9.1.

9.7.14 Use the definition of a Steiner triple system.

9.7.15 Use the definition of $d(x, z)$.

9.7.16 Use Theorem 9.2.1.

9.7.17 Use the definition of a $2-(v, k, \lambda)$ design.

9.7.18 Use double counting.

9.7.19 Any two distinct blocks have at most $t-1$ points in common.

9.7.20 Prove by contradiction.

Chapter 10. Planar Graphs

10.4.1 If f_i is the number of faces of length i, then $2e = \sum_i if_i \geq \gamma f$.

10.4.2 The girth is the length of the shortest cycle.

10.4.3 Use Heawood's Theorem 10.3.2.

10.4.4 Use Exercise 10.4.1 or Kuratowski's Theorem.

10.4.5 Find a plane drawing of $K_{3,3} \setminus e$ without any crossings.

10.4.6 Find a plane drawing of $K_5 \setminus f$ without any crossings.

10.4.7 Show that $K_{4,4}$ without a perfect matching is isomorphic to the 3-dimensional cube graph Q_3.

10.4.8 Join any two points by an edge if and only if their distance in the plane is 1. Show this graph is planar.

10.4.9 A nonplanar graph has crossing at least 1.

10.4.10 Use Exercises 10.4.9 and 10.4.1.

10.4.11 Use Exercise 10.4.10 and find a drawing of K_6 with 3 crossings.

10.4.12 Use the definition of outerplanar graphs. For K_4, assume it is outerplanar and derive a contradiction.

10.4.13 Assume $K_{2,3}$ is outerplanar and derive a contradiction. Find a plane drawing of $K_{2,3}$.

10.4.14 Use a greedy colouring.

10.4.15 Decompose the polygon into triangles using its diagonals and use Exercise 10.4.14.

10.4.16 Use Exercises 10.4.1 and 10.4.9.

10.4.17 Use induction or the four colour theorem.

10.4.18 The chromatic number of a planar graph is at most 4.

10.4.19 Use induction on n.

10.4.20 Use induction on the number of inside edges to show that $\sum_i (i-2)f'_i = n-2$ and a similar result for the outside edges.

Chapter 11. Edges and Cycles

11.4.1 Use the definition of the line graph.

11.4.2 Show that the Petersen graph without any of its perfect matchings is formed by two cycles of length 5.

11.4.3 Use Exercise 11.4.2.

11.4.4 Use the greedy colouring.

11.4.5 Use the definition of a Hamiltonian cycle.

11.4.6 Use the definition of a Hamiltonian cycle.

11.4.7 Use the definition of a Hamiltonian cycle.

11.4.8 Follow the proof of Theorem 11.2.3.

11.4.9 Use the pigeonhole principle.

11.4.10 Use the pigeonhole principle.

11.4.11 Use induction and the pigeonhole principle.

11.4.12 Use the pigeonhole principle.

11.4.13 Modify the argument which shows that any red-blue edge-colouring of K_6 results in a monochromatic triangle.

11.4.14 Use induction.

11.4.15 Consider the polygon whose vertices are among the five points and which contains all of them inside it.

11.4.16 Use 11.4.16.

11.4.17 Use induction.

11.4.18 The vertex set can be partitioned into 4 cliques.

11.4.19 Use 11.4.18 and the pigeonhole principle.

11.4.20 Use induction.

Chapter 12. Regular Graphs

12.9.1 If A is the adjacency matrix of X, then the adjacency matrix of $\overline{X}$ is $J - I - A$.

12.9.2 If J is a linear combination of powers of A, then $AJ = JA$. Compare the ij-th entry of AJ and JA. If X is k-regular and connected, then the minimal polynomial of A has the form $(\lambda - k)p(\lambda)$. This means each column of $p(A)$ is an eigenvector of A corresponding to the eigenvalue k.

12.9.3 Use 12.9.2.

12.9.4 Calculate A^2 in terms of I, A and J.

12.9.5 If x is an eigenvector of an eigenvalue $\lambda \neq k$, then $Jx = 0$.

12.9.6 If a is a non-square in $\mathbb{F}_q$, then $x \mapsto ax$ is a bijection between squares and non-squares in $\mathbb{F}_q$.

12.9.7 Use 4.5.19.

12.9.8 Use 12.9.1 and 12.9.7 .

12.9.9 Multiply the matrix C by the column vector $[1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j}]^t$, for $j \in \{0, 1, \dots, n-1\}$.

12.9.10 Find an isomorphism between $L(K_5)$ and the Petersen graph.

12.9.11 Use 12.9.7, 12.9.8 and 12.9.9.

12.9.12 The matrix C can be written as the sum of n circulant matrices.

12.9.13 Calculate the sum of the elements in each row of the adjacency matrix.

12.9.14 Use 12.9.11 and 12.9.12.

12.9.15 Consider the adjacency matrix of C_n.

12.9.16 Use 12.9.14.

12.9.17 Consider the adjacency matrix of M_{2n}.

12.9.18 Use 12.9.14.

12.9.19 Use the definition of a Ramanujan graph.

12.9.20 Use the definition of W.

Bibliography

[1] J.A. Bondy and U.S.R. Murty, *Graph Theory*, Springer Graduate Texts in Mathematics 244, (2008).

[2] B. Bollobás, *Modern Graph Theory*, Springer Graduate Texts in Mathematics 184, (1998).

[3] R. Diestel, *Graph Theory*, Springer Graduate Texts in Mathematics 173, (2000). Available free at
`http://www.math.uni-hamburg.de/home/diestel/`

[4] D.B. West, *Introduction to Graph Theory*, 2nd Edition, Prentice Hall, (2000).

[5] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, (1996).

[6] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, (1992).

[7] R. Stanley, *Enumerative Combinatorics, Vol. I and Vol. II*, Cambridge University Press, (2000/2001).

[8] R. Bhatia, *Matrix Analysis*, Springer Graduate Texts in Mathematics 169, (1996).

[9] L. Lovász, *Combinatorial Problems and Exercises*, AMS Chelsea Publishing, 2nd Edition, (2007).

[10] A. Herzberg and M.R. Murty, Sudoku Puzzles and Chromatic Polynomials, *Notices of the Amer. Math. Society*, 54(2007), no. 6, 708-717

[11] R. Bhatia, *Perturbation Bounds for Matrix Eigenvalues*, SIAM Classics in Applied Mathematics, (2007).

[12] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer Graduate Texts in Mathematics 207, (2001).

[13] F.R.K. Chung, *Spectral Graph Theory*, CBMS Regional Conference Series in Mathematics, (1997).

[14] S. Hoory, N. Linial and A. Wigderson, Expander Graphs and their Applications, *Bulletin of the AMS*, Volume 43, Number 4, (2006), 439561.

[15] N. Alon and J. Spencer, *The Probabilistic Method*, Wiley-Interscience, 2nd Edition, (2000).

[16] M.R. Murty, Ramanujan Graphs, *Journal of the Ramanujan Math. Society*, 18, No. 1, (2003), 1-20.

[17] S.M. Cioabă and M.R. Murty, Expander Graphs and Gaps between Primes, *Forum Mathematicum*, Volume 20, Issue 4, (2008), 745-756.

Index

Texts and Readings in Mathematics

1. R. B. Bapat: Linear Algebra and Linear Models (Second Edition)
2. Rajendra Bhatia: Fourier Series (Second Edition)
3. C. Musili: Representations of Finite Groups
4. H. Helson: Linear Algebra (Second Edition)
5. D. Sarason: Complex Function Theory (Second Edition)
6. M. G. Nadkarni: Basic Ergodic Theory (Second Edition)
7. H. Helson: Harmonic Analysis (Second Edition)
8. K. Chandrasekharan: A Course on Integration Theory
9. K. Chandrasekharan: A Course on Topological Groups
10. R. Bhatia (ed.): Analysis, Geometry and Probability
11. K. R. Davidson: C* – Algebras by Example
12. M. Bhattacharjee et al.: Notes on Infinite Permutation Groups
13. V. S. Sunder: Functional Analysis — Spectral Theory
14. V. S. Varadarajan: Algebra in Ancient and Modern Times
15. M. G. Nadkarni: Spectral Theory of Dynamical Systems
16. A. Borel: Semisimple Groups and Riemannian Symmetric Spaces
17. M. Marcolli: Seiberg – Witten Gauge Theory
18. A. Bottcher and S. M. Grudsky: Toeplitz Matrices, Asymptotic Linear Algebra and Functional Analysis
19. A. R. Rao and P. Bhimasankaram: Linear Algebra (Second Edition)
20. C. Musili: Algebraic Geometry for Beginners
21. A. R. Rajwade: Convex Polyhedra with Regularity Conditions and Hilbert's Third Problem
22. S. Kumaresan: A Course in Differential Geometry and Lie Groups
23. Stef Tijs: Introduction to Game Theory
24. B. Sury: The Congruence Subgroup Problem
25. R. Bhatia (ed.): Connected at Infinity
26. K. Mukherjea: Differential Calculus in Normed Linear Spaces (Second Edition)
27. Satya Deo: Algebraic Topology: A Primer (Corrected Reprint)
28. S. Kesavan: Nonlinear Functional Analysis: A First Course
29. S. Szabó: Topics in Factorization of Abelian Groups
30. S. Kumaresan and G. Santhanam: An Expedition to Geometry
31. D. Mumford: Lectures on Curves on an Algebraic Surface (Reprint)
32. J. W. Milnor and J. D. Stasheff: Characteristic Classes (Reprint)
33. K. R. Parthasarathy: Introduction to Probability and Measure (Corrected Reprint)
34. A. Mukherjee: Topics in Differential Topology
35. K. R. Parthasarathy: Mathematical Foundations of Quantum Mechanics
36. K. B. Athreya and S. N. Lahiri: Measure Theory
37. Terence Tao: Analysis I (Second Edition)
38. Terence Tao: Analysis II (Second Edition)

39. W. Decker and C. Lossen: Computing in Algebraic Geometry
40. A. Goswami and B. V. Rao: A Course in Applied Stochastic Processes
41. K. B. Athreya and S. N. Lahiri: Probability Theory
42. A. R. Rajwade and A. K. Bhandari: Surprises and Counterexamples in Real Function Theory
43. G. H. Golub and C. F. Van Loan: Matrix Computations (Reprint of the Third Edition)
44. Rajendra Bhatia: Positive Definite Matrices
45. K. R. Parthasarathy: Coding Theorems of Classical and Quantum Information Theory
46. C. S. Seshadri: Introduction to the Theory of Standard Monomials
47. Alain Connes and Matilde Marcolli: Noncommutative Geometry, Quantum Fields and Motives
48. Vivek S. Borkar: Stochastic Approximation: A Dynamical Systems Viewpoint
49. B. J. Venkatachala: Inequalities: An Approach Through Problems
50. Rajendra Bhatia: Notes on Functional Analysis
51. A. Clebsch (ed.): Jacobi's Lectures on Dynamics (Second Revised Edition)
52. S. Kesavan: Functional Analysis
53. V. Lakshmibai and Justin Brown: Flag Varieties: An Interplay of Geometry, Combinatorics, and Representation Theory
54. S. Ramasubramanian : Lectures on Insurance Models